**Immigrant Petition for Alien Worker (I-140)**
**for the Alien with Extraordinary Ability in Science (EB-1A)**
**Original Submission**

TABLE OF CONTENTS

# Authorization for Credit Card Transactions

**Department of Homeland Security**
U.S. Citizenship and Immigration Services

**USCIS**
**Form G-1450**

## How To Fill Out Form G-1450

1. Type or print legibly in black ink.
2. Complete the "**Applicant's/Petitioner's/Requester's Information**," "**Credit Card Billing Information**," and "**Credit Card Information**" sections and sign the authorization. **NOTE:** The credit card must be issued by a U.S. bank.
3. Place your Form G-1450 ON TOP of your application, petition, or request package.

**NOTE:** Failure to provide the requested information may result in USCIS and your financial institution not accepting the payment. USCIS cannot process credit card payments without an authorized signature.

**NOTE:** Please see the USCIS Form G-1450 website for additional information.

**We recommend that you print or save a copy of your completed Form G-1450 to review in the future and for your records.**

By completing this transaction, you agree that you have paid for a government service and that the filing fee, biometric services fee and all related financial transactions are final and not refundable, regardless of any action USCIS takes on an application, petition, or request. You must submit all fees in the exact amounts. USCIS will charge your credit card up to the amount you authorize below.

Please refer to the form(s) you are filing for additional information, or you may call the USCIS Customer Contact number at **1-800-375-5283**. For TTY (deaf or hard of hearing) call: **1-800-767-1833**.

| **Applicant's/Petitioner's/Requester's Information (Full Legal Name)** | | |
|---|---|---|
| Given Name (First Name)<br>[name] | Middle Name (if any) | Family Name (Last Name) |
| **Credit Card Billing Information (Credit Card Holder's Name as it Appears on the Card)** | | |
| Given Name (First Name)<br>[name] | Middle Name (if any) | Family Name (Last Name) |
| **Credit Card Holder's Billing Address:** | | |
| Street Number and Name<br>[address] | Apt. Ste. Flr.<br>☐ ☐ ☐ | Number |
| City or Town | State | ZIP Code |
| **Credit Card Holder's Signature and Contact Information:** | | |
| Credit Card Holder's Signature | | |
| Credit Card Holder's Daytime Telephone Number<br>[phone] | Credit Card Holder's Email Address<br>[email] | |

| **Credit Card Information** | | |
|---|---|---|
| Credit Card Number | **Credit Card Type:** ☐ Visa<br>☐ MasterCard<br>☐ American Express<br>☐ Discover | Authorized Payment Amount<br>**$ 715 .00** |
| Credit Card Expiration Date (mm/yyyy) | | |

# Authorization for Credit Card Transactions

**Department of Homeland Security**
U.S. Citizenship and Immigration Services

**USCIS**
**Form G-1450**

## How To Fill Out Form G-1450

1. Type or print legibly in black ink.
2. Complete the "**Applicant's/Petitioner's/Requester's Information**," "**Credit Card Billing Information**," and "**Credit Card Information**" sections and sign the authorization. **NOTE:** The credit card must be issued by a U.S. bank.
3. Place your Form G-1450 ON TOP of your application, petition, or request package.

**NOTE:** Failure to provide the requested information may result in USCIS and your financial institution not accepting the payment. USCIS cannot process credit card payments without an authorized signature.

**NOTE:** Please see the USCIS Form G-1450 website for additional information.

**We recommend that you print or save a copy of your completed Form G-1450 to review in the future and for your records.**

By completing this transaction, you agree that you have paid for a government service and that the filing fee, biometric services fee and all related financial transactions are final and not refundable, regardless of any action USCIS takes on an application, petition, or request. You must submit all fees in the exact amounts. USCIS will charge your credit card up to the amount you authorize below.

Please refer to the form(s) you are filing for additional information, or you may call the USCIS Customer Contact number at **1-800-375-5283**. For TTY (deaf or hard of hearing) call: **1-800-767-1833**.

| **Applicant's/Petitioner's/Requester's Information (Full Legal Name)** | | |
|---|---|---|
| Given Name (First Name)<br>[name] | Middle Name (if any) | Family Name (Last Name) |
| **Credit Card Billing Information (Credit Card Holder's Name as it Appears on the Card)** | | |
| Given Name (First Name)<br>[name] | Middle Name (if any) | Family Name (Last Name) |
| **Credit Card Holder's Billing Address:** | | |
| Street Number and Name<br>[address] | Apt. Ste. Flr. ☐ ☐ ☐ | Number |
| City or Town | State | ZIP Code |
| **Credit Card Holder's Signature and Contact Information:** | | |
| Credit Card Holder's Signature | | |
| Credit Card Holder's Daytime Telephone Number<br>[phone] | Credit Card Holder's Email Address<br>[email] | |
| **Credit Card Information** | | |
| Credit Card Number | **Credit Card Type:** ☐ Visa ☐ MasterCard ☐ American Express ☐ Discover | Authorized Payment Amount<br>**$ 300 .00** |
| Credit Card Expiration Date (mm/yyyy) | | |



# Authorization for Credit Card Transactions

**Department of Homeland Security**
U.S. Citizenship and Immigration Services

**USCIS**
**Form G-1450**

## How To Fill Out Form G-1450

1. Type or print legibly in black ink.
2. Complete the "**Applicant's/Petitioner's/Requester's Information**," "**Credit Card Billing Information**," and "**Credit Card Information**" sections and sign the authorization. **NOTE:** The credit card must be issued by a U.S. bank.
3. Place your Form G-1450 ON TOP of your application, petition, or request package.

**NOTE:** Failure to provide the requested information may result in USCIS and your financial institution not accepting the payment. USCIS cannot process credit card payments without an authorized signature.

**NOTE:** Please see the USCIS Form G-1450 website for additional information.

**We recommend that you print or save a copy of your completed Form G-1450 to review in the future and for your records.**

By completing this transaction, you agree that you have paid for a government service and that the filing fee, biometric services fee and all related financial transactions are final and not refundable, regardless of any action USCIS takes on an application, petition, or request. You must submit all fees in the exact amounts. USCIS will charge your credit card up to the amount you authorize below.

Please refer to the form(s) you are filing for additional information, or you may call the USCIS Customer Contact number at **1-800-375-5283**. For TTY (deaf or hard of hearing) call: **1-800-767-1833**.

| **Applicant's/Petitioner's/Requester's Information (Full Legal Name)** | | |
|---|---|---|
| Given Name (First Name)<br>[name] | Middle Name (if any) | Family Name (Last Name) |
| **Credit Card Billing Information (Credit Card Holder's Name as it Appears on the Card)** | | |
| Given Name (First Name)<br>[name] | Middle Name (if any) | Family Name (Last Name) |
| **Credit Card Holder's Billing Address:** | | |
| Street Number and Name<br>[address] | Apt. Ste. Flr.<br>☐ ☐ ☐ | Number |
| City or Town | State | ZIP Code |
| **Credit Card Holder's Signature and Contact Information:** | | |
| Credit Card Holder's Signature | | |
| Credit Card Holder's Daytime Telephone Number<br>[phone] | Credit Card Holder's Email Address<br>[email] | |

| **Credit Card Information** | | |
|---|---|---|
| Credit Card Number | **Credit Card Type:** ☐ Visa<br>☐ MasterCard<br>☐ American Express<br>☐ Discover | Authorized Payment Amount<br>**$ 2805.00** |
| Credit Card Expiration Date (mm/yyyy) | | |

# e-Notification of Application/Petition Acceptance

**Department of Homeland Security**
U.S. Citizenship and Immigration Services

**USCIS**
**Form G-1145**

## What Is the Purpose of This Form?

Use this form to request an electronic notification (e-Notification) when U.S. Citizenship and Immigration Services accepts your immigration application. This service is available for applications filed at a USCIS Lockbox facility.

## General Information

Complete the information below and clip this form to the first page of your application package. You will receive one e-mail and/or text message for each form you are filing.

We will send the e-Notification within 24 hours after we accept your application. Domestic customers will receive an e-mail and/or text message; overseas customers will only receive an e-mail. Undeliverable e-Notifications cannot be resent.

The e-mail or text message will display your receipt number and tell you how to get updated case status information. It will not include any personal information. The e-Notification does not grant any type of status or benefit; rather it is provided as a convenience to customers.

USCIS will also mail you a receipt notice (I-797C), which you will receive within 10 days after your application has been accepted; use this notice as proof of your pending application or petition.

## USCIS Privacy Act Statement

**AUTHORITIES:** The information requested on this form is collected pursuant to section 103(a) of the Immigration and Nationality Act, as amended INA section 101, et seq.

**PURPOSE:** The primary purpose for providing the information on this form is to request an electronic notification when USCIS accepts immigration form. The information you provide will be used to send you a text and/or email message.

**DISCLOSURE:** The information you provide is voluntary. However, failure to provide the requested information may prevent USCIS from providing you a text and/or email message receipting your immigration form.

**ROUTINE USES:** The information provided on this form will be used by and disclosed to DHS personnel and contractors in accordance with approved routine uses, as described in the associated published system of records notices [**DHS/USCIS-007 - Benefits Information System and DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS)**, which can be found at **www.dhs.gov/privacy**]. The information may also be made available, as appropriate for law enforcement purposes or in the interest of national security.

**Complete this form and clip it on top of the first page of your immigration form(s).**

| Applicant/Petitioner Full Last Name<br>**[lastname]** | Applicant/Petitioner Full First Name<br>**[firstname]** | Applicant/Petitioner Full Middle Name |
|---|---|---|
| Email Address<br>**[email]** | Mobile Phone Number (Text Message)<br>**[phone]** | |

# Immigrant Petition for Alien Workers

**Department of Homeland Security**
U.S. Citizenship and Immigration Services

**USCIS Form I-140**
OMB No. 1615-0015
Expires 02/28/2027

| For USCIS Use Only | Fee Stamp | Priority Date | Consulate | Action Block |
|---|---|---|---|---|
| | | | | |

**Classification**

- ☐ 203(b)(1)(A) Alien of Extraordinary Ability
- ☐ 203(b)(1)(B) Outstanding Professor or Researcher
- ☐ 203(b)(1)(C) Multinational Executive or Manager
- ☐ 203(b)(2) Member of Professions with Advanced Degree/Exceptional Ability
- ☐ 203(b)(3)(A)(i) Skilled Worker
- ☐ 203(b)(3)(A)(ii) Professional
- ☐ 203(b)(3)(A)(iii) Other Worker

**Certification**

- ☐ National Interest Waiver (NIW)
- ☐ Schedule A, Group I
- ☐ Schedule A, Group II

**Remarks**

| To be completed by an Attorney or Accredited Representative (if any). | ☐ Select this box if Form G-28 or Form G-28I is attached. | Attorney State Bar Number (if applicable) | Attorney or Accredited Representative USCIS Online Account Number (if any) |
|---|---|---|---|
| | | | |

► **START HERE - Type or print in black ink.**

## Part 1. Information About the Person or Organization Filing This Petition

If an individual is filing this petition, answer **Item Numbers 1.a. - 1.c.** If a company or organization is filing this petition, answer **Item Number 2.**

**1.a.** Family Name (Last Name): Nikitin

**1.b.** Given Name (First Name): Kirill

**1.c.** Middle Name:

**2.** Company or Organization Name:

### *Mailing Address*

*(USCIS ZIP Code Lookup)*

**3.a.** In Care Of Name:

**3.b.** Street Number and Name: [address]

**3.c.** ☐ Apt. ☐ Ste. ☐ Flr.

**3.d.** City or Town:

**3.e.** State: **3.f.** ZIP Code:

**3.g.** Province:

**3.h.** Postal Code:

**3.i.** Country: USA

### *Other Information*

**4.** IRS Employer Identification Number (EIN) ►

**5.** Are you a nonprofit organized as tax exempt or a governmental research organization? ☐ Yes ☒ No

**6.** Do you currently employ a total of 25 or fewer full-time equivalent employees in the United States, including all affiliates or subsidiaries of this company/organization? ☒ Yes ☐ No

**7.** U.S. Social Security Number (SSN) (if any) ►

**8.** USCIS Online Account Number (if any) ►

## Part 2. Petition Type

This petition is being filed for (select **only one** box):

**1.a.** ☒ An alien of extraordinary ability.

**1.b.** ☐ An outstanding professor or researcher.

**1.c.** ☐ A multinational executive or manager.

**1.d.** ☐ A member of the professions holding an advanced degree or an alien of exceptional ability (who is **NOT** seeking a National Interest Waiver (NIW)).

**1.e.** ☐ A professional (at a minimum, possessing a bachelor's degree or a foreign degree equivalent to a U.S. bachelor's degree).

## Part 2. Petition Type (continued)

**1.f.** ☐ A skilled worker (requiring at least two years of specialized training or experience).

**1.g.** ☐ Any other worker (requiring less than two years of training or experience).

**1.h.** ☐ An alien applying for an NIW (who **IS** a member of the professions holding an advanced degree or an alien of exceptional ability).

This petition is being filed (select **only one** box):

**2.a.** ☐ To amend a previously filed petition.

Previous Petition Receipt Number

► 

**2.b.** ☐ For the Schedule A, Group I or II designation.

## Part 3. Information About the Person for Whom You Are Filing

**1.a.** Family Name (Last Name) `Nikitin`

**1.b.** Given Name (First Name) `Kirill`

**1.c.** Middle Name

### *Mailing Address*

**2.a.** In Care Of Name

**2.b.** Street Number and Name `[address]`

**2.c.** ☒ Apt. ☐ Ste. ☐ Flr.

**2.d.** City or Town

**2.e.** State **2.f.** ZIP Code

**2.g.** Province

**2.h.** Postal Code

**2.i.** Country `USA`

### *Other Information*

**3.** Date of Birth (mm/dd/yyyy) `[date]`

**4.** City/Town/Village of Birth `[city]`

**5.** State or Province of Birth `[province]`

**6.** Country of Birth `Russia`

**7.** Country of Citizenship or Nationality `Russia`

**8.** Alien Registration Number (A-Number) (if any)

► **A-**

**9.** U.S. SSN (if any) ►

### *Information About His or Her Last Arrival in the United States*

If the person for whom you are filing is in the United States, provide the following information.

**10.** Date of Last Arrival (mm/dd/yyyy) `[date]`

**11.a.** Form I-94 Arrival-Departure Record Number

► `[ n u m b e r ]`

**11.b.** Expiration Date of Authorized Stay Shown on Form I-94 (mm/dd/yyyy) `D/S`

**11.c.** Status on Form I-94 (for example, class of admission, or paroled, if paroled) `J1`

**12.** Passport Number `[passport]`

**13.** Travel Document Number

**14.** Country of Issuance for Passport or Travel Document `Russia`

**15.** Expiration Date for Passport or Travel Document (mm/dd/yyyy) `[date]`

## Part 4. Processing Information

Provide the following information for the person named in **Part 3.** (select **only one** box):

**1.a.** ☐ Alien will apply for a visa abroad at a U.S. Embassy or U.S. Consulate at:

**1.b.** City or Town

**1.c.** Country

**2.a.** ☒ Alien is in the United States and will apply for adjustment of status to that of lawful permanent resident.

## Part 4. Processing Information (continued)

**2.b.** Alien's current country of residence or, if now in the United States, last country of permanent residence abroad.

Russia

If you provided a United States address in **Part 3.**, provide the person's foreign address in **Item Numbers 3.a. - 3.f.**:

**3.a.** Street Number and Name: [address]

**3.b.** ☐ Apt. ☐ Ste. ☐ Flr.

**3.c.** City or Town

**3.d.** Province

**3.e.** Postal Code

**3.f.** Country: Russia

If the person's native alphabet is other than Roman letters, type or print the person's foreign name and address in the native alphabet in **Item Numbers 4.a. - 4.c.**:

**4.a.** Family Name (Last Name): Никитин

**4.b.** Given Name (First Name): Кирилл

**4.c.** Middle Name

### *Mailing Address*

**5.a.** In Care Of Name

**5.b.** Street Number and Name: адрес

**5.c.** ☒ Apt. ☐ Ste. ☐ Flr.

**5.d.** City or Town

**5.e.** Province

**5.f.** Postal Code

**5.g.** Country: Россия

If you answer "Yes" to **Item Numbers 6.a. - 10.**, provide the case number, office location, date of decision, and disposition of the decision in the space provided in **Part 11. Additional Information**.

**6.a.** Are you filing any other petitions or applications with this Form I-140? ☐ Yes ☒ No

**6.b.** If you answered "Yes" **to Item Number 6.a.**, select all applicable boxes:

- ☐ Form I-485
- ☐ Form I-131
- ☐ Form I-765
- ☐ Other (Provide an explanation in **Part 11. Additional Information**.)

**7.** Is the person for whom you are filing in removal proceedings? ☐ Yes ☒ No

**8.** Has any immigrant visa petition ever been filed by or on behalf of this person? ☐ Yes ☒ No

**9.** Are you filing this petition without an original labor certification because the original labor certification was previously submitted in support of another Form I-140? ☐ Yes ☐ No

**10.** If you are filing this petition without an original labor certification, are you requesting that U.S. Citizenship and Immigration Services (USCIS) request a duplicate labor certification from the Department of Labor (DOL)? ☐ Yes ☐ No

## Part 5. Additional Information About the Petitioner

Type of petitioner (select **only one** box):

**1.a.** ☐ Employer

**1.b.** ☒ Self

**1.c.** ☐ Other (For example, Lawful Permanent Resident, U.S. citizen or any other person filing on behalf of the alien)

If a company or an organization is filing this petition, provide the following information:

**2.** Type of Business

**3.** Date Established (mm/dd/yyyy)

**4.** Current Number of U.S. Employees

**5.** Gross Annual Income $

**6.** Net Annual Income $

**7.** NAICS Code ►

**8.** Labor Certification DOL Case Number

## Part 5. Additional Information About the Petitioner (continued)

**9.** Labor Certification DOL Filing Date (mm/dd/yyyy)

**10.** Labor Certification Expiration Date (mm/dd/yyyy)

If an individual is filing this petition, provide the following information.

**11.** Occupation

Postdoctoral Research Associate

**12.** Annual Income $ xxx

## Part 6. Basic Information About the Proposed Employment

**1.** Job Title

N/A

**2.** SOC Code ► ___ - ___

**3.** Nontechnical Job Description

**4.** Is this a full-time position? ☐ Yes ☐ No

**5.** If the answer to **Item Number 4.** is "No," how many hours per week for the position?

**6.** Is this a permanent position? ☐ Yes ☐ No

**7.** Is this a new position? ☐ Yes ☐ No

**8.** Wages (Specify hour, week, month, or year):
$ _____ per _____

### *Worksite Location*

For **Item Numbers 9.a. - 9.e.**, provide the address where the person will work if different from the address provided in **Part 1.**

**9.a.** Street Number and Name: N/A

**9.b.** ☐ Apt. ☐ Ste. ☐ Flr.

**9.c.** City or Town

**9.d.** State **9.e.** ZIP Code

## Part 7. Information About the Spouse and All Children of the Person for Whom You Are Filing

For **Part 7.**, provide information on the spouse and all children related to the individual for whom you are filing this petition. Also, note if the individual will apply for a visa abroad or adjustment of status as the dependent of the individual for whom the petition is filed. If you need extra space to provide information about additional family members, use the space provided in **Part 11. Additional Information**.

**Person 1**

**1.a.** Family Name (Last Name): N/A

**1.b.** Given Name (First Name)

**1.c.** Middle Name

**2.** Date of Birth (mm/dd/yyyy)

**3.** Country of Birth

**4.** Relationship

**5.** Is he or she applying for adjustment of status? ☐ Yes ☐ No

**6.** Is he or she applying for a visa abroad? ☐ Yes ☐ No

**Person 2**

**7.a.** Family Name (Last Name)

**7.b.** Given Name (First Name)

**7.c.** Middle Name

**8.** Date of Birth (mm/dd/yyyy)

**9.** Country of Birth

**10.** Relationship

**11.** Is he or she applying for adjustment of status? ☐ Yes ☐ No

**12.** Is he or she applying for a visa abroad? ☐ Yes ☐ No

## Part 7. Information About Spouse and All Children of the Person for Whom You Are Filing (continued)

**Person 3**

**13.a.** Family Name (Last Name)

**13.b.** Given Name (First Name)

**13.c.** Middle Name

**14.** Date of Birth (mm/dd/yyyy)

**15.** Country of Birth

**16.** Relationship

**17.** Is he or she applying for adjustment of status? ☐ Yes ☐ No

**18.** Is he or she applying for a visa abroad? ☐ Yes ☐ No

**Person 4**

**19.a.** Family Name (Last Name)

**19.b.** Given Name (First Name)

**19.c.** Middle Name

**20.** Date of Birth (mm/dd/yyyy)

**21.** Country of Birth

**22.** Relationship

**23.** Is he or she applying for adjustment of status? ☐ Yes ☐ No

**24.** Is he or she applying for a visa abroad? ☐ Yes ☐ No

**Person 5**

**25.a.** Family Name (Last Name)

**25.b.** Given Name (First Name)

**25.c.** Middle Name

**26.** Date of Birth (mm/dd/yyyy)

**27.** Country of Birth

**28.** Relationship

**29.** Is he or she applying for adjustment of status? ☐ Yes ☐ No

**30.** Is he or she applying for a visa abroad? ☐ Yes ☐ No

**Person 6**

**31.a.** Family Name (Last Name)

**31.b.** Given Name (First Name)

**31.c.** Middle Name

**32.** Date of Birth (mm/dd/yyyy)

**33.** Country of Birth

**34.** Relationship

**35.** Is he or she applying for adjustment of status? ☐ Yes ☐ No

**36.** Is he or she applying for a visa abroad? ☐ Yes ☐ No

## Part 8. Contact Information, Certification, and Signature of the Petitioner or Authorized Signatory

### *Petitioner or Authorized Signatory's Contact Information*

**1.a.** Petitioner's or Authorized Signatory's Family Name (Last Name)

Nikitin

**1.b.** Petitioner's or Authorized Signatory's Given Name (First Name)

Kirill

**2.** Petitioner's or Authorized Signatory's Title

**3.** Petitioner's or Authorized Signatory's Daytime Telephone Number

[phone]

**4.** Petitioner's or Authorized Signatory's Mobile Telephone Number (if any)

[phone]

**5.** Petitioner's or Authorized Signatory's Email Address (if any)

[email]

### *Petitioner's or Authorized Signatory's Certification and Signature*

If filing this petition on behalf of an organization, I certify that I am authorized to do so by the organization:

**a.** I reviewed and provided or authorized all of the responses and information in my petition;

**b.** I understood all of the responses and information contained in, and submitted with, my petition; and

**c.** All of the responses and information were complete, true, and correct at the time of filing

Furthermore, I authorize the release of any information from any and all of my records as authorized signatory and the petitioner's records that USCIS may need to determine the petitioner's eligibility for an immigration request and to other entities and persons where necessary for the administration and enforcement of U.S. immigration law.

**6.a.** Petitioner's or Authorized Signatory's Signature

[sign here]

**6.b.** Date of Signature (mm/dd/yyyy) [date]

## Part 9. Interpreter's Contact Information, Certification, and Signature

### *Interpreter's Full Name*

**1.a.** Interpreter's Family Name (Last Name)

**1.b.** Interpreter's Given Name (First Name)

**2.** Interpreter's Business or Organization Name

### *Interpreter's Contact Information*

**3.** Interpreter's Daytime Telephone Number

**4.** Interpreter's Mobile Telephone Number (if any)

**5.** Interpreter's Email Address (if any)

### *Interpreter's Certification and Signature*

I certify, under penalty of perjury, that I am fluent in English and , and I have interpreted every question on the petition and Instructions and interpreted the petitioner's or authorized signatory's answers to the questions in that language, and the petitioner or authorized signatory informed me that they understood every instruction, question, and answer on the petition.

**6.a.** Interpreter's Signature

**6.b.** Date of Signature (mm/dd/yyyy)

## Part 10. Contact Information, Certification, and Signature of the Person Preparing this Petition, if Other Than the Petitioner or Authorized Signatory

### *Preparer's Full Name*

**1.** Preparer's Family Name (Last Name)

Preparer's Given Name (First Name)

**2.** Preparer's Business or Organization Name

### *Preparer's Contact Information*

**3.** Preparer's Daytime Telephone Number

**4.** Preparer's Mobile Telephone Number (if any)

**5.** Preparer's Email Address (if any)

### *Preparer's Certification and Signature*

I certify, under penalty of perjury, that I prepared this petition for the petitioner or authorized signatory at their request and with express consent and that all of the responses and information contained in and submitted with the petition are complete, true, and correct and reflects only information provided by the petitioner or authorized signatory. The petitioner or authorized signatory reviewed the responses and information and informed me that they understand the responses and information in or submitted with the petition.

**6.** Preparer's Signature

Date of Signature (mm/dd/yyyy)

## Part 11. Additional Information

If you need extra space to provide any additional information within this petition, use the space below. If you need more space than what is provided, you may make copies of this page to complete and file with this petition or attach a separate sheet of paper. Type or print your name and A-Number (if any) at the top of each sheet; indicate the **Page Number**, **Part Number**, and **Item Number** to which your answer refers; and sign and date each sheet.

**1.** Family Name (Last Name)

Given Name (First Name)

Middle Name

**2.** IRS EIN ►

**3.** Page Number | Part Number | Item Number

**4.** Page Number | Part Number | Item Number

**5.** Page Number | Part Number | Item Number

**6.** Page Number | Part Number | Item Number

**7.** Page Number | Part Number | Item Number

# Request for Premium Processing Service

**Department of Homeland Security**
U.S. Citizenship and Immigration Services

**USCIS**
**Form I-907**
OMB No. 1615-0048
Expires 02/28/2027

| For USCIS Use Only | Request Physically Received by USCIS | Returned | Resubmitted | Receipt |
|---|---|---|---|---|
| | Date _____ Date _____ | Date _____ Date _____ | Date _____ Date _____ | Action Block |
| | Remarks | | | |

| To be completed by an attorney or accredited representative (if any). | ☐ Select this box if Form G-28 or Form G-28I is attached. | Attorney State Bar Number (if applicable) | Attorney or Accredited Representative USCIS Online Account Number (if any) |
|---|---|---|---|
| | | | |

▶ **START HERE - Type or print in black ink.**

## Part 1. Information About the Person Filing This Request

**1.** Alien Registration Number (A-Number) (if any)
▶ A- N / A

**2.** USCIS Online Account Number (if any)
▶ N / A

**3.** Family Name (Last Name): Nikitin
Given Name (First Name): Kirill
Middle Name:

**4.** Company or Organization Named in the Related Case (If filed on behalf of a company or organization)

**5.** Mailing Address

In Care Of Name

Street Number and Name: [Address]
Apt. ☐ Ste. ☐ Flr. ☐ Number

City or Town
State
ZIP Code *USPS ZIP Code Lookup*

Province
Postal Code
Country: USA

**6.** Is your current mailing address the same as your physical address? ☒ Yes ☐ No

If you answered "No" to **Item Number 6.**, provide your physical address in **Item Number 7.**

## Part 1. Information About the Person Filing This Request (continued)

**7.** Physical Address

Street Number and Name | Apt. ☐ Ste. ☐ Flr. ☐ Number

City or Town | State | ZIP Code

Province | Postal Code | Country

**8.** Request for Premium Processing Service (select **only one** box):

☐ I am the **petitioner** who is filing or has filed a petition eligible for Premium Processing Service.

☐ I am the attorney or accredited representative **for the petitioner** who is filing or has filed a petition eligible for Premium Processing Service. (Complete and submit Form G-28, Notice of Entry of Appearance as Attorney or Accredited Representative, or Form G-28I, Notice of Entry of Appearance as Attorney In Matters Outside the Geographical Confines of the United States, if Form G-28 or Form G-28I has not been submitted with the petition.)

☒ I am the **applicant** who is filing or has filed an application eligible for Premium Processing Service.

☐ I am the attorney or accredited representative **for the applicant** who is filing or has filed an application eligible for Premium Processing Service. (Complete and submit Form G-28 or Form G-28I, if Form G-28 or Form G-28I has not been submitted with the application.)

## Part 2. Information About the Request

**1.** Form Number of Related Petition or Application: I-140

**2.** Receipt Number of Related Petition or Application

**3.** Classification or Eligibility Requested

**4.** Petitioner or Applicant in the Related Case

Family Name (Last Name): Nikitin | Given Name (First Name): Kirill | Middle Name

**5.** Beneficiary in the Related Case

Family Name (Last Name): Nikitin | Given Name (First Name): Kirill | Middle Name

**6.** Name of Point of Contact for the Company or Organization

Family Name (Last Name) | Given Name (First Name) | Middle Name

Position Title

**7.** Company or Organization IRS Employer Identification Number (EIN) (if any)

## Part 2. Information About the Request (continued)

**8.** Address of Petitioner, Applicant, Company, or Organization Named in Related Case

Street Number and Name: [Address]

Apt. ☐ Ste. ☐ Flr. ☐ Number:

City or Town:

State:

ZIP Code:

Province:

Postal Code:

Country: USA

## Part 3. Requestor's Statement, Contact Information, Declaration, Certification, and Signature

**NOTE:** Read the **Penalties** section of the Form I-907 Instructions before completing this section.

I understand that U.S. Citizenship and Immigration Services (USCIS) will refund the Premium Processing Service fee to the person listed in **Part 1.** of this request if USCIS does not take an action on the related case within the applicable processing timeframe. I understand that case actions include a referral for investigation of suspected fraud, misrepresentation, or the issuance of an approval notice, a request for evidence, a notice of intent to deny, or a denial notice.

### *Requestor's Statement*

**NOTE**: Select the box for either **Item A.** or **B.** in **Item Number 1.** If applicable, select the box for **Item Number 2.**

**1.** Requestor's Statement Regarding the Interpreter

**A.** ☒ I can read and understand English, and I have read and understand every question and instruction on this request and my answer to every question.

**B.** ☐ The interpreter named in **Part 4.** read to me every question and instruction on this request and my answer to every question in _____, a language in which I am fluent, and I understood everything.

**2.** Requestor's Statement Regarding the Preparer

☐ At my request, the preparer named in **Part 5.**, _____, prepared this request for me based only upon information I provided or authorized.

### *Requestor's Contact Information*

**3.** Requestor's Daytime Telephone Number: [phone]

**4.** Requestor's Mobile Telephone Number (if any): [phone]

**5.** Requestor's Fax Number (if any)

**6.** Requestor's Email Address (if any): [email]

### *Requestor's Declaration and Certification*

Copies of any documents I have submitted are exact photocopies of unaltered, original documents, and I understand that USCIS may require that I submit original documents to USCIS at a later date. Furthermore, I authorize the release of any information from any and all of my records that USCIS may need to determine my eligibility for the immigration benefit that I seek.

I furthermore authorize release of information contained in this request, in supporting documents, and in my USCIS records, to other entities and persons where necessary for the administration and enforcement of U.S. immigration law.

## Part 3. Requestor's Statement, Contact Information, Declaration, Certification, and Signature (continued)

I certify, under penalty of perjury, that all of the information in my request and any document submitted with it were provided or authorized by me, that I reviewed and understand all of the information contained in, and submitted with, my request and that all of this information is complete, true, and correct.

### *Requestor's Signature*

**7.** Requestor's Signature: [Sign here]

Date of Signature (mm/dd/yyyy): [date]

**NOTE TO ALL REQUESTORS:** If you do not completely fill out this request or fail to submit required documents listed in the Instructions, USCIS may deny your request.

## Part 4. Interpreter's Contact Information, Certification, and Signature

Provide the following information about the interpreter.

### *Interpreter's Full Name*

**1.** Interpreter's Family Name (Last Name)

Interpreter's Given Name (First Name)

**2.** Interpreter's Business or Organization Name (if any)

### *Interpreter's Mailing Address*

**3.** Street Number and Name

Apt. ☐ Ste. ☐ Flr. ☐ Number

City or Town

State

ZIP Code

Province

Postal Code

Country

### *Interpreter's Contact Information*

**4.** Interpreter's Daytime Telephone Number

**5.** Interpreter's Mobile Telephone Number (if any)

**6.** Interpreter's Email Address (if any)

### *Interpreter's Certification*

I certify, under penalty of perjury, that:

I am fluent in English and _____, which is the same language specified in **Part 3.**, **Item B.** in **Item Number 1.**, and I have read to this requestor in the identified language every question and instruction on this request and his or her answer to every question. The requestor informed me that he or she understands every instruction, question, and answer on the request, including the **Requestor's Declaration and Certification**, and has verified the accuracy of every answer.

## Part 4. Interpreter's Contact Information, Certification, and Signature (continued)

### *Interpreter's Signature*

**7.** Interpreter's Signature

Date of Signature (mm/dd/yyyy)

## Part 5. Contact Information, Declaration, and Signature of the Person Preparing this Request, if Other Than the Requestor

Provide the following information about the preparer.

### *Preparer's Full Name*

**1.** Preparer's Family Name (Last Name)

Preparer's Given Name (First Name)

**2.** Preparer's Business or Organization Name (if any)

### *Preparer's Mailing Address*

**3.** Street Number and Name

Apt. ☐ Ste. ☐ Flr. ☐ Number

City or Town

State

ZIP Code

Province

Postal Code

Country

### *Preparer's Contact Information*

**4.** Preparer's Daytime Telephone Number

**5.** Preparer's Mobile Telephone Number (if any)

**6.** Preparer's Email Address (if any)

### *Preparer's Statement*

**7.A.** ☐ I am not an attorney or accredited representative but have prepared this request on behalf of the requestor with the requestor's consent.

**B.** ☐ I am an attorney or accredited representative and my representation of the requestor in this case

☐ extends ☐ does not extend beyond the preparation of this request.

**NOTE:** If you are an attorney or accredited representative, you may need to submit a completed Form G-28 or Form G-28I with this request.

## Part 5. Contact Information, Declaration, and Signature of the Person Preparing this Request, if Other Than the Requestor (continued)

### *Preparer's Certification*

By my signature, I certify, under penalty of perjury, that I prepared this request at the request of the requestor. The requestor then reviewed this completed request and informed me that he or she understands all of the information contained in, and submitted with, his or her request, including the **Requestor's Declaration and Certification**, and that all of this information is complete, true, and correct. I completed this request based only on information that the requestor provided to me or authorized me to obtain or use.

### *Preparer's Signature*

**8.** Preparer's Signature

Date of Signature (mm/dd/yyyy)

## Part 6. Additional Information

If you need extra space to provide any additional information within this petition, use the space below. If you need more space than what is provided, you may make copies of this page to complete and file with this petition or attach a separate sheet of paper. Type or print your name and A-Number (if any) at the top of each sheet; indicate the **Page Number**, **Part Number**, and **Item Number** to which your answer refers; and sign and date each sheet.

**1.** Family Name (Last Name) | Given Name (First Name) | Middle Name

**2.** A-Number (if any) ► **A-**

**3.A.** Page Number **3.B.** Part Number **3.C.** Item Number

**3.D.**

**4.A.** Page Number **4.B.** Part Number **4.C.** Item Number

**4.D.**

**5.A.** Page Number **5.B.** Part Number **5.C.** Item Number

**5.D.**

# Title Page of the Passport

# Expired Exchange Visitor Visa (J-1)

# Employment-authorization forms DS-2019

# Current form I-94 and travel history

# Initial Evidence in Support of the I-140 Immigrant Petition

**Petitioner and Beneficiary:** Dr. Kirill Nikitin
**Classification Sought:** Employment-Based Immigration, First Preference Extraordinary Ability in Science (EB-1A). Sec. 203(b)(1) INA [8 U.S.C. 1153].

Dear USCIS Officer:

This letter is respectfully submitted in support of the petition of Dr. Kirill Nikitin for classification as a qualified immigrant under the first preference employment immigration for Aliens of Extraordinary Ability pursuant to section 203(b)(1)(A) of the Immigration and Nationality Act ("the Act"). This evidence shows that Dr. Nikitin is an alien of extraordinary ability in the sciences, specifically in Data Privacy and Computer Security, who sustained national and international acclaim and his achievements have been recognized in the field of his expertise. More precisely, this letter provides evidence that:

1. Dr. Nikitin satisfies **four** of the ten criteria listed in 8 CFR, Section 204.5(h)(3), namely:
    - Evidence of Dr. Nikitin's original scientific and scholarly contributions of major significance in the field (Section 2.1).
    - Dr. Nikitin's authorship of scholarly articles in the field in professional media (Section 2.2).
    - Participation of Dr. Nikitin as a judge of the work of others in the field of Data Privacy and Computer Security (Section 2.3).
    - Evidence that Dr. Nikitin's work has been featured in published materials in major professional media (Section 2.4).
2. Dr. Nikitin's employment has both substantial merit and of national importance for the United States (Section 3).
3. Dr. Nikitin has sustained national and international acclaim and his achievements have been recognized in the field of Data Privacy and Computer Security (Section 4).

Pursuant to 8 CFR, Section 204.5(h)(1), Dr. Nikitin may file an I-140 visa petition for classification under Section 203(b)(1)(A) of the Act as an alien of extraordinary ability in the sciences on his own behalf.

Pursuant to 8 CFR, Section 204.5(h)(5), neither an offer for employment in the United States nor a labor certification is required for this classification.

Dr. Nikitin's work will substantially benefit the United States where he will continue to work in the field of his expertise. (Please refer to the Statement from Dr. Nikitin detailing plans on how he intends to continue work in the United States).

# 1 Summary of Dr. Nikitin's achievements and qualifications

Dr. Kirill Nikitin is a Postdoctoral Researcher at Columbia University and the New York Genome Center where he analyzes the leakage of sensitive information from encrypted data and develops methods for privacy-preserving data sharing, specifically for medical applications. Prior to that, Dr. Nikitin was a Postdoctoral Researcher at Cornell University where he conducted research on the privacy of user communications. He received his Ph.D. in Computer and Communication Sciences from the École Polytechnique Fédérale de Lausanne, Switzerland, in 2021 and his M.Sc. in Information and Communication Technology from KTH Royal Institute of Technology, Sweden, in 2015 (see Exhibit 17 for his educational credentials). Each of these institutions is in the top ranks globally [Exhibit 23].

Dr. Nikitin is an internationally recognized expert in the field of Data Privacy and Computer Security. He specializes in communication security, user privacy, and the protection of sensitive data. Dr. Nikitin is known for his work on methods for protecting the properties of encrypted data, robust protocols for private data retrieval, the design of systems for secure software distribution, and techniques for strengthening blockchain networks. All these components are critical for the protection of user data and the secure operation of modern computer systems, which has been repeatedly recognized by the U.S. government in various executive orders [Exhibit 25].

Dr. Nikitin has made scientific contributions of major significance to his field of expertise. His methods for protecting the properties of encrypted data have been implemented in Facebook Messenger and in iMessage on Apple devices (Section 2.1.1). Dr. Nikitin's work on private data access for users has addressed a critical vulnerability in the existing approaches and has brought the technology closer to real-world deployment. It has also spurred a series of follow-up works from other scientists worldwide (Section 2.1.2). Dr. Nikitin's work on securing software-update systems targeted the problem of supply-chain attacks that had become a major concern in the industry and were recognized by the U.S. government as a national security threat [Exhibit 25]. The work influenced the design of multiple follow-up architectures for software distribution. The corresponding publication by Dr. Nikitin has been both cited more than 180 times to date and included in the curriculum of graduate courses at several universities (Section 2.1.3). Lastly, Dr. Nikitin has contributed to improving the efficiency of blockchain networks (Section 2.1.4).

Dr. Nikitin has authored five peer-reviewed scientific articles that have been published exclusively in the top-tier venues of the field, including the IEEE Symposium on Security and Privacy, the USENIX Security Symposium, and the Privacy Enhancing Technologies Symposium (Section 2.2). The articles Dr. Nikitin authored have gathered 333+ citations by researchers throughout the United States and in numerous countries around the world [Exhibit 2].

Dr. Nikitin has been a judge for the work of others, having been a member of the Program Committee and a reviewer of more than 68 submissions to the top conferences in computer security, data privacy and blockchain research, including the ACM Conference on Computer and Communications Security, the USENIX Security Symposium, and the IEEE International Conference on Blockchain and Cryptocurrency (Section 2.3). In recognition of his service, Dr. Nikitin was invited to become a professional member of the Association for Computing Machinery (ACM) [Exhibit 20]. Dr. Nikitin also was an organizer of a conference on biomedical data privacy and equity [Exhibit 21].

Major medias have published materials about Dr. Nikitin's work (Section 2.4). ZDNET.com, a technology-focused platform with 24 million monthly visits, covered Dr. Nikitin's work on the pro-

tection of encryption metadata, whereas CyberScoop.com, a platform for cybersecurity news with 6 million unique monthly engagements, featured Dr. Nikitin's work on the security of software-update systems (see Exhibit 22 for the articles and the readership statistics). Furthermore, Dr. Nikitin's work has been highlighted by multiple scientific surveys published in professional media.

As evidenced by *eight* letters of support from distinguished professors within academia and from industry scientists (enclosed at Exhibit 3-Exhibit 10), his highly cited scientific publications, his service as a reviewer for premier scientific conferences, and the featuring of his work in major media outlets, Dr. Nikitin has risen to the top of the field of Data Privacy and Computer Security. He has firmly established himself as a leading expert in the field, has made a significant impact on the scientific community, and, thus, clearly meets the criteria for the EB-1A classification.

# 2 Proof of Dr. Nikitin's Extraordinary Ability in Data Privacy and Computer Security

## 2.1 Evidence of Dr. Nikitin's original scientific and scholarly contributions of major significance to the field

The Beneficiary's field of specialization is Data Privacy and Computer Security, which involves researching methods for protecting secrecy of data and communication. Dr. Nikitin's particular expertise is in designing techniques for protecting metadata and integrity in encrypted files and communication.

Metadata are auxiliary information, such as the data recipients or the communicating parties, the algorithms used for encryption, and the length of the encrypted data. Protection of metadata is crucial for ensuring the data and users' privacy. In 2023, the U.S. government published the *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, which emphasized the importance of developing privacy-enhancing technologies *"to protect privacy and to combat the broader legal and societal risks that result from the improper collection and use of people's data."* Consequently, the National Science and Technology Council developed *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics, 2023* and *National Privacy Research Strategy, 2025* (see Exhibit 25 for the executive order and the strategy reports). Dr. Nikitin's work is directly aligned with the goals of the National Strategy, specifically, in its recommendation to develop tools and techniques for protecting privacy-sensitive information in transit and at rest.

Data integrity is the assurance that the data has not been tampered with during transit to a user or when stored on a server. In his research, Dr. Nikitin developed methods for ensuring data integrity in software-update systems, which represent the so-called *software supply-chain*, and in systems for private information retrieval. The software supply chain is a sequence of steps that a software package goes through from the initial development to the final deployment on a user's device. In 2022, in response to the *Executive Order on America's Supply Chains* and the *Executive Order on Improving the Nation's Cybersecurity*, the Action Plan on Securing Defense-Critical Supply Chains was developed [Exhibit 25]. This directive highlighted the growing risks posed by vulnerabilities in the software supply chain, such as the insertion of malicious code or unauthorized modifications to software during its distribution. Dr. Nikitin's methods address these challenges by introducing robust cryptographic techniques and blockchain algorithms to verify the authenticity and integrity of software updates, ensuring that only

verified code reaches end users. These advancements provide means for fortifying critical infrastructure and safeguarding sensitive systems against evolving cyber threats.

Dr. Nikitin's major scientific contributions have been recognized by *experts in the field worldwide*. We discuss these contributions in greater detail below.

### 2.1.1 Evidence of original scientific contribution: Methods for protecting metadata in encrypted data and communications

Dr. Nikitin invented methods for efficient protection of metadata in encrypted data and communications, which he presented at the Privacy Enhancing Technologies Symposium and published in the corresponding proceedings [Exhibit 12]. When a message is encrypted in storage or sent over an encrypted network channel, it is commonly supplemented with unprotected auxiliary information, called *metadata*, which can specify the message's recipient, the encryption parameters, or the message's length. It is added to facilitate the message's decryption by the recipient, who, otherwise, would not know what cryptographic key to use or how to interpret the ciphertext. These metadata, however, can be used to infer sensitive information about the message or the communicating parties, which poses a threat to the users' privacy. The techniques invented by Dr. Nikitin facilitate encryption of data that protects both the content and the metadata, and the recipient still can efficiently decrypt such a zero-leakage ciphertext. These methods have been recognized by both the scientific community and large technological companies as a contribution that solves a long-standing challenge.

**The method for obfuscating the size of encrypted data, developed by Dr. Nikitin, is already being used by iMessage and Facebook Messenger.** Starting with iOS 17.3, iMessage (an instant messaging service developed by Apple Inc.) uses Padmé, the padding heuristics developed by Dr. Nikitin, as a part of the metadata-protection methods, to protect the length of messages in transit between iMessage users. Apple specifically chose Padmé as it *"strikes an excellent balance between privacy and efficiency, and preserves the user experience in limited device connectivity scenarios"* (**see the announcement by the Apple Security Engineering and Architecture team, which describes the usage of Dr. Nikitin's invention** [Exhibit 12]). Furthermore, Facebook Messenger (an instant messaging service developed by Meta Platforms) uses the same invention of Dr. Nikitin to protect the messages in encrypted storage, as outlined by the Labyrinth protocol that specifies the encryption of messages history on the devices of each user's account (**see the announcement by Facebook Engineering and the protocol documentation that details the usage** [Exhibit 12]). iMessage and Messenger are reported to have over 1.3 and 1 billion active users each month, respectively (see Exhibit 12 for evidence of iMessage and Facebook Messenger's active users' count).

**Independent** expert Dr. JJ, XX at Violet Inc., describes the reasons for adopting Dr. Nikitin's work in his letter of support enclosed at Exhibit 10 as follows:

"..."

**Independent** expert Dr. GG, XX at Violet Inc., who is a Program Committee member of the conference where the original publication on Dr. Nikitin's work was presented, elaborates on Dr. Nikitin's original contribution in his letter of support enclosed at Exhibit 9:

"..."

Dr. BB, XX at Red University, a leading expert in privacy-enhancing technologies, describes the significance of Dr. Nikitin's work from the scientific perspective (see Exhibit 4):

> "***Dr. Nikitin's work on reducing metadata leakage from encrypted files and communications is one of his most influential contributions***. *Dr. Nikitin studied a fundamental problem in the existing encryption schemes: standard formats for encrypted data (aka ciphertexts) expose auxiliary information (aka metadata), including encryption suites used and payload length. This exposure can be exploited by traffic analysis, de-anonymization, website fingerprinting, and many other attacks, and has thus been a focus of much research in the security and privacy community. Instead of the previous, fragile approaches that aimed to distinguish between sensitive and not-sensitive metadata,* ***Dr. Nikitin proposed a radical innovation of leaving no unencrypted metadata whatsoever in the ciphertexts. While ideal from the privacy perspective, this approach faced serious efficiency challenges because recipients of encrypted data would not know what algorithm or cryptographic key to use to decrypt it. To address this challenge, Dr. Nikitin invented a new way of handling decryption.*** *He proposed decoding techniques that enable a ciphertext recipient to, first, efficiently find and decrypt the auxiliary markers, then decrypt the data.* ***This innovation has made it significantly more difficult for adversaries to perform traffic analysis or infer sensitive information from encrypted data at rest, greatly improving protection for sensitive files and communications.***"

**Independent** expert Dr. EE, XX at Purple Inc., and YY at Cyan University, and a recognized leader in cryptography and privacy-enhancing technologies, describes the impact of Dr. Nikitin's work from the industrial perspective in his letter of support enclosed at Exhibit 7, stating:

> "*Dr. Nikitin's innovation in iMessage is a technique for obfuscating the length of encrypted data. Most encryption algorithms nowadays preserve the length of data when encrypting it. For example, the word "yes" would commonly be encrypted with three symbols, whereas the word "no" with two symbols. This is obviously a privacy issue in the messaging context because, even when encrypted, the two words would be easily distinguishable. Dr. Nikitin proposed a padding technique that struck the optimal balance between the size protection and the induced bandwidth overhead.* ***Minimizing the overhead while providing the best possible protection is critical, as a system like iMessage might be exchanging billions of messages every day. The fact that Dr. Nikitin's innovation provides this balance and that it is directly translated into deployment by a major technology company underscores the real-world impact of his work and its importance in securing communications at scale.***"

Further highlighting the impact of Dr. Nikitin's contributions, expert **independent** letter of support from Dr. FF, XX at White University, and a renown researcher in security and privacy of large-scale distributed computer systems states (see Exhibit 8):

> "*Kirill is known for his scientific contributions in data privacy and, specifically, for his work on metadata protection.* ***In his paper titled "Reducing metadata leakage from encrypted files and communication with PURBs", published in the Proceedings on Privacy Enhancing Technologies, Kirill presented techniques for both obfuscating the length of encrypted content and protecting encryption metadata. This work***

***is important as the length of an encrypted payload can reveal important information about content; yet protecting it in an efficient way is a non-trivial task because digital objects can radically differ in size.***

*For example, one user might send a short email of less than 1000 characters in length, while another user may wish to download a high-definition movie one million times larger than the email. It is grossly inefficient, and therefore impractical, to require all communications to be of the same length. In this paper Kirill developed padding techniques which ensure messages conform to a small set of lengths which maximize privacy while ensuring practicality. The technique has been adopted by several major tech companies including Apple and Meta.*

*One line of my own research work concerns anonymity networks. Such networks allow users to communicate without revealing the identities of the communicating parties to the network operator. As a result, these networks require cryptographic methods and system engineering designs which do not expose the identities of either the sender or the receiver. Such systems have traditionally focused on direct, one-to-one communication.* ***Kirill has developed techniques which can encrypt a message which is readable by multiple recipients without revealing who those recipients are. This approach is therefore more scalable, opening up new opportunities in future applications.***"

### 2.1.2 Evidence of original scientific contribution: Novel techniques for private information retrieval

Private information retrieval (PIR) is a paradigm in which a user can download data from a server without revealing which data are being retrieved. PIR is one of the highlighted research areas in The National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (see page 18 of the strategy report enclosed at Exhibit 25). Dr. Nikitin's work is the first to develop a solution to the setting where the server is fully malicious, i.e., the server can arbitrarily deviate from the correct behavior, hereby violating the user's privacy. **This advancement brings the PIR technology closer to practical deployment in real-world systems.** The developed techniques were published in the proceedings of the USENIX Security Symposium [Exhibit 13], one of the top conferences in the field, and were immediately recognized by the scientific community. The manuscript has been cited over 30 times in the first year after its publication and has spurred a series of follow-up works. Here is a quote from one of the follow-up works, published in another major conference of the field, that builds on top of Dr. Nikitin's contributions:

"*Only very recently, [Colombo, Nikitin et al. ] initiated the study of selective-failure attacks in the context of PIR.*" (Dietz, M., Tessaro, S. Fully malicious authenticated PIR. In Annual International Cryptology Conference 2024.)

**Independent** expert Dr. CC, XX at Blue University, and an expert in secure computation, blockchain, and privacy-enhancing technologies, explains the significance of Dr. Nikitin's work on PIR (see Exhibit 5 for the full letter):

"*Dr. Nikitin has made significant, original contributions to the field of data and computer privacy, particularly through his research on Private Information Retrieval (PIR). PIR enables users to retrieve data from a computer database without revealing what data they are accessing.* ***This technology is crucial for improving the privacy guarantees of online***

> ***communication, for example, in instant messaging applications, such as WhatsApp.*** *Previously, research in PIR assumed that database servers always followed the protocol perfectly. In real-world applications, however, a corrupted or compromised server can violate the protocol and attempt to break the user's privacy. Dr. Nikitin has demonstrated that such a server can alter its response to a user's query, ob- serve whether the user accepts this response, and, subsequently, infer what data have been accessed.* ***Dr. Nikitin's proposed schemes are the first efficient solution to ensure the privacy of information retrieval even when the database server is malicious. This achievement bridges the gap between theoretical PIR protocols and their practical security in real-world scenarios.***"

**Independent** expert Dr. EE, XX at Purple Inc. and YY at Cyan University, states (see Exhibit 7):

> "*Dr. Nikitin's work on protecting user access patterns follows a long line of research on private information retrieval (PIR). PIR is a set of techniques for enabling a computer user to fetch an item from a database without revealing to the database which item it is.* ***While PIR has been extensively studied in academic settings, all the prior approaches have been unsuitable for real-world deployment due to being insecure in the adversarial setting. Dr. Nikitin's work is the first to demonstrate how to make such protocols secure even when the database operator actively attempts to break the user's privacy.*** *These security properties are crucial in applications requiring strong guarantees, such as secure cloud storage and privacy-preserving search.* ***Dr. Nikitin's contributions bring the PIR technology significantly closer to practical deployment, enabling robust privacy protections in real-world systems.***"

### 2.1.3 Evidence of original scientific contribution: Securing software-update systems

As highlighted by the Executive Order on America's Supply Chains, the Executive Order on Improving the Nation's Cybersecurity, and the Action Plan on Securing Defense-Critical Supply Chains, software supply chains, and, specifically, software-update systems, are the critical component of the nation's infrastructure, and they are also a potential target for cyberattacks. Dr. Nikitin has developed CHAINIAC, a framework for securing software-update systems via decentralization and the application of blockchain technology. The framework was presented and published in the proceedings of the USENIX Security Symposium [Exhibit 14]. The publication has gained significant attention in the scientific community and has already gathered impressive **185+ citations** by scientists across the world (see the Google Scholar profile of Dr. Nikitin at Exhibit 2).

**Independent** expert Dr. DD, XX at Yellow University and a leading expert in verifiable computation and distributed systems, explains the national importance of Dr. Nikitin's work for the United States (see Exhibit 6 for his letter of support):

> "***Dr. Nikitin is one of the world experts in security of software-update systems, a research area of national importance to the United States. Without robust software update, adversaries can target the software supply chain. This has been demonstrated by recent attacks. For example, government agencies were breached through SolarWinds's software.*** *The key point is that, unfortunately, software-update systems are a lucrative target for malicious actors because compromising a single access point can enable them to distribute malware to tens of thousands of companies and hundreds of*

> *millions of users.* ***Failures in the software-update process can also lead to the disruption of critical services. For example, the CrowdStrike-related outage several months ago resulted in grounded flights, halted governmental services, and closed banks with the estimated worldwide financial damages of at least $10 billion; it was caused by faulty software update. Hence, it is of paramount importance to design robust and secure mechanisms for the software supply chain.***
>
> ***As a response to this critical challenge, Dr. Nikitin developed an innovative framework, named CHAINIAC, that was the first to leverage decentralization and transparency to eliminate single points of failure and to enforce integrity in the software-release pipeline.*** *At a high level, the framework secures each step of the software production process, from the development of the source code to the installation of the corresponding update on a user's device. Among other techniques, the framework introduced the concepts of collectively verified builds and skipchains. Prior artifact-verifiability approaches provided the guarantee that a given source code could be deterministically compiled into some binary but did not establish any binding between the source code and the actual release delivered to user devices. CHAINIAC's innovation was to employ multiple servers that independently compiled a binary and then attested to a single valid release result that end users can trust. By leveraging skipchains, a novel data structure that Dr. Nikitin designed, CHAINIAC implemented a public release log that deflected targeted attacks on high-profile individuals.* ***This work of Dr. Nikitin constituted a major contribution to the field and influenced the design of multiple follow-up architectures, including Google's Binary Transparency project.***"

The innovation of Dr. Nikitin's work is further explained by Dr. AA, XX at Black University, in his letter of support enclosed at Exhibit 3:

> "..."

**The final evidence of the significance of Dr. Nikitin's work on securing the software supply chain is that it has been included in the curriculum of graduate-level courses at multiple universities in the United States and abroad**. These universities are the University of Chicago, the University of California, San Diego, the University of Illinois at Urbana-Champaign, and the Technical University of Munich, Germany (see Exhibit 14 for copies of the curricula).

### 2.1.4 Evidence of original scientific contribution: Improving the efficiency of blockchain networks

Blockchain is a novel technology that enables distributed parties to perform shared operations without the need for a trusted intermediary. Blockchain networks rely on this technology to implement crucial services, such as digital finance, supply chain management, and identity management. Scaling such networks to support a large number of users and a high volume of transactions, however, is a challenging task. The recent Executive Order on Strengthening American Leadership in Digital Financial Technology highlighted the importance of the responsible growth and use of digital assets and blockchain technology for supporting innovation and economic development in the United States.

Dr. Nikitin has made two major contributions to the field. In his work presented at the IEEE Symposium on Security and Privacy, Dr. Nikitin demonstrated how to drastically increase the throughout of blockchain networks by changing the approach to transaction verification (see the details in Exhibit 15). Dr. Nikitin demonstrated that, instead of requiring all nodes in a network to verify each transaction, it would be more efficient to allow a single untrusted prover node to generate a cryptographic proof for the validity of multiple transactions and let the other nodes in the network verify that proof. It turned out to be much more efficient than the traditional approach and became the first ever instance of verifiable-computation techniques being used to improve the efficiency of a system. The second contribution of Dr. Nikitin was the design of novel data structure named skipchain. Unlike a blockchain that guarantees that only the past blocks are unchanged, a skipchain facilitates both backward and forward verification. Furthermore, this verification is significantly more efficient than in a regular blockchain due to the skipchain's structure.

**Independent** expert Dr. DD, XX at Yellow University, explains the practical importance of Dr. Nikitin's original contributions to blockchain research (see Exhibit 6):

> "*Another influential work by Dr. Nikitin that I am closely familiar with showed how to improve the performance of Replicated State Machines (RSMs) by using outsourced verifiable computation. Dr. Nikitin demonstrated that, in a distributed system where multiple computer nodes executed the same operations, it could be more efficient for a single node to execute an operation, while generating a proof of correct execution, and to convince the other nodes of this correctness by letting them verify the proof.* ***To achieve the required efficiency, Dr. Nikitin co-developed multiple complex cryptographic techniques to reduce the cost of proof generation and verification. This was a groundbreaking result because the research community had previously considered outsourced verifiable computation to be a high-overhead tool that inevitably caused efficiency decline.*** *The demonstration that this tool could, instead, improve efficiency was a landmark advancement.*
>
> ***The result above also had a profound practical impact. The modern example of RSMs are blockchains systems, a recent technology that has applications in finance, governance, and regulation. Dr. Nikitin showed how his techniques could be applied to Ethereum, the second largest cryptocurrency and a platform with the market cap of $400 billion. Concretely, his techniques could increase the throughput of the Ethereum network fivefold which would translate in millions of dollars on saved transaction fees.*** *Several cryptocurrency solutions later adopted and deployed this approach. Retaining researchers, such as Dr. Nikitin, with a deep expertise in new developing technologies is critical for the United States to maintain its position as the world technological leader.* "

**Independent** expert Dr. CC, XX at Blue University describes the key contributions of Dr. Nikitin's work as follows (see Exhibit 5):

> "*Dr. Nikitin has also advanced blockchain research by demonstrating how to integrate state-of-the-art verifiable outsourced computation into permissioned or permissionless blockchains. In essence, a blockchain achieves strong integrity protection through the redundant verification of all blocks and the transactions they contain by numerous—e.g., thousands or tens of thousands—of independent decentralized participants.* ***The key idea of Piperine, the system that Dr. Nikitin and his collaborators from Microsoft Research designed,***

> ***is to reduce this large redundant verification cost by allowing a single untrusted prover to produce a verifiable cryptographic proof of the correctness of a block of transactions and the many independent verifiers to merely verify these proofs, instead of the transactions themselves.*** *While simple in concept, the key technical challenges are in bridging the huge remaining efficiency gap between state-of-the-art outsourced computation and direct re-execution, as well as the many limitations and impedance mismatches between current outsourced computation methods and the requirements of the blockchain context.* ***I believe that Piperine represents a major contribution both to blockchain and outsourced computation research, and it illustrates Dr. Nikitin's breadth and independent collaboration abilities in security/privacy research.***"

Finally, **independent** expert Dr. FF, XX at White University explains how these contributions are representative of Dr. Nikitin's expertise (see Exhibit 8):

> "*Dr. Nikitin has also made notable contributions in the field of blockchains — immutable distributed datastores of information. In his paper titled "Replicated state machines without replicated execution", he demonstrates that the throughput of blockchain networks can be increased by using verifiable computation. Specifically, instead of replicating multiple transactions across many nodes, a blockchain node instead proves the correctness of their cumulative execution and sends this proof. Using this approach, other nodes can verify the proof instead of redoing the computation, and it turns out this is faster.* ***This is a surprising result and demonstrates Kirill's expertise and creative thinking in this domain.***
>
> *Another example can be found in his paper titled "Chainiac: Proactive software-update transparency via collectively signed skipchains and verified builds". In this paper Kirill introduces the novel skipchain data structure. Unlike traditional blockchains, a skipchain facilitates verifiable forward traversal of blocks and more efficient backward traversal.* ***It is another example of an innovative creation which provides significant performance improvements, demonstrating that Kirill is a leading researcher in the field.***"

As clearly outlined in the detailed discussion above, Dr. Nikitin has not only made original scientific contributions to the field of Data Privacy and Computer Security, specializing in metadata protection, the security of software-update systems, and the efficiency of blockchain networks, but they have also been contributions of major significance, including their use by *billions* of users, which exceeds the requirement for this criterion.

## 2.2 Evidence of Dr. Nikitin's authorship of scholarly articles in professional or major trade publications or other major media

Dr. Nikitin's status as a top scientist is further established by his publications in top-ranked scientific journals and conference proceedings. To date, Dr. Nikitin has published five peer-reviewed scientific articles, all as either the first or second author, in international journals and conferences and has submitted one more publication for peer review to another top journal in the field. Enclosed at Exhibit 12-Exhibit 16 is a selection of Dr. Nikitin's publications.

**The conferences and journals in which Dr. Nikitin has published his work are the top, most prestigious venues in his field**, as indicated by factors such as their high rankings and in-

ternational program committees staffed by panels of experts [Exhibit 18, Metrics of the journals and conferences in which Dr. Nikitin has published]. For example, Dr. Nikitin has several publications in the IEEE Security & Privacy Symposium and the USENIX Security Symposium, the top two conferences in the field of Computer Security & Cryptography according to the Google Scholar Metrics ranking [Exhibit 18]. In addition, he has published in the Proceedings on Privacy Enhancing Technologies and in the ACM Transactions on Embedded Computing Systems, which are both the premier venues for research into their corresponding topics.

Because of its significant impact in the field, Dr. Nikitin's research has been widely cited by his peers in major scientific publications. The frequency with which other scholars cite and discuss Dr. Nikitin's work is evident from Google Scholar, the scholarly literature-specific search tool offered by the Google search engine, which yields impressive **333+ citations to Dr. Nikitin's publications** by other researchers in peer-reviewed articles and books [Exhibit 2, Evidence of the total number of citations to Dr. Nikitin's publications]. **These citations are from articles authored by researchers throughout the United States and in numerous countries around the world. The fact that Dr. Nikitin's research has received such widespread attention all over the world is a testament to its significance and impact on the field.**

In his **independent** letter of support enclosed at Exhibit 6, Dr. DD, YY at Yellow University, elaborates on the status of the venues in which Dr. Nikitin has published:

> "*As further evidence of his international recognition in the field, Dr. Nikitin's work has been published in the most prestigious conferences and journals, including IEEE Symposium on Security and Privacy, USENIX Security Symposium, Privacy Enhancing Technologies Symposium, and ACM Transactions on Embedded Computing Systems.* ***Due to the fast pace of the field, conferences are the primary publishing venues for computer security and privacy researchers. The conferences in which Dr. Nikitin has published are commonly regarded as the most selective and impactful in the field. Moreover, Dr. Nikitin is a highly cited researcher, meaning that others in his field have found his work to be novel and useful for their own research. At this time, his original work has been cited 330 times by researchers from around the world.*** *Considering that most scientific papers are scarcely cited, this is a clear indication of the significant and worldwide impact of Dr. Nikitin's research.*"

Dr. BB, XX at Red University, who has closely worked with Dr. Nikitin on a research project, echoes Dr. Nikitin's recognition in the field in his letter of support enclosed at Exhibit 4:

> "*Dr. Nikitin is an established scientist in computer security and in data and communication privacy.* ***He has published multiple works in the most prestigious scientific venues, including top-tier, rigorously peer-reviewed, academic outlets such as the IEEE Symposium on Security and Privacy and the USENIX Security Symposium. These venues are extremely selective and attract groundbreaking research from leading worldwide experts in computer security and privacy.*** *The impact of Dr. Nikitin's work is reflected in its significant academic recognition—his publications have been cited more than 331 times by other researchers, which is an impressive number for a scientist at his career stage. This level of citation demonstrates that his contributions are not only relevant but also influential, shaping ongoing research and advancements in privacy enhancing technologies.*"

Finally, another **independent** expert Dr. FF, YY at White University, explains the significance of Dr. Nikitin's high citation count (see Exhibit 8):

> "*He has publications in top computer security and privacy venues, such as USENIX Security Symposium and IEEE Symposium on Security and Privacy. His work has already received over 300 citations from other scholarly work (source: Google Scholar), attesting to his influence on the field.* ***His track record is impressive for his career stage and underscores the importance and impact of his research work. His work contributes to both academic research and drives the development of real-world solutions in data privacy and security. His contributions to date clearly demonstrate his outstanding ability and promise considerable benefits to the global community.***"

## 2.3 Evidence that Dr. Nikitin has been a judge of the work of others in Data Privacy and Computer Security and adjacent areas

Dr. Nikitin has been a reviewer for multiple years for the top conferences and journals in the field of Data Privacy and Computer Security. Dr. Nikitin has also reviewed multiple manuscripts in the area of Blockchain research thanks to his expertise in the topic and due to the topic's significant overlap with the science of Data Privacy and Computer Security. He has served on the Program Committee and provided reviews for, among others, the ACM Conference for Computer and Communication Security, the USENIX Security Symposium, and the IEEE International Conference on Blockchain and Cryptocurrency, which are the most prestigious and selective conferences in the field.

**Dr. Nikitin has judged a total of 68 submissions to top international scientific conferences and journals (see Exhibit 19 for the collection of reviews written by Dr. Nikitin)**:

- (32 reviews) ACM Conference on Computer and Communications Security (CCS): with an h5-index of 92, it is ranked #1 by Research.com among Computer Security and Cryptography conferences (see Exhibit 18 for the conference ranking by Research.com). Dr. Nikitin served on the Program Committee of the conference during the years 2024, 2023, and 2021.
- (16 reviews) USENIX Security Symposium: with an h5-index of 92, it is ranked #3 by Research.com among Computer Security and Cryptography conferences [Exhibit 18]. Dr. Nikitin is currently serving on the conference's Program Committee during the year of 2025.
- (1 review) Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt): with an h5-index of 63, it is ranked #9 by Research.com among Computer Security and Cryptography conferences [Exhibit 18]. Dr. Nikitin served as an invited expert-reviewer in 2022.
- (6 reviews) IEEE International Conference on Blockchain and Cryptocurrency (ICBC): with an h5-index of 39, it is considered a flagship conference in the emerging field of Blockchain, and specifically Blockchain Security and Privacy [Exhibit 18]. Dr. Nikitin served on the conference's Program Committee during the year of 2019.
- (1 review) IEEE Transactions on Industrial Informatics (TII): with an impact factor of 12.3 and an h5-index of 167, it is ranked #1 by Research.com among Databases & Information Systems

journals [Exhibit 18]. Dr. Nikitin was an invited expert-reviewer for a submission on securing blockchain smart contracts.

- (2 reviews) IEEE Transactions on Parallel and Distributed Systems (TPDS): with an impact factor of 5.3 and an h5-index of 74, it is a premier venue for articles on distributed systems, software and algorithms [Exhibit 18]. Dr. Nikitin was invited as an expert in securing software-update computer systems.
- (2 reviews) International Conference on Research in Computational Molecular Biology (RECOMB): it is ranked #4 by Research.com among conferences in Genetics and Molecular Biology [Exhibit 18]. Dr. Nikitin was invited as an external expert to review a submission on privacy of genetic data.
- (1 review) International conference on Intelligent Systems for Molecular Biology (ISMB): it is the flagship meeting of the International Society for Computational Biology. Dr. Nikitin was invited as an external expert to review a submission on quantifying privacy risks of genomic data sharing.
- (5 reviews) Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock): Dr. Nikitin served on the Program Committee of the workshop during the years of 2019 and 2020.
- (2 reviews) International Conference on Blockchain and Trustworthy Systems (BlockSys): Dr. Nikitin served on the Program Committee of the conference during the year of 2019.

Dr. Nikitin has extensively reviewed for conferences in Computer Security, Data Privacy, Blockchain, and related fields. In these rapidly evolving disciplines, most researchers prefer to publish in conferences over journals. According to Google Scholar, 15 out of 20 scientific venues with the most cited publications in the field of Computer Security and Cryptography are conferences [Exhibit 18]. Most of these conference papers are not merely abstracts but are full scientific articles, typically 11-13 pages long, often accompanied by substantial supplementary material, and they present significant theoretical and experimental advancements in the subject matter. **The invitations to serve on the Program Committee of the top conferences in the field is a recognition of Dr. Nikitin's expertise and standing in the scientific community.**

**Independent** expert Dr. CC, YY Blue University, served with Dr. Nikitin on the Program Committee of the ACM Conference on Computer and Communications Security, a premier conference in the field, which he highlights in his letter of support enclosed at Exhibit 5:

> "*Another evidence of Dr. Nikitin's recognition as a leading expert in the field is his role in judging the work of other researchers. He has already served on the Program Committee for such prestigious conferences in computer security and privacy as the ACM Conference Computer and Communications Security, the USENIX Security Symposium, and the IEEE International Conference on Blockchain and Cryptocurrency.* ***Invitations to join the Program Committee of such conferences are extended only to internationally renowned scientists, as the members do not only provide their experts reviews but also participate in the discussion and make collective final decisions of either accepting or rejecting submissions. I can confirm that Dr. Nikitin possesses the highest level of expertise required for this role, as both he and I were active***

> ***Program Committee members of the ACM Conference on Computer and Communications Security.*** *His contributions underscore his deep understanding of complex technical concepts and his ability to evaluate their significance and potential impact. Finally, his active participation demonstrates not only his professional standing among peers but also his dedication to advancing the field of computer security and privacy.*"

**Membership in the Association for Computing Machinery (ACM).** In recognition of his contribution to the review process of the ACM Conference on Computer and Communications Security, Dr. Nikitin was invited to become a professional member of the Association for Computing Machinery (ACM) which he has accepted (see Exhibit 20 for Dr. Nikitin's membership certificate). Dr. Nikitin is also a professional member of the Institute of Electrical and Electronics Engineers (IEEE) society, which is the world's largest association of computing professionals and a leading organization in the field of computer science and engineering [Exhibit 20].

**An organizer of RECOMB-PRIEQ 2024.** Dr. Nikitin was one of the organizers of The Satellite Conference on Biomedical Data Privacy and Equity (RECOMB-PRIEQ) 2024, that targeted challenges in privacy, security, bias, and fairness in biomedical research. This was a highly specialized conference for scientists working on privacy of biomedical data, which Dr. Nikitin was entrusted to co-organize due to his expertise in data privacy [Exhibit 21].

## 2.4 Evidence of the published material in professional or major trade publications or other major media about Dr. Nikitin's work in the field

One of the key indicators of extraordinary ability is the publication of material about the individual's work in professional, major trade publications, or other major media outlets. Dr. Nikitin's work in Data Privacy and Computer Security has garnered substantial recognition in both industry and media, demonstrating the impact and significance of his contributions. Below are some examples of such published material:

- **ZDNET:** ZDNET.com, a highly respected global platform for technology news and analysis, has published material about Dr. Nikitin's work on protection of encryption metadata, specifically on Padded Uniform Random Blobs (PURBs), the encrypted-data format devised by Dr. Nikitin. According to semrush.com, ZDNET.com receives over 24 million visits per month, with a significant portion of its readership being IT professionals, industry leaders, and decision-makers across the globe, which ranks it among the top technology news websites in the world (see Exhibit 22 for ZDNET.com's article about Dr. Nikitin's work and the statistics on ZDNET.com's readership). The coverage by ZDNET.com highlights the innovative nature of Dr. Nikitin's work, particularly in Data Privacy, and its potential to impact the broader tech landscape.
- **Wikipedia:** A Wikipedia article about Padded Uniform Random Blobs (PURBs) has been published, providing an independent and widely accessible overview of his work [Exhibit 22, A Wikipedia article]. Wikipedia is a globally recognized source of information, and the existence of a dedicated article signifies the public interest and the relevance of Dr. Nikitin's invention, which further demonstrates the broad impact and recognition of his work.
- **CyberScoop:** An article about Dr. Nikitin's work on security of software-update systems appeared on CyberScoop.com, a leading media outlet that focuses on cybersecurity news and in-

sights with more 6 million unique monthly engagements [Exhibit 22, CyberScoop's article about a framework devised by Dr. Nikitin]. Their coverage has delved into the technical aspects and implications of Dr. Nikitin's work, reinforcing his standing as a key innovator in the industry.

- **The 311 Institute:** In addition to ZDNET and CyberScoop, The 311 Institute, a future-focused research and technology platform, has also recognized Dr. Nikitin's contributions. Its article has reviewed Dr. Nikitin's work on the security of software-update systems, acknowledging its potential to drive significant advancements in Computer Security [Exhibit 22, The 311 Institute's atricle about a framework devised by Dr. Nikitin].

Dr. AA, XX at Black University describes the appearances of Dr. Nikitin's work in major media outlets in his letter of support (see [Exhibit 3]):

> "*In addition to the industry adoption, Dr. Nikitin's work has received significant media attention. His work on PURBs, for example, has been featured on ZDNET.com—a large international online media that covers groundbreaking innovations in technology. The published article acknowledged that PURBs pointed the way for rearchitecting encryption suites to dramatically improve security. Similarly, the work on CHAINIAC has been featured in CyberScoop—another leading public-sector media that reports on news and events impacting technology and security.* ***This level of media coverage demonstrates that Dr. Nikitin's work resonates far beyond the confines of the academic community. His contributions are shown to address issues of critical relevance to both industry professionals and the general public.***"

**Reviews by other experts and researchers.** Dr. Nikitin's work has also been cited by numerous published scientific articles within the field of Data Privacy and Computer Security [Exhibit 2, Google Scholar profile of Dr. Nikitin]. For instance, Dr. Nikitin's work on securing group communication in the Internet Of Things has been featured in several highly-cited surveys of the field's challenges and prominent solutions [Exhibit 22, Publications that review Dr. Nikitin's work]. Similarly, Dr. Nikitin's work on securing software-update systems has been featured in The Morning Paper, a popular blog provides short summaries of important, influential, topical or otherwise interesting papers in the field of computer science [Exhibit 22].

**The recognition of Dr. Nikitin's work in these major media outlets, combined with the citations by other experts and researchers, highlights Dr. Nikitin's extraordinary ability and significant role in advancing the field of Data Privacy and Computer Security. These publications serve as objective evidence of the widespread impact of Dr. Nikitin's work and its importance to the global community.**

# 3 Dr. Nikitin's proposed employment has both substantial merit and national importance for the United States.

Dr. Nikitin's proposed employment directly addresses critical challenges in safeguarding sensitive data and the integrity of digital infrastructure, and mitigating risks associated with emerging technologies. His work contributes to the development of innovative solutions for secure data sharing and privacy-preserving analytics—the key priorities in the National Strategy to Advance Privacy-Preserving Data

Sharing and Analytics [Exhibit 25]. In addition to enhancing national security, these solutions bolster public trust in the digital economy, which is vital for the sustained growth and competitiveness of the United States on the global stage.

Dr. Nikitin's expertise is particularly crucial as cyber threats and data breaches increasingly target the nation's critical infrastructure, financial systems, healthcare institutions, and governmental operations. By advancing the field of Data Privacy and Computer Security, his research supports the objectives outlined in the Executive Order on Improving the Nation's Cybersecurity [Exhibit 25], which emphasizes the need for robust measures to protect sensitive systems and information from adversaries. His work also aligns with the goals of the Executive Order on America's Supply Chains, by addressing vulnerabilities in the software supply chain—the key area of concern for both economic resilience and national defense—and with the goals of the Executive Order on Strengthening American Leadership in Digital Financial Technology, by promoting the development of secure and efficient blockchain technologies (see Exhibit 25 for both executive orders).

**Independent** expert Dr. EE, XX at Purple Inc. and YY at Cyan University, underscores the importance of Dr. Nikitin's work in his letter of support enclosed at Exhibit 7:

> "*Given my expertise and service to the U.S. government, I believe that I am well-qualified to assess Dr. Nikitin's extraordinary ability and the national importance of his scientific contributions. While I am aware of Dr. Nikitin's contributions in several subfields of computer security and data privacy, I believe that his most outstanding achievements are in developing techniques for protection of metadata. Metadata come in many forms. What resources users access, who they communicate with, and how they do it constitute sensitive information that is often as important as the content of the communication itself.* ***Dr. Nikitin's research focuses on protecting side information exposed during data encryption and protecting user access patterns—areas that are both technically challenging and vital to national security and individual privacy. As I testified to . . . , all data are personally identifiable information because even innocuous-looking data about an individual can be correlated with her identity. In an era where cyber threats and mass surveillance pose increasing risks, Dr. Nikitin's innovations contribute directly to the protection of U.S. infrastructure, businesses, and citizens from data exploitation.***"

Dr. BB, YY at Red University, highlights the national importance of Dr. Nikitin's research work (see Exhibit 4):

> "*Dr. Nikitin's expertise in data protection and digital privacy is of national significance to the United States. In recent years, the U.S. government has increasingly recognized the urgent need for advancements in privacy-preserving technologies, particularly in response to escalating cybersecurity threats. This has led to a rise in federally funded grant programs dedicated to this critical area.* ***Dr. Nikitin contributed to a project funded by the Defense Advanced Research Projects Agency (DARPA), a government agency focused on developing cutting-edge technologies for national defense.*** *As part of this project, he devised techniques for metadata-private communication that make an individual user's network activity appear indistinguishable to hostile network observers and render it resistant to traffic analysis.* ***By continuing his research in the United States, Dr. Nikitin will be well-positioned to further these vital efforts, advancing technologies that***

> ***not only safeguard individual privacy but also strengthen national security and reinforce our country's leadership in technological innovation.***"

Dr. Nikitin's unique background and accomplishments further underscore the substantial merit and national importance of his work. With over 10 years of research experience, a Ph.D. from the École Polytechnique Fédérale de Lausanne, Switzerland (ranked as the $10^{\text{th}}$ best university in the world in Engineering & Technology), a M.Sc. from KTH Royal Institute of Technology, Sweden (the $37^{\text{th}}$ best)—globally top-ranked institutions in computer science—and postdoctoral training at Cornell University and Columbia University, he brings exceptional expertise to the field (see Exhibit 17 for proof of Dr. Nikitin's degrees and Exhibit 23 for the QS World University Rankings).

Dr. AA, XX at Black University comments on the potential and future job prospects of Dr. Nikitin (see Exhibit 3):

> "..."

In summary, Dr. Nikitin's contributions are not only timely but essential. His proposed employment in the United States will drive innovation in fields of national importance, strengthen the country's leadership in privacy and security technologies, and advance its strategic objectives in safeguarding digital infrastructure and promoting economic prosperity.

# 4 Final merits determination

In accordance with the Kazarian opinion, the second step of the two-part approach is a final merits determination that considers all of the evidence in the context of whether the beneficiary meets the required level of high achievement and sustained international reputation in the field. The aggregated evidence establishes that Dr. Nikitin not only meets at least four of the regulatory criteria, but also that he has been recognized internationally as outstanding in his field of expertise.

Throughout his professional career, Dr. Nikitin has made numerous critical discoveries that have advanced the field. These groundbreaking contributions are detailed above and have been corroborated by internationally recognized experts in the field (see Exhibit 3-Exhibit 10). **As these experts confirm, Dr. Nikitin has made original contributions with wide-reaching practical applications throughout his research career.** His work on metadata protection has been adopted by iMessage and Facebook Messenger, real-world systems with over billion users (Section 2.1.1), his work on private information retrieval has addressed a long-lasting security flaw in the design of existing schemes and has started a new line of research in the field (Section 2.1.2), his work on the security of software supply-chain has been highly cited by other researchers and has been used in graduate-level courses at various universities (Section 2.1.3), and, finally, his work on the efficiency of blockchain networks was the first to demonstrate the practical benefits of verifiable computation (Section 2.1.4).

**Dr. Nikitin is a scientist of extraordinary ability, who is recognized to have risen to the very top of the field of his expertise.** He has both published his research findings in and judged the work of other researchers in the most prestigious, top-ranked conference proceedings and journals. Concretely, Dr. Nikitin has published in or served on the program committee of each of the top three venues in Data Privacy and Computer Security, according to Research.com and Google Scholar Metrics (see Exhibit 18 for the rankings). His work has been cited 333+ times by other scientists

worldwide (Section 2.2) and has been covered by major media outlets (Section 2.4). He has completed 68 full-length reviews for the top conferences and journals in the field (Section 2.3).

**Dr. Nikitin has not only had contributions of international acclaim, but has also sustained them.** His publications were cited 50+ times in the past year alone, more than in any year prior. Dr. Nikitin continues to be invited to participate in the program committees of the top conferences and receives invitations to review articles from the top journals in his field. Just recently, he organized The Satellite Conference on Biomedical Data Privacy and Equity 2024, a highly specialized conference for scientists working on the privacy of biomedical data, which confirmed his standing in the field.

Dr. Nikitin's work has both substantial merit and national importance for the United States, as his work aligns with national priorities in strengthening the country's leadership in privacy and security technologies. The totality of the presented evidence clearly shows that Dr. Nikitin has been internationally recognized as outstanding in the field. As such, Dr. Nikitin meets the requirements for the EB-1A classification as a person of extraordinary ability in sciences.

# 5 Conclusion

Dr. Nikitin is a well-recognized expert in the field of Data Privacy and Computer Security who has risen to the very top of his field of endeavor, which is supported by the presented evidence and the letters from experts in the field. He will continue working in the field of his expertise, which will benefit the United States. Thus, Dr. Nikitin fully satisfies all the requirements and regulations listed in INA Section 203(b)(1)(A) and 8 CFR Section 204.5(h), and the reviewer is kindly asked to approve Dr. Nikitin's petition for permanent residence under the category of an alien of extraordinary ability.

Please inquire at the following address for any additional evidence.

Yours faithfully,

Dr. Kirill Nikitin

Address:
Tel:
Email:
Personal website: `https://nikirill.com`

## Statement from Dr. Nikitin on how he intends to continue work in the United States

July 29, 2025

I am the beneficiary of this I-140 Immigrant Petition for an Alien Worker, seeking EB-1A classification as an individual of extraordinary ability. I have a vast experience in the field of Data Privacy and Computer Security, and I intend to continue carrying out research in this area in the United States.

I am already employed as a postdoctoral researcher and I conduct research in the area of my expertise. Specifically, I analyze the leakage of sensitive information from de-identified medical data and develop privacy-preserving methods for data sharing. I began my work in the United States at Cornell University, and then continued to conduct research at Columbia University and the New York Genome Center, all of which are the top-ranked research institutions in the world (see Exhibit 24 for the corresponding employment offer letters). I also have experience in applied science, as I interned at Microsoft Research—the research arm of one of the largest technology companies in the world.

After completing my postdoctoral appointment, I plan to apply for professorship positions in Computer Science at research universities in the United States. Having become one of the top experts in the field of Data Privacy and Computer Security, I believe that I have a duty to use my expertise to advance the state of the art in privacy technologies and to share my knowledge with the next generation of scientists, engineers, and policy-makers in the United States. I will also continue my presenting research results at international conferences and serving as a reviewer for conferences and journals in my field.

My research will continue to focus on strengthening privacy protections for users and improving the cybersecurity posture of computer systems, including software-update systems and blockchain networks. I will work on developing mechanisms for private communication and the private retrieval of information, which, I believe, will become even more in demand in the future. I will also continue my work on developing tools for privacy-preserving analysis and sharing of medical data, which is a field of growing importance in the upcoming era of personalized medicine. The National Strategy to Advance Privacy-Preserving Data Sharing and Analytics highlights the importance of such tools for responsible scientific research and innovation, especially in healthcare research where data are highly sensitive and their sharing is limited by the existing regulations.

Getting the permanent residence in the United States will increase my research opportunities. For example, many research grants at the National Science Foundation (NSF) or the National Institutes of Health (NIH) are restricted to U.S. citizens and permanent residents. With the permanent residency, I will be able not only to apply for such grants but, thereby, attract and fund the most talented students.

I would like to see more of my research inventions deployed in real-world systems by U.S.-based companies, as it happened with my work on metadata protection that was adopted by Apple in iMessage and by Facebook in Messenger. Such deployment can require my advisory and engagement that I am currently not permitted to provide due to my non-immigrant visa status. As an alternative career path, I consider starting my own company. I would specifically target privacy-preserving data analytics—the priority that the National Science and Technology Council highlights in their national strategy report. Unfortunately, my non-immigrant status also restricts my ability start a business and to translate my research into real-world applications that would benefit the U.S. population. Obtaining

the permanent residency will lift these limitations and allow me to maximize the positive impact of my research and to contribute more significantly to the United States' innovation ecosystem.

Yours faithfully,

Dr. Kirill Nikitin

Address:
Tel:
Email:
Personal website: `https://nikirill.com`

# List of Exhibits

## Academic and professional background

Exhibit 1: Curriculum Vitae of Dr. Kirill Nikitin.

Exhibit 2: Google Scholar Profile of Dr. Kirill Nikitin.

## Letters of support

Exhibit 3: Letter of support from Dr. AA (Black University), followed by his CV.

Exhibit 4: Letter of support from Dr. BB (Red University), followed by his CV.

Exhibit 5: Independent letter of support from Dr. CC (Blue University), followed by his CV.

Exhibit 6: Independent letter of support from Dr. DD (Yellow University), followed by his CV.

Exhibit 7: Independent letter of support from Dr. EE (White University), followed by his CV.

Exhibit 8: Independent letter of support from Dr. FF (Purple Inc. and Cyan University), followed by his CV.

Exhibit 9: Independent letter of support from Dr. GG (Violet Inc.), followed by his CV.

Exhibit 10: Independent letter of support from Dr. JJ (Violet Inc.), followed by his CV.

## Key scientific contributions by Dr. Kirill Nikitin

Exhibit 11: The title page and abstract of Dr. Nikitin's Ph.D. thesis on the protection of metadata and data integrity.

Exhibit 12: The first pages of the publication by Dr. Nikitin on protecting metadata in encrypted data and communication, **alongside the evidence of Dr. Nikitin's inventions being used in Apple's iMessage and in Facebook Messenger**:

- *Nikitin K., Barman L., Lueks W., Underwood M., Hubaux J. P., and Ford B. Reducing Metadata Leakage from Encrypted Files and Communication with PURBs. Proceedings on Privacy Enhancing Technologies, 2019(4).*
- The announcement by Apple Security Engineering and Architecture about the changes in iMessage which describes the use of Dr. Nikitin's inventions in the "Padding and Encryption" section.
- The announcement by Facebook Engineering about upgrading Messenger's security which presents the Labyrinth encrypted storage protocol. The Labyrinth protocol uses Dr. Nikitin's inventions.
- Extracts from Labyrinth's documentation that describe the protocol's design goals and the use of Dr. Nikitin's inventions in the "2. Padding" section.
- Statistics on the number of active users of iMessage and Facebook Messenger.

Exhibit 13: The first pages of the publication by Dr. Nikitin on ensuring data integrity in private information retrieval:

- *Colombo S., Nikitin K., Corrigan-Gibbs H., Wu D. J., and Ford B. Authenticated Private Information Retrieval. In USENIX Security Symposium 2023.*

Exhibit 14: The first pages of the publication by Dr. Nikitin on securing the software supply chain, **alongside the evidence that this work has been included in the graduate-level curriculum at multiple US and international universities**:

- *Nikitin K., Kokoris-Kogias E., Jovanovic P., Gailly N., Gasser L., Khoffi I., Cappos J., Ford B. CHAINIAC: Proactive Software-Update transparency via collectively signed skipchains and verified builds. In USENIX Security Symposium 2017.*
- A course syllabus from the University of Chicago.
- A course syllabus from the University of California, San Diego.
- A course syllabus from the University of Illinois at Urbana-Champaign.
- A course syllabus from the Technical University of Munich, Germany.

Exhibit 15: The first page of the publication authored by Dr. Nikitin on improving the efficiency of blockchain networks:

- *Lee J., Nikitin K., Setty S. Replicated state machines without replicated execution. In IEEE Symposium on Security and Privacy 2020.*

Exhibit 16: The first page of an additional publication authored by Dr. Nikitin on securing group communication in the Internet of Things:

- *Tiloca M., Nikitin K., Raza S. Axiom: DTLS-based secure IoT group communication. ACM Transactions on Embedded Computing Systems (TECS), 2017.*

### Other

Exhibit 17: Proof of Dr. Kirill Nikitin's advanced degrees (Ph.D., M.Sc., and M.Sc.) in Computer and Communication Sciences, Information and Communication Technology, and Information Security, respectively.

Exhibit 18: Conference and journal rankings by category.

Exhibit 19: Proof of 68 scientific reviews undertaken by Dr. Nikitin in conferences and journals on data privacy, computer security, and blockchain.

Exhibit 20: Proof of Dr. Nikitin's membership in the Association for Computing Machinery (ACM) and in the Institute of Electrical and Electronics Engineers (IEEE).

Exhibit 21: Evidence that Dr. Nikitin co-organized The Satellite Conference on Biomedical Data Privacy and Equity (RECOMB-PRIEQ 2024).

Exhibit 22: Evidence of published material about Dr. Nikitin's work in professional and major trade publications.

Exhibit 23: QS World University Rankings.

Exhibit 24: The current employment letter and the offer letters that Dr. Nikitin received for postdoctoral researcher positions:

- The latest employment extension letter from XX (current).
- The offer letters from XX and YY (accepted, currently employed).
- The offer letter from ZZ (accepted).
- The offer letter from WW (declined).

Exhibit 25: Executive orders, a national strategy report, and an action plan by the federal government which highlight the national importance of Dr. Nikitin's area of research and proposed employment.

- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023).
- National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (2023).
- National Privacy Research Strategy (2025).
- Executive Order on America's Supply Chains (2024).
- Executive Order on Improving the Nation's Cybersecurity (2021).
- An Action Plan on Securing Defense-Critical Supply Chains (2022).
- Executive Order on Strengthening American Leadership in Digital Financial Technology (2025).

# Exhibit 1

Curriculum Vitae of Dr. Kirill Nikitin

# Exhibit 2

Google Scholar Profile of Dr. Kirill Nikitin

# Kirill Nikitin

FOLLOW

Columbia University & New York Genome Center
Verified email at columbia.edu - Homepage

Privacy Genomics Computer Security Blockchain

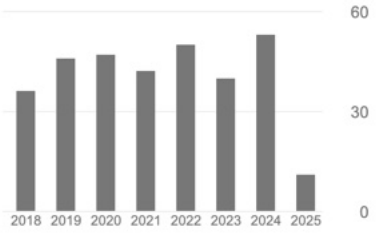
| TITLE | CITED BY | YEAR |
|---|---|---|
| CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds<br>K Nikitin, E Kokoris-Kogias, P Jovanovic, N Gailly, L Gasser, I Khoffi, ...<br>26th USENIX Security Symposium (USENIX Security 17), 1271-1287 | 186 | 2017 |
| Replicated state machines without replicated execution<br>J Lee, K Nikitin, S Setty<br>IEEE Symposium on Security and Privacy | 46 | 2020 |
| Axiom: DTLS-based secure IoT group communication<br>M Tiloca, K Nikitin, S Raza<br>ACM Transactions on Embedded Computing Systems (TECS) 16 (3), 1-29 | 39 | 2017 |
| Authenticated private information retrieval<br>S Colombo, K Nikitin, H Corrigan-Gibbs, DJ Wu, B Ford<br>32nd USENIX security symposium (USENIX Security 23), 3835-3851 | 31 | 2023 |
| Reducing metadata leakage from encrypted files and communication with PURBs<br>K Nikitin, L Barman, W Lueks, M Underwood, JP Hubaux, B Ford<br>Proceedings on Privacy Enhancing Technologies 2019 (4), 6-33 | 16 | 2019 |
| Crux: Locality-Preserving Distributed Services<br>C Basescu, MF Nowlan, K Nikitin, JM Faleiro, B Ford<br>arXiv preprint arXiv:1405.0637 | 7 | 2014 |
| Secure Two-Way DTLS-Based Group Communication in the IoT, draft-tilocadice-secure-groupcomm-00 (work in progress)<br>M Tiloca, S Raza, K Nikitin, S Kumar<br>Internet Engineering Task Force | 6 | 2015 |
| DTLS adaptation for efficient secure group communication<br>K Nikitin | 2 | 2015 |
| Integrity and Metadata Protection in Data Retrieval<br>K Nikitin<br>EPFL | | 2021 |

Articles 1–9 SHOW MORE

## Cited by

VIEW ALL

| | All | Since 2020 |
|---|---|---|
| Citations | 333 | 243 |
| h-index | 6 | 5 |
| i10-index | 5 | 5 |




## Public access

VIEW ALL

0 articles — not available

2 articles — available

Based on funding mandates

## Co-authors

EDIT

- Bryan Ford, EPFL
- Philipp Jovanovic, University College London
- Justin Cappos, Professor of Computer Science ...
- Lefteris Kokoris Kogias, MystenLabs
- Marco Tiloca, RISE Research Institutes of Swe...
- Srinath Setty, Principal Researcher at Microsof...
- Shahid Raza, Full Professor & Cybersecurity C...
- Henry Corrigan-Gibbs, MIT CSAIL
- David Wu, University of Texas at Austin
- Simone Colombo, King's College London
- Wouter Lueks, CISPA Helmholtz Center for Infor...
- Jean-Pierre Hubaux, Professor, EPFL
- Ludovic Barman, EPFL

# Exhibit 3

Letter of support from Dr. AA (Black University), followed by his CV

# Exhibit 4

Letter of support from Dr. BB (Red University), followed by his CV

January 30, 2025

Department of Homeland Security
USCIS

Re: Letter of Support for Dr. Kirill Nikitin's Immigration Petition

To Whom It May Concern:

I am pleased to write this letter to express my full support for the immigrant petition submitted by Dr. Kirill Nikitin. Having closely worked with him, I can confirm that Dr. Nikitin is a scientist of outstanding talent, who has made contributions of major impact to our research field and whose expertise is of national importance to the United States.

Ny name is …

Dr. Nikitin is an established scientist in data and computer privacy. He has published multiple works in the most prestigious scientific venues, including the top-tier peer-reviewed conferences, such as the IEEE Symposium on Security and Privacy and the USENIX Security Symposium. These conferences are highly selective and attract groundbreaking research from leading experts in the field. The impact of Dr. Nikitin's work is reflected in its significant academic recognition—his publications have been cited more than 331 times by other researchers, which is an impressive number for a scientist at his career stage. This level of citation demonstrates that his contributions are not only relevant but also influential, shaping ongoing research and advancements in privacy enhancing technologies.

Dr. Nikitin's work on reducing metadata leakage from encrypted files and communication is one of his most influential contributions. Dr. Nikitin has studied the problem of encrypted-data formats exposing auxiliary information, such as the encryption suites used or the payload length. This kind of exposure can be exploited by traffic analysis, de-anonymization and website fingerprinting attacks and it has been extensively studied by the research community. Instead of sustaining the fragile balance and trying to distinguish which metadata were sensitive and could be exposed and which were not, Dr. Nikitin proposed a radical innovation of leaving no unencrypted metadata in ciphertexts whatsoever. While being ideal from the privacy perspective, this approach faced efficiency challenges due to requiring new ways of handling decryption, as a recipient would not know what algorithm or cryptographic key to use to decrypt a ciphertext without unencrypted markers. Dr. Nikitin's proposed decoding techniques enabled a recipient to

first efficiently find and decrypt the auxiliary markers and then to decrypt the data. This innovation has made it significantly more difficult for adversaries to perform traffic analysis or to infer sensitive information from encrypted data at-rest.

Dr. Nikitin's expertise in data privacy is of national significance to the United States. In recent years, the U.S. government has increasingly recognized the urgent need for advancements in privacy-preserving technologies, particularly in response to escalating cybersecurity threats. This has led to a rise in federally funded grant programs dedicated to this critical area. Dr. Nikitin contributed to a project funded by the Defense Advanced Research Projects Agency (DARPA), a government agency focused on developing cutting-edge technologies for national security. As part of this project, he devised techniques for metadata-private communication that made an individual's web activity to appear indistinguishable to a network observer, rendering it resistant to traffic analysis. By continuing his research in the United States, Dr. Nikitin will be well-positioned to further these vital efforts, advancing technologies that not only safeguard individual privacy but also strengthen national security and reinforce the country's leadership in technological innovation.

To conclude, Dr. Nikitin is a recognized leader in data and computer privacy research. If he is to stay in the United States, he will be a great asset to the country and will continue making important contributions in research and beyond. I, therefore, urge you to favorably consider his application for permanent residence in the United States.

# Exhibit 5

Independent letter of support from Dr. CC (Blue University), followed by his CV

January 22, 2025

Department of Homeland Security
United States Citizenship and Immigration Services

Re: Independent Letter of Support for Dr. Kirill Nikitin

Dear USCIS Officer,

I am providing this independent letter to confirm that Dr. Nikitin is an outstanding researcher, and I enthusiastically support the petition to classify him as a scientist of extraordinary ability based on his impressive scientific contributions and his reputation as a leader in the field.

I am …

Although I have not worked directly with Dr. Nikitin, I offered him a position as a postdoctoral researcher in my group in 2021, which has allowed me to become well-acquainted with his work and accomplishments. Dr. Nikitin has made significant, original contributions to the field of data and computer privacy, particularly through his research on Private Information Retrieval (PIR). PIR enables users to retrieve data from a computer database without revealing what data they are accessing. This technology is crucial for improving the privacy guarantees of online communication, for example, in instant messaging applications, such as WhatsApp. Previously, research in PIR assumed that database servers always followed the protocol perfectly. In real-world applications, however, a corrupted or compromised server can violate the protocol and attempt to break the user's privacy. Dr. Nikitin has demonstrated that such a server can alter its response to a user's query, observe whether the user accepts this response, and, subsequently, infer what data have been accessed. Dr. Nikitin's proposed schemes are the first efficient solution to ensure the privacy of information retrieval even when the database server is malicious. This achievement bridges the gap between theoretical PIR protocols and their practical security in real-world scenarios.

Dr. Nikitin has also advanced blockchain research by demonstrating how to integrate state-of-the-art verifiable outsourced computation into permissioned or permissionless blockchains. In essence, a blockchain achieves strong integrity protection through the redundant verification of all blocks and the transactions they contain by numerous—e.g., thousands or tens of thousands—of independent decentralized participants. The key idea of Piperine, the system that Dr. Nikitin and his collaborators from Microsoft

Research designed, is to reduce this large redundant verification cost by allowing a single untrusted prover to produce a verifiable cryptographic proof of the correctness of a block of transactions and the many independent verifiers to merely verify these proofs, instead of the transactions themselves. While simple in concept, the key technical challenges are in bridging the huge remaining efficiency gap between state-of-the-art outsourced computation and direct re-execution, as well as the many limitations and impedance mismatches between current outsourced computation methods and the requirements of the blockchain context. I believe that Piperine represents a major contribution both to blockchain and outsourced computation research, and it illustrates Dr. Nikitin's breadth and independent collaboration abilities in security/privacy research.

Another evidence of Dr. Nikitin's recognition as a leading expert in the field is his role in judging the work of other researchers. He has already served on the Program Committee for such prestigious conferences in computer security and privacy as the ACM Conference on Computer and Communications Security, the USENIX Security Symposium, and the IEEE International Conference on Blockchain and Cryptocurrency. Invitations to join the Program Committee of such conferences are extended only to internationally renowned scientists, as the members do not only provide their experts reviews but also participate in the discussion and make collective final decisions of either accepting or rejecting submissions. I can confirm that Dr. Nikitin possesses the highest level of expertise required for this role, as both he and I were active Program Committee members of the ACM Conference on Computer and Communications Security. His contributions underscore his deep understanding of complex technical concepts and his ability to evaluate their significance and potential impact. Finally, his active participation demonstrates not only his professional standing among peers but also his dedication to advancing the field of computer security and privacy.

In conclusion, Dr. Nikitin is recognized internationally for his research contributions and his service to the research community. His abilities and knowledge are an important asset to the economy and scientific standing of the United States. I strongly support his petition for classification as a scientist of extraordinary ability.

Sincerely yours,

CCC

# Exhibit 6

Independent letter of support from Dr. DD (Yellow University),
followed by his CV

**January 20, 2025**

Center Director
Department of Homeland Security
USCIS

**Re: Independent Reference in Support of Dr. Kirill Nikitin's EB-1A Petition**

Dear Immigration Officer:

I am pleased to write an independent reference letter on behalf of Dr. Kirill Nikitin in support of his Alien of Extraordinary Ability petition. Dr. Nikitin is one of a select few researchers who has risen to the very top of the field of computer security, specializing in software-update security, blockchains, and verifiable computation. Although we have never worked together personally or professionally, I am very familiar with Dr. Nikitin's work by way of his publications. I can confidently affirm his international reputation as an outstanding researcher and offer my full support of this petition.

My name is ...

Given my expertise, I can offer a good account of Dr. Nikitin's contributions to the field.

Dr. Nikitin is one of the world experts in security of software-update systems, a research area of national importance to the United States. As recent attacks, such as the breaches of government agencies through SolarWinds's software, have shown, software-update systems are a lucrative target for malicious actors because compromising a single access point can enable them to distribute malware to thousands of companies and users. Failures in the software-update process can also lead to the disruption of critical services. CrowdStrike-related outage, caused by a faulty software update, several months ago resulted in grounded flights, halted governmental services, and closed banks with the estimated worldwide financial damages of at least $10 billion. Hence, it is of paramount importance to design robust and secure mechanisms for the software supply chain.

As a response to this critical challenge, Dr. Nikitin developed an innovative framework, named CHAINIAC, that was the first to leverage decentralization and transparency to eliminate single points of failure and to enforce integrity in the software-release pipeline. At a high level, the framework secures each step of the software production process, from the development of the source code to the installation of the corresponding update on a user's device. Among other techniques, the framework introduced the concepts of collectively verified builds and skipchains. Prior artifact-verifiability approaches provided the guarantee

that a given source code could be deterministically compiled into some binary but did not establish any binding between the source code and the actual release delivered to user devices. CHAINIAC's innovation was to employ multiple servers that independently compiled a binary and then attested to a single valid release result that end users could trust. By leveraging skipchains, a novel data structure that Dr. Nikitin designed, CHAINIAC implemented a public release log that deflected targeted attacks on high-profile individuals. This work of Dr. Nikitin constituted a major contribution to the field and influenced the design of multiple follow-up architectures, including the Google's Binary Transparency project.

Another influential work by Dr. Nikitin that I am closely familiar with showed how to improve the performance of Replicated State Machines (RSMs) by utilizing outsourced verifiable computation. Dr. Nikitin demonstrated that, in a distributed system where multiple computer nodes executed the same operations, it could be more efficient for a single node to execute an operation, while generating a proof of correct execution, and to convince the other nodes of this correctness by letting them verify the proof. To achieve the required efficiency, Dr. Nikitin co-developed multiple complex cryptographic techniques to reduce the cost of proof generation and verification. This was a groundbreaking result because the research community had previously considered outsourced verifiable computation to be a high-overhead tool that inevitably caused efficiency decline. The demonstration that this tool could, instead, improve efficiency was a landmark advancement in the field.

The result above also had a profound practical impact. The modern example of RSMs are blockchains systems, a recent technology that has applications in finance, governance, and regulation. Dr. Nikitin showed how his techniques could be applied to Ethereum, the second largest cryptocurrency and a platform with the market cap of $400 billion. Concretely, they could increase the throughput of the Ethereum network fivefold which would translate in millions of dollars on saved transaction fees. Several cryptocurrency solutions later adopted and deployed this approach. Retaining researchers, such as Dr. Nikitin, with a deep expertise in new developing technologies is critical for the United States to maintain its position as the world technological leader.

As further evidence of his international recognition in the field, Dr. Nikitin's work has been published in the most prestigious conferences and journals, including IEEE Symposium on Security and Privacy, USENIX Security Symposium, Privacy Enhancing Technologies Symposium, and ACM Transactions on Embedded Computing Systems. Due to the fast pace of the field, conferences are the primary publishing venues for computer security and privacy researchers. The conferences in which Dr. Nikitin has published are commonly regarded as the most selective and impactful in the field. Moreover, Dr. Nikitin is a highly cited researcher, meaning that others in his field have found his work to be novel and useful

for their own research. At this time, his original work has been cited 330 times by researchers from around the world. Considering that most scientific papers are scarcely cited, this is a clear indication of the significant and worldwide impact of Dr. Nikitin's research.

In sum, researchers of Dr. Nikitin's caliber are extremely rare. His superior expertise and success of his research endeavors make him an invaluable asset to any employer or any country that hosts him. For these reasons, I strongly encourage your approval of this petition.

# Exhibit 7

Independent letter of support from Dr. EE (White University), followed by his CV

February 27, 2025

United States Citizenship and Immigration Services

**Re: Independent Supporting Letter for the Immigration Petition of Dr. Kirill Nikitin**

Dear Sir/Madam,

I write this letter in my capacity as … to offer my strong endorsement of Dr. Kirill Nikitin's immigration petition. Although I have never worked with Dr. Nikitin, I have followed his research with great interest. As a distinguished researcher in computer privacy and security, Dr. Nikitin has conducted innovative work that has significantly advanced both the theoretical and practical aspects of the field. His exceptional contributions clearly demonstrate his extraordinary abilities and promise considerable benefits to the global community.

I would like to begin by introducing myself. My name is …

My research work examines …

Dr. Nikitin is foremost known for his scientific contributions in data privacy and, specifically, in the area of metadata protection. In his paper titled "Reducing metadata leakage from encrypted files and communication with PURBs" published in the Proceedings on Privacy Enhancing Technologies, Dr. Nikitin presented techniques for both obfuscating the length of encrypted content and protecting encryption metadata. The length can reveal a significant amount of information about content but protecting it is a non-trivial task because digital objects can radically differ in size. A user might send a short email or download a large movie in the same Web session and making the two the same size is impractical—the Internet does not have enough bandwidth to handle emails that are gigabytes in size. Dr. Nikitin came up with padding technique that accounts for the size of an object and adds just enough protection bytes to provide provable privacy guarantees while still ensuring practicality. The technique is one of the kind and has already been adopted by some major technological companies.

The techniques for protecting encryption metadata by Dr. Nikitin were the first to provide scalable encryption functionality for ciphertexts (encrypted data) with hundreds of recipients. Part of my research is on anonymity networks where users can communicate

with each other without revealing their communication patterns. These networks require that ciphertexts do not expose the identities of their recipients, but prior protection approaches for this scaled to only several recipients. The fact that Dr. Nikitin's techniques overcome this barrier and further extend the protection to other types of encryption metadata is a major achievement for the field.

Dr. Nikitin has also made notable advance in blockchain research. In his paper titled "Replicated state machines without replicated execution", he demonstrates that the throughput of blockchains networks can be increased by using verifiable computation. Specifically, if, instead of sending out multiple transactions, a blockchain node proves the correctness of their cumulative execution and sends out this proof, other nodes can verify the proof faster than they would have re-executed the transactions. This was a surprising result that showcased Dr. Nikitin's expertise on the topic and his ability to design innovative solutions. Furthermore, in his other paper titled "Chainiac: Proactive software-update transparency via collectively signed skipchains and verified builds", he introduced a novel data structure named skipchain. Unlike traditional blockchains, a skipchain facilitates verifiable forward traversal of the blocks and more efficient backward traversal. This is another example of an innovative creation that makes Dr. Nikitin is a leading researcher in the field.

It comes as no surprise that the work by Dr. Nikitin is widely published and cited by researchers worldwide. He has publications in premier computer security and privacy venues, such as the USENIX Security Symposium and the IEEE Symposium on Security and Privacy. His work has already attained over 300 citations from his peers, attesting to its significant influence on the field. This impressive for his career stage citation count underscores the far-reaching impact of his research, which not only enriches academic discourse but also drives the development of real-world solutions in data privacy and security. Such widespread recognition is a clear indicator of Dr. Nikitin's exceptional contributions and reinforces his eligibility as an individual of extraordinary ability.

In summary, I offer my unequivocal support for Dr Kirill Nikitin's immigration petition. His pioneering research and outstanding contributions to computer privacy and security not only advance our understanding of critical challenges in the field, but also facilitate the development of innovative solutions. I am confident that his work will continue to have a significant impact on both academic research and technological practice, and I trust that his application will be granted the favourable consideration it richly deserves. Should you require any further information, please do not hesitate to contact me.

Yours faithfully,

EEE

# Exhibit 8

Independent letter of support from Dr. FF (Purple Inc. and Cyan University), followed by his CV

February 10, 2025

USCIS

Re: Support Letter for Dr. Kirill Nikitin's EB-1A petition

Dear USCIS Officer,

I am honored to support Dr. Kirill Nikitin's petition for classification as an Alien of Extraordinary Ability under the EB-1A category. Dr. Nikitin has made significant contributions to data privacy and computer security, advancing both theoretical foundations and practical applications. His exceptional expertise and innovative research firmly establish him as a leader in the field, while the nature of his work makes him an invaluable asset to the United States.

I offer this support as an internationally recognized expert in …

Given my expertise and service to the U.S. government, I believe that I am well-qualified to assess Dr. Nikitin's extraordinary ability and the national importance of his scientific contributions. While I am aware of Dr. Nikitin's contributions in several subfields of computer security and data privacy, I believe that his most outstanding achievements are in developing techniques for protection of metadata. Metadata come in many forms. What resources users access, who they communicate with, and how they do it constitute sensitive information that is often as important as the content of the communication itself. Dr. Nikitin's research focuses on protecting side information exposed during data encryption and protecting user access patterns—areas that are both technically challenging and vital to national security and individual privacy. As I testified to …, all data are personally identifiable information because even innocuous-looking data about an individual can be correlated with her identity. In an era where cyber threats and mass surveillance pose increasing risks, Dr. Nikitin's innovations contribute directly to the protection of U.S. infrastructure, businesses, and citizens from data exploitation.

I should clarify that Dr. Nikitin and I have never collaborated, and I know of him solely because of his research contributions. I, however, saw his in-person presentation at a research seminar at Purple Inc. offices because we invited him to present his work on protecting attributes of encrypted data, after it had just been adopted by Apple for use in iMessage. Dr. Nikitin's innovation in iMessage is a technique for obfuscating the length of encrypted data. Most encryption algorithms nowadays preserve the length of data when encrypting it. For example, the word "yes" would commonly be encrypted with three symbols, whereas the word "no" with two symbols. This is obviously a privacy issue in the messaging context because, even when encrypted, the two words would be easily distinguishable. Dr. Nikitin proposed a padding technique that struck the optimal balance between the size protection and the induced bandwidth overhead. Minimizing the overhead while providing the best possible protection is

critical, as a system like iMessage might be exchanging billions of messages every day. The fact that Dr. Nikitin's innovation provides this balance and that it is directly translated into deployment by a major technology company underscores the real-world impact of his work and its importance in securing communications at scale.

Dr. Nikitin's work on protecting user access patterns follows a long line of research on private information retrieval (PIR). PIR is a set of techniques for enabling a computer user to fetch an item from a database without revealing to the database which item it is. While PIR has been extensively studied in academic settings, all the prior approaches have been unsuitable for real-world deployment due to being insecure in the adversarial setting. Dr. Nikitin's work is the first to demonstrate how to make such protocols secure even when the database operator actively attempts to break the user's privacy. These security properties are crucial in applications requiring strong guarantees, such as secure cloud storage and privacy-preserving search. Dr. Nikitin's contributions bring the PIR technology significantly closer to practical deployment, enabling robust privacy protections in real-world systems.

In summary, I wholeheartedly endorse Dr. Nikitin's EB-1A petition. His exceptional abilities, pioneering research, and tangible real-world impact make him an extraordinary asset to the United States. I am confident that his continued contributions will further enhance America's leadership in data privacy, computer security, and innovation. For these reasons, I urge you to favorably consider his application.

Yours faithfully,

FFF

# Exhibit 9

Independent letter of support from Dr. GG (Violet Inc.), followed by his CV

# Exhibit 10

Independent letter of support from Dr. JJ (Violet Inc.), followed by his CV

# Exhibit 11

The title page and abstract of Dr. Nikitin's Ph.D. thesis on protection of metadata and data integrity

EPFL

Thèse n° 7391

# Integrity and Metadata Protection in Data Retrieval

Présentée le 26 novembre 2021

Faculté informatique et communications
Laboratoire de systèmes décentralisés et distribués
Programme doctoral en informatique et communications

pour l'obtention du grade de Docteur ès Sciences

par

**Kirill NIKITIN**

Acceptée sur proposition du jury

Prof. J.-P. Hubaux, président du jury
Prof. B. A. Ford, directeur de thèse
Prof. J. Cappos, rapporteur
Prof. S. Capkun, rapporteur
Prof. K. Argyraki, rapporteuse

École
polytechnique
fédérale
de Lausanne

2021

# Abstract

Secure retrieval of data requires integrity, confidentially, transparency, and metadata-privacy of the process. Existing protection mechanisms, however, provide only partially these properties: encryption schemes still expose cleartext metadata, protocols for private information retrieval neglect data integrity, and data-distribution architectures forego transparency. In this dissertation, by designing new cryptographic primitives and security architectures that provide a more comprehensive protection, we improve on the current security and privacy practices in data retrieval. First, we propose a new format for encrypted data; it protects both content and all encryption metadata, such as the application, the intended recipients, and the algorithms used. The format comes with a cryptographically-agile encoding scheme that facilitates efficient decryption of such ciphertexts without cleartext markers. Second, to address the lack of integrity in privacy-preserving data-retrieval protocols, we introduce the concept of single-server verifiable private information retrieval. In contrast to existing solutions where, in some deployment scenarios, a malicious server can violate client privacy by selectively tampering with the data, our approach ensures that an honest client either correctly obtains the data from the system's server or detects server misbehavior and aborts. Finally, we present a software-update framework that reinforces software-distribution processes. Building on the concepts of decentralization and verifiability, our framework eliminates single points of failure, enforces transparency, and ensures integrity and authenticity of software releases. By implementing and experimentally evaluating our primitives and framework, we demonstrate that better protection is practical and incurs only a modest additional cost.

**Keywords:** privacy, integrity, security, metadata protection, private information retrieval, verifiable, software updates, transparency.

# Exhibit 12

The first pages of the peer-reviewed publication authored by Dr. Nikitin on protecting metadata in encrypted data and communication, alongside evidence of the Dr. Nikitin's inventions being used in Apple's iMessage and in Facebook Messenger:

1. *Nikitin K., Barman L., Lueks W., Underwood M., Hubaux J. P., and Ford B. Reducing Metadata Leakage from Encrypted Files and Communication with PURBs. Proceedings on Privacy Enhancing Technologies, 2019(4).*
2. The announcement by the Apple Security Engineering and Architecture team about the changes in iMessage which describes the use of Dr. Nikitin's inventions in the "Padding and Encryption" section.
3. The announcement by Facebook Engineering about upgrading Messenger's security which presents the Labyrinth encrypted storage protocol. The Labyrinth protocol uses Dr. Nikitin's inventions.
4. Extracts from Labyrinth's documentation that describe the protocol's design goals and the use of Dr. Nikitin's inventions in the "2. Padding" section.
5. Statistics on the number of active users of iMessage and Facebook Messenger.

Kirill Nikitin*, Ludovic Barman*, Wouter Lueks, Matthew Underwood, Jean-Pierre Hubaux und Bryan Ford

# Reducing Metadata Leakage from Encrypted Files and Communication with PURBs

**Abstract:** Most encrypted data formats leak metadata via their plaintext headers, such as format version, encryption schemes used, number of recipients who can decrypt the data, and even the recipients' identities. This leakage can pose security and privacy risks to users, *e.g.,* by revealing the full membership of a group of collaborators from a single encrypted e-mail, or by enabling an eavesdropper to fingerprint the precise encryption software version and configuration the sender used.

We propose that future encrypted data formats improve security and privacy hygiene by producing *Padded Uniform Random Blobs* or PURBs: ciphertexts indistinguishable from random bit strings to anyone without a decryption key. A PURB's content leaks *nothing at all*, even the application that created it, and is padded such that even its length leaks as little as possible.

Encoding and decoding ciphertexts with *no* cleartext markers presents efficiency challenges, however. We present cryptographically agile encodings enabling legitimate recipients to decrypt a PURB efficiently, even when encrypted for any number of recipients' public keys and/or passwords, and when these public keys are from different cryptographic suites. PURBs employ Padmé, a novel padding scheme that limits information leakage via ciphertexts of maximum length $M$ to a practical optimum of $O(\log \log M)$ bits, comparable to padding to a power of two, but with lower overhead of at most 12% and decreasing with larger payloads.

**Keywords:** metadata, leakage, padding, traffic analysis

DOI 10.2478/popets-2019-0056
Received 2019-02-28; revised 2019-06-15; accepted 2019-06-16.

***Corresponding Author: Kirill Nikitin:** EPFL, E-mail: kirill.nikitin@epfl.ch
***Corresponding Author: Ludovic Barman:** EPFL, E-mail: ludovic.barman@epfl.ch
**Wouter Lueks:** EPFL, E-mail: wouter.lueks@epfl.ch
**Matthew Underwood:** unaffiliated
**Jean-Pierre Hubaux:** EPFL, E-mail: jean-pierre.hubaux@epfl.ch
**Bryan Ford:** EPFL, E-mail: bryan.ford@epfl.ch

## 1 Introduction

Traditional encryption schemes and protocols aim to protect only their data payload, leaving related metadata exposed. Formats such as PGP [64] reveal in cleartext headers the public keys of the intended recipients, the algorithm used for encryption, and the actual length of the payload. Secure-communication protocols similarly leak information during key and algorithm agreement. The TLS handshake [45], for example, leaks in cleartext the protocol version, chosen cipher suite, and the public keys of the parties. This metadata exposure is traditionally assumed not to be security-sensitive, but important for the recipient's decryption efficiency.

Research has consistently shown, however, that attackers can exploit metadata to infer sensitive information about communication content. In particular, an attacker may be able to fingerprint users [40, 52] and the applications they use use [63]. Using traffic analysis [17], an attacker may be able to infer websites a user visited [17, 21, 39, 56, 57] or videos a user watched [43, 44, 50]. On VoIP, metadata can be used to infer the geo-location [35], the spoken language [61], or the voice activity of users [15]. Side-channel leaks from data compression [32] facilitate several attacks on SSL [5, 25, 48]. The lack of proper padding might enable an active attacker to learn the length of the user's password from TLS [53] or QUIC [1] traffic. In social networks, metadata can be used to draw conclusions about users' actions [26], whereas telephone metadata has been shown to be sufficient for user re-identification and for determining home locations [36]. Furthermore, by observing the format of packets, oppressive regimes can infer which technology is used and use this information for the purposes of incrimination or censorship. Most TCP packets that Tor sends, for example, are 586 bytes due to its standard cell size [27].

As a step towards countering these privacy threats, we propose that encrypted data formats should produce *Padded Uniform Random Blobs* or PURBs: ciphertexts designed to protect *all* encryption metadata. A PURB encrypts application content and metadata into a single blob that is indistinguishable from a random string,

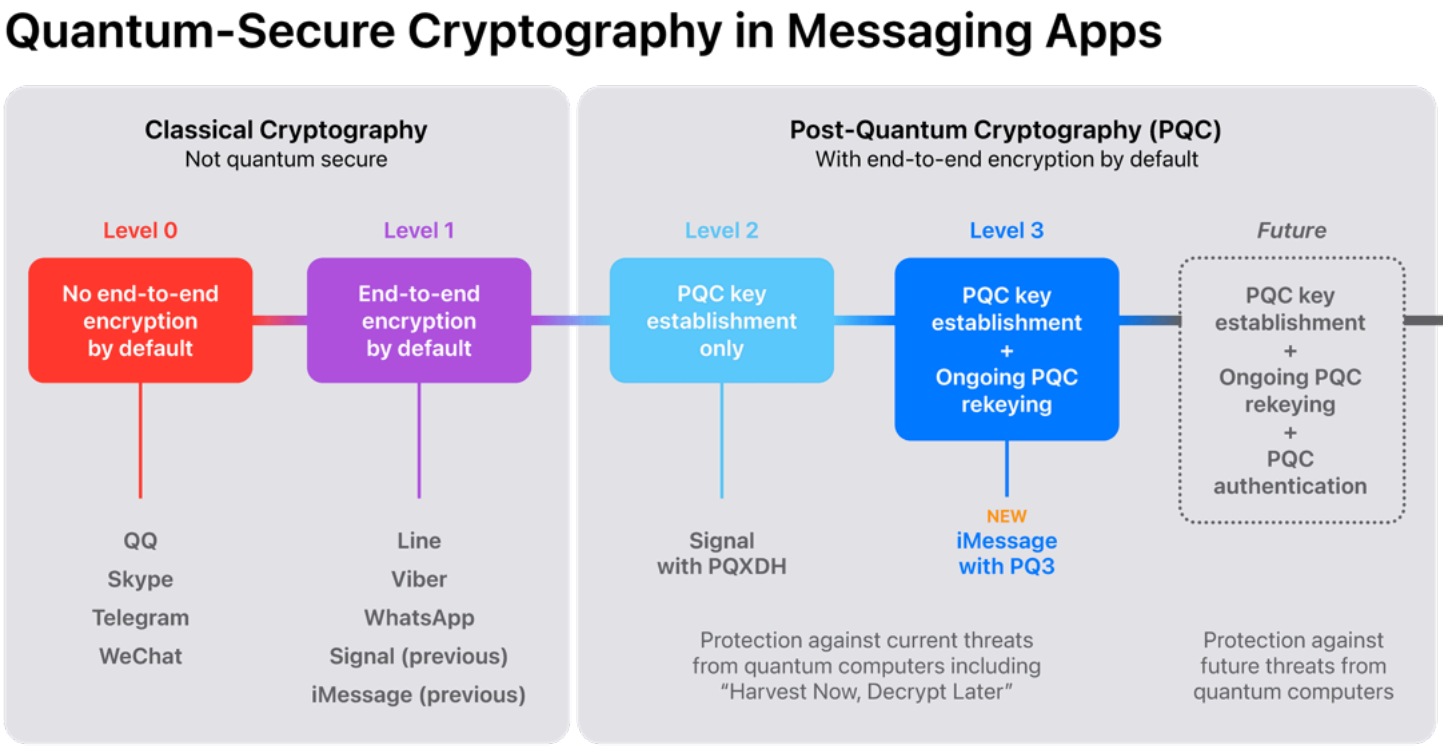
Blog

February 21, 2024

# iMessage with PQ3: The new state of the art in quantum-secure messaging at scale

Posted by Apple Security Engineering and Architecture (SEAR)

Today we are announcing the most significant cryptographic security upgrade in iMessage history with the introduction of PQ3, a groundbreaking post-quantum cryptographic protocol that advances the state of the art of end-to-end secure messaging. With compromise-resilient encryption and extensive defenses against even highly sophisticated quantum attacks, PQ3 is the first messaging protocol to reach what we call Level 3 security — providing protocol protections that surpass those in all other widely deployed messaging apps. To our knowledge, PQ3 has the strongest security properties of any at-scale messaging protocol in the world.




*Note: This comparison evaluates only the cryptographic aspect of messaging security, and therefore focuses on end-to-end encryption and quantum security. Such a comparison doesn't include automatic key verification, which we believe is a critical protection for modern messaging apps. As of the time of this writing, only iMessage and WhatsApp provide automatic key verification. The iMessage implementation, called Contact Key Verification, is the state of the art – it provides the broadest automatic protections and applies across all of a user's devices.*

When iMessage launched in 2011, it was the first widely available messaging app to provide end-to-end encryption by default, and we have significantly upgraded its cryptography over the years. We most recently strengthened the iMessage cryptographic protocol in 2019 by switching from RSA to Elliptic Curve cryptography (ECC), and by protecting encryption keys on device with the Secure Enclave, making them significantly harder to extract from a device even for the most sophisticated adversaries. That protocol update went even further with an additional layer of defense: a periodic rekey mechanism to provide cryptographic self-healing even in the extremely unlikely case that a key ever became compromised. Each of these advances were formally verified by symbolic evaluation, a best practice that provides strong assurances of the security of cryptographic protocols.

Historically, messaging platforms have used classical public key cryptography, such as RSA, Elliptic Curve signatures, and Diffie-Hellman key exchange, to establish secure end-to-end encrypted connections between devices. All these algorithms are based on difficult mathematical problems that have long been considered too computationally intensive for computers to solve, even when accounting for Moore's law. However, the rise of quantum computing threatens to change the equation. A sufficiently powerful quantum computer could solve these classical mathematical problems in fundamentally different ways, and therefore — in theory — do so fast enough to threaten the security of end-to-end encrypted communications.

Although quantum computers with this capability don't exist yet, extremely well-resourced attackers can already prepare for their possible arrival by taking advantage of the steep decrease in modern data storage costs. The premise is simple: such attackers can collect large amounts of today's encrypted data and file it all away for future reference. Even though they can't decrypt any of this data today, they can retain it until they acquire a quantum computer that can decrypt it in the future, an attack scenario known as *Harvest Now, Decrypt Later*.

To mitigate risks from future quantum computers, the cryptographic community has been working on post-quantum cryptography (PQC): new public key algorithms that provide the building blocks for quantum-secure protocols but don't require a quantum computer to run — that is, protocols that can run on the classical, non-quantum computers we're all using today, but that will remain secure from known threats posed by future quantum computers.

To reason through how various messaging applications mitigate attacks, it's helpful to place them along a spectrum of security properties. There's no standard comparison to employ for this purpose, so we lay out our own simple, coarse-grained progression of messaging security levels in the image at the top of this post: we start on the left with classical cryptography and progress towards quantum security, which addresses current and future threats from quantum computers. Most existing messaging apps fall either into Level 0 — no end-to-end encryption by default and no quantum security — or Level 1 — with end-to-end encryption by default, but with no quantum security. A few months ago, Signal added support for the PQXDH protocol, becoming the first large-scale messaging app to introduce post-quantum security in the initial key establishment. This is a welcome and critical step that, by our scale, elevated Signal from Level 1 to Level 2 security.

At Level 2, the application of post-quantum cryptography is limited to the initial key establishment, providing quantum security only if the conversation key material is never compromised. But today's sophisticated adversaries already have incentives to compromise encryption keys, because doing so gives them the ability to decrypt messages protected by those keys for as long as the keys don't change. To best protect end-to-end encrypted messaging, the post-quantum keys need to change on an ongoing basis to place an upper bound on how much of a conversation can be exposed by any single, point-in-time key compromise — both now and with future quantum computers. Therefore, we believe messaging protocols should go even further and attain Level 3 security, where post-quantum cryptography is used to secure both the initial key establishment and the ongoing message exchange, with the ability to rapidly and automatically restore the cryptographic security of a conversation even if a given key becomes compromised.

iMessage now meets this goal with a new cryptographic protocol that we call PQ3, offering the strongest protection against quantum attacks and becoming the only widely available messaging service to reach Level 3 security. Support for PQ3 will start to roll out with the public releases of iOS 17.4, iPadOS 17.4, macOS 14.4, and watchOS 10.4, and is already in the corresponding developer preview and beta releases. iMessage conversations between devices that support PQ3 are automatically ramping up to the post-quantum encryption protocol. As we gain operational experience with PQ3 at the massive global scale of iMessage, it will fully replace the existing protocol within all supported conversations this year.

## Designing PQ3

More than simply replacing an existing algorithm with a new one, we rebuilt the iMessage cryptographic protocol from the ground up to advance the state of the art in end-to-end encryption, and to deliver on the following requirements:

- Introduce post-quantum cryptography from the start of a conversation, so that all communication is protected from current and future adversaries.
- Mitigate the impact of key compromises by limiting how many past and future messages can be decrypted with a single compromised key.
- Use a hybrid design to combine new post-quantum algorithms with current Elliptic Curve algorithms, ensuring that PQ3 can can never be less safe than the existing classical protocol.
- Amortize message size to avoid excessive additional overhead from the added security.
- Use formal verification methods to provide strong security assurances for the new protocol.

PQ3 introduces a new post-quantum encryption key in the set of public keys each device generates locally and transmits to Apple servers as part of iMessage registration. For this application, we chose to use Kyber post-quantum public keys, an algorithm that received close scrutiny from the global cryptography community, and was selected by NIST as the Module Lattice-based Key Encapsulation Mechanism standard, or ML-KEM. This enables sender devices to obtain a receiver's public keys and generate post-quantum encryption keys for the very first message, even if the receiver is offline. We refer to this as initial key establishment.

We then include — within conversations — a periodic post-quantum rekeying mechanism that has the ability to self-heal from key compromise and protect future messages. In PQ3, the new keys sent along with the conversation are used to create fresh message encryption keys that can't be computed from past ones, thereby bringing the conversation back to a secure state even if previous keys were extracted or compromised by an adversary. PQ3 is the first large scale cryptographic messaging protocol to introduce this novel post-quantum rekeying property.

PQ3 employs a hybrid design that combines Elliptic Curve cryptography with post-quantum encryption both during the initial key establishment and during rekeying. Thus, the new cryptography is purely additive, and defeating PQ3 security requires defeating both the existing, classical ECC cryptography and the new post-quantum primitives. It also means the protocol benefits from all the experience we accumulated from deploying the ECC protocol and its implementations.

Rekeying in PQ3 involves transmitting fresh public key material in-band with the encrypted messages that devices are exchanging. A new public key based on Elliptic Curve Diffie-Hellman (ECDH) is transmitted inline with every response. The post-quantum key used by PQ3 has a significantly larger wire size than the existing protocol, so to meet our message size requirement we designed the quantum-secure rekeying to happen periodically rather than with every message. To determine whether a new post-quantum key is transmitted, PQ3 uses a rekeying condition that aims to balance the average size of messages on the wire, preserve the user experience in limited connectivity scenarios, and keep the global volume of messages within the capacity of our server infrastructure. Should the need arise, future software updates can increase the rekeying frequency in a way that's backward-compatible with all devices that support PQ3.

With PQ3, iMessage continues to rely on classical cryptographic algorithms to authenticate the sender and verify the Contact Key Verification account key, because these mechanisms can't be attacked retroactively with future quantum computers. To attempt to insert themselves in the middle of an iMessage conversation, an adversary would require a quantum computer capable of breaking one of the authentication keys before or at the time the communication takes place. In other words, these attacks cannot be performed in a *Harvest Now, Decrypt Later* scenario — they require the existence of a quantum computer capable of performing the attacks contemporaneously with the communication being attacked. We believe any such capability is still many years away, but as the threat of quantum computers evolves, we will continue to assess the need for post-quantum authentication to thwart such attacks.

## A formally proven protocol

Our final requirement for iMessage PQ3 is formal verification — a mathematical proof of the intended security properties of the protocol. PQ3 received extensive review from Apple's own multi-disciplinary teams in Security Engineering and Architecture (SEAR) as well as from some of the world's foremost experts in cryptography. This includes a team led by Professor David Basin, head of the Information Security Group at ETH Zürich and one of the inventors of Tamarin — a leading security protocol verification tool that was also used to evaluate PQ3 — as well as Professor Douglas Stebila from the University of Waterloo, who has performed extensive research on post-quantum security for internet protocols. Each took a different but complementary approach, using different mathematical models to demonstrate that as long as the underlying cryptographic algorithms remain

secure, so does PQ3. Finally, a leading third-party security consultancy supplemented our internal implementation review with an independent assessment of the PQ3 source code, which found no security issues.

In the first mathematical analysis, Security analysis of the iMessage PQ3 protocol, Professor Douglas Stebila focused on so-called game-based proofs. This technique, also known as reduction, defines a series of "games" or logical statements to show that the protocol is at least as strong as the algorithms that underpin it. Stebila's analysis shows that PQ3 provides confidentiality even in the presence of some key compromises against both classical and quantum adversaries, in both the initial key establishment and the ongoing rekeying phase of the protocol. The analysis decomposes the many layers of key derivations down to the message keys and proves that, for an attacker, they are indistinguishable from random noise. Through an extensive demonstration that considers different attack paths for classical and quantum attackers in the proofs, Stebila shows that the keys used for PQ3 are secure as long as either the Elliptic Curve Diffie-Hellman problem remains hard or the Kyber post-quantum KEM remains secure.

> *The iMessage PQ3 protocol is a well-designed cryptographic protocol for secure messaging that uses state-of-the-art techniques for end-to-end encrypted communication. In my analysis using the reductionist security methodology, I confirmed that the PQ3 protocol provides post-quantum confidentiality, which can give users confidence in the privacy of their communication even in the face of potential improvements in quantum computing technology. —Professor Douglas Stebila*

In the second evaluation, A Formal Analysis of the iMessage PQ3 Messaging Protocol, Prof. David Basin, Felix Linker, and Dr. Ralf Sasse at ETH Zürich use a method called symbolic evaluation. As highlighted in the paper's abstract, this analysis includes a detailed formal model of the iMessage PQ3 protocol, a precise specification of its fine-grained security properties, and machine-checked proofs using the state-of-the-art symbolic Tamarin prover. The evaluation yielded a fine-grained analysis of the secrecy properties of PQ3, proving that "in the absence of the sender or recipient being compromised, all keys and messages transmitted are secret" and that "compromises can be tolerated in a well-defined sense where the effect of the compromise on the secrecy of data is limited in time and effect," which confirms that PQ3 meets our goals.

> *We provide a mathematical model of PQ3 as well as prove its secrecy and authenticity properties using a verification tool for machine-checked security proofs. We prove the properties even when the protocol operates in the presence of very strong adversaries who can corrupt parties or possess quantum computers and therefore defeat classical cryptography. PQ3 goes beyond Signal with regards to post-quantum defenses. In PQ3, a post-quantum secure algorithm is part of the ratcheting and used repeatedly, rather than only once in the initialization as in Signal. Our verification provides a very high degree of assurance that the protocol as designed functions securely, even in the post-quantum world. —Professor David Basin*

## Diving into the details

Because we know PQ3 will be of intense interest to security researchers and engineers as well as the cryptographic community, this blog post is really two posts in one. Up to now, we laid out our design goals, outlined how PQ3 meets them, and explained how we verified our confidence in the protocol with independent assessments. If you'd like to understand more detail about the cryptographic underpinnings, the remainder of the post is a deeper dive into how we constructed the PQ3 protocol.

## Post-quantum key establishment

iMessage allows a user to register multiple devices on the same account. Each device generates its own set of encryption keys, and the private keys are never exported to any external system. The associated public keys are registered with Apple's Identity Directory Service (IDS) to enable users to message each other using a simple identifier: email address or phone number. When a user sends a message from one of their devices, all of their other devices and all of the recipient's devices receive the message. The messages are exchanged through pair-wise sessions established between the sending device and each receiving device. The same message is encrypted successively to each receiving device, with keys uniquely derived for each session. For the rest of this description, we will focus on a single device-to-device session.

Because the receiving device might not be online when the conversation is established, the first message in a session is encrypted using the public encryption keys registered with the IDS server.

Each device with PQ3 registers two public encryption keys and replaces them regularly with fresh ones:

1. A post-quantum Kyber-1024 key encapsulation public key
2. A classical P-256 Elliptic Curve key agreement public key

These encryption keys are signed with ECDSA using a P-256 authentication key generated by the device's Secure Enclave, along with a timestamp used to limit their validity. The device authentication public key is itself signed by the Contact Key Verification account key, along with some attributes such as the supported cryptographic protocol version. This process allows the sender to verify that the recipient device's public encryption keys were uploaded by the intended recipient, and it guards against downgrade attacks.

When Alice's device instantiates a new session with Bob's device, her device queries the IDS server for the key bundle associated with Bob's device. The subset of the key bundle that contains the device's authentication key and versioning information is validated using Contact Key Verification. The device then validates the signature covering the encryption keys and timestamps, which attests that the keys are valid and have not expired.

Alice's device can then use the two public encryption keys to share two symmetric keys with Bob. The first symmetric key is computed through an ECDH key exchange that combines an ephemeral encryption key from Alice with Bob's registered P-256 public key. The second symmetric key is obtained from a Kyber key encapsulation with Bob's post-quantum public key.

To combine these two symmetric keys, we first extract their entropy by invoking HKDF-SHA384-Extract twice — once for each of the keys. The resulting 48-byte secret is further combined with a domain separation string and session information — which includes the user's identifiers, the public keys used in the key exchange, and the encapsulated secret — by invoking HKDF-SHA384-Extract again to derive the session's initial keying state. This combination ensures that the initial session state cannot be derived without knowing both of the shared secrets, meaning an attacker would need to break both algorithms to recover the resulting secret, thus satisfying our hybrid security requirement.

## Post-quantum rekeying

Ongoing rekeying of the cryptographic session is designed such that keys used to encrypt past and future messages cannot be recomputed even by a powerful hypothetical attacker who is able to extract the cryptographic state of the device at a given point in time. The protocol generates a new unique key for each message, which periodically includes new entropy that is not deterministically derived from the current state of the conversation, effectively providing self-healing properties to the protocol. Our rekeying approach is modeled after ratcheting, a technique that consists of deriving a new session key from other keys and ensuring the cryptographic state always moves forward in one direction. PQ3 combines three ratchets to achieve post-quantum encryption.

The first ratchet, called the symmetric ratchet, protects older messages in a conversation to achieve forward secrecy. For every message, we derive a per-message encryption key from the current session key. The current session key itself is then further derived into a new session key, ratcheting the state forward. Each message key is deleted as soon as a corresponding message is decrypted, which prevents older harvested ciphertexts from being decrypted by an adversary who is able to compromise the device at a later time, and provides protection against replayed messages. This process uses 256-bit keys and intermediate values, and HKDF-SHA384 as a derivation function, which provides protection against both classical and quantum computers.

The second ratchet, called the ECDH ratchet, protects future messages by updating the session with fresh entropy from an Elliptic Curve key agreement, ensuring that an adversary loses the ability to decrypt new messages even if they had compromised past session keys — a property called post-compromise security. The ECDH-based ratchet has a symmetrical flow: the private key of the outgoing ratchet public key from the sender is used with the last public key received from the recipient to establish a new shared secret between sender and receiver, which is then mixed into the session's key material. The new PQ3 protocol for iMessage uses NIST P-256 Elliptic Curve keys to perform this ratchet, which imposes only a small 32-byte overhead on each message.

Because the second ratchet uses classical cryptography, PQ3 also adds a conditionally executed Kyber KEM-based ratchet. This third ratchet complements the ECDH-based ratchet to provide post-compromise security against *Harvest Now, Decrypt*

*Later* quantum attacks as well.

The use of a post-quantum ratchet can cause significant network overhead compared to an ECDH-based ratchet at the same security level. The post-quantum KEM requires sending both a public key and an encapsulated secret instead of a single outgoing public key. In addition, the underlying mathematical structure for quantum security requires significantly larger parameter sizes for public keys and encapsulated keys compared to Elliptic Curves.

To limit the size overhead incurred by frequent rekeying while preserving a high level of security, the post-quantum KEM is instantiated with Kyber-768. Unlike the IDS-registered public keys used for the initial key establishment, ratcheting public keys are used only once to encapsulate a shared secret to the receiver, significantly limiting the impact of the compromise of a single key. However, while a 32-byte ECDH-based ratchet overhead is acceptable on every message, the post-quantum KEM ratchet increases the message size by more than 2 kilobytes. To avoid visible delays in message delivery when device connectivity is limited, this ratchet needs to be amortized over multiple messages.

We therefore implemented an adaptive post-quantum rekeying criterion that takes into account the number of outgoing messages, the time elapsed since last rekeying, and current connectivity conditions. At launch, this means the post-quantum ratchet is performed approximately every 50 messages, but the criterion is bounded such that rekeying is always guaranteed to occur at least once every 7 days. And as we mentioned earlier, as the threat of quantum computers and infrastructure capacity evolves over time, future software updates can increase the rekeying frequency while preserving full backward compatibility.

Completing the public key ratchets, whether based on ECDH or Kyber, requires sending and receiving a message. Although users may not immediately reply to a message, iMessage includes encrypted delivery receipts that allow devices to rapidly complete the ratchet even without a reply from the recipient, as long as the device is online. This technique avoids delays in the rekeying process and helps support strong post-compromise recovery.

Similar to the initial session key establishment, the secrets established through the three ratchets are all combined with an evolving session key using HKDF-SHA384 through sequential calls to the Extract function. At the end of this process, we obtain a final message key, which can now be used to encrypt the payload.

## Padding and encryption

To avoid leaking information about the message size, PQ3 adds padding to the message before encryption. This padding is implemented with the Padmé heuristic, which specifically limits the information leakage of ciphertexts with maximum length M to a practical optimum of O(log log M) bits. This is comparable to padding to a power of two but results in a lower overhead of at most 12 percent and even lower for larger payloads. This approach strikes an excellent balance between privacy and efficiency, and preserves the user experience in limited device connectivity scenarios.

The padded payload is encrypted with AES-CTR using a 256-bit encryption key and initialization vector, both derived from the message key. While public key algorithms require fundamental changes to achieve quantum security, symmetric cryptography algorithms like the AES block cipher only require doubling the key size to maintain their level of security against quantum computers.

## Authentication

Each message is individually signed with ECDSA using the elliptic curve P-256 device authentication key protected by the Secure Enclave. The receiving device verifies the mapping between the sender's identifier (email address or phone number) and the public key used for signature verification. If both users have enabled Contact Key Verification and verified each other's account key, the device verifies that the device authentication keys are present in the Key Transparency log and that the corresponding account key matches the account key stored in the user's iCloud Keychain.

The device's authentication key is generated by the Secure Enclave and never exposed to the rest of the device, which helps prevent extraction of the private key even if the Application Processor is completely compromised. If an attacker were to compromise the Application Processor, they might be able to use the Secure Enclave to sign arbitrary messages. But after the device recovers from the compromise through a reboot or a software update, they would no longer be able to impersonate the user. This approach offers stronger guarantees than other messaging protocols where the authentication key is sometimes shared between devices or where the authentication takes place only at the beginning of the session.

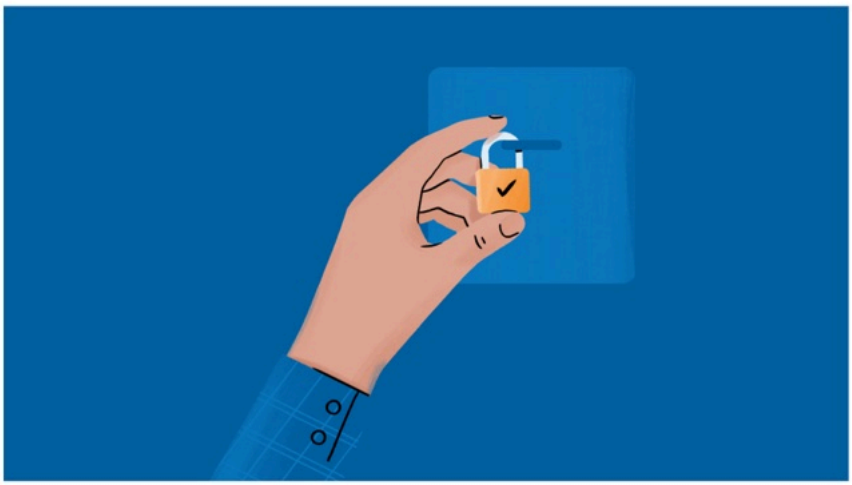
The message signature covers a wide range of fields, including the unique identifiers of the users and their push notification tokens, the encrypted payload, authenticated data, a ratchet-derived message key indicator that binds the signature to a unique location in the ratchet, and any public key information used in the protocol. The inclusion of these fields in the signature guarantees that the message can only be used in the context intended by the sender, and all the fields are exhaustively documented in the research papers from Stebila, Basin, and collaborators.

## Conclusion

End-to-end encrypted messaging has seen a tremendous amount of innovation in recent years, including significant advances in post-quantum cryptography from Signal's PQXDH protocol and in key transparency from WhatsApp's Auditable Key Directory. Building on its pioneering legacy as the first widely available messaging app to provide end-to-end encryption by default, iMessage has continued to deliver advanced protections that surpass existing systems. iMessage Contact Key Verification is the most sophisticated key transparency system for messaging deployed at scale, and is the current global state of the art for automatic key verification. And the new PQ3 cryptographic protocol for iMessage combines post-quantum initial key establishment with three ongoing ratchets for self-healing against key compromise, defining the global state of the art for protecting messages against *Harvest Now, Decrypt Later* attacks and future quantum computers.

POSTED ON DECEMBER 6, 2023 TO SECURITY

# Building end-to-end security for Messenger



By Jon Millican, Reed Riley

- We are beginning to upgrade people's personal conversations on Messenger to use end-to-end encryption (E2EE) by default.
- Meta is publishing two technical white papers on end-to-end encryption:
  - Our Messenger end-to-end encryption whitepaper describes the core cryptographic protocol for transmitting messages between clients.
  - The Labyrinth encrypted storage protocol whitepaper explains our protocol for end-to-end encrypting stored messaging history between devices on a user's account.

Today, we're announcing that we've begun to upgrade people's personal conversations on Messenger to use E2EE by default. Our aim is to ensure that everyone's personal messages on Messenger can only be accessed by the sender and the intended recipients, and that everyone can be sure the messages they receive are from an authentic sender.

This is the most significant milestone yet for this project, which began in earnest after Mark Zuckerberg outlined his vision for it in 2019. Bringing E2EE to Messenger has been a complex process, with every feature and product goal revealing further challenges that required careful consideration.

Enabling E2EE on Messenger meant fundamentally rebuilding many aspects of the application protocols to improve privacy, security, and safety while simultaneously maintaining the features that have made Messenger so popular.

## Why we're bringing E2EE to Messenger

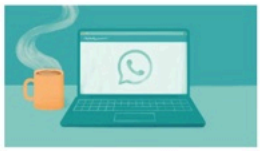
Messenger first built end-to-end encrypted chats in 2016 as a feature called Secret Conversations. Since then, we've learned a great deal in regards to rolling out E2EE for a wider user base. For example, we recently published an updated white paper, "Meta's Approach to Safer Private Messaging on Messenger and Instagram Direct Messaging," that sets out the industry-leading safety systems and tools available on Messenger.

End-to-end encryption isn't about the technology at its core. It's about protecting people's communications, so they can feel safe expressing themselves with their friends and loved ones. To achieve this, we typically focus on two aims:

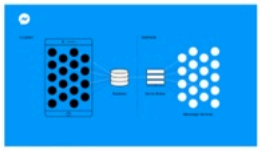
1. Only the sender and recipients of an E2EE message can see its contents.
2. Nobody (not even Meta) should be able to forge messages to appear to have been

Related Posts

Jul 28, 2022
Five security principles for billions of messages across Meta's apps



Mar 10, 2022
Code Verify: An open source browser extension for verifying code authenticity on the web



Mar 02, 2020
Project LightSpeed: Rewriting the Messenger codebase for a faster, smaller, and simpler messaging app

Related Positions

Security Analyst - Bug Bounty
TEL AVIV, ISRAEL

Security Analyst - Bug Bounty
LONDON, UK

GRC Integrity Program Manager
BELLEVUE, US

GRC Integrity Program Manager
AUSTIN, US

GRC Integrity Program Manager
MENLO PARK, US

See All Jobs

sent from someone they weren't.

In other words, the aim is that only you and the people you're corresponding with can read your messages – not even the app's provider (in this case, Meta) could interfere with their contents – and you can be confident in who sent the messages.

## Understanding these goals

These two aims are broad. However, when we reflect on our approach to addressing them, they end up breaking down into eight overlapping concepts that we believe achieve a cohesive approach to meaningful E2EE:

### 1. Confidentiality in transit

Message contents are authentically and securely transmitted between your devices and those of the people you're talking to. This is, perhaps, the primary goal of E2EE, and is where much E2EE research and design work is targeted, such as the Signal protocol we use in our products (such as WhatsApp, Messenger, and Instagram Direct), or the IETF's Messaging Layer Security protocol, which we helped to design and was recently standardized.

### 2. Confidentiality in storage

Typically, E2EE messaging services rely on local storage and encryption keys to secure encrypted messages. Messenger, however, has a long history of storing people's messages for them so that they can access them whenever they need without having to store them locally. That's why we've designed a server-based solution where encrypted messages can be stored on Meta's servers while only being readable using encryption keys under the user's control.

### 3. Control over endpoints

For something to be "end-to-end encrypted," it is necessary to have a notion of what the "ends" are. For an E2EE messaging app this means that users should have the ability to verify and manage their set of endpoint devices that are receiving their messages, as well as visibility into when this set of devices changes.

### 4. Private feature designs

Product features in an E2EE setting typically need to be designed to function in a device-to-device manner, without ever relying on a third party having access to message content. This was a significant effort for Messenger, as much of its functionality has historically relied on server-side processing, with certain features difficult or impossible to exactly match with message content being limited to the devices.

### 5. Logging limitations

Maintaining the confidentiality of message content extends to avoiding accidentally leaking it back to us in telemetry. In a product of Messenger's scale, complexity, and iteration speed, this creates particular challenges as telemetry is vital in ensuring that the product is working well for people, and in debugging when things go wrong.

### 6. Application security

It's a common saying that, "You can't have privacy without security," and this is absolutely true in the end-to-end encrypted domain. Security is important for any consumer product, but E2EE exacerbates the challenges in two important ways: it reduces the provider's ability to protect the user from attacks, and, in fact, it expands the threat model to include the service provider itself. Our security team is keenly aware of these challenges and works closely with product teams to secure design and implementation of E2EE functionality. For example, we've been working to improve the memory safety of our apps; and our E2EE surfaces are covered by our bug bounty program.

### 7. Being deliberate about what's being protected

E2EE protects message content. However, this is a complex term to define, and, while certain things are relatively clear – such as the strings contained in a text message, or a photograph sent from your camera roll – in a sufficiently complex messaging application, it turns out there's a surprisingly large grey area. Our focus is on determining the appropriate boundaries, ensuring that we remain true to our commitments, setting the correct user expectations, and avoiding creating meaningful privacy risks, while still ensuring that the product retains its usefulness to our users.

### 8. Third-party scrutiny

E2EE implies confidentiality even if the provider wants to access the contents of a communication. We aim for this to be verifiable externally, and, to this end, have published

communication. We aim for this to be verifiable externally, and, to this end, have published two white papers to provide transparency into our operations. We describe the properties of some features in our Help Center, and we encourage submissions to our bug bounty program. Throughout the project, we have consulted with a diverse range of external parties to ensure that we're making the right set of tradeoffs. To improve people's ability to scrutinize us, we also support the Code Verify browser extension for our web-based end-to-end encrypted messaging, to give security researchers greater confidence that the code version that they are assessing is being used globally.

## High-level approach

With all of this in mind, our high-level approach was to build off of Meta's prior learnings in E2EE, from both WhatsApp and Messenger's Secret Conversations, and then to iterate on our most challenging problems.

Working from the baseline of these two approaches, we then had to address a series of significant technical challenges, including:

1. **Multi-device capability**: Messenger's model of multi-device reflects the Facebook network, which allows people to authenticate on new devices with a username and password, in order to send and receive messages. Since WhatsApp's multi-device capability relies on a single primary device that must cryptographically authenticate companion devices, we adopted the Secret Conversations model of multi-device, while ensuring that it functions well for all of our users.
2. **Feature support**: Messenger has a number of messaging features that either don't exist in WhatsApp, or function differently. Some of these just had to be rebuilt from scratch, while others required deploying new applied privacy technology. For example, we used OHAI and Anonymous Credentials to support searches of Facebook's first-party sticker library, without revealing to us who is sending them.
3. **Message history**: Messenger has always allowed clients to operate off of a small stored local cache, relying on a server-side database for their message history. Neither WhatsApp nor Secret Conversations operated in this manner, and we didn't want all users to have to rely on a device-side storage system. Instead, we designed an entirely new encrypted storage system called Labyrinth, with ciphertexts uploaded to our servers and loaded on-demand by clients, while operating in a multi-device manner and supporting key rotation when clients are removed.
4. **Web support**: We needed to support E2EE within our existing web surfaces, including the main Facebook site. The Web platform carries significantly different constraints from native apps, meaning that we needed to take custom approaches to many different aspects of the product. Further, Web users often add and remove devices in very different patterns from mobile-only users, increasing the complexity of our multi-device challenge.

## Learn more about E2EE on Messenger

Today, we are sharing two white papers:

- Our Messenger end-to-end encryption whitepaper, which describes the core cryptographic protocol for transmitting messages between clients.
- The Labyrinth encrypted storage protocol whitepaper, describing our protocol for end-to-end encrypting stored messages history between devices on a user's account.

These add to a number of publications that we have shared which cover Messenger's E2EE, including:

- Our recently updated Safety whitepaper
- The independent E2EE Human Rights Impact Assessment
- Our Security Principles whitepaper
- The Code Verify browser extension

## Beyond E2EE for Messenger

The journey to bring E2EE to Messenger has been a long one, but it's not yet finished. While we are globally launching default E2EE for personal one-to-one messages on Messenger, we are still in the testing phase for group messaging and some other products, like Instagram Direct Messages. On Instagram, we are currently testing "disappearing messages" for one-to-one Instagram Direct conversations in select countries. Disappearing messages are ephemeral and, as with those in Messenger, expire 24 hours after being sent. They are built leveraging our E2EE infrastructure and provide an increased level of privacy. We plan to expand this work as well as conduct additional testing around E2EE on Instagram over the next year.

# The Labyrinth Encrypted Message Storage Protocol

December 6, 2023
Version 1

Meta

# Abstract

End-to-end encrypted messaging creates significant new challenges regarding data storage and accessing message history between devices. Labyrinth is a novel storage system, currently being developed and rolled out in Messenger, which aims to serve this purpose while maintaining a high bar for message content privacy. It is designed to protect messages against non-members (devices and entities which are not enrolled in a user's Labyrinth mailbox) , including preventing new messages from being decryptable on revoked devices which may have previously had access to earlier messages, while achieving low operational overheads and high reliability.

This document describes the Labyrinth protocol as designed, and as it is intended to operate. Details of Meta's implementation may differ in places and will likely evolve over time. This white paper should not be read as making any assurances or commitments to users on Meta's products or services.

## 1. AES-GCM-Extended

AES-GCM-Extended is the approach that Labyrinth follows to avoid nonce reuse concerns. It takes inspiration from XChaCha20-Poly1305 in its approach, but uses AES-GCM-256 as its underlying cipher, as this is already present and used elsewhere in Messenger's codebase.

AES-GCM-Extended takes a 32-byte key and a 28-byte nonce. From these it generates a subkey and subnonce, as follows:

```
subkey := hchacha20(nonce[0:16], key)
subnonce := nonce[16:28]
```

These are then used directly within AES-GCM-256 to encrypt/decrypt the data. The 28 byte nonce is prepended to the ciphertext.

## 2. Padding

When Labyrinth encrypts messages using AES-GCM-Extended, padding is also applied to protect ciphertext lengths. Padding involves a tradeoff between privacy and storage overhead: longer padding hides message lengths better, but uses more storage space. We use the PADMÉ scheme[3], which provides a good balance.

For messages with fewer than 10 characters, the plaintext is simply padded to 10 characters. Otherwise, the PADMÉ scheme is applied. This scheme bounds leakage to no more than `O(log log N)` bits for messages of length `N`, and uses at most around 12% overhead.

Each message plaintext is prefixed with a 4 byte unsigned big-endian integer indicating the length of the unpadded plaintext.

[3] https://nikirill.com/files/purbs.pdf

MOBILE > IOS AND IOS APPS

# Why iMessage is such a big deal: A guide for the rest of the world

*iMessage isn't just about texting, it's a crafty play to win over the next generation of customers.*

By Robert Triggs • October 17, 2022


The "green bubble" phenomenon is back in the headlines, following accusations that Apple leverages its iMessage platform to exert "peer pressure and bullying as a way to sell products." A bold but increasingly well-substantiated claim, at least as far as the US is concerned.

iMessage launched in 2011 and you'll find instances of anti-green bubble tweets and memes dating back just about as long as the app has existed. It's hardly a new phenomenon, popping up in various pop culture references over the years, from articles on The Bachelorette contestants to the pitfalls of dating Android users.

Like far too much modern news, the narrative is dictated by a predominantly US-based trend. The rest of the world seems far less obsessed with the smartphone you own or your messaging platform of choice. Many readers might wonder just what the iMessage fuss is all about and why they keep hearing about a platform they never use.



## Blue and green bubbles explained

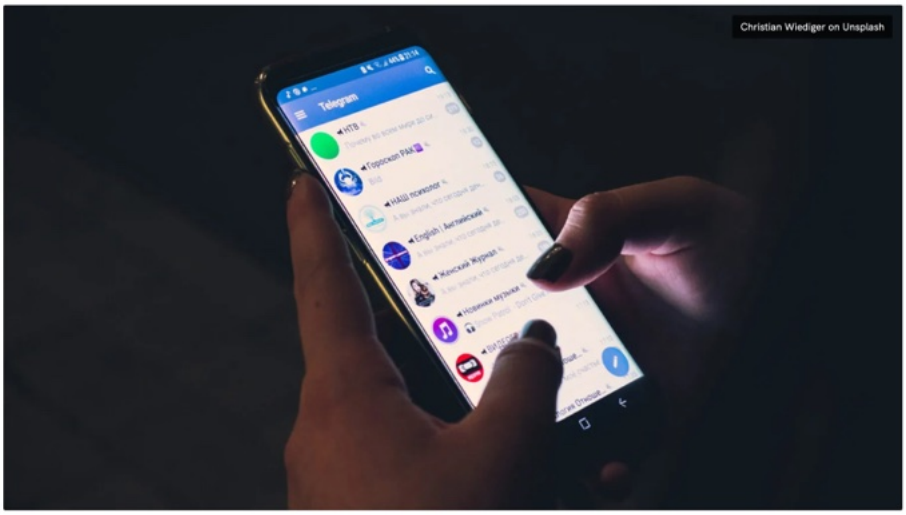

If you're just catching up on the saga, Apple's default messaging app displays blue bubbles when sending texts, photos, and videos to other iMessage users. These messages use Wi-Fi or mobile data but are otherwise free to send and receive.

The app displays green bubbles when communicating with non-iMessage users, such as Android phones, falling back to SMS/MMS for text, pictures, etc. While SMS or standard text messages are regularly unlimited on US and European phone plans, it's not a given around the entire world. So some iPhone customers may have to pay to message their Android friends. Depending on carrier limits, media might also be compressed when sent as MMS.

**More reading:** Don't forget — A green bubble on an iPhone is a person

iMessage to iMessage communication has other advantages too. Messages are encrypted and the app also displays read and typing notifications. In other words, blue bubble iMessage users benefit from features you might recognize from WhatsApp and other services, while green bubbles do not. While innocuous sounding on its own, this lack of feature parity has led some iPhone users to stigmatize their green bubble contacts.

## Where does iMessage fit in the big picture?




To put the discussion in some perspective, iMessage is far from the most widely used message app on a global scale. That title belongs to Whatsapp, with some 2 billion monthly active global users in February 2022, according to Statista. Followed by WeChat (1.2 billion), Facebook Messenger (988 million), then QQ (574 million), Snapchat (557 million), and Telegram (550 million). Unfortunately, no comparative data for iMessage exists. Some estimates suggest close to 1.3 billion users, but as iMessage is the iPhone's default SMS app, any user that receives a text message or just plain old spam could be counted among those numbers.

Regional trends from May 2022 confirm a diverse range of messaging apps in use around the world. WhatsApp claims the most use in 60 countries, spanning Europe, India, and South America. WeChat is the platform of choice in China, while Viber is particularly popular in Bulgaria, Greece, and Ukraine. Telegram is widely used in Armenia, Jordan, and Cambodia.

***Facebook messenger may be the most popular US platform today but Gen Z is gravitating towards iPhone-exclusivity.***

Even in the US, home of the iPhone, Facebook Messenger is the most popular messaging app. According to a separate survey from June 2020, 32% of US adults used Facebook Messenger, 20% used Instagram, 17% iMessage, and 12% Whatsapp. Popular global apps such as WeChat, Viber, and Telegram barely registered 2% each, painting quite a different picture of messaging habits compared to the rest of the world. But even in the US, iMessage isn't the most popular app across the general population. At least not yet.

The data reveals that platform-agnostic messaging apps are favored when looking at both US-centric and global pictures. So where does this obsession with iMessage originate?

## iMessage — a US teenage phenomenon


The key to understanding the green bubble phenomenon is found in a survey by Consumer Intelligence Research Partners. The research highlights huge growth in recent US iPhone sales in the 18-24 age bracket. Gen Z iPhone adoption has jumped from 47% in 2018 to 74% in 2021 — meanwhile, ownership rose slightly from 34% to 40% in the same period for those over 24. Internal Apple research claims that iPhone users predominantly use iMessage (85% of users) and so iMessage's US user base continues to grow. This is especially so in younger age groups — and with it, the pressure to keep using the same platform as their peers.

With such rapid growth driven, in part, by the social status associated with iMessage use, Apple is vindicated in its decision to keep its messaging service exclusive. Apple's senior VP of software and services, Eddy Cue, wanted to bring iMessage to Android in 2013 but was vetoed by other executives. Apple didn't want to give away one of its unique selling points.

***Leaving Apple free to capture an entire generation of the US market is a huge risk for its rivals.***

The explosion of a young US user base is likely to convert into brand loyalty that could last a lifetime. Even though iPhones and iMessage aren't the biggest players on a global scale, this should concern rival companies like Google, Samsung, and the tech industry at large. For starters, they are at risk of losing a generation of lucrative US business. And not just in the smartphone space — Apple brand loyalty extends to the PC, audio/music, TV, and smart home markets now too. These product segments could soon fall victim to the allure of status over classic technological competence too.

Furthermore, the importance and influence of brand perception on the global picture cannot be overstated. Brands and trends that flourish in the US have a habit of trickling their way into Europe and regions beyond. Currently, Android enjoys a 71% global market share, hitting highs of 88% in South Africa, but reaching as low as just 40% in the US and falling. It's not just messaging apps — there's a growing gap between the US and the rest of the world when it comes to mobile and desktop operating systems, tablets, and smart home use too. US examples often skew towards the Apple camp.

Leaving Apple unchecked to capture an entire generation of the US market is a huge risk for companies, even those currently enjoying success in other regions.

## Solutions to end green bubble bullying


Circling back to the nature of iMessage, one of the more interesting aspects of the green bubble phenomenon

is that it doesn't really matter that iMessage features can be found elsewhere. Rather, it's the social perceptions from purposely curated technological exclusivity and the resulting perceived difference between those blue and green bubbles that is driving the issue. Encouraging Google to set up a rival Android application wouldn't solve the problem, even if the company didn't already have a terrible track record in this space over the past decade. In fact, you'll find the same and often more advanced features available on third-party internet messaging platforms already in use around the world.

Google is instead advocating for Apple to support RCS messaging as a replacement for basic SMS features when communicating with Android users. RCS would help produce parity between blue and green bubbles, as it supports typing indicators, read receipts, and many other features currently lacking from the green bubble hoi polloi. However, RCS isn't a complete global solution, as it depends on carrier and handset support. Alternatively, persuading Apple to bring iMessage to Android would work. But this seems unlikely given the company's historic comments and what it stands to gain from iMessage exclusivity.

**See also:** How to enable RCS messaging on your phone

Google claims that Apple is holding back innovation by failing to support the latest messaging features. That's a fair criticism and similar complaints could be made about Apple's stubborn support for the Lightning connector. However, unlike the latter, it's doubtful we'll see Apple come under legal scrutiny for anti-competitive behavior regarding iMessage. Instead, for now, the only option appears to be to ask Apple to play nicely.

**Next:** iOS 16 will let you unsend iMessages: here's how it works



## You might like


- **Dear iPhone users: Please don't forget that a green bubble is a person.**
- **I tried out RCS messages between iPhone and Android: Here's how it works**
- **iPhone Mirroring on macOS hands-on: Windows Phone Link could never...**


**FEATURES**

Apple, Google, Messaging Apps

# Exhibit 13

The first pages of the peer-reviewed publication authored by Dr. Nikitin on ensuring data integrity in private information retrieval:

- *Colombo S., Nikitin K., Corrigan-Gibbs H., Wu D. J., and Ford B. Authenticated Private Information Retrieval. In USENIX Security Symposium 2023.*


# Authenticated private information retrieval

Simone Colombo, *EPFL;* Kirill Nikitin, *Cornell Tech;* Henry Corrigan-Gibbs, *MIT;*
David J. Wu, *UT Austin;* Bryan Ford, *EPFL*

https://www.usenix.org/conference/usenixsecurity23/presentation/colombo

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the
32nd USENIX Security Symposium
is sponsored by USENIX.

# Authenticated private information retrieval

Simone Colombo *EPFL*
Kirill Nikitin *Cornell Tech*
Henry Corrigan-Gibbs *MIT*
David J. Wu *UT Austin*
Bryan Ford *EPFL*

**Abstract.** This paper introduces protocols for *authenticated* private information retrieval. These schemes enable a client to fetch a record from a remote database server such that (a) the server does not learn which record the client reads, and (b) the client either obtains the "authentic" record or detects server misbehavior and safely aborts. Both properties are crucial for many applications. Standard private-information-retrieval schemes either do not ensure this form of output authenticity, or they require multiple database replicas with an honest majority. In contrast, we offer multi-server schemes that protect security as long as at least one server is honest. Moreover, if the client can obtain a short digest of the database out of band, then our schemes require only a single server. Performing an authenticated private PGP-public-key lookup on an OpenPGP key server's database of 3.5 million keys (3 GiB), using two non-colluding servers, takes under 1.2 core-seconds of computation, essentially matching the time taken by unauthenticated private information retrieval. Our authenticated single-server schemes are 30-100× more costly than state-of-the-art unauthenticated single-server schemes, though they achieve incomparably stronger integrity properties.

## 1 Introduction

Private information retrieval (PIR) [29] enables a client to fetch a record from a database while hiding from the database server(s) which specific record(s) the client retrieves. PIR has numerous privacy-protection uses, such as in metadata-private messaging [5, 6], certificate transparency [62, 80], video streaming [50], password-breach alerting [4, 59, 83], retrieval of security updates [22], public-key directories [63], and private SQL-like queries on public data [72, 88].

Most PIR protocols, however, do not ensure data authenticity in the presence of malicious servers. In many multi-server PIR schemes [17, 29], a single adversarial server can flip any subset of bits in the client's recovered output. In all single-server PIR schemes we know of (c.f., [1, 4, 5, 18, 20, 31, 36, 45, 51, 56, 61, 65, 70, 74, 76] for a non-exhaustive list), a malicious server can choose the exact output that the client will receive by substituting all the database records with a chosen record before processing the client's request. In applications where data integrity matters, such as a PGP public-key directory, unauthenticated PIR is inadequate.

This paper introduces *authenticated private information retrieval*, which augments the standard privacy properties of classic PIR with strong authenticity guarantees. In the multi-server setting, we propose authenticated-PIR schemes for:

- *Point queries*, in which a client wants to fetch a particular database record. For example, "What is the public key for `user@usenix.org`?"
- *Predicate queries*, where a client wants to apply an aggregation operator – such as `COUNT`, `SUM`, or `AVG` – to all records matching a predicate. For example, "How many keys are registered for email addresses ending in `@usenix.org`?"

Our corresponding authenticated-PIR schemes guarantee integrity in the *anytrust* model [90]: as long as at least one of the PIR servers is honest. In contrast, prior work that deals with malicious or faulty PIR servers in the multi-server setting either requires a majority or supermajority of servers to be honest [11, 12, 38, 48] or requires expensive public-key cryptography operations [94]. Our schemes use only fast symmetric-key cryptography in the multi-server setting.

In the single-server setting, we offer authenticated-PIR schemes for point queries which provide authentication as long as the client can obtain a short digest of the database via out-of-band means (Fig. 1). Prior work for the single-server setting [56, 89, 95] ensures only that the server truthfully answers the query with respect to *some* database—not necessarily the database the client queried. Table 2 summarizes prior work and Section 8 gives the complete discussion.

**New definitions.** Our first contribution is a new definition of integrity for private information retrieval. In our multi-server PIR schemes, a client communicates with several database servers, and client privacy holds as long as at least one server is honest. In this multi-server setting, we say that a PIR scheme satisfies integrity if, whenever the client accepts the servers' answers, the client's output is consistent with an honest server's view of the database.

Defining integrity in the single-server setting is more tricky: If the single database server is malicious, who is to say what the "right" database is? Our approach assumes that the client can obtain a short digest of the database via some out-of-band means. A single-server PIR protocol satisfies integrity if the client accepts the protocol's output only if the output is consistent with the database that the digest represents. In some applications of PIR, the client could obtain this database digest via a gossip mechanism, as in CONIKS [64], or from a collective authority [81], or from a signature-producing blockchain [71]. In other applications of PIR such as video streaming [50], a

The full version of this paper is available at https://eprint.iacr.org/2023/297.

# Exhibit 14

The first pages of the peer-reviewed publication authored by Dr. Nikitin on securing the software supply chain, alongside the evidence that this work has been included in the graduate-level curriculum at multiple US and international universities:

- *Nikitin K., Kokoris-Kogias E., Jovanovic P., Gailly N., Gasser L., Khoffi I., Cappos J., Ford B. CHAINIAC: Proactive Software-Update transparency via collectively signed skipchains and verified builds. In USENIX Security Symposium 2017.*
- Course syllabi from the following universities (the entires about Dr. Nikitin's work are highlighted):
  - The University of Chicago
  - The University of California, San Diego
  - The University of Illinois at Urbana-Champaign
  - The Technical University of Munich, Germany


# CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds

**Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, and Linus Gasser,** *École polytechnique fédérale de Lausanne* **(*EPFL*);** **Ismail Khoffi,** *University of Bonn;* **Justin Cappos,** *New York University;* **Bryan Ford,** *École polytechnique fédérale de Lausanne* **(*EPFL*)**

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/nikitin

**This paper is included in the Proceedings of the 26th USENIX Security Symposium**

**August 16–18, 2017 • Vancouver, BC, Canada**

ISBN 978-1-931971-40-9

**Open access to the Proceedings of the 26th USENIX Security Symposium is sponsored by USENIX**

# CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds

Kirill Nikitin[1], Eleftherios Kokoris-Kogias[1], Philipp Jovanovic[1], Linus Gasser[1], Nicolas Gailly[1], Ismail Khoffi[2], Justin Cappos[3], and Bryan Ford[1]

[1]École polytechnique fédérale de Lausanne (EPFL)
[2]University of Bonn
[3]New York University

## Abstract

Software-update mechanisms are critical to the security of modern systems, but their typically centralized design presents a lucrative and frequently attacked target. In this work, we propose CHAINIAC, a decentralized software-update framework that eliminates single points of failure, enforces transparency, and provides efficient verifiability of integrity and authenticity for software-release processes. Independent *witness servers* collectively verify conformance of software updates to release policies, *build verifiers* validate the source-to-binary correspondence, and a tamper-proof release log stores collectively signed updates, thus ensuring that no release is accepted by clients before being widely disclosed and validated. The release log embodies a *skipchain*, a novel data structure, enabling arbitrarily out-of-date clients to efficiently validate updates and signing keys. Evaluation of our CHAINIAC prototype on reproducible Debian packages shows that the automated update process takes the average of 5 minutes per release for individual packages, and only 20 seconds for the aggregate timeline. We further evaluate the framework using real-world data from the PyPI package repository and show that it offers clients security comparable to verifying every single update themselves while consuming only one-fifth of the bandwidth and having a minimal computational overhead.

## 1 Introduction

Software updates are essential to the security of computerized systems as they enable the addition of new security features, the minimization of the delay to patch disclosed vulnerabilities and, in general, the improvement of their security posture. As software-update systems [17, 24, 34, 35, 48] are responsible for managing, distributing, and installing code that is eventually executed on end systems, they constitute valuable targets for attackers who might, *e.g.*, try to subvert the update infrastructure to inject malware. Furthermore, powerful adversaries might be able to compromise a fraction of the developers' machines or tamper with software-update centers. Therefore, securing update infrastructure requires addressing four main challenges:

First, the integrity and authenticity of updates traditionally depends on a single signing key, prone to loss [53] or theft [29, 32, 70]. Having proper protection for signing keys to defend against such single points of failure is therefore a top priority. Second, the lack of transparency mechanisms in the current infrastructure of software distribution leaves room for equivocation and stealthy backdooring of updates by compromised [15, 46], coerced [11, 28, 66], or malicious [36] software vendors and distributors. Recent work on reproducible software builds [49, 59] attempts to counteract this deficit by improving on the source-to-binary correspondence. However, it is unsuitable for widespread deployment in its current form, as rebuilding packages puts a high burden on end users (*e.g.*, building the Tor Browser bundle takes 32 hours on a modern laptop [60]). Third, attackers might execute a man-in-the-middle attack on the connections between users and update providers (*e.g.*, with DNS cache poisoning [67] or BGP hijacking [6]), thus enabling themselves to mount replay and freeze attacks [15] against their targets. To prevent attackers from exploiting unpatched security vulnerabilities as a consequence of being targeted by one of the above attacks [72], clients must be able to verify timeliness of updates. Finally, revoking and renewing signing keys (*e.g.*, in reaction to a compromise) and informing all their clients about these changes is usually cumbersome. Hence, modern software-update systems should provide efficient and secure means to evolve signing keys and should enable client notification in a timely manner.

To address these challenges, we propose CHAINIAC, a decentralized software-update framework that removes

# Course Schedule

Spring 2018

This schedule is subject to change. Please check back frequently.

| Week | Date | Topic | Readings |
|---|---|---|---|
| Week 1 | Mar 27 | **Intro; Security & Crypto Crash Course I** | |
| | Mar 29 | **Accountability & Transparency I** | Assigned:<br>CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds. Nikitin, Kokoris-Kogias, Jovanovic, Gasser, Gailly, Khoffi, Cappos, Ford. USENIX Security. 2017. |
| Week 2 | Apr 3 | **Accountability & Transparency II; Security & Crypto Crash Course II** | Assigned:<br>Accountable Virtual Machines. Haeberlen, Aditya, Rodrigues, Druschel. OSDI. 2010.<br>Recommended:<br>• PeerReview: Practical Accountability for Distributed Systems. Haeberlen, Kouznetsov, Druschel. SOSP. 2007.<br>• Efficient Data Structures for Tamper-Evident Logging. Crosby, Wallach. Usenix Security. 2009.<br>• Verena: End-to-End Integrity Protection for Web Applications. Karapanos, Filios, Popa, Capkun, Berkeley. Oakland. 2016. |
| | Apr 5 | **Accountability & Transparency III** | Assigned:<br>The Efficient Server Audit Problem, Deduplicated Re-execution, and the Web. Tan, Yu, Leners, Walfish. SOSP. 2017. |
| Week 3 | Apr 10 | **Certificates & Keys** | Assigned:<br>• **[Present]** CONIKS: Bringing Key Transparency to End Users. Melara, Blankstein, Bonneau, Felten, Freedman. Usenix Security. 2015.<br>• Certificate Transparency with Privacy. Eskandarian, Messeri, Bonneau, Boneh. PETS. 2017.<br>Recommended:<br>• SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. Clark, Van Oorschot. Oakland. 2013.<br>• Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning. Syta, Tamas, Visher, Wolinsky, Gasser, Gailly, Ford. Oakland. 2016.<br>• Tracking Certificate Misissuance in the Wild. Kumar, Wang, Hyder, Dickinson, Beck, Adrian, Mason, Durumeric, Halderman, Bailey. Oakland. 2018. |
| | Apr 12 | **TLS and HTTPS** | Assigned:<br>TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing for Disintermediation. Ritzdorf, Wüst, Gervais, Felley, Čapkun. NDSS. 2018. |
| Week 4 | Apr 17 | **Anonymity I** | Assigned:<br>• **[Present]** Atom: Horizontally Scaling Strong Anonymity. Kwon, Corrigan-Gibbs, Devadas, Ford. SOSP. 2017.<br>• Tor: The second-generation onion router. Dingledine, Mathewson, Syverson. Usenix Security. 2004. |
| | Apr 19 | **Anonymity II** | Assigned:<br>Stadium: A Distributed Metadata-Private Messaging System. Tyagi, Gilad, Zaharia, Zeldovich. SOSP. 2017. |
| Week 5 | Apr 24 | No class. | |
| | Apr 26 | **Oblivious Storage** | Assigned:<br>ObliviSync: Practical Oblivious File Backup and Synchronization. Aviv, Choi, Mayberry, Roche. NDSS. 2017. |
| Week 6 | May 1 | **Trusted Execution Environments** | Assigned:<br>• Shielding applications from an untrusted cloud with haven. Baumann, Peinado, Hunt. SOSP. 2014.<br>• **[Present]** Opaque: An Oblivious and Encrypted Distributed Analytics Platform. Zheng, Dave, Beekman, Popa, Gonzalez, Stoica. NSDI. 2017.<br>Recommended:<br>• Intel SGX Explained. Costan, Devadas. 2015.<br>• OpenSGX: An Open Platform for SGX Research. Jain, Desai, Kim, Shih, Lee, Choi, Shin, Kim, Kang, Han. NDSS. 2016. |
| | May 3 | **Side Channels I** | Assigned:<br>CLKSCREW: Exposing the perils of security-oblivious energy management. Tang, Sethumadhavan, Stolfo. Usenix Security. 2017. |
| Week 7 | May 8 | **Side Channels II** | Assigned:<br>• Meltdown. Lipp, Schwarz, Gruss, Prescher, Haas, Mangard, Kocher, Genkin, Yarom, Hamburg. *ArXiv e-prints*. 2018.<br>• **[Present]** Spectre Attacks: Exploiting Speculative Execution. Kocher, Genkin, Gruss, Haas, Hamburg, Lipp, Mangard, Prescher, Schwarz, Yarom. *ArXiv e-prints*. 2018. |
| | May 10 | **Side Channels III** | Assigned:<br>SgxPectre Attacks: Leaking Enclave Secrets via Speculative Execution. Chen, Chen, Xiao, Zhang, Lin, Lai. CoRR. 2018. |
| Week 8 | May 15 | **Cryptocurrencies: Intro.** | Assigned:<br>• **[Present]** SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Bonneau, Miller, Clark, Narayanan, Kroll, Felten, Foundation. Oakland. 2015.<br>• **[Present]** Bitcoin's Academic Pedigree. Narayanan, Clark. Communications of the Acm. 2017.<br>Recommended:<br>• Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto. 2008.<br>• Bitcoin and Cryptocurrency Technologies. Narayanan, Bonneau, Felten, Miller, Goldfeder. 2016. **Ch. 1-5,7-8.** |
| | May 17 | **Cryptocurrencies: Buying Physical Goods** | Assigned:<br>Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin. Goldfeder, Bonneau, Gennaro, Narayanan. Financial Cryptography and Data Security. 2017. |
| Week 9 | May 22 | **Verifiable Computation** | Assigned:<br>• Verifying computations without reexecuting them: from theoretical possibility to near practicality. Walfish, Blumberg. ECCC. 2013.<br>• **[Present]** Pinocchio: Nearly practical verifiable computation. Parno, Howell, Gentry, Raykova. Oakland. 2013.<br>Recommended:<br>• Verifying computations with state. Braun, Feldman, Ren, Setty, Blumberg, Walfish. SOSP. 2013.<br>• Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. Ben-sasson, Chiesa, Tromer. Usenix Security. 2014.<br>• Geppetto: Versatile Verifiable Computation. Costello, Fournet, Howell, Kohlweiss, Kreuter, Naehrig, Parno, Zahur. Oakland. 2015. |
| | May 24 | **Cryptocurrencies: Anonymity** | Assigned:<br>• **[Present]** Zerocash: Decentralized Anonymous Payments from Bitcoin. Ben-sasson, Chiesa, Garman, Green, Miers, Tromer. Oakland. 2014.<br>• **[Present]** TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub. Heilman, Alshenibr, Baldimtsi, Scafuro, Goldberg. NDSS. 2017.<br>Recommended:<br>Bitcoin and Cryptocurrency Technologies. Narayanan, Bonneau, Felten, Miller, Goldfeder. 2016. **Ch. 6.** |
| Week 10 | May 29 | **Cryptocurrencies: Smart Contracts** | Assigned:<br>Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. Kosba, Miller, Shi, Wen, Papamanthou. Oakland. 2016.<br>Recommended:<br>• Ethereum: a secure decentralised generalised transaction ledger. Wood. Ethereum Project. 2014.<br>• Town Crier: An Authenticated Data Feed for Smart Contracts. Zhang, Cecchetti, Croman, Juels, Shi. CCS. 2016.<br>• Bitcoin and Cryptocurrency Technologies. Narayanan, Bonneau, Felten, Miller, Goldfeder. 2016. **Ch. 10-11.** |
| | May 31 | **Cryptocurrencies as a Platform** | Assigned:<br>Blockstack: A Global Naming and Storage System Secured by Blockchains. Ali, Nelson, Shea, Freedman. USENIX ATC. 2016.<br>Recommended:<br>• Catena: Efficient Non-equivocation via Bitcoin. Tomescu, Devadas. Oakland. 2017.<br>• Bitcoin and Cryptocurrency Technologies. Narayanan, Bonneau, Felten, Miller, Goldfeder. 2016. **Ch. 9.** |

# Syllabus

| Date | Papers |
|---|---|
| Oct 1 | **Overview and Introduction**<br>How to Read a Paper by S. Keshav<br>The Rise of Worse is Better by R. P. Gariel |
| | **Low-Level Vulnerabilities and Defenses** |
| Oct 3 | How Memory Safety Violations Enable Exploitation of Programs by M. Payer<br>A Modern History of Offensive Security Research by D. Dai Zovi<br>*See also:* Low-Level Software Security by Example by U. Erlingssona et al. |
| Oct 8 [1] | Control-Flow Integrity: Precision, Security, and Performance by N. Burow et al.<br>Control-Flow Bending: On the Effectiveness of Control-Flow Integrity by N. Carlini et al. |
| Oct 10 | Principles and Implementation Techniques of Software-Based Fault Isolation by G. Tan<br>Bringing the Web up to Speed with WebAssembly by A. Haas et al. |
| | **Web Security** |
| Oct 15 [2] | Beware of Finer-Grained Origins by C. Jackson and A. Barth<br>Securing Frame Communication in Browsers by A. Barth et al.<br>Chromium's design documents on Site Isolation and Cross-Origin Read Blocking<br>The Web Origin Concept by A. Barth |
| Oct 17 | Blueprint: Robust Prevention of Cross-site Scripting Attacks for Existing Browsers by M. T. Louw and V.N. Venkatakrishnan<br>Robust Defenses for Cross-Site Request Forgery by A. Barth et al.<br>Using positive tainting and syntax-aware evaluation to counter SQL injection attacks by W. G. J. Halfond et al. |
| Oct 22 | CSP is dead, long live CSP! On the insecurity of whitelists and the future of content security policy by L. Weichselbaum et al.<br>Protecting Users by Confining JavaScript with COWL by D. Stefan et al. |
| | **Web Privacy** |
| Oct 24 | Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies by G. Franken et al.<br>An Analysis of Private Browsing Modes in Modern Browsers by G. Aggarwal et al.<br>Browser History re:visited by M. Smith et al. |
| Oct 29 | Trusted Browsers for Uncertain Times by D. Kohlbrenner and H. Shacham<br>The Design and Implementation of the Tor Browser by M. Perry |
| | **The Hardware-Software Boundary** |
| Oct 31 | Spectre Attacks: Exploiting Speculative Execution by P. Kocher et al.<br>Meltdown: Reading Kernel Memory from User Space by M. Lipp et al.<br>Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution by J. Van Bulck et al. |
| Nov 5 | Hyperflow: A Processor Architecture for Nonmalleable, Timing-Safe Information-Flow Security by A. Ferraiuolo et al.<br>GhostRider: A Hardware-Software System for Memory Trace Oblivious Computation by C. Liu et al. |
| | **Automatic Vulnerability Discovery** |
| Nov 7 | A Survey of Symbolic Execution Techniques by R. Baldoni et al.<br>Under-Constrained Symbolic Execution: Correctness Checking for Real Code by D. A. Ramos and D. Engler<br>SAGE: Whitebox Fuzzing for Security Testing by P. Godefroid et al. |
| Nov 19 | AEG: Automatic Exploit Generation by T. Avgerinos et al.<br>NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications by A. Alhuzali et al.<br>Driller: Augmenting Fuzzing Through Selective Symbolic Execution by N. Stephens et al. |
| | **Package managers and sofware distribution** |
| Nov 26 | Docker ecosystem–Vulnerability Analysis by A. Martin et al.<br>A Look In the Mirror: Attacks on Package Managers by J. Cappos et al. |
| Nov 28 | CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds by K. Nikitin et al.<br>Contour: A Practical System for Binary Transparency by M. Al-Bassam and S. Meiklejohn |
| | **Stepping Back** |
| Dec 3 | Thirty Years Later: Lessons from the Multics Security Evaluation by P. A. Karger and R. R. Schell<br>This World of Ours by J. Mickens<br>Looking Back: Addendum by D. E. Bell |
| Dec 5 | How to Write a Great Research Paper by S. P. Jones<br>How to Give a Great Research Talk by S. P. Jones<br>On Preparing Good Talks by R. Jhala |

1. Form project groups.
2. Submit project proposal.

**UIUC Advanced Computer Security - Spring 21**

ECE 524 / CS 563 Spring 2021 Advanced Computer Security

---

Tags: HW/OS, SOFT, APP, THEORY, NET, DATA

## Preliminary

- Lattice-based access control models. Ravi S. Sandhu.

## First week

- The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86) Hovav Shacham. CCS 2007.
- "Weird Machines" in ELF: A Spotlight on the Underappreciated Metadata. Rebecca Shapiro, Sergey Bratus, Sean W. Smith. WOOT 2013.

## Language-based approach to software security

- Information-Flow Security for a Core of JavaScript Daniel Hedin, Andrei Sabelfeld. CSF 2012.
- Verifying policy-based security for web services Karthikeyan Bhargavan, Cédric Fournet, Andrew D Gordon. CCS 2004.
- Small World with High Risks: A Study of Security Threats in the npm Ecosystem. Markus Zimmermann, Cristian-Alexandru Staicu, Cam Tenny, Michael Pradel. Usenix Security 2019.
- Secure web applications via automatic partitioning Stephen Chong, Jed Liu, Andrew Myers, Xin Qi, K. Vikram, Lantian Zheng, Xin Zheng. SOSP 2007.
- Joe-E: A Security-Oriented Subset of Java Adrian Mettler, David Wagner, Tyler Close. NDSS 2010.
- Robust Declassification Steve Zdancewic Andrew C. Myers. CSF 2001.
- Certificate Transparency. Ben Laurie. Communications of the ACM, 2014.
- Transparency overlays and their applications. Melissa Chase, Sarah Meiklejohn. CCS 2016.
- CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Justin Cappos, Bryan Ford. Usenix Sec 2017.
- Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. Ivica Nikolic, Aashish Kolluri, Ilya Sergey, Prateek Saxena, Aquinas Hobor. ACSAC 2018.
- Securify: Practical Security Analysis of Smart Contracts. Ivica Nikolic, Aashish Kolluri, Ilya Sergey, Prateek Saxena, and Aquinas Hobor. CCS 2019
- ZEUS: Analyzing Safety of Smart Contracts. Sukrit Kalra, Seep Goel, Mohan Dhawan, and Subodh Sharma. NDSS 2018

## Cutting edge of cryptography-based system design

- ZoKrates - Scalable Privacy-Preserving Off-Chain Computations Jacob Eberhardt, Stefan Tai. CPSCom 2018.
- PhotoProof: Cryptographic Image Authentication for Any Set of Permissible Transformations. Assa Naveh and Eran Tromer. SP 2016.
- MP-SPDZ: A Versatile Framework for Multi-Party Computation Marcel Keller. CCS 2020.
- Secure Evaluation of Quantized Neural Networks. Anders Dalskov, Daniel Escudero, and Marcel Keller. PoPETS 2020.
- Bulletproofs: Short Proofs for Confidential Transactions and More. Benedikt Bunz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. SP 2018.
- DIZK.
- xJsnark: a framework for efficient verifiable computation Ahmed Kosba, Charalampos Papamanthou, Elaine Shi. SP 2018

## Usability in Security

- Rethinking Connection Security Indicators. Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Maximilian Walker, Christopher Albert Thompson, Mustafa Emre Acer, Elisabeth Morant, Sunny Consolvo. SOUPS 2016.
- Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I. Hong. SOUPS2014.
- A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. Sauvik Das, Laura A. Dabbish, Jason I. Hong. SOUPS 2019.
- Deja Vu-A User Study: Using Images for Authentication. Rachna Dhamija and Adrian Perrig. Usenix Security 2000.
- "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. I. Reyes, P. Wijesekera, J. Reardon, A. E. B. On, A. Razaghpanah, N. Vallina-Rodriguez, S. Egelman. PoPETS 2018.
- Better managed than memorized? studying the impact of managers on password strength and reuse Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, Sven Bugiel. (USENIX'18)
- On Enforcing the Digital Immunity of a Large Humanitarian Organization Stevens Le Blond, Alejandro Cuevas, Juan Ramon Troncoso-Pastoriza, Philipp Jovanovic ´ Bryan Ford, Jean-Pierre Hubaux. Oakland 2018.

## Security and social media infrastructure

- SATE: Robust and Private Allegation Escrows Venkat Arun, Aniket Kate, Deepak Garg, Peter Druschel, Bobby Bhattacharjee. NDSS 2020.
- The Many Kinds of Creepware Used for Interpersonal Attacks Kevin A. Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, Acar Tamersoy. IEEE SP 2020.
- The Spyware Used in Intimate Partner Violence. Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, Thomas Ristenpart. IEEE SP 2018.
- Disinformation's spread: bots, trolls and all of us. Kate Starbird. Nature 571, 449 (2019).
- Trafficking fraudulent accounts: The role of the underground market in Twitter spam and abuse. Usenix security 2013.
- Detecting Fake Accounts in Online Social Networks at the Time of Registrations CCS 2019.
- Deceptive Previews: A Study of the Link Preview Trustworthiness in Social Platforms. Giada Stivala, Giancarlo Pellegrino. NDSS 2020.
- SoK: Hate, Harassment, and the Changing Landscape of Online Abuse Kurt Thomas Devdatta Akhawe Michael Bailey Dan Boneh Elie Bursztein Sunny Consolvo Nicola Dell Zakir Durumeric Patrick Gage Kelley Deepak Kumar Damon McCoy Sarah Meiklejohn Thomas Ristenpart Gianluca Stringhini. SP 2021.
- A taste of tweets: reverse engineering Twitter spammers Chao Yang, Jialong Zhang, Guofei Gu. ACSAC 2014.
- On the Detection of Disinformation Campaign Activity with Network Analysis. Luis Vargas, Patrick Emami, Patrick Traynor, Traynor. CCSW 2020.
- Information security: where computer science, economics and psychology meet Ross Anderson and Tyler Moore. Phil. Trans. R. Soc.

## Other topics

- Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet. Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, Dave Levin. NDSS 2019.
- Practicing a Science of Security: A Philosophy of Science Perspective Jonathan M. Spring, Tyler Moore, David J Pym. NSPW 2017.
- The Security Impact of HTTPS Interception. Z Durumeric, Z Ma, D Springall, R Barnes, N Sullivan, E Bursztein. NDSS 2017.
- Spectre Attacks: Exploiting Speculative Execution Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, Yuval Yarom. IEEE SP 2019
- Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Hye Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu.

# Next Generation Secure Computer Architectures

**Seminare** 2 SWS / 5 ECTS (Kursbeschreibung)
**Veranstalter:** Thomas Kittel
**Beginn:**

**Vorbesprechung**: Di, 06.2. um 09:30 Uhr im Raum 01.08.033 [Folien]

**Termine (geplant)**:

- Zwischenevaluation:
  - Fr, 27.04.2018 - 10-12 Uhr - 01.08.033
- Vorträge:
  - Do, 28.06.2018 - 09-18 Uhr - 01.08.033
  - Fr, 29.06.2018 - 09-18 Uhr - 01.08.033

**Verantwortliche**:

- Matthias Hiller
- Lukas Auer
- Vincent Immler

**Mögliche Themen umfassen**:

- AEGIS: Architecture for Tamper-Evident and Tamper-Resistant Processing
  - AEGIS is a processor architecture, secure against both physical and software attacks. It assumes that all external components, as well as the operation system, are untrustable. Physical and software tampering is detected by tamper-evident and authenticated environments. In addition, environments are private to prevent an adversary from obtaining information by tampering with or observing system operation.
    - https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/AEGIS_Suh.pdf
    - http://csg.csail.mit.edu/pubs/memos/Memo-461/memo-461.pdf

- Oblivious RAM Protocols
  - Oblivious RAM (ORAM) prevents access pattern leakage to hide the sequence of operations being performed. Specifically, the sequence in which memory locations are accessed is equivalent for all inputs with the same access time. ORAM solutions provide strong privacy guarantees since an observer is unable to distinguish accesses from random. They are used in applications such as secure cloud storage, secure multi-party computation, and secure processors.
    - https://acmccs.github.io/papers/p523-doernerA.pdf
    - https://acmccs.github.io/papers/p507-rocheA.pdf
    - http://web.cs.ucla.edu/~rafail/PUBLIC/09.pdf

- Survey over Intel SGX Extensions and ARM TrustZone
  - Intel Software Guard Extensions (SGX) allows user-code to run in isolated memory regions (enclaves), which are protected from code running at higher privilege levels. It aims to provide integrity and confidentiality guarantees (secure remote computation) in a potentially malicious software environment.
    - https://eprint.iacr.org/2016/086.pdf

- Sanctum Hardware Extensions for Strong Software Isolation
  - Sanctum is an alternative to Intel's Software Guard Extensions (SGX). It provides strong provable isolation of software modules running concurrently with shared resources. Unlike SGX, which is implemented in microcode, Sanctum is mostly implemented with trusted software and is therefore easier to analyze. A prototype of the extension is implemented with the Rocket RISC-V core.
    - https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_costan.pdf
    - https://github.com/pwnall/sanctum

- The CHERI capability model: Revisiting RISC in an age of risk
  - CHERI (Capability Hardware Enhanced RISC Instructions) is an extension to 64-bit RISC instruction set architectures (ISA). It introduces a hybrid capability-system to allow software to efficiently implement fine-grained memory protection policies and software compartmentalization. FreeBSD and the LLVM compiler have been modified to take advantage of the CHERI extension.
    - https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201406-isca2014-cheri.pdf
    - https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201505-oakland2015-cheri-compartmentalization.pdf
    - https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-907.pdf
    - https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/

- CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds
  - CHAINIAC is a decentralized software-update framework with the goal of eliminating single points of failure, enforcing transparency, and providing efficient verifiability of integrity and authenticity. Signed software-updates are collected in a tamper-proof release log based on the skipchain, a cryptographically-traversable, offline- and peer-to-peer-verifiable blockchain structure.
    - https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-nikitin.pdf
    - https://www.usenix.org/sites/default/files/conference/protected-files/usenixsecurity17_slides_nikitin.pdf
    - https://bford.github.io/2017/08/01/skipchain/

- Invasive Computing
  - Invasive computing is a new processing paradigm for Multi-Processor Systems-on-Chip (MPSoCs). Programs can dynamically scale from running on just one processor to multiple, neighboring processors. This first phase of expanding to multiple processors is the invasion step. After the highly parallel processing phase, programs scale the consumed resources back in the retreat step.
    - https://invasic.informatik.uni-erlangen.de/publications/invasic-overview.pdf

- Formal Foundation for Secure Remote Execution of Enclave
  - This paper introduces a verification methodology for trusted hardware platforms such as Intel SGX and the MIT Sanctum extension. It formalizes an idealized enclave platform along with a parameterized adversary. In addition, it formalizes the notion of secure remote execution and presents machine-checked proofs for its three key security properties: integrity, confidentiality, and secure measurement.
    - https://people.eecs.berkeley.edu/~rsinha/research/pubs/ccs2017.pdf

- Weitere Themenvorschläge durch Studierende können berücksichtigt werden.

## Upcoming Events

- MA Abschlussvortrag Christopher Sendlinger / Kilian Tscharke, Pascal Debus
  Jan 16, 2025 10:00 AM
  (Europe/Berlin) – per Videokonferenz
- MA Abschlussvortrag Boris-Chengbiao Zhou / Fabian Franzen
  Jan 16, 2025 01:00 PM
  (Europe/Berlin) – per Videokonferenz
- MA Abschlussvortrag Jason Lochert / Sebastian Peters, David Emeis, Lukas Lautenschlager
  Jan 23, 2025 11:00 AM
  (Europe/Berlin) – per Videokonferenz
- BA Abschlussvortrag Leon Birkel / Fabian Franzen
  Jan 28, 2025 03:00 PM
  (Europe/Berlin) – per Videokonferenz

Previous events...
Upcoming events...

## News

- Prof. Claudia Eckert erhält höchste Auszeichnung der TUM, die Heinz Maier-Leibnitz-Medaille
  Dec 13, 2023
- Die Lehrveranstaltungsplanung für das SS 2024 ist noch nicht abgeschlossen
  Oct 11, 2023
- Preis für gute Lehre: Claudia Eckert ausgezeichnet
  Apr 28, 2023
- Experience Cybersecurity @ Fraunhofer AISEC
  Apr 21, 2023
- Wir suchen ab sofort 1 wissenschaftliche Mitarbeiter/innen für ein Projekt zusammen mit SAP
  Mar 21, 2023

More news...

# Exhibit 15

The first page of the peer-reviewed publication authored by Dr. Nikitin on improving the efficiency of blockchain networks

- *Lee J., Nikitin K., Setty S. Replicated state machines without replicated execution. In IEEE Symposium on Security and Privacy 2020.*

# Replicated state machines without replicated execution

Jonathan Lee Kirill Nikitin* Srinath Setty
*Microsoft Research* **EPFL*

## Abstract

This paper introduces a new approach to reduce end-to-end costs in large-scale replicated systems built under a Byzantine fault model. Specifically, our approach transforms a given replicated state machine (RSM) to another RSM where nodes incur lower costs by *delegating* state machine execution: an untrusted prover produces succinct cryptographic proofs of correct state transitions along with state changes, which nodes in the transformed RSM verify and apply respectively.

To realize our approach, we build *Piperine*, a system that makes the proof machinery profitable in the context of RSMs. Specifically, Piperine reduces the costs of both proving and verifying the correctness of state machine execution while retaining liveness—a distinctive requirement in the context of RSMs. Our experimental evaluation demonstrates that, for a payment service, employing Piperine is more profitable than naive reexecution of transactions as long as there are $> 10^4$ nodes. When we apply Piperine to ERC-20 transactions in Ethereum (a real-world RSM with up to $10^5$ nodes), it reduces per-transaction costs by 5.4× and network costs by 2.7×.

## 1 Introduction

A modern example of a large-scale replicated system is a blockchain network [64, 86], which employs replication to enable mutually-distrusting entities to transact *without* relying on trusted authorities. Specifically, blockchains instantiate *replicated state machines* (RSMs) [71] under a Byzantine fault model in an open, permissionless network where each node executes and validates every transaction. Unfortunately, the most popular blockchains achieve a throughput of only a handful of transactions per second. This has motivated research to improve throughput and to reduce costs, for example, by changing the underlying consensus protocol used to realize RSMs [41, 46, 50]. These proposals, however, introduce additional assumptions for safety and/or liveness (§7).

We consider a different approach, one that applies to any existing replicated state machine in a Byzantine fault model (including blockchains) *without* any changes to the underlying consensus protocol. Naturally, it does not introduce any strong assumptions for safety or liveness. In fact, this approach is complementary to aforementioned advances [41, 46, 50] and can be used in conjunction with those proposals. Our approach is based on work in the area of *proof-based verifiable computation* (see [83] for a survey), which has developed a powerful primitive called *verifiable state machines* [24, 73]: for a state machine $S$ and a batch of transactions $x$, an untrusted *prover* can produce outputs $y$ and a short proof $\pi$ such that a *verifier* can check if $y$ is the correct output of $S$ with $x$ as input (using $\pi$)—*without* reexecuting the state transitions. Furthermore, the cost of verifying such a proof is less than reexecuting the corresponding state transitions and the size of the proof is far less than the size of the original batch of transactions. Thus, nodes (in an RSM) that replicate a state machine $S$ can delegate $S$ to an untrusted prover and then replicate the verifier at each node to verify the prover's proofs. Naturally, if the end-to-end resource costs of the transformed RSM (CPU, storage, network, etc.) is cheaper than the original RSM, verifiable delegation leads to lower costs.

In theory, the above picture is straightforward and offers a principled solution to reduce end-to-end costs of a replicated system. However, in practice, the above approach is completely impractical. Specifically, even with state-of-the-art systems for verifiable outsourcing, the verifier is more resource-efficient compared to reexecution only under narrow regimes [80, 81, 83]. Furthermore, in the context of RSMs, the verifier running at each node must have a copy of the delegated state machine's state, otherwise liveness of the transformed RSM hinges on the liveness of the prover (relying on the prover for liveness introduces attack vectors for mounting denial of service). Finally, the prover's cost to produce a proof is $10^4$–$10^7\times$ higher than natively executing the corresponding state transition (the overheads depends on whether the outsourced computation is efficiently representable in the computational model of the proof machinery) [73, 81].

The primary contribution of this paper is a set of techniques to reduce the costs of verifiable state machines in the context of RSMs and to ensure liveness without increasing the costs of the prover. To demonstrate the benefits of these techniques, we build a system called *Piperine*. When we apply Piperine to a popular type of state machine on Ethereum's blockchain, Piperine's proofs act as compressed information (e.g., there is no need to transmit digital signatures or the raw transactions over the blockchain), which allows Piperine to transparently reduce per-transaction network costs by 2.7× and per-transaction end-to-end costs by 5.4×. Beyond cost reductions, Piperine resolves an open question in the context of replicated systems: Piperine offers the first approach to build RSMs with concurrent transaction processing in a permissionless model. Note that prior works that achieve concurrent transaction processing in RSMs [9, 49] require substantial changes to the underlying consensus protocol and apply only to a permissioned membership model.

**Reducing costs.** To tame costs imposed by the proof machinery, Piperine leverages the following observations: (1) in our target state machines, the primary computational bottleneck of a state transition is authenticating a transaction by verify-



DOI 10.1109/SP40000.2020.00068

# Exhibit 16

The first page of an additional peer-reviewed publication authored by Dr. Nikitin on securing group communication in the Internet of Things

- *Tiloca M., Nikitin K., Raza S. Axiom: DTLS-based secure IoT group communication. ACM Transactions on Embedded Computing Systems (TECS), 2017.*

# Axiom: DTLS-Based Secure IoT Group Communication

MARCO TILOCA, KIRILL NIKITIN, and SHAHID RAZA, SICS Swedish ICT AB

This article presents Axiom, a DTLS-based approach to efficiently secure multicast group communication among IoT-constrained devices. Axiom provides an adaptation of the DTLS record layer, relies on key material commonly shared among the group members, and does not require one to perform any DTLS handshake. We made a proof-of-concept implementation of Axiom based on the tinyDTLS library for the Contiki OS and used it to experimentally evaluate performance of our approach on real IoT hardware. Results show that Axiom is affordable on resource-constrained platforms and performs significantly better than related alternative approaches.

CCS Concepts: • **Security and privacy** → **Security protocols**; • **Computer systems organization** → *Embedded and cyber-physical systems;*

Additional Key Words and Phrases: Security, DTLS, multicast, group communication, Internet of Things

**ACM Reference Format:**
Marco Tiloca, Kirill Nikitin, and Shahid Raza. 2017. Axiom: DTLS-based secure IoT group communication. ACM Trans. Embed. Comput. Syst. 16, 3, Article 66 (April 2017), 29 pages.
DOI: http://dx.doi.org/10.1145/3047413



## 1. INTRODUCTION

We have been rapidly moving toward a pervasive networked society where all devices that can benefit from a connection will be connected with one another. This technology trend is commonly referred to as the *Internet of Things* (*IoT*) [Atzori et al. 2010; Kortuem et al. 2010], and it aims at connecting the physical and cyber world by means of tiny resource-constrained devices, embedded in everyday physical objects. To this end, different protocols have been standardized to enable interaction in the IoT. For instance, *6LoWPAN* [Hui and Thubert 2011] enables IP capabilities, *RPL* [Winter et al. 2012] enables routing capabilities, and *CoAP* [Shelby et al. 2014] enables web capabilities.

Several IoT application scenarios such as smart lighting applications, collective building control, and emergency broadcast services can benefit from the adoption of a group communication model, regardless of the specific application-level protocol. According to this communication model, a device becomes a member of a group by

This project was funded by the EU's FP7 program for research, technological development, and demonstration under grant agreement no. 607109; the EU H2020 project NobelGrid under grant no. 646184; VINNOVA, the EIT Digital HII project ACTIVE; and a Swedish Institute scholarship. This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 246016.
Authors' addresses: M. Tiloca and S. Raza, RISE SICS AB, Isafjordsgatan 22, Kista, Sweden; emails: {marco.tiloca, shahid.raza}@ri.se; K. Nikitin, School of Computer and Communication Sciences, EPFL, EDOC-IC INN 134 (Bâtiment INN) Station 14, Lausanne, Switzerland; email: kirill.nikitin@epfl.ch.

DOI: http://dx.doi.org/10.1145/3047413

# Exhibit 17

Proof of Dr. Kirill Nikitin's advanced degrees (Ph.D., M.Sc., and M.Sc.) in Computer and Communication Sciences, Information and Communication Technology, and Information Security

- An academic credentials report by Foreign Credentials Service of America, a member of National Association of Credential Evaluation Services (NACES), certifying the U.S. equivalency of Dr. Nikitin's degrees
- The Doctor of Science (Ph.D.) degree in Computer and Communication Sciences from the École Polytechnique Fédérale de Lausanne, Switzerland
  - The Ph.D. diploma, alongside its official translation to English by the university, and the transcript
- The Master of Science (M.Sc.) degree in Information and Communication Technology from KTH Royal Institute of Technology, Sweden
  - The degree certificate and the transcript, in both Swedish and English
- The Specialist (M.Sc.) degree in Information Security from Kazan Federal University, Russia
  - The degree certificate and the transcript, alongside their official translation to English by the university

# Exhibit 18

Conference and journal rankings by category:

1. Top Conferences for Computer Security and Cryptography
2. Top Journals for Computer Security and Cryptography
3. Top Journals for Databases and Information Systems
4. h5-index of Top conferences and journals for Computer Security and Cryptography
5. h5-index of top conferences and journals for Computing systems
6. h5-index of top conferences and journals for general Engineering and Computer Science
7. The ranking of the ACM Conference on Computer and Communications Security (CCS)
8. The ranking of the USENIX Security Symposium
9. The ranking of the IEEE Symposium on Security and Privacy (S&P)
10. The ranking of the Privacy Enhancing Technologies Symposium (PETS)
11. The ranking of the ACM Transactions on Embedded Computing Systems (TECS)
12. The ranking of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC)

# Best Computer Science Conferences for Computer Security and Cryptography

This ranking of best conferences for Computer Security and Cryptography was generated by Research.com, one of the prominent sites for Computer Science research offering accurate analyses on scientific contributions since 2014.

The position in the ranking is based on Impact Score values aggregated on 21-12-2022. It was based on a detailed examination of as much as 3,549 conference profiles and websites. Show more

Computer Security and ( | All publishers | All countries | Paper submission open

Search by name

| Rank | Conference Details | Impact Score |
|---|---|---|
| 18 | **Computer and Communications Security**<br>26-11-2023 - 30-11-2023 - **Copenhagen** | 13.10 |
| 19 | **IEEE Symposium on Security and Privacy**<br>22-05-2023 - 26-05-2023 - **San Francisco** | 12.90 |
| 30 | **USENIX Security Symposium**<br>09-08-2023 - 11-08-2023 - **Anaheim** | 10.90 |
| 31 | **Theory of Cryptography Conference**<br>29-11-2023 - 02-12-2023 - **Taipei** | 10.50 |
| 37 | **Network and Distributed System Security**<br>27-02-2023 - 03-03-2023 - **San Diego** | 9.10 |
| 49 | **USENIX Annual Technical Conference**<br>11-07-2022 - 13-07-2022 - **Carlsbad** | 6.90 |
| 73 | **International Cryptology Conference**<br>19-08-2023 - 24-08-2023 - **Santa Barbara** | 5.40 |
| 76 | **IEEE European Symposium on Security and Privacy**<br>03-07-2023 - 07-07-2023 - **Delft** | 5.10 |
| 88 | **Theory and Application of Cryptographic Techniques**<br>23-04-2023 - 27-04-2023 - **Lyon** | 4.90 |
| 94 | **Financial Cryptography and Data Security**<br>01-05-2023 - 05-05-2023 - **Brač** | 4.70 |
| 117 | **Annual Computer Security Applications Conference**<br>04-12-2023 - 08-12-2023 - **Austin** | 3.90 |
| 126 | **Trust, Security And Privacy In Computing And Communications**<br>01-11-2023 - 03-11-2023 - **Exeter** | 3.70 |
| 135 | **Cyber-Physical Systems**<br>09-05-2023 - 12-05-2023 - **San Antonio** | 3.60 |

| | | | |
|---|---|---|---|
| 135 | | **Cyber-Physical Systems**<br>09-05-2023 - 12-05-2023 - **San Antonio** | 3.60 |
| 148 | Springer | **Cryptographic Hardware and Embedded Systems**<br>10-09-2023 - 14-09-2023 - **Prague** | 3.40 |
| 161 | Springer | **International Conference on Practice and Theory of Public-Key Cryptography**<br>08-03-2022 - 11-03-2022 | 3.20 |
| 164 | | **Data and Application Security and Privacy**<br>24-04-2023 - 26-04-2023 - **Charlotte** | 3.10 |
| 168 | IEEE | **IEEE International Conference on Systems, Man and Cybernetics**<br>01-10-2023 - 04-10-2023 - **Maui** | 3.00 |
| 175 | | **Security and Privacy in Wireless and Mobile Networks**<br>29-05-2023 - 01-06-2023 - **Guildford** | 3.00 |
| 176 | IEEE | **IEEE International Conference on Blockchain**<br>01-05-2023 - 05-05-2023 - **Dubai** | 3.00 |
| 192 | | **International Symposium on Research in Attacks, Intrusions and Defenses**<br>16-10-2023 - 18-10-2023 - **Hong Kong Polytechnic University** | 2.80 |
| 194 | Springer | **European Symposium on Research in Computer Security**<br>25-09-2023 - 29-09-2023 - **The Hague** | 2.80 |
| 200 | IEEE | **IEEE Symposium on Security and Privacy Workshops**<br>22-05-2023 - 26-05-2023 - **San Francisco** | 2.80 |
| 210 | | **ACM Symposium on Information, Computer and Communications Security**<br>10-07-2023 - 14-07-2023 - **Melbourne** | 2.70 |
| 214 | Springer | **Applied Cryptography and Network Security**<br>19-06-2023 - 22-06-2023 - **Kyoto** | 2.70 |
| 215 | FEDERICO II | **Symposium On Usable Privacy and Security**<br>07-08-2022 - 09-09-2022 - **Boston** | 2.70 |
| 227 | IEEE | **Military Communications**<br>30-10-2023 - 03-11-2023 - **Boston** | 2.60 |
| 247 | | **ASIA CCS: ACM Symposium on Information, Computer and Communications Security**<br>30-05-2022 - 30-05-2022 - **Nagasaki** | 2.40 |
| 254 | IEEE | **IEEE Computer Security Foundations Symposium**<br>10-07-2023 - 14-07-2023 - **Dubrovnik** | 2.40 |
| 279 | Springer | **International Conference on Computer Safety, Reliability, and Security**<br>20-09-2023 - 22-09-2023 - **Toulouse** | 2.20 |
| 309 | IEEE | **International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)**<br>22-08-2022 - 25-08-2022 - **Espoo** | 2.10 |

| | | | |
|---|---|---|---|
| 326 | IEEE | **IEEE International Symposium on Dependable, Autonomic and Secure Computing**<br>13-11-2023 - 17-11-2023 - **Abu Dhabi** | 2.00 |
| 334 | IEEE | **IEEE International Conference on Blockchain and Cryptocurrency**<br>01-05-2023 - 05-05-2023 - **Dubai** | 2.00 |
| 341 | | **International Conference of Distributed Computing and Networking**<br>04-01-2024 - 07-01-2024 - **IIT Madras** | 2.00 |
| 343 | IEEE | **IEEE International Workshop on Information Forensics and Security**<br>04-12-2023 - 07-12-2023 - **Nuremberg** | 2.00 |
| 363 | Springer | **International Conference on the Theory and Application of Cryptology and Information Security**<br>04-12-2023 - 08-12-2023 - **Guangzhou** | 1.90 |
| 369 | | **Symposium on Access Control Models and Technologies**<br>08-06-2022 - 10-06-2022 | 1.90 |
| 393 | IEEE | **Intelligence and Security Informatics**<br>02-11-2021 - 03-11-2021 - **Online** | 1.80 |
| 394 | IEEE | **Hardware-Oriented Security and Trust**<br>01-05-2023 - 04-05-2023 - **San Jose** | 1.80 |
| 399 | BRADFORD | **International Conference on Internet of Things, Big Data and Security**<br>21-04-2023 - 23-04-2023 - **Prague** | 1.70 |
| 419 | Springer | **Post-Quantum Cryptography**<br>16-08-2023 - 18-08-2023 - **College Park** | 1.70 |
| 444 | IEEE | **Dependable and Secure Computing**<br>08-11-2023 - 10-11-2023 - **Tampa** | 1.60 |
| 445 | Springer | **Australasian Conference on Information Security and Privacy**<br>28-11-2022 - 30-11-2022 - **Wollongong** | 1.60 |
| 452 | Springer | **Network and System Security**<br>16-08-2023 - 18-08-2023 - **Canterbury** | 1.60 |
| 458 | IEEE | **International Conference on Identity, Security and Behavior Analysis**<br>22-01-2019 - 22-01-2019 - **Hyderabad** | 1.60 |
| 459 | Springer | **International Conference on Detection of intrusions and malware, and vulnerability assessment**<br>29-06-2022 - 01-07-2022 - **Cagliari** | 1.60 |
| 481 | | **Information Hiding and Multimedia Security**<br>27-06-2022 - 29-06-2022 - **Santa Barbara** | 1.50 |
| 489 | IEEE | **Security, Privacy and Anonymity in Computation, Communication and Storage**<br>30-09-2021 - 03-10-2021 - **New York** | 1.50 |
| 491 | IEEE | **International Workshop on Biometrics and Forensics**<br>19-04-2023 - 20-04-2023 - **Barcelona** | 1.50 |

| | | | |
|---|---|---|---|
| 494 | Springer | **Security and Cryptography for Networks**<br>11-09-2024 - 13-09-2024 - **Amalfi** | 1.50 |
| 495 | Springer | **Decision and Game Theory for Security**<br>18-10-2023 - 20-10-2023 - **Avignon** | 1.50 |
| 498 | Springer | **International Conference on Selected areas in Cryptography**<br>27-03-2023 - 31-03-2023 - **Tallinn** | 1.50 |
| 521 | IEEE | **IEEE International Conference on Technologies for Homeland Security**<br>14-11-2022 - 15-11-2022 | 1.40 |
| 532 | IEEE | **New Technologies, Mobility and Security**<br>19-04-2021 - 21-04-2021 | 1.40 |
| 549 | IEEE | **Conference on Privacy, Security and Trust**<br>22-07-2022 - 24-07-2022 | 1.30 |
| 559 | Bradford | **International Conference on Security and Cryptography**<br>10-07-2023 - 12-07-2023 - **Rome** | 1.30 |
| 572 | IEEE | **Cybersecurity Development**<br>18-10-2023 - 20-10-2023 - **Atlanta** | 1.30 |
| 589 | Bradford | **International Conference on Information Systems Security and Privacy**<br>22-02-2023 - 24-02-2023 - **Lisbon** | 1.20 |
| 609 | Springer | **IFIP Annual Conference on Data and Applications Security and Privacy**<br>18-07-2022 - 20-07-2022 - **Newark** | 1.20 |
| 618 | IEEE | **Big Data Security on Cloud, High Performance and Smart Computing and Intelligent Data and Security**<br>06-05-2022 - 08-05-2022 - **Jinan** | 1.20 |
| 652 | Springer | **International Conference on Security and Privacy in Communication Systems**<br>19-10-2023 - 21-10-2023 - **Hong Kong SAR** | 1.10 |
| 662 | Springer | **International Workshop on Security**<br>29-08-2023 - 31-08-2023 - **Yokohama + Online** | 1.10 |
| 682 | Springer | **Provable Security**<br>20-10-2023 - 22-10-2023 - **Wuhan** | 1.10 |
| 719 | IEEE | **Cyberworlds**<br>03-10-2023 - 05-10-2023 - **Sousse** | 1.00 |
| 732 | IEEE | **International Conference on Software Quality, Reliability and Security**<br>22-10-2023 - 26-10-2023 - **Chiang Mai** | 1.00 |
| 759 | Springer | **Machine Learning for Cyber Security**<br>02-12-2023 - 04-12-2023 - **Nadi** | 1.00 |
| 760 | Springer | **International Conference on Information and Communication Security**<br>18-11-2023 - 20-11-2023 - **Tianjin** | 1.00 |
| 769 | Springer | **Security and Trust Management**<br>08-10-2021 - 08-10-2021 - **Darmstadt** | 1.00 |

# Best Computer Science Journals for Computer Security and Cryptography

The ranking of best journals for Computer Science was published by Research.com, one of the prominent websites for computer science research providing trusted data on scientific contributions since 2014.

The position in the ranking is based on a unique bibliometric score created by Research.com which is computed using the estimated h-index and the number of leading scientists who have endorsed the journal during the last three previous years. Show more

Computer Security and Cryptography

All publishers

Search by name

| Rank | Journal Details | Best Scientists | Documents | Impact Score |
|---|---|---|---|---|
| 23 | **IEEE Transactions on Information Forensics and Security**<br>1556-6013 , Monthly | 401 | 562 | 16.00 |
| 44 | **IEEE Transactions on Dependable and Secure Computing**<br>1545-5971 , Bimonthly | 335 | 469 | 11.10 |
| 85 | **Computers and Security**<br>0167-4048 , Bimonthly | 220 | 277 | 7.60 |
| 132 | **Proceedings on Privacy Enhancing Technologies** | 106 | 137 | 5.70 |
| 201 | **Journal of Information Security and Applications**<br>2214-2126 | 97 | 116 | 4.10 |
| 204 | **IEEE Security and Privacy**<br>1540-7993 , Bimonthly | 112 | 148 | 4.00 |
| 218 | **ACM Transactions on Cyber-Physical Systems**<br>2378-962X | 117 | 108 | 3.80 |
| 228 | **Security and Communication Networks**<br>1939-0122 | 116 | 167 | 3.60 |
| 283 | **Journal of Cryptology**<br>0933-2790 , Quarterly | 68 | 74 | 3.00 |
| 284 | **ACM Transactions on Privacy and Security**<br>2471-2566 | 58 | 47 | 3.00 |

# Best Computer Science Journals for Databases & Information Systems

The ranking of best journals for Computer Science was published by Research.com, one of the prominent websites for computer science research providing trusted data on scientific contributions since 2014.

The position in the ranking is based on a unique bibliometric score created by Research.com which is computed using the estimated h-index and the number of leading scientists who have endorsed the journal during the last three previous years. Show more

Databases & Information Systems | All publishers

Search by name

| Rank | Journal Details | Best Scientists | Documents | Impact Score |
|---|---|---|---|---|
| 5 | **IEEE Transactions on Industrial Informatics**<br>1551-3203 , Quarterly | 537 | 1092 | 23.60 |
| 9 | **Information Sciences**<br>0020-0255 , Semi-monthly | 679 | 1364 | 20.10 |
| 10 | **ACM Computing Surveys**<br>0360-0300 , Quarterly | 364 | 321 | 20.00 |
| 16 | **IEEE Transactions on Knowledge and Data Engineering**<br>1041-4347 , Monthly | 621 | 1025 | 17.40 |
| 17 | **Information Fusion**<br>1566-2535 , Quarterly | 256 | 331 | 16.70 |
| 18 | **IEEE Transactions on Multimedia**<br>1520-9210 , Bimonthly | 528 | 933 | 16.50 |
| 24 | **Expert Systems with Applications**<br>0957-4174 , Semi-monthly | 427 | 674 | 15.90 |
| 32 | **Knowledge-Based Systems**<br>0950-7051 , Bimonthly | 430 | 803 | 13.70 |
| 46 | **IEEE Transactions on Cloud Computing**<br>2168-7161 | 299 | 414 | 10.90 |
| 48 | **Proceedings of the VLDB Endowment**<br>2150-8097 | 290 | 511 | 10.70 |
| 58 | **IEEE Transactions on Information Theory**<br>0018-9448 , Monthly | 223 | 578 | 9.20 |
| 62 | **Information Processing and Management**<br>0306-4573 , Bimonthly | 186 | 185 | 9.00 |
| 65 | **IEEE Transactions on Emerging Topics in Computing**<br>2168-6750 | 167 | 171 | 8.90 |
| 68 | **IEEE Transactions on Big Data**<br>2332-7790 | 240 | 239 | 8.80 |
| 90 | **International Journal of Information Management**<br>0268-4012 | 51 | 83 | 7.20 |
| 93 | **Computers and Industrial Engineering**<br>0360-8352 , Bimonthly | 126 | 239 | 7.00 |
| 95 | **SIAM Journal on Computing**<br>0097-5397 , Bimonthly | 125 | 133 | 6.90 |
| 103 | **ACM Transactions on Knowledge Discovery from Data**<br>1556-4681 , Quarterly | 216 | 228 | 6.50 |

Google Scholar

Top publications

Categories > Engineering & Computer Science > **Computer Security & Cryptography**

| | Publication | h5-index | h5-median |
|---|---|---|---|
| 1. | IEEE Symposium on Security and Privacy | 112 | 179 |
| 2. | USENIX Security Symposium | 106 | 154 |
| 3. | IEEE Transactions on Information Forensics and Security | 100 | 146 |
| 4. | Computers & Security | 98 | 142 |
| 5. | ACM Symposium on Computer and Communications Security | 92 | 136 |
| 6. | Network and Distributed System Security Symposium (NDSS) | 73 | 130 |
| 7. | IEEE Transactions on Dependable and Secure Computing | 70 | 109 |
| 8. | Journal of Information Security and Applications | 65 | 96 |
| 9. | International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT) | 63 | 99 |
| 10. | International Cryptology Conference (CRYPTO) | 61 | 95 |
| 11. | Security and Communication Networks | 56 | 73 |
| 12. | IACR Transactions on Cryptographic Hardware and Embedded Systems | 53 | 86 |
| 13. | Proceedings on Privacy Enhancing Technologies | 51 | 78 |
| 14. | International Conference on Financial Cryptography and Data Security | 47 | 86 |
| 15. | IEEE European Symposium on Security and Privacy | 47 | 84 |
| 16. | International Conference on The Theory and Application of Cryptology and Information Security (ASIACRYPT) | 46 | 66 |
| 17. | IEEE International Conference on Blockchain | 42 | 73 |
| 18. | ACM Asia Conference on Computer and Communications Security | 39 | 57 |
| 19. | IEEE International Conference on Blockchain and Cryptocurrency | 39 | 54 |
| 20. | Symposium On Usable Privacy and Security | 38 | 58 |

## Top publications

Categories > Engineering & Computer Science > **Computing Systems**

| | Publication | h5-index | h5-median |
|---|---|---|---|
| 1. | IEEE Internet of Things Journal | 186 | 261 |
| 2. | Future Generation Computer Systems | 146 | 208 |
| 3. | Cluster Computing | 80 | 115 |
| 4. | IEEE Transactions on Parallel and Distributed Systems | 74 | 111 |
| 5. | The Journal of Supercomputing | 73 | 105 |
| 6. | Internet of Things | 72 | 110 |
| 7. | International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS) | 71 | 122 |
| 8. | Journal of Parallel and Distributed Computing | 67 | 102 |
| 9. | IEEE Transactions on Services Computing | 66 | 95 |
| 10. | International Symposium on Computer Architecture (ISCA) | 62 | 96 |
| 11. | USENIX Symposium on Networked Systems Design and Implementation | 62 | 88 |
| 12. | IEEE/ACM International Symposium on Microarchitecture | 61 | 96 |
| 13. | Concurrency and Computation: Practice and Experience | 56 | 91 |
| 14. | USENIX Annual Technical Conference | 55 | 102 |
| 15. | Symposium on Operating Systems Design and Implementation (OSDI) | 54 | 84 |
| 16. | Journal of Systems Architecture | 54 | 81 |
| 17. | IEEE Transactions on Cloud Computing | 51 | 70 |
| 18. | International Conference for High Performance Computing, Networking, Storage and Analysis | 50 | 89 |
| 19. | IEEE International Symposium on High Performance Computer Architecture | 50 | 86 |
| 20. | ACM European Conference on Computer Systems | 48 | 86 |

*Dates and citation counts are estimated and are determined automatically by a computer program.*

Google Scholar

Top publications

Categories > Engineering & Computer Science > **Engineering & Computer Science (general)**

| | Publication | h5-index | h5-median |
|---|---|---|---|
| 1. | IEEE Access | 266 | 364 |
| 2. | Chemical engineering journal | 232 | 287 |
| 3. | Sensors | 191 | 250 |
| 4. | Advanced Science | 172 | 233 |
| 5. | IEEE Transactions on Industrial Informatics | 167 | 224 |
| 6. | ACS Energy Letters | 167 | 220 |
| 7. | International Journal of Information Management | 165 | 298 |
| 8. | Applied Sciences | 165 | 216 |
| 9. | ACM Computing Surveys (CSUR) | 157 | 258 |
| 10. | Sustainable Cities and Society | 147 | 196 |
| 11. | IEEE Transactions on Industrial Electronics | 144 | 181 |
| 12. | Information Sciences | 136 | 190 |
| 13. | TIDEE: TERI Information Digest on Energy and Environment | 134 | 207 |
| 14. | Fuel | 133 | 175 |
| 15. | ACS Sustainable Chemistry & Engineering | 129 | 155 |
| 16. | Nature Electronics | 123 | 189 |
| 17. | Mechanical Systems and Signal Processing | 122 | 163 |
| 18. | Chem | 121 | 190 |
| 19. | Nature Machine Intelligence | 116 | 176 |
| 20. | Electronics | 116 | 158 |

# 30th ACM Conference on Computer and Communications Security (CCS)

Research Impact Score
**16.30**

- Copenhagen, Denmark
- Submission Deadline: **Thursday 04 May 2023**
- Conference Dates: **Nov 26, 2023 - Nov 30, 2023**

OFFICIAL WEBSITE

Conference Organizers: Deadline extended?
Click here to edit

## Ranking & Metrics

| | | | |
|---|---|---|---|
| Research Impact Score: | 16.30 | Papers published by Best Scientists | 467 |
| Contributing Best Scientists: | 319 | Research Ranking (Computer Science) | 14 |
| H5-index: | | Research Ranking (Electronics and Electrical Engineering) | 182 |
| | | Research Ranking (Electronics and Electrical Engineering) | 152 |
| | | Research Ranking (Computer Science) | 18 |

## Conference Call for Papers

The 30th ACM Conference on Computer and Communications Security (CCS) seeks submissions presenting novel contributions related to all real-world aspects of computer security and privacy. Theoretical papers must make a convincing case for the relevance of their results to practice. Authors are encouraged to write the abstract and introduction of their paper in a way that makes the results accessible and compelling to a general computer-security researcher. In particular, authors should bear in mind that anyone on the program committee may be asked to review any paper.https://www.sigsac.org/ccs/CCS2023/index.htmlhttps://www.sigsac.org/ccs/CCS2023/index.html

# 32nd USENIX Security Symposium

Research Impact Score
**15.40**

OFFICIAL WEBSITE

Conference Organizers: Deadline extended?
Click here to edit

Anaheim, United States
Submission Deadline: **Tuesday 11 Oct 2022**
Conference Dates: **Aug 09, 2023 - Aug 11, 2023**

## Ranking & Metrics

| | | | |
|---|---|---|---|
| Research Impact Score: | 15.40 | Papers published by Best Scientists | 378 |
| Contributing Best Scientists: | 245 | Research Ranking (Computer Science) | 17 |
| H5-index: | | Research Ranking (Computer Science) | 30 |

## Conference Call for Papers

Symposium Topics
Refereed paper submissions are solicited in all areas relating to systems research in security and privacy. This topic list is not meant to be exhaustive; USENIX Security is interested in all aspects of computing systems security and privacy. Papers without a clear application to security or privacy of computing systems, however, will be considered out of scope and may be rejected without full review.

System security
Operating systems security
Web security
Mobile systems security
Distributed systems security
Cloud computing security
Network security
Intrusion and anomaly detection and prevention
Network infrastructure security
Denial-of-service attacks and countermeasures
Wireless security
Security analysis
Malware analysis
Analysis of network and security protocols
Attacks with novel insights, techniques, or results
Forensics and diagnostics for security
Automated security analysis of hardware designs and implementation
Automated security analysis of source code and binaries
Program analysis
Machine learning security and privacy
Machine learning applications to security and privacy
Machine learning privacy issues and methods
Adversarial machine learning
Data-driven security and measurement studies
Measurements of fraud, malware, spam
Measurements of human behavior and security
Privacy
Privacy metrics
Anonymity
Web and mobile privacy
Privacy-preserving computation
Privacy attacks
Usable security and privacy
User studies related to security and privacy
Human-centered security and privacy design
Language-based security
Hardware security
Secure computer architectures
Embedded systems security
Methods for detection of malicious or counterfeit hardware
Side channels
Research on surveillance and censorship
Social issues and security
Research on computer security law and policy
Ethics of computer security research
Research on security education and training
Information manipulation, misinformation, and disinformation
Protecting and understanding at-risk users
Emerging threats, harassment, extremism, and online abuse
Applications of cryptography
Analysis of deployed cryptography and cryptographic protocols
Cryptographic implementation analysis
New cryptographic protocols with real-world applications

# IEEE Symposium on Security and Privacy

Research Impact Score
**13.60**

San Francisco, United States
Submission Deadline: **Friday 01 Apr 2022**
Conference Dates: **May 22, 2023 - May 26, 2023**

OFFICIAL WEBSITE

Conference Organizers: Deadline extended?
Click here to edit

## Ranking & Metrics

| | | | |
|---|---|---|---|
| Research Impact Score: | 13.60 | Papers published by Best Scientists | 207 |
| Contributing Best Scientists: | 193 | Research Ranking (Computer Science) | 20 |
| H5-index: | | Research Ranking (Computer Science) | 19 |

## Conference Call for Papers

Topics of interest include:

Applied cryptography
Attacks with novel insights, techniques, or results
Authentication, access control, and authorization
Blockchains and distributed ledger security
Cloud computing security
Cyber physical systems security
Distributed systems security
Economics of security and privacy
Embedded systems security
Formal methods and verification
Hardware security
Hate, Harassment, and Online Abuse
Intrusion detection and prevention
Machine learning and computer security
Malware and unwanted software
Network security
Operating systems security
Privacy-enhancing technologies, anonymity, and censorship
Program and binary analysis
Protocol security
Security and privacy metrics
Security and privacy policies
Security architectures
Security foundations
Systems security
Usable security and privacy
Web security
Wireless and mobile security/privacy

# Proceedings on Privacy Enhancing Technologies

Research Impact Score*

**5.7**

OFFICIAL WEBSITE

## Ranking & Metrics

| | |
|---|---|
| Research Impact Score*: | 5.7 |
| Research Ranking (Computer Science) | 119 |
| Research Ranking (Computer Science) | 132 |
| Number of Best scientists*: | 106 |
| Documents by best scientists*: | 137 |

## Journal Information

| | |
|---|---|
| Publisher: | |
| Editors-in-Chief: | Aaron Johnson , Florian Kerschbaum |
| Journal & Submission Website: | https://content.sciendo.com/view/journals/popets/popets-overview.xml |

## Aims & Scope of the Journal

Proceedings on Privacy Enhancing Technologies publishes original research contributions in the arena of Computer Security and Cryptography. The journal is intended for professors, practitioners and scientists who are focused on such areas of scientific research. Proceedings on Privacy Enhancing Technologies publishes novel scholarly contributions which undergo peer review by experts in the field. The journal welcomes submissions from the research community where the priority will be on the innovativeness and the practical importance of the reported findings.
Proceedings on Privacy Enhancing Technologies is covered by many abstracting/indexing services including Scopus, Journal Citation Reports ( Clarivate ) and Research.com. Many prominent scientists considered this journal to publish their scholarly documents including Ian Goldberg, Ian Goldberg, Arvind Narayanan, Nicholas Hopper and Arvind Narayanan.

For extra details on the rules and submission provisions for authors, please see the official website for the journal for Proceedings on Privacy Enhancing Technologies at https://content.sciendo.com/view/journals/popets/popets-overview.xml .

# ACM Transactions on Embedded Computing Systems

Research Impact Score*

**1.4**

OFFICIAL WEBSITE

## Ranking & Metrics

| | |
|---|---|
| Research Impact Score*: | 1.4 |
| Impact Factor: | 2 |
| Citescore: | 4.5 |
| SCIMAGO SJR: | 0.796 |
| SCIMAGO H-index: | 61 |

| | |
|---|---|
| Research Ranking (Computer Science) | 152 |
| Research Ranking (Electronics and Electrical Engineering) | 151 |
| Research Ranking (Electronics and Electrical Engineering) | 303 |
| Research Ranking (Computer Science) | 248 |
| Number of Best scientists*: | 24 |
| Documents by best scientists*: | 31 |

## Journal Information

| | |
|---|---|
| ISSN: | 1539-9087 |
| Publisher: | Association for Computing Machinery |
| Periodicity: | Quarterly |
| Editors-in-Chief: | Tulika Mitra |
| Journal & Submission Website: | https://dl.acm.org/journal/tecs |

# IEEE 5th IEEE International Conference on Blockchain and Cryptocurrency

Research Impact Score
**1.60**

- Dubai, United Arab Emirates
- Submission Deadline: **Sunday 04 Dec 2022**
- Conference Dates: **May 01, 2023 - May 05, 2023**

OFFICIAL WEBSITE

Conference Organizers: Deadline extended?
Click here to edit

## Ranking & Metrics

| | | | |
|---|---|---|---|
| Research Impact Score: | 1.60 | Papers published by Best Scientists | 33 |
| Contributing Best Scientists: | 24 | Research Ranking (Computer Science) | 460 |
| H5-index: | | Research Ranking (Computer Science) | 334 |

## Conference Call for Papers

ICBC 2023 will be the 5th edition of the IEEE International Conference on Blockchain and Cryptocurrency, sponsored by the IEEE Communications Society. ICBC 2023 is seeking submissions of technical papers (both full and short), posters, and tutorial proposals in the following areas related to Blockchains and Cryptocurrencies as well as emerging areas of Blockchains.

Distributed Consensus

Fault Tolerance Algorithms

Performance and Scalability Issues

Distributed Database Technologies for Blockchains

Blockchain Platforms

Blockchain-based Applications and Services

Decentralized App Development

Smart Contracts and Verification

Security, Privacy, Attacks, and Forensics

Transaction Monitoring and Analysis

Token Economy

Novel Mechanisms for the Creation, Custody, and Exchange of Crypto-Assets

Anonymity and Criminal Activities of/with Cryptocurrencies

Managing Risks of Cryptocurrencies

Distributed Trust

Decentralized Internet Infrastructure

Decentralized Financial Services (DeFi)

Blockchains for Internet of Things

Blockchains for Cyber Physical Services

Blockchain and Machine Learning/Artificial Intelligence

# Exhibit 19

Proof of 68 scientific reviews undertaken by Dr. Nikitin in conferences and journals on data privacy, computer security, and blockchain

- (32 reviews) The ACM Conference on Computer and Communications Security (CCS)
  - The invitation to join the Program Committee of the conference in year 2024, a submission page that lists 8 reviews by Dr. Nikitin in Cycles A and B of the conference, and copies of the submitted reviews.
  - The invitation to join the Program Committee of the conference in year 2023, a submission page that lists 6 reviews by Dr. Nikitin, and copies of the submitted reviews.
  - The invitation to join the Program Committee of the conference in year 2021, a submission page that lists 17 reviews by Dr. Nikitin, and copies of the submitted reviews.
  - The invitation to provide an expert review for an additional submission to ACM CSS 2021, and a copy of the review submitted by Dr. Nikitin.
- (16 reviews) The invitation to join the Program Committee of the USENIX Security Symposium in year 2025, a submission page that lists 8 reviews in Cycle 1 and 4 reviews in Cycle 2 by Dr. Nikitin, and copies of the submitted reviews.
- (1 review) The invitation to provide an expert review for Eurocrypt 2022, and a copy of the review submitted by Dr. Nikitin.
- (6 reviews) The invitation to join the Program Committee of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC) in year 2019, a submission page that lists 6 reviews by Dr. Nikitin, and copies of the submitted reviews.
- (1 review) The invitation to provide an expert review for a submission to the IEEE Transactions on Industrial Informatics (TII), and a confirmation of the review submitted by Dr. Nikitin.
- (2 reviews) Two invitations to provide an expert review for submissions to the IEEE Transactions on Parallel and Distributed Systems (TPDS) and copies of the reviews submitted by Dr. Nikitin.
- (2 reviews) The invitations to provide an expert review for a submission to the International Conference on Research in Computational Molecular Biology (RECOMB), and copies of the reviews submitted by Dr. Nikitin.

- (1 review) The invitation to provide an expert review for a submission to the Annual International Conference on Intelligent Systems for Molecular Biology (ISMB), and a copy of the review submitted by Dr. Nikitin.
- (5 reviews) The invitations to join the Program Committee of the Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock) in the years 2019 and 2020, the submission pages that list the reviews by Dr. Nikitin and copies of the reviews.
- (2 reviews) The invitation to join the Program Committee of the International Conference on Blockchain and Trustworthy Systems (BlockSys) in the year 2019, a submission page that lists 2 reviews by Dr. Nikitin, and copies of the submitted reviews.

# Exhibit 20

Proof of Dr. Nikitin's membership in the Association for Computing Machinery (ACM) and in the Institute of Electrical and Electronics Engineers (IEEE)

# Exhibit 21

Evidence that Dr. Nikitin co-organized The Satellite Conference on Biomedical Data Privacy and Equity (RECOMB-PRIEQ 2024). Dr. Nikitin's name appears at the top of the Program Committee list with the track chair role.

# Exhibit 22

Evidence of published material about Dr. Nikitin's work in professional and major trade publications:

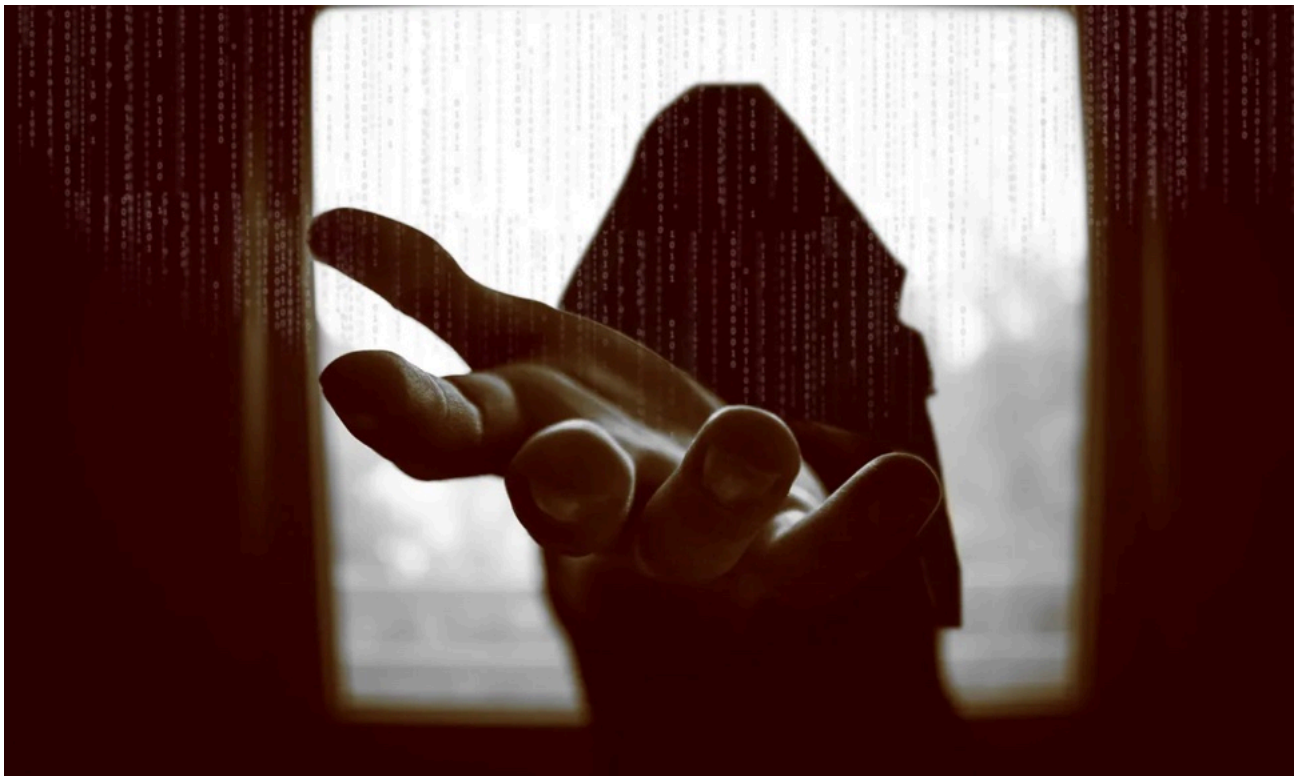
- An article published by ZDNET on Padded Uniform Random Blobs, Dr. Nikitin's inventions for protection of encryption metadata.
- Statistics by semrush.com on the readership of ZDNET.
- A Wikipedia article about the same invention, which provides more in-depth overview of techniques and their applications.
- An article published by CyberScoop on Dr. Nikitin's work on security of software-update systems.
- An article published by The 311 Institute on Dr. Nikitin's work on security of software-update systems.
- An excerpt from Google Scholar listing the prominent scientific surveys that review Dr. Nikitin's work on securing IoT group communication.
- A post in the popular computer science blog "The Morning Paper" that covers Dr. Nikitin's work on securing software-update systems.

# PGP encryption won't protect your data. But PURBs can.

**You may think that encrypting your sensitive files with, say, PGP may protect your data - but you'd be wrong. Most encryption formats leak a lot of plaintext metadata, and that's a problem. Here's what you need to know.**

Written by **Robin Harris,** Contributor

June 25, 2018 at 5:51 a.m. PT



Getty Images/iStockphoto

**/ special feature**

**Cyberwar and the Future of Cybersecurity**

Today's security threats have expanded in scope and seriousness. There can now be millions -- or even billions -- of dollars at risk when information security isn't handled properly.

**Read now** →

Most encrypted data formats have plaintext headers, because, how the heck are you supposed to know anything about the encrypted file - such as which encryption tool protected it - without *some* plaintext info? But this creates a serious security problem.

The plaintext may reveal how many recipients can decrypt the data, and possibly their identities. Info about the encryption software configuration and version level can be used to fingerprint a specific endpoint, facilitating targeted attacks against system weaknesses.

In a network environment - and we're all networked today - a digital fingerprint can facilitate traffic analysis, videos watched, geo-location, social networks, language, password length, and even if you are using TOR.

OK, plaintext metadata can be a security risk. But how far can plaintext metadata be reduced before no one can access it?

#### PURBs

Pretty far, according to researchers at the Swiss ETF in Lausanne. In a new paper, Reducing Metadata Leakage from Encrypted Files and Communication with PURBs, they propose an encrypted format similar to PGP that minimizes file length and metadata leakage. They call it *Padded Uniform Random Blobs.*

> **A PURB is indistinguishable from a uniform random bit-string to an observer without a decryption key. Legitimate recipients can efficiently decrypt the PURB even when it is encrypted for any number of recipients' public keys and/or passwords, and when those public keys are of different cryptographic schemes.**

#### How does it work?

A PURB is a file or message whose content and metadata are contained in an encrypted blob that is padded to a standard set of sizes. With a given size, the PURBs are cryptographically indistinguishable from each other, and do not leak the encryption scheme, who or how many recipients can decrypt it, file sizes, or what software created it.

#### Making it work

There are two main challenges to overcome in designing PURBs. First, there's the problem of allowing any number of recipients to use different cryptographic keys, perhaps from several different cipher suites, to get the info they need to decrypt the PURB.

PURBs solve this by encrypting content with one algorithm, and then adding a variable length encrypted header containing metadata for recipients. The header contains multiple entry points, so users with different decryption tools can read the header and get the data they need to access the content.

/ security

**Cyber security 101: Protect your privacy from hackers, spies, and the government**

Simple steps can make the difference between losing your online accounts or maintaining what is now a precious commodity: Your privacy.

**Read now** →

The second challenge is reducing the leakage of information about the length of the file. The proposed padding scheme groups files in sets of logarithmically increasing sizes, and leaks much fewer bits than padding to a fixed block size.

**How well does it work?**

In their testing, the researchers found that encrypting a PURB for 100 recipients, using 10 different enciphering tools, took less than half a second on a 3.1 Ghz laptop. Decoding performance is comparable to PGP.

Of course, the bigger issue is how well does it hide file lengths, since that single number can easily identify many kinds of objects, from YouTube videos to software packages. They found that, for example, PURBs reduced the percentage of uniquely identifiable videos from 87 to 3 percent, while adding less than 12 percent space overhead.

**The Storage Bits take**

In a world with billion dollar criminal hacker rings, and massive state-supported hacking cadres, nobody's data is safe. It's easy for civilians to underestimate the ways in which their data can be compromised by clever and determined hackers.

PURB is not a commercial product, but as research it points the way for rearchitecting encryption suites to dramatically improve security. Let's hope that vendors are taking note.

**RELATED AND PREVIOUS CONTENT:**

**Uninstall PGP: EFF warns of exploit that may reveal plaintext of encrypted emails**

**European researchers claim to have found a vulnerability that could reveal plaintext of encrypted emails, including those in the past.**

**IBM warns of instant breaking of encryption by quantum computers: 'Move your data today'**

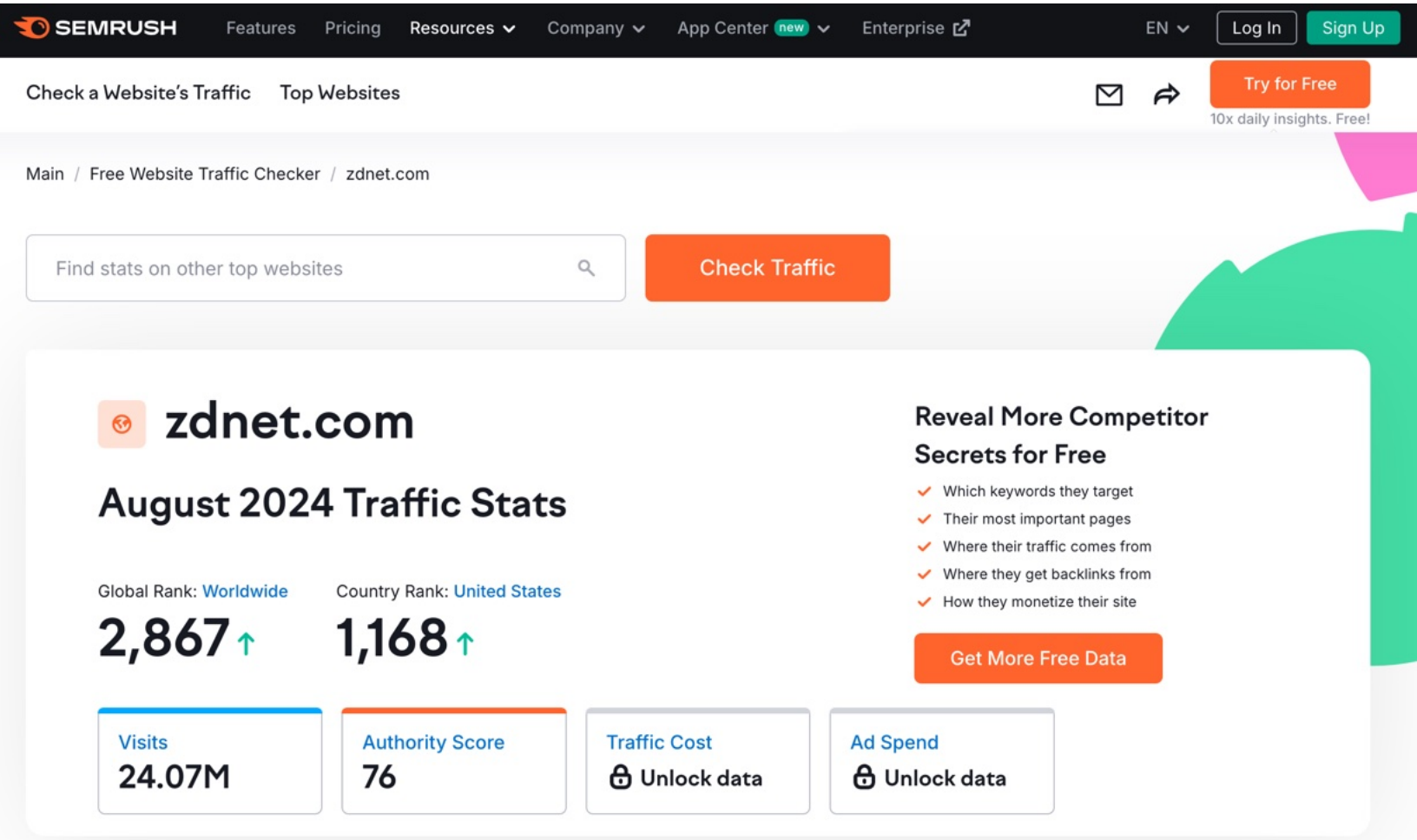
**Welcome to the future transparency of today as quantum computers reveal all currently encrypted secrets -- a viable scenario within just a few years.**

**MIT engineers crack IoT encryption problem with ultra-efficient chip**

**IoT's limited capabilities have caused issues for security, but perhaps, no more.**

**Courteous comments welcome, of course.**

Editorial standards


SEMRUSH
Features
Pricing
Resources
Company
App Center new
Enterprise
EN
Log In
Sign Up
Check a Website's Traffic
Top Websites
Try for Free
10x daily insights. Free!
Main / Free Website Traffic Checker / zdnet.com
Find stats on other top websites
Check Traffic
zdnet.com
August 2024 Traffic Stats
Global Rank: Worldwide
2,867
Country Rank: United States
1,168
Visits
24.07M
Authority Score
76
Traffic Cost
Unlock data
Ad Spend
Unlock data
Reveal More Competitor Secrets for Free
Which keywords they target
Their most important pages
Where their traffic comes from
Where they get backlinks from
How they monetize their site
Get More Free Data

# PURB (cryptography)

In cryptography, a **padded uniform random blob** or **PURB** is a discipline for encrypted data formats designed to minimize unintended information leakage either from its encryption format metadata or from its total length.[1]

## Properties of PURBs

When properly created, a PURB's content is indistinguishable from a uniform random bit string to any observer without a relevant decryption key. A PURB therefore leaks *no* information through headers or other cleartext metadata associated with the encrypted data format. This leakage minimization "hygiene" practice contrasts with traditional encrypted data formats such as Pretty Good Privacy, which include cleartext metadata encoding information such as the application that created the data, the data format version, the number of recipients the data is encrypted for, the identities or public keys of the recipients, and the ciphers or suites that were used to encrypt the data. While such encryption metadata was considered non-sensitive when these encrypted formats were designed, modern attack techniques have found numerous ways to employ such incidentally-leaked metadata in facilitating attacks, such as by identifying data encrypted with weak ciphers or obsolete algorithms, fingerprinting applications to track users or identify software versions with known vulnerabilities, or traffic analysis techniques such as identifying all users, groups, and associated public keys involved in a conversation from an encrypted message observed between only two of them.

In addition, a PURB is padded to a constrained set of possible lengths, in order to minimize the amount of information the encrypted data could potentially leak to observers via its total length. Without padding, encrypted objects such as files or bit strings up to $M$ bits in length can leak up to $O(\log M)$ bits of information to an observer - namely the number of bits required to represent the length exactly. A PURB is padded to a length representable in a floating point number whose mantissa is no longer (i.e., contains no more significant bits) than its exponent. This constraint limits the maximum amount of information a PURB's total length can leak to $O(\log \log M)$ bits, a significant asymptotic reduction and the best achievable in general for variable-length encrypted formats whose multiplicative overhead is limited to a constant factor of the unpadded payload size. This asymptotic leakage is the same as one would obtain by padding encrypted objects to a power of some base, such as to a power of two. Allowing some significant mantissa bits in the length's representation rather than just an exponent, however, significantly reduces the overhead of padding. For example, padding to the next power of two can impose up to 100% overhead by nearly doubling the object's size, while a PURB's padding imposes overhead of at most 12% for small strings and decreasing gradually (to 6%, 3%, etc.) as objects get larger.

Experimental evidence indicate that on data sets comprising objects such as files, software packages, and online videos, leaving objects unpadded or padding to a constant block size often leaves them uniquely identifiable by total length alone.[2][3][1] Padding objects to a power of two or to a PURB length, in contrast, ensures that most objects are indistinguishable from at least some other objects and thus have a nontrivial *anonymity set*.[1]

## Encoding and decoding PURBs

Because a PURB is a discipline for designing encrypted formats and not a particular encrypted format, there is no single prescribed method for encoding or decoding PURBs. Applications may use any encryption and encoding scheme provided it produces a bit string that appears uniformly random to an observer without an appropriate key, provided the appropriate hardness assumptions are satisfied of course, and provided the PURB is padded to one of the allowed lengths. Correctly-encoded PURBs therefore *do not identify the application that created them* in their ciphertext. A decoding application, therefore, cannot readily tell before decryption whether a PURB was encrypted for that application or its user, other than by trying to decrypt it with any available decryption keys.

Encoding and decoding a PURB presents technical efficiency challenges, in that traditional parsing techniques are not applicable because a PURB by definition has no metadata *markers* that a traditional parser could use to discern the PURB's structure before decrypting it. Instead, a PURB must be *decrypted first* obliviously to its internal structure, and then parsed only after the decoder has used an appropriate decryption key to find a suitable cryptographic *entrypoint* into the PURB.

Encoding and decoding PURBs intended to be decrypted by several different recipients, public keys, and/or ciphers presents the additional technical challenge that each recipient must find a different entrypoint at a distinct location in the PURB non-overlapping with those of the other recipients, but the PURB presents no cleartext metadata indicating the positions of those entrypoints or even the total number of them. The paper that proposed PURBs[1] also included algorithms for encrypting objects to multiple recipients using multiple cipher suites. With these algorithms, recipients can find their respective entrypoints into the PURB with only a logarithmic number of *trial decryptions* using symmetric-key cryptography and only one expensive public-key operation per cipher suite.

A third technical challenge is representing the public-key cryptographic material that needs to be encoded into each entrypoint in a PURB, such as the ephemeral Diffie-Hellman public key a recipient needs to derive the shared secret, in an encoding indistinguishable from uniformly random bits. Because the standard encodings of elliptic-curve points are readily distinguishable from random bits, for example, special *indistinguishable* encoding algorithms must be used for this purpose, such as Elligator[4] and its successors.[5][6]

## Tradeoffs and limitations

The primary privacy advantage that PURBs offer is a strong assurance that correctly-encrypted data leaks nothing incidental via internal metadata that observers might readily use to identify weaknesses in the data or software used to produce it, or to fingerprint the application or user that

created the PURB. This privacy advantage can translate into a security benefit for data encrypted with weak or obsolete ciphers, or by software with known vulnerabilities that an attacker might exploit based on trivially-observable information gleaned from cleartext metadata.

A primary disadvantage of the PURB encryption discipline is the complexity of encoding and decoding, because the decoder cannot rely on conventional parsing techniques before decryption. A secondary disadvantage is the overhead that padding adds, although the padding scheme proposed for PURBs incurs at most only a few percent overhead for objects of significant size.

The Padme padding proposed in the PURB paper only creates files of specific very distinct sizes. Thus, an encrypted file may often be identified as PURB encrypted with high confidence, as the probability of any other file having exactly one of those padded sizes is very low. Another padding problem occurs with very short messages, where the padding does not effectively hide the size of the content.

One critique of incurring the complexity and overhead costs of PURB encryption is that the *context* in which a PURB is stored or transmitted may often leak metadata about the encrypted content anyway, and such metadata is outside of the encryption format's purview or control and thus cannot be addressed by the encryption format alone. For example, an application's or user's choice of filename and directory in which to store a PURB on disk may indicate allow an observer to infer the application that likely created it and to what purpose, even if the PURB's data content itself does not. Similarly, encrypting an E-mail's body as a PURB instead of with traditional PGP or S/MIME format may eliminate the encryption format's metadata leakage, but cannot prevent information leakage from the cleartext E-mail headers, or from the endpoint hosts and E-mail servers involved in the exchange. Nevertheless, separate but complementary disciplines are typically available to limit such contextual metadata leakage, such as appropriate file naming conventions or use of pseudonymous E-mail addresses for sensitive communications.

# References


1. Nikitin, Kirill; Barman, Ludovic; Lueks, Wouter; Underwood, Matthew; Hubaux, Jean-Pierre; Ford, Bryan (2019). "Reducing Metadata Leakage from Encrypted Files and Communication with PURBs" (https://petsymposium.org/2019/files/papers/issue4/popets-2019-0056.pdf) (PDF). *Proceedings on Privacy Enhancing Technologies (PoPETS)*. **2019** (4): 6–33. arXiv:1806.03160 (https://arxiv.org/abs/1806.03160). doi:10.2478/popets-2019-0056 (https://doi.org/10.2478%2Fpopets-2019-0056). S2CID 47011059 (https://api.semanticscholar.org/CorpusID:47011059).
2. Hintz, Andrew (April 2002). *Fingerprinting Websites Using Traffic Analysis*. International Workshop on Privacy Enhancing Technologies. doi:10.1007/3-540-36467-6_13 (https://doi.org/10.1007%2F3-540-36467-6_13).
3. Sun, Qixiang; Simon, D.R.; Wang, Yi-Min; Russell, W.; Padmanabhan, V.N.; Qiu, Lili (May 2002). *Statistical Identification of Encrypted Web Browsing Traffic*. IEEE Symposium on Security and Privacy. doi:10.1109/SECPRI.2002.1004359 (https://doi.org/10.1109%2FSECPRI.2002.1004359).
4. Bernstein, Daniel J.; Hamburg, Mike; Krasnova, Anna; Lange, Tanja (November 2013). *Elligator: Elliptic-curve points indistinguishable from uniform random strings* (https://dl.acm.org/citation.cfm?id=2516734). Computer Communications Security (https://dl.acm.org/citation.cfm?id=2508859).

5. Tibouchi, Mehdi (March 2014). *Elligator Squared: Uniform Points on Elliptic Curves of Prime Order as Uniform Random Strings* (https://www.ifca.ai/fc14/papers/fc14_submission_25.pdf) (PDF). Financial Cryptography and Data Security (https://www.ifca.ai/fc14/index.html).
6. Aranha, Diego F.; Fouque, Pierre-Alain; Qian, Chen; Tibouchi, Mehdi; Zapalowicz, Jean-Christophe (August 2014). *Binary Elligator Squared* (https://eprint.iacr.org/2014/486.pdf) (PDF). International Conference on Selected Areas in Cryptography.

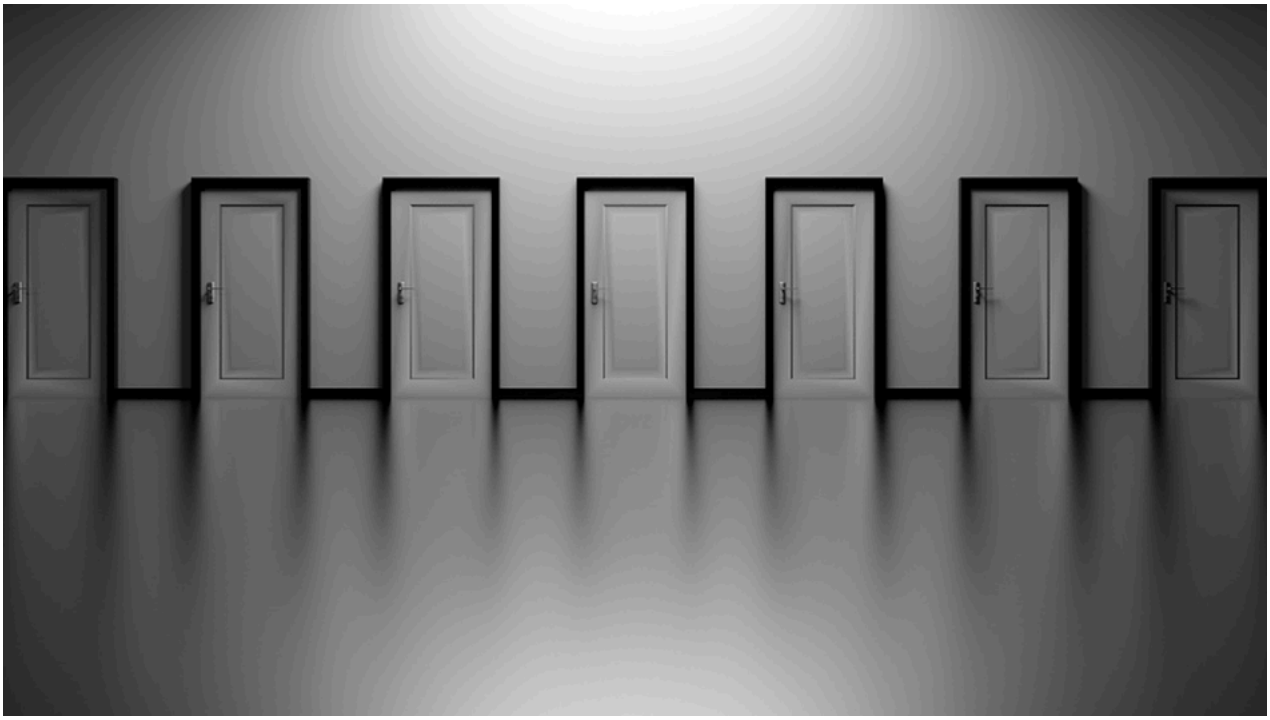
---

GOVERNMENT

# New tool can help prevent government-mandated backdoors in software, Swiss researchers say

The framework, dubbed "Chainiac," makes it extremely difficult for governments to force vulnerabilities into the software supply chain.

BY J.M PORUP • JULY 25, 2017



By: qimono -- via CC0



A new framework from a lab in Switzerland could help prevent malware like Petya from spreading, but would also make it difficult — if not impossible — for governments to force software companies to deliver backdoored software updates in secret.

The Petya ransomware, and its wiperware variant NotPetya, spread on the wings of a software update unwittingly issued by Ukrainian accounting software company M.E. Doc. An attacker, who many believe to be agents of the Russian government, owned M.E. Doc's network and injected malicious code into a legitimate software update.

This new proof-of-concept technology, dubbed "Chainiac" by the Decentralized/Distributed Systems (DEDIS) lab at the Swiss Federal Institute of Technology in Lausanne (EPFL), offers a decentralized framework that eliminates such single points of failure and enforces transparency, making it possible for security analysts to continuously review updates for potential vulnerabilities.

"What Chainiac is trying to do," Bryan Ford, leader of the group that conducted the research, told CyberScoop, "is create an end-to-end architecture for software life cycle management, all the way from the developers to deployment and updates on end-user devices."

As criminals and nation-states attack the software supply chain, it becomes increasingly important to ensure the integrity of the software used by the public.

Documents released by NSA whistleblower Edward Snowden revealed that as early as 2011, the NSA was looking at how to compromise the Google Play Store (then called the "Android Store") in order to replace legitimate smartphone apps with backdoored versions to spy on users or even manipulate them with targeted propaganda.

In the U.K., the government may now legally compel software makers to backdoor their code using secret court orders, as part of the Investigatory Powers Act, which came into force in January of this year. Other nations around the world are engaged in similar practices.

"How do we know what software we are really running?" Emin Gün Sirer, associate professor at Cornell University and co-director of the Initiative for Cryptocurrencies and Smart Contracts, told CyberScoop. "A lot of attacks go after that exact foundation. Someone switches the binaries you're using but everything appears to be the same."

---

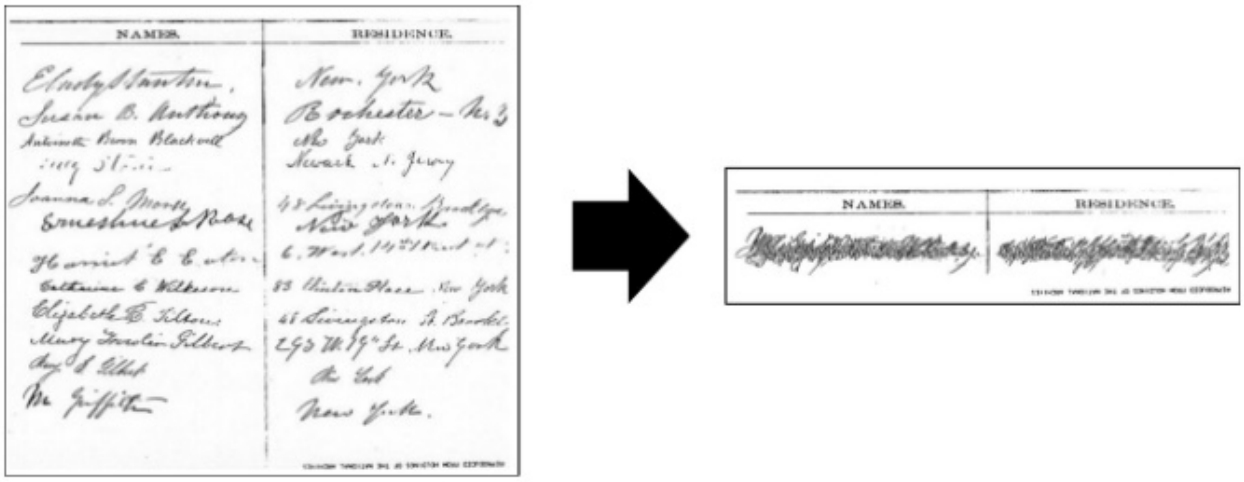
*"How do we know what software we are really running?"*

---

Chainiac builds on Cothority, a transparency tool Ford's team released after the 2015 San Bernardino shooting that enables collective signing of software updates by independent

witnesses.

Collective signing means that each time Apple, for example, released a new iOS update — for all users, for a targeted individual or for a group, perhaps as the result of a secret court order — the iOS device would not accept the update unless the code had been collectively signed by a threshold number of thousands of trusted witnesses attesting publicly that an update had been issued.




What an old-fashioned multi-signature would look like in Chainiac/Cothority

A collectively-signed software update might still contain backdoored code — developers could be bribed, blackmailed, or threatened to insert a backdoor — but Cothority, a component of Chainiac, would make it impossible to ship the update in secret.

Chainiac also integrates reproducible builds, a system which lets technical end users, or automated witness servers, to recompile the source code and get a byte-for-byte identical binary, ensuring the distributed binaries have not been tampered with.

“The essence of the idea is that [Chainiac] allows users, who just want the latest binary, to check this one collective signature,” Ford said, “and see that this signature shows that this group of Cothority servers has independently reproduced this binary, and tested that this is the one and only correct output corresponding to the source code that the developer has produced.”

The Debian Project has already deployed reproducible builds for 94 percent of the tens of thousands of software packages that make up that Linux distribution, which is widely used on cloud servers and embedded devices, plus its downstream variant Ubuntu. Ford’s team tested Chainiac on Debian packages with good results, and Debian seems likely to be an early adopter of the transparency tool.

Proprietary software, such as Apple's iOS or Microsoft's Windows, could also use Chainiac to achieve similar levels of transparency, Ford emphasized. "In that case the Cothority nodes responsible for checking the reproducible builds need to be run by … organizations that have NDAs with the software provider giving them access to the source code for this purpose."

"That makes it at least in principle feasible for proprietary software," he added.

The project also incorporates a novel form of blockchain technology, called a "skipchain." Software updates are announced on a distributed ledger.

"Blockchains are used to transfer things, but that's not their only use," Sirer said. "They're great for transferring things like Bitcoin, but they're also great for announcing facts. … [Chainiac] is a broadcast medium for vetting software updates."

Ford's research seems unlikely to please government leaders frustrated at the growing use of encryption, including the prime minister of Australia, Malcolm Turnbull, whose recent comments that the laws of Australia trump the laws of mathematics were widely mocked within the technical community.

Chainiac is the latest salvo in an increasingly bitter war between software makers and governments for control of the code on which our lives depend. Nation-states wanting to subvert the software development process for law enforcement or espionage purposes will look for ways to counter transparency mechanisms like Chainiac, sources speculated.

"We've seen sovereign states put enormous resources into hacking," Sirer said. "Will [Chainiac] be open to gaming? Will it be more secure or open to attack?… There is every reason for hope and every reason for experimentation."

Cryptographers have been vocal against government use of backdoored software updates, arguing that destroying trust in software updates makes everyone less safe. A few weeks ago cryptographer Matthew Green of Johns Hopkins University blasted the practice on Twitter.


Security expert Bruce Schneier, a fellow at the Berkman Klein Center at Harvard University, said it is never acceptable for governments to use backdoored software updates.

"It is akin to a public health issue," he told CyberScoop in an email. "We need everyone to trust the update process implicitly — that it will always work in the best interests of the user."

"Hijacking that process for surveillance purposes," he added, "threatens to undermine trust in one of the critical security technologies we need."

---


## Written by J.M Porup

J.M Porup J.M Porup j-m-porup 50627
jmporup@scoopnewsgroup.com


## In This Story

FEDERAL IT SURVEILLANCE ENCRYPTION

NATIONAL SECURITY AGENCY (NSA) INTELLIGENCE COMMUNITY (IC)

# BLOCKCHAIN EXPERTS ARE PUTTIN A STOP TO GOVERNMENTS PUTTIN BACKDOORS IN SOFTWARE


By Matthew Griffin

Security and Privacy

27th August 2017



WHY THIS MATTERS IN BRIEF

- Governments want backdoors in software and criminals want to exploit them to spread malware, now a blockchain based system from Switzerland could put a stop to both

A new blockchain based software update framework from the team at the Decentralized-Distributed Systems (DEDIS) lab at the Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland could help prevent the spread of malware like Petya, but, as an added bonus it would also make it difficult, if not impossible, for governments to force software companies to deliver software updates with backdoors in them in secret.

The Petya ransomware, and its "wiperware" variant NotPetya, were both spread after an attacker managed to take over the network of Ukrainian accounting firm, M.E. Doc, and inject malicious code into one of their legitimate software updates.

The new proof-of-concept technology, which has been dubbed "Chainiac" by its team is a first of a kind decentralised framework that eliminates these single points of failure and enforces a new level of transparency on software updates which, in turn, makes it possible for security analysts and other interested individuals to continuously review and monitor the authenticity of updates and identify vulnerabilities.

"What Chainiac is trying to do," said Bryan Ford who led the group that conducted the research, "is create an end-to-end architecture for software life cycle management, all the way from the developers to deployment and updates on end-user devices."

See also Unhackable quantum technologies debut in France

As criminals and nation states continue to increase their attacks on the software supply ch it's going to become increasingly important that we can ensure the integrity of the software we all use, and rely on. After all, I doubt you'll want to download a version of Apple's next iOS update only to then find the NSA, or someone else is watching you via your webcam.

Wave and say hi, now go and get the sticky tape and shove it over the lens – who says beating the government isn't easy? For example, documents released by NSA whistleblower Edward Snowden revealed that in 2011, the NSA was looking at how to compromise the Google Play Store in order to replace legitimate smartphone apps with backdoor versions they could use to spy on users or even manipulate them with targeted propaganda. And over in the UK, under the Investigatory Powers Act, which came into force in January this year, the government's currently considering passing a law that will legally compel software makers to build backdoors into their software using secret court orders – and other nations are following suit.

See also Autonomous AI could create an autonomous

“How do we know what software we are really running?” said Emin Gün Sirer, associate professor at Cornell University and co-director of the Initiative for Cryptocurrencies and Smart Contracts, “a lot of attacks go after that exact foundation. Someone switches the binaries you’re using but everything appears to be the same.”

Chainiac builds on Cothority, a blockchain based transparency tool Ford’s team released in 2015 that allows independent individuals and experts to collectively sign off on the authenticity of software updates.

Collective signing means that every time Apple, for example, releases a new iOS update the iOS device won’t accept the update until it’s been collectively signed and verified by a threshold number of thousands of trusted witnesses attesting publicly that a valid, non-backdoored update had been issued.

See also The internet pioneer behind Apache pushes blockchain to fuel the next big internet revolution

However, while a collectively signed software updates could still contain backdoored code, example, developers could be bribed, blackmailed, or threatened to insert a backdoor, Cothority, now a component of Chainiac, would make it impossible to ship the update in secret. Chainiac also integrates reproducible builds, a system which lets technical end users, or automated witness servers, to recompile the source code and get a byte-for-byte identical binary, ensuring the distributed binaries haven’t been tampered with.

“The essence of the idea is that [Chainiac] allows users, who just want the latest binary, to check this one collective signature,” Ford said, “and see that this signature shows that this group of Cothority servers has independently reproduced this binary, and tested that this is the one and only correct output corresponding to the source code that the developer has produced.”

See also Apple iMessage has been upgraded with post quantum encryption

cloud servers and embedded devices, plus its downstream variant Ubuntu. Ford's team tested Chainiac on Debian packages with good results, and Debian seems like they could be an early adopter.

Meanwhile, proprietary software, such as Apple's iOS or Microsoft's Windows, could also use Chainiac to achieve similar levels of transparency, Ford emphasized.

"In that case the Cothority nodes responsible for checking the reproducible builds need to be run by organisations that have NDAs with the software provider giving them access to the source code for this purpose. That makes it at least in principle feasible for proprietary software," he added.

See also First fake regulatory filing sent Blackrock's XRP crypto to the moon

The project also incorporates a novel form of blockchain technology, called a "Skipchain," t allows software updates to be announced on a distributed ledger.

"Blockchains are used to transfer things, but that's not their only use," Sirer said, "they're gre for transferring things like Bitcoin, but they're also great for announcing facts. … [Chainiac] also a broadcast medium for vetting software updates."

Ford's research seems unlikely to please government leaders who are increasingly frustrated at the growing use of encryption, as well as the upcoming 5G standard, and how it cuts off their ability in some ways, but not completely, to surveil people.

See also A dead gradma story fooled Bing chat into helping solve a CAPTCHA

If you're a government type though put down those tissues, and stop wiping your eyes, because, thanks to Quantum Computers, you'll soon be able to crack over 70 percent of all the encryption

Chainiac is the latest salvo in an increasingly bitter war between software makers and governments for control of the integrity of the code on which our lives depend, and it's also likely that nation states who want to subvert the software development process for law enforcement or espionage purposes are already looking for new ways to undermine these new "transparency mechanisms."

See also Self-destructing algorithms could usher in a new era of cyber security

"We've seen sovereign states put enormous resources into hacking," Sirer said, "will [Chain' be open to gaming? Will it be more secure or open to attack? There is every reason for hope a..d every reason for experimentation."

Cryptographers have been vocal against government use of backdoored software updates, arguing that destroying trust in software updates makes everyone less safe, and security e Bruce Schneier, a fellow at the Berkman Klein Center at Harvard University, said it is never acceptable for governments to use backdoored software updates.

"It is akin to a public health issue," he said, "we need everyone to be able to trust the update process implicitly, and that it will always work in the best interests of the user. Hijacking th process for surveillance or espionage purposes threatens to undermine trust in one of the r critical security technologies we need and all rely on."

Backdoors Blockchain Cyber Security Debian Project Linux Foundation M.E. Doc Malware NSA Public Sector Ransomware Security Software Updates Swiss Federal Institute of Technology Switzerland Technology Sector

Google Scholar

Articles

About 40 results (**0.04** sec)

Any time
Since 2024
Since 2023
Since 2020
Custom range...

Sort by relevance
Sort by date

Create alert

## Axiom: DTLS-based secure IoT group communication

Search within citing articles

**[HTML]** IoT-based enterprise resource planning: Challenges, open issues, applications, architecture, and future research directions — **[HTML]** sciencedirect.com

M Tavana, V Hajipour, S Oveisi - Internet of Things, 2020 - Elsevier

In today's highly competitive markets, organizations can create a competitive advantage through the successful implementation of Enterprise Resource Planning (ERP) systems …

☆ Save  Cite  Cited by 144  Related articles  All 2 versions

**[HTML]** Systematic review of internet of things security — **[HTML]** proquest.com

A Amiruddin, AAP Ratna… - International Journal of …, 2019 - search.proquest.com

Abstract The Internet of Things has become a new paradigm of current communications technology that requires a deeper overview to map its application domains, advantages, and …

☆ Save  Cite  Cited by 18  Related articles  All 2 versions

**[PDF]** Cyber Secure Framework for Smart Containers Based on Novel Hybrid DTLS Protocol. — **[PDF]** techscience.cn

WU Khan, SNK Marwat, S Ahmed - Computer Systems Science …, 2022 - cdn.techscience.cn

The Internet of Things (IoTs) is apace growing, billions of IoT devices are connected to the Internet which communicate and exchange data among each other. Applications of IoT can …

☆ Save  Cite  Cited by 11  Related articles  All 2 versions  »

## Security architecture for secure multicast coap applications

CS Park - IEEE Internet of Things Journal, 2020 - ieeexplore.ieee.org

Multicast communication has been recently supported by the constrained application protocol (CoAP), for the purpose of managing and controlling a group of homogeneous …

☆ Save  Cite  Cited by 27  Related articles

# CHAINIAC: Proactive software update transparency via collectively signed skipchains and verified builds

OCTOBER 12, 2017 – ADRIAN COLYER

CHAINIAC: Proactive software-update transparency via collectively signed skipchains and verified builds Nikitin et al., *USENIX Security '17*

So hopefully you've put in place some kind of software supply chain management process that will pick up the availability of new package versions, particularly of course those with fixes for discovered vulnerabilities, and ensure those updates are propagated through your environment in a timely manner. But have you ever thought about this: with the advent of continual[1] delivery pipelines an attacker has a wonderful opportunity to inject a vulnerability anywhere upstream in your process (from the source code control system onwards) and have that picked up and handily deployed into your production systems for them. This is not just a theoretical risk. So you also need to think about *securing your software supply chain*.

> Software-update mechanisms are critical to the security of modern systems, but their typically centralized design presents a lucrative and frequently attacked target…

CHAINIAC addresses the challenge of securing package update managers – and it turns out to be quite a complex issue when you start digging into it. It's an important one though: what's the one command you probably always run and implicitly always trust: `apt-get upgrade` or its equivalent! Starting from a design typical of today's software update systems, the authors walk us through a seven-stage evolution to arrive at a more trustworthy design. Along the way we're going to learn about reproducible builds, collective signing and cothorities, and a new kind of blockchain-based structure called a *skipchain*. The end destination looks like this:

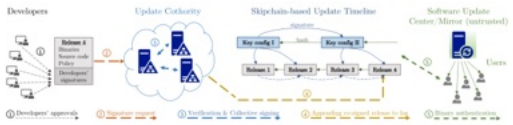



Figure 1: Architectural overview of CHAINIAC

CHAINIAC provides the following properties:

1. No single point of failure – the security guarantees still hold in the event that any single component (software or human) is compromised.
2. Source-to-binary affirmation (what you're running matches source code you can inspect)
3. Efficient release search and *verifiability*.
4. Linear immutable public release history.
5. Support for evolution of signing keys
6. Timely updates – clients can verify that the software really does correspond to the latest one available.

## The Starting Point

We begin with a system in which a single key pair is used to sign and verify software releases. The private key is most likely shared among a group of developers, and the public key is installed on client devices. To distribute a new release, one of the developers builds the source code, signs the resulting binary, and pushes it to a trusted software update centre. Users receive authenticated releases with minimal overhead.

> This design, though common, is rife with precarious assumptions. Expecting the signing key to be uncompromisable is unrealistic, especially if shared among multiple parties, as attackers need to subvert only a single developer's machine to retrieve the secret key or to coerce only one of the key owners. For similar reasons, it is utopian to assume that the software update center is trustworthy…

## Improvement #1: Decentralised release approval

Instead of using a single shared key to sign updates, each individual software developer signs using their own *individual keys*. Developer's public keys are collected in a policy file, together with a threshold value specifying the minimal number of valid signatures required to make a release valid.

> We assume that this policy file, as a trust anchor, is obtained securely by users at the initial acquisition of the software, e.g., it can reside on a project's website as often is the case with a single signing key in the current software model.

To make a release, developers check the *source code*, and if they approve, sign a hash of it with their individual keys. The source code plus signature list is pushed to the update center. Why source code instead of binaries? It's much easier to verify human-readable code (though still impractical for projects of any size I would argue!), and it is otherwise very hard to verify the mapping between a given set of source code, and a particular binary. We'll restore the convenience of binary updates in the following steps...

## Improvement #2: Pre-built binaries you can trust

Asking users to build binaries for themselves is a step backwards in usability. So the second improvement on our journey allows *developers* to build the binaries rather than end-users. After validating the source code, each developer compiles it using *reproducible build techniques*. If the result of a developer's build matches the announced binary, she or he signs the software release. A release now constitutes the source code, binary, and signatures packet.

> Reproducible builds are [sic] software development techniques that enable users to compile deterministically a given source code into one same binary, independent of factors such as system time or build machines. An ongoing collaboration of projects is dedicated to improving these techniques, e.g., Debian claims that 90% of its packages in the testing suite are reproducible...

You can find out more about at reproducible-builds.org.

## Improvement #3: Introducing cothority

As things now stand, every developer needs to perform a reproducible build, and client devices need to verify many developer signatures. It would be more convenient if a trusted third-party could take the developers' commitments, run the reproducible build, and produce a result easily verifiable by clients. But 'trusted third-party' is a red flag from a security perspective. So to maintain decentralisation, CHAINIAC implements the intermediary as a *collective authority*, aka., a *cothority*.

> CoSi is a protocol for large-scale collective signing. Aggregation techniques and communication trees enable CoSi to efficiently produce compact Schnorr multi-signatures and to scale to thousands of participants. A complete group of signers, or witnesses, is called a collective authority, or cothority.

Developers send the release data and their signatures to the cothority, which collectively validates and signs the release. Clients can download and validate the release source code and/or binary by verifying only a *single collective signature* and Merkle inclusion proofs for the components of interest.

These *verified builds* give clients the guarantee of source-to-binary correspondence without the resource-consuming building work (and also without needing to install the build toolchain on machines where you simply want to verify and apply updates).

## Improvement #4: Anti-equivocation

If a threshold number of developers *could* be coerced into creating a secret backdoored release used for targeted attacks, the protocol as described so far would still be vulnerable. We're talking about very determined or maybe even nation-state attackers at this point.

> In our next step towards CHAINIAC, we tackle the problem of such stealthy developer-equivocation, as well as the threat of an (untrusted) software-update center that accidentally or intentionally forgets parts of the software release history.

Step 4 adds *cothority-controlled hashchains* that create a *public history* of the releases for each software project. This blockchain includes a new block for each public release, and a (signed) new release include the Merkle root of the software's previous version. This makes it impossible for a group to sign a compromised release and keep it off the public record.

> This approach prevents attackers from secretly creating malicious updates targeted at specific users without being detected. It also prevents software update centers from

> "forgetting" old software releases, as everything is stored in a decentralized hash chain.

The collective signature for the new block corresponding to the release is created using the BFT-CoSi protocol introduced in ByzCoin. It implements PBFT using collective signing with two CoSi rounds for PBFT's prepare and commit phases.

## Improvement #5: Evolving keys

Key compromise is only a matter of time, so we're going to need the ability to rotate keys – ideally with different schedules for different witnesses. CHAINIAC adds another decentralised mechanism for trust delegation that enable evolution of keys.

> As a result, developers and cothorities can change, when necessary, their signing keys and create a moving target for an attacker, and the cothority becomes more robust to churn.

The trust delegation mechanism is implemented by a new derivative of a blockchain structure the authors call a *skipchain*. Each cothority configuration becomes a block in the skipchain, and when a new cothority configuration needs to be introduced the current cothority witnesses run BFT on it. (It's somewhat analogous to changing epochs in consensus protocols). To rotate developer keys, the project policy file is the root of trust. This is included in the Merkle tree of the release, and hence also protected by the hash chain.

A skipchain combines ideas from blockchains and skiplists, enabling clients to securely traverse the timeline in both *forward* and backward directions, and to efficiently traverse long distances in the chain using multi-hop links. Multi-hop link lengths can be determined randomly or deterministically. In both cases, skipchains enable logarithmic-cost timeline traversal.

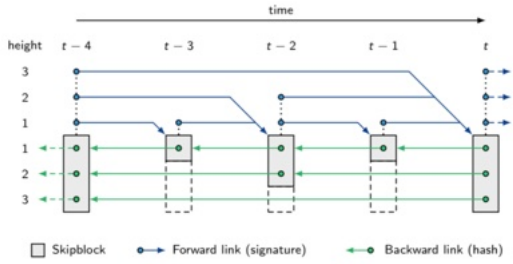



Figure 2: A deterministic skipchain $\mathcal{S}_2^3$

Now, how exactly do you put *forward* links (i.e., links to blocks that haven't been created yet), in a *immutable* data structure?

> Forward links are added retroactively to blocks in the log, as future blocks do not yet exist at the time of block creation. Furthermore, the forward links cannot be cryptographic hashes, as this would result in a circular dependency between the forward link of the current and the backward link of the next block. For these reasons, forward links are created as digital (multi-) signatures.

For more detail, see section 4.1 in the paper. The authors note that skipchains may have applications in several other domains requiring efficient timeline tracking.

## Improvement #6: Ensuring timeliness

> In addition to verifying and authenticating updates, a software-update system must ensure update timeliness, so that a client cannot unknowingly become a victim of freeze or replay attacks. To retain decentralization in CHAINIAC, we rely on the update authority to provide a timestamp service.

How this is done is kind of neat, with a multi-layer skipchain architecture in which the skipchains are interconnected via upward and downward links:

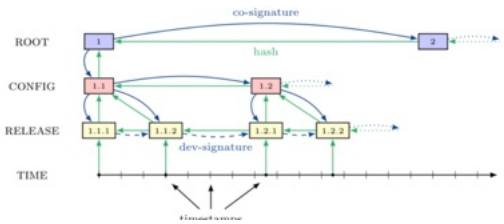


Figure 3: Trust delegation in CHAINIAC

The Root chain is CHAINIACs root of trust – the most security critical signing keys, kept offline. The Config chain holds the online keys of the update cothority, and is CHAINIACs control plane. The Release chain manages the release log as described so far, with the addition of upward links to the root and config chains.

The *time* chain provides a timestamp service that informs clients of the latest version of a package within a coarse-grained time interval (e.g., one hour).

> Every TIME block contains a wall-clock timestamp and a hash of the latest release.

### Improvement #7: Multi-package projects

The final enhancement makes support of multi-package projects more efficient, via an aggregate layer that pulls together all of the packages in a project into a single Merkle tree.

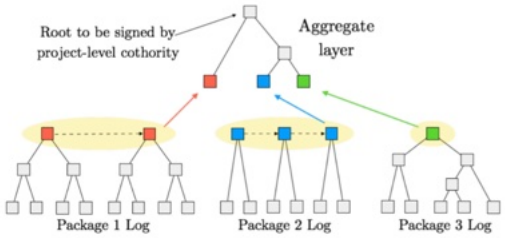



Figure 4: Constructing an aggregate layer in CHAINIAC

## Implementation

> We implemented CHAINIAC in Go and made it publicly available, along with instructions on how to reproduce the evaluation experiment. We built on existing open-source code implementing CoSi and BFT-CoSi. The new code implementing the CHAINIAC prototype was about 1.8kLOC, whereas skipchains, network communication, and BFT-CoSi were 1.2k, 1.5k, and 1.8k lines of code respectively. Although the implementation is not yet production quality, it is practical and usable for experimentation purposes.

1. That one's for you, @tastapod! ↩

POSTED IN UNCATEGORIZED

SECURITY

« PREVIOUS
*TrustBase: an architecture to repair and strengthen certificate-based authentication*

NEXT »
*BadNets: Identifying vulnerabilities in the machine learning model supply chain*

# Exhibit 23

## QS World University Rankings

The universities and their respective world rankings where Dr. Kirill Nikitin obtained his advanced degrees and conducted research activity as a postdoctoral scientist:

- The QS World University Rankings 2025: Top global universities.
  - Cornell University is ranked 16th (the university of Dr. Nikitin's first postdoctoral employment).
  - École polytechnique fédérale de Lausanne is ranked 26th (the university from which Dr. Nikitin obtained his Ph.D. degree).
  - Columbia University is ranked 34th (the university of Dr. Nikitin's current postdoctoral employment).
- The QS World University Rankings by Subject 2024: Engineering & Technology.
  - École polytechnique fédérale de Lausanne is ranked 10th (the university from which Dr. Nikitin obtained his Ph.D. degree).
  - Cornell University is ranked 30th (the university of Dr. Nikitin's first postdoctoral employment).
  - KTH Royal Institute of Technology is ranked 37th (the university from which Dr. Nikitin obtained his MS degree).
  - Columbia University is ranked 44th (the university of Dr. Nikitin's current postdoctoral employment).

In partnership with ELSEVIER

# QS World University Rankings 2025: Top global universities

Discover the world's best universities with the QS World University Rankings 2025.

This year's ranking is the largest ever, featuring over 1,500 universities across 105 higher education systems.... Read more




1503 Results

Apply Filters 0

Download Excel Table

Published on: 04 June 2024

| Rank | University | Research & Discovery | | Learning Experience | |
|---|---|---|---|---|---|
| | | Academic Reputation | Citations per Faculty | Faculty Student Ratio | |
| 1 | Massachusetts Institute of Technology (MIT)<br>Cambridge, United States | 100 | 100 | 100 | 100 |
| 2 | Imperial College London<br>London, United Kingdom<br>View Programmes | 98.5 | 93.9 | 98.2 | 99.5 |
| 3 | University of Oxford<br>Oxford, United Kingdom | 100 | 84.8 | 100 | 100 |
| 4 | Harvard University<br>Cambridge, United States | 100 | 100 | 96.3 | 100 |
| 5 | University of Cambridge<br>Cambridge, United Kingdom | 100 | 84.6 | 100 | 100 |
| 6 | Stanford University<br>Stanford, United States | 100 | 99 | 100 | 100 |
| 7 | ETH Zurich<br>Zürich, Switzerland | 98.8 | 97.9 | 65.9 | 87.2 |
| 8 | National University of Singapore (NUS)<br>Singapore, Singapore<br>View Programmes | 99.5 | 93.1 | 68.8 | 91.1 |
| 9 | UCL<br>London, United Kingdom<br>View Programmes | 99.5 | 72.2 | 95.9 | 98.3 |
| 10 | California Institute of Technology (Caltech)<br>Pasadena, United States | 96.5 | 100 | 100 | 95.3 |
| 11 | University of Pennsylvania<br>Philadelphia, United States | 96.3 | 74 | 99.8 | 91.9 |
| 12 | University of California, Berkeley (UCB)<br>Berkeley, United States | 100 | 98.2 | 23.5 | 100 |
| 13 | The University of Melbourne<br>Parkville, Australia | 98.5 | 93 | 15.4 | 93.9 |
| 14 | Peking University<br>Beijing, China (Mainland) | 99.5 | 97.7 | 92.6 | 96.6 |
| 15 | Nanyang Technological University, Singapore (NTU Singapore)<br>Singapore, Singapore<br>View Programmes | 91.9 | 92.4 | 80.6 | 73.3 |
| 16 | Cornell University<br>Ithaca, United States | 98.3 | 97.5 | 52.7 | 93.1 |
| 17 | The University of Hong Kong<br>Hong Kong, Hong Kong SAR | 97.4 | 86.4 | 81.2 | 59.4 |
| 18 | The University of Sydney<br>Sydney, Australia<br>View Programmes | 96.4 | 93.7 | 10.9 | 90 |
| 19 | The University of New South Wales (UNSW Sydney)<br>Sydney, Australia<br>View Programmes | 90.5 | 94.9 | 20.6 | 90.4 |
| 20 | Tsinghua University<br>Beijing, China (Mainland) | 99.2 | 99.1 | 95 | 97.7 |

| | | | | | |
|---|---|---|---|---|---|
| 21 | University of Chicago<br>Chicago, United States | 99.1 | 60.8 | 94.2 | 96.4 |
| 22 | Princeton University<br>Princeton, United States | 99.8 | 100 | 57 | 98.3 |
| 23 | Yale University<br>New Haven, United States | 99.9 | 38.6 | 100 | 99.9 |
| 24 | Université PSL<br>Paris, France | 74.4 | 87.6 | 98.1 | 97.6 |
| 25 | University of Toronto<br>Toronto, Canada | 99.7 | 50.8 | 44.9 | 96.9 |
| 26 | EPFL – École polytechnique fédérale de Lausanne<br>Lausanne, Switzerland | 84.2 | 93.6 | 91.2 | 67.2 |
| 27 | **The University of Edinburgh**<br>Edinburgh, United Kingdom<br>View Programmes | 98.3 | 47.7 | 65.5 | 97.2 |
| 28 | Technical University of Munich<br>Munich, Germany | 83 | 75.9 | 76.8 | 98.6 |
| 29 | **McGill University**<br>Montreal, Canada<br>View Programmes | 94.3 | 57.9 | 62.3 | 87.6 |
| 30 | **Australian National University (ANU)**<br>Canberra, Australia<br>View Programmes | 93.8 | 84.6 | 34.6 | 75.4 |
| 31 | Seoul National University<br>Seoul, South Korea | 98.5 | 71.7 | 83.1 | 98.6 |
| =32 | Johns Hopkins University<br>Baltimore, United States | 86 | 84.2 | 100 | 62.6 |
| =32 | The University of Tokyo<br>Tokyo, Japan | 100 | 57.3 | 89.3 | 99.8 |
| =34 | Columbia University<br>New York City, United States | 99.6 | 31.7 | 100 | 98.8 |
| =34 | The University of Manchester<br>Manchester, United Kingdom | 95.6 | 45.1 | 51.3 | 98.1 |
| 36 | **The Chinese University of Hong Kong (CUHK)**<br>Hong Kong, Hong Kong SAR<br>View Programmes | 86.7 | 92.9 | 64.2 | 53.3 |
| 37 | Monash University<br>Melbourne, Australia | 89.2 | 87.6 | 9.4 | 79.6 |
| 38 | University of British Columbia<br>Vancouver, Canada | 98.3 | 57.7 | 34.5 | 94.3 |
| 39 | Fudan University<br>Shanghai, China (Mainland) | 85.7 | 80.7 | 79.7 | 87.8 |
| =40 | King's College London<br>London, United Kingdom | 90.3 | 53.6 | 64.3 | 85.7 |
| =40 | **The University of Queensland**<br>Brisbane City, Australia<br>View Programmes | 86.7 | 90.2 | 21.2 | 74 |
| 42 | University of California, Los Angeles (UCLA)<br>Los Angeles, United States | 100 | 74 | 35.4 | 99.8 |
| 43 | New York University (NYU)<br>New York City, United States | 96.3 | 28.6 | 90.5 | 98.8 |
| 44 | University of Michigan-Ann Arbor<br>Ann Arbor, United States | 97.9 | 47.6 | 80.3 | 92.1 |
| 45 | Shanghai Jiao Tong University<br>Shanghai, China (Mainland) | 84 | 99.6 | 58.6 | 86.3 |
| 46 | **Institut Polytechnique de Paris**<br>Palaiseau Cedex, France<br>View Programmes | 44.7 | 86.1 | 95.9 | 99.6 |
| =47 | The Hong Kong University of Science and Technology<br>Hong Kong, Hong Kong SAR | 81.1 | 99.7 | 56.7 | 50.3 |
| =47 | Zhejiang University<br>Hangzhou, China (Mainland) | 75.3 | 99.5 | 54.7 | 95.4 |
| 49 | **Delft University of Technology**<br>Delft, Netherlands<br>View Programmes | 74.4 | 79.7 | 39.4 | 83 |
| =50 | Kyoto University<br>Kyoto, Japan | 98.8 | 39.3 | 94.2 | 99 |

# QS World University Rankings by Subject 2024: Engineering & Technology

In partnership with ELSEVIER


Discover the best universities in the world for studying engineering & technology with the QS World University Rankings by Subject 2024.

The broad subject area of engineering & technology encompasses eight individual subjects, including a range of engineering disciplines and computer science....
Read more



555 Results | Apply Filters 0

Download Excel Table

Published on: **10 April 2024**

Other subject rankings: Arts and Humanities | Life Sciences and Medicine | Natural Sciences | Social Sciences and Management | Accounting and

| Rank | University | Employability | Research & Discovery | | |
|---|---|---|---|---|---|
| | | Employer Reputation | Academic Reputation | Citations per Paper | H-ir |
| 1 | Massachusetts Institute of Technology (MIT)<br>Cambridge, United States | 97.9 | 100 | 96.2 | 96 |
| 2 | Stanford University<br>Stanford, United States | 95.3 | 96.1 | 100 | 99 |
| 3 | University of Oxford<br>Oxford, United Kingdom | 96.5 | 91 | 95 | 90.4 |
| 4 | University of Cambridge<br>Cambridge, United Kingdom | 95.6 | 92.7 | 92.8 | 88.9 |
| 5 | University of California, Berkeley (UCB)<br>Berkeley, United States | 89.7 | 94.4 | 99.4 | 97.1 |
| 6 | ETH Zurich<br>Zürich, Switzerland | 87.3 | 95.3 | 93.7 | 92 |
| 7 | **Imperial College London**<br>London, United Kingdom<br>View Programmes | 84.1 | 95.8 | 92.1 | 89.9 |
| 8 | Harvard University<br>Cambridge, United States | 100 | 82.6 | 95.1 | 91.1 |
| 9 | California Institute of Technology (Caltech)<br>Pasadena, United States | 86.5 | 98.9 | 89.3 | 80.9 |
| 10 | EPFL – École polytechnique fédérale de Lausanne<br>Lausanne, Switzerland | 82.8 | 93 | 92.1 | 86.4 |
| 11 | Tsinghua University<br>Beijing, China (Mainland) | 82.1 | 89.6 | 92.6 | 100 |
| 12 | Georgia Institute of Technology<br>Atlanta, United States | 77.4 | 96 | 92.3 | 90.7 |
| =13 | **Delft University of Technology**<br>Delft, Netherlands<br>View Programmes | 78.5 | 93 | 85.7 | 81.1 |
| =13 | **National University of Singapore (NUS)**<br>Singapore, Singapore<br>View Programmes | 90.2 | 81.8 | 96.2 | 93.9 |
| 15 | **Nanyang Technological University, Singapore (NTU Singapore)**<br>Singapore, Singapore<br>View Programmes | 87 | 84.2 | 96.7 | 96.4 |
| 16 | Carnegie Mellon University<br>Pittsburgh, United States | 76 | 91.7 | 97.4 | 93.3 |
| 17 | University of Toronto<br>Toronto, Canada | 87.6 | 82.9 | 93.5 | 87.7 |
| 18 | The University of Tokyo<br>Tokyo, Japan | 84.6 | 89.7 | 80.4 | 82.6 |
| 19 | Technical University of Munich<br>Munich, Germany | 72.7 | 92.9 | 85 | 83 |
| 20 | **KAIST - Korea Advanced Institute of Science & Technology**<br>Daejeon, South Korea<br>View Programmes | 78.9 | 93.2 | 88.8 | 81.5 |

| | | | | | |
|---|---|---|---|---|---|
| 21 | University of California, Los Angeles (UCLA)<br>Los Angeles, United States | 86.5 | 83.7 | 92.2 | 86.9 |
| 22 | University of Illinois at Urbana-Champaign<br>Champaign, United States | 76 | 90.7 | 88.2 | 84.4 |
| 23 | **Politecnico di Milano**<br>Milan,, Italy<br>View Programmes | 79.9 | 89.3 | 80.4 | 76 |
| 24 | University of Texas at Austin<br>Austin, United States | 76.1 | 86.7 | 91.1 | 87.2 |
| 25 | University of British Columbia<br>Vancouver, Canada | 85.3 | 80.6 | 89.6 | 81.3 |
| 26 | Purdue University<br>West Lafayette, United States | 78 | 88.1 | 84.4 | 80.7 |
| =27 | Seoul National University<br>Seoul, South Korea | 82.5 | 87.7 | 86.9 | 82.2 |
| =27 | The University of Manchester<br>Manchester, United Kingdom | 77.9 | 82 | 89.7 | 81.5 |
| =27 | University of Michigan-Ann Arbor<br>Ann Arbor, United States | 78.6 | 85.1 | 90 | 85.4 |
| 30 | Cornell University<br>Ithaca, United States | 81.1 | 81.6 | 96.5 | 85.7 |
| 31 | **The University of New South Wales (UNSW Sydney)**<br>Sydney, Australia<br>View Programmes | 76.4 | 81 | 91.7 | 85.9 |
| 32 | Princeton University<br>Princeton, United States | 83.9 | 80.8 | 95.9 | 84.1 |
| 33 | Peking University<br>Beijing, China (Mainland) | 81.2 | 79.9 | 93.8 | 95.1 |
| 34 | **Institut Polytechnique de Paris**<br>Palaiseau Cedex, France<br>View Programmes | 75.8 | 85.7 | 84.2 | 73.2 |
| =35 | **UCL**<br>London, United Kingdom<br>View Programmes | 77.5 | 78.8 | 91 | 85.4 |
| =35 | Université Paris-Saclay<br>Gif-sur-Yvette,, France | 74.8 | 81.9 | 82.5 | 83 |
| =37 | **KTH Royal Institute of Technology**<br>Stockholm, Sweden<br>View Programmes | 67.2 | 87.9 | 86.6 | 79.1 |
| =37 | Shanghai Jiao Tong University<br>Shanghai, China (Mainland) | 73.8 | 85.5 | 87.1 | 91.6 |
| 39 | **McGill University**<br>Montreal, Canada<br>View Programmes | 82.6 | 78.8 | 88.5 | 78.2 |
| =40 | Tokyo Institute of Technology (Tokyo Tech)<br>Tokyo, Japan | 74.4 | 91.2 | 78.4 | 71.3 |
| =40 | University of Waterloo<br>Waterloo, Canada | 76.1 | 80.6 | 89.9 | 83.3 |
| 42 | **King Abdulaziz University (KAU)**<br>Jeddah, Saudi Arabia<br>View Programmes | 73.1 | 79.5 | 94.3 | 86.2 |
| 43 | Zhejiang University<br>Hangzhou, China (Mainland) | 74.4 | 79.4 | 88.2 | 91.2 |
| 44 | Columbia University<br>New York City, United States | 82.4 | 73.6 | 93.9 | 84.9 |
| =45 | Indian Institute of Technology Bombay (IITB)<br>Mumbai, India | 83.1 | 84.6 | 80 | 66.1 |
| =45 | Indian Institute of Technology Delhi (IITD)<br>New Delhi, India | 81.3 | 83.8 | 81.6 | 69.6 |
| =45 | Technische Universität Berlin (TU Berlin)<br>Berlin, Germany | 66.7 | 87 | 85.3 | 79.1 |
| 48 | KIT, Karlsruhe Institute of Technology<br>Karlsruhe, Germany | 65.4 | 85.8 | 84 | 79.7 |
| =49 | The University of Melbourne<br>Parkville, Australia | 76 | 77.9 | 89.2 | 81.3 |
| =49 | University of California, San Diego (UCSD)<br>San Diego, United States | 71.3 | 79.4 | 93 | 86.4 |

# Exhibit 24

The current employment letter and the offer letters that Dr. Nikitin received for postdoctoral researcher positions:

1. The latest employment extension letter from XX (current).
2. The offer letters from XX and YY (accepted, currently employed).
3. The offer letter from ZZ (accepted).
4. The offer letter from WW (declined).

# Exhibit 25

Executive orders, a national strategy report, and an action plan by the federal government which highlight the national importance of Dr. Nikitin's area of research and proposed employment:

- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 2023 (the opening page).
- National Strategy to Advance Privacy-Preserving Data Sharing and Analytics, 2023 (the title page, the table of contents, the executive summary, and page 18).
- National Privacy Research Strategy, 2025 (the title page, the table of contents, and the executive summary).
- Executive Order on America's Supply Chains, 2024 (the opening page).
- Executive Order on Improving the Nation's Cybersecurity, 2021 (the opening page).
- An Action Plan on Securing Defense-Critical Supply Chains, 2022 (the title page, the table of contents, and the executive summary).
- Executive Order on Strengthening American Leadership in Digital Financial Technology, 2025 (the opening page).

OCTOBER 30, 2023

# Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence



By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.

My Administration places the highest urgency on governing the development and use of AI safely and responsibly, and is therefore advancing a coordinated, Federal Government-wide approach to doing so. The rapid speed at which AI capabilities are advancing compels the United States to lead in this moment for the sake of our security, economy, and society.

In the end, AI reflects the principles of the people who build it, the people who use it, and the data upon which it is built. I firmly believe that the power of our ideals; the foundations of our society; and the creativity, diversity, and decency of our people are the reasons that America thrived in past eras of rapid change. They are the reasons we will succeed again in this moment. We are more than capable of harnessing AI for justice, security, and opportunity for all.

Sec. 2. Policy and Principles. It is the policy of my Administration to advance and govern the development and use of AI in accordance with eight guiding principles and priorities. When undertaking the actions set forth in this order, executive departments and agencies (agencies) shall, as appropriate and consistent with applicable law, adhere to these principles, while, as feasible, taking into account the views of other agencies, industry, members of academia, civil society, labor unions, international allies and partners, and other relevant organizations:

(a) Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use. It also requires addressing AI systems' most pressing security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers — while navigating AI's opacity and complexity. Testing and evaluations, including post-deployment performance monitoring, will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner, and are compliant with applicable Federal laws and policies. Finally, my Administration will help develop effective labeling and content provenance mechanisms, so that Americans are able to determine when content is generated using AI and when it is not. These actions will provide a vital foundation for an approach that addresses AI's risks without unduly reducing its benefits.

(b) Promoting responsible innovation, competition, and collaboration will allow the United States to lead in AI and unlock the technology's potential to solve some of society's most difficult challenges. This effort requires investments in AI-related education, training, development, research, and capacity, while simultaneously tackling novel intellectual property (IP) questions and other problems to protect inventors and creators. Across the Federal Government, my Administration will support programs to provide Americans the skills they need for the age of AI and attract the world's AI talent to our shores — not just to study, but to stay — so that the companies and technologies of the future are made in America. The Federal Government will promote a fair, open, and competitive ecosystem and marketplace for AI and related technologies so that small developers and entrepreneurs can continue to drive innovation. Doing so requires stopping unlawful collusion and addressing risks from dominant firms' use of key assets such as semiconductors, computing power, cloud storage, and data to disadvantage competitors, and it requires supporting a marketplace that harnesses the benefits of AI to provide new opportunities for small businesses, workers, and entrepreneurs.

(c) The responsible development and use of AI require a commitment to


# *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics*

*A Report by the*

FAST-TRACK ACTION COMMITTEE ON ADVANCING PRIVACY-PRESERVING DATA SHARING AND ANALYTICS

NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT SUBCOMMITTEE

*of the*

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

March 2023

# Table of Contents

## Executive Summary

Data are vital resources for solving society's biggest problems. Today, significant amounts of data are accumulated every day—fueled by widespread data generation methods, new data collection technologies, faster means of communication, and more accessible cloud storage. Advances in computing have significantly reduced the cost of data analytics and artificial intelligence, making it even easier to use this data to derive valuable insights and enable new possibilities. However, this potential is often limited by legal, policy, technical, socioeconomic, and ethical challenges involved in sharing and analyzing sensitive information. These opportunities can only be fully realized if strong safeguards that protect privacy[1]—a fundamental right in democratic societies—underpin data sharing and analytics.

Privacy-preserving data sharing and analytics (PPDSA) methods and technologies can unlock the beneficial power of data analysis while protecting privacy. PPDSA solutions include methodological, technical, and sociotechnical approaches that employ privacy-enhancing technologies to derive value from, and enable an analysis of, data to drive innovation while also providing privacy and security. However, adoption of PPDSA technologies has been slow because of challenges related to inadequate understanding of privacy risks and harms, limited access to technical expertise, trust, transparency among participants with regard to data collection and use,[2] uncertainty about legal compliance, financial cost, and the usability and technical maturity of solutions.[3]

PPDSA technologies have enormous potential, but their benefit is tied to how they are developed and used. Existing confidentiality and privacy laws and policies provide important protections to individuals and communities, and attention is needed to determine how to uphold these protections through the use of PPDSA technologies and maintain commitments to equity, transparency, and accountability. Consideration of how individuals may control the collection, linking, and use of their data should also factor into the design and use of PPDSA technologies.

Recognizing the untapped potential of PPDSA technologies, the White House Office of Science and Technology Policy (OSTP) initiated a national effort to advance PPDSA technologies.

This National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (Strategy) lays out a path to advance PPDSA technologies to maximize their benefits in an equitable manner, promote trust, and mitigate risks. This Strategy takes great care to incorporate socioeconomic and technological contexts that are vital to responsible use of PPDSA technologies, including their impact on equity, fairness, and bias—and how they might introduce privacy harms, especially to disadvantaged groups.

This Strategy first sets out a vision for a future data ecosystem that incorporates PPDSA approaches:

> *Privacy-preserving data sharing and analytics technologies help advance the well-being and prosperity of individuals and society, and promote science and innovation in a manner that affirms democratic values.*

This Strategy then lays out the following foundational guiding principles to achieve this vision:

- PPDSA technologies will be created and used in ways that protect privacy, civil rights, and civil liberties.
- PPDSA technologies will be created and used in a manner that stimulates responsible scientific research and innovation, and enables individuals and society to benefit equitably from the value derived from data sharing and analytics.

harmonizing electronic health record data from health systems across the US and using PPRL to connect different COVID-19-related patient data from multiple organizations. Various techniques including secure multiparty computation or data perturbation approaches can be used to support PPRL.[71]

- *Private information retrieval* is another useful technique that allows a client to retrieve data from a database server without the server knowing what was retrieved or queried. This protects a user's access privacy by making sure the data owner cannot track what content or types of information the user is accessing. Similar access privacy issues relate to a server learning about what a user is accessing based on observable access patterns. Oblivious random access memory is a technique that has been used to address such access privacy issues.
- *Federated learning* allows multiple entities to collaborate in building a machine learning model on distributed data. It provides inherent privacy protection as participants do not have to share their raw data. Instead, each participant trains a local model on their data which is then integrated into the collaborative model. Recent research[72] has identified persistent privacy risks in federated learning, which are also found more generally in ML, such as model inversion attacks that can reconstruct the private training data or membership inference attacks that can identify if a data sample is part of the training dataset. Research is ongoing in combining some of the above-referenced cryptographic techniques to close these vulnerabilities and create privacy-preserving federated learning.

**Summary and challenges.** The *t*echniques mentioned above are some of the key existing technical approaches relevant for privacy-preserving data publishing or analytics, but not an exhaustive list. The technologies described are at different levels of maturity with some such as differential privacy or secure multiparty computation seeing initial, limited success in deployment, and others still in earlier stages of development. Cross-cutting technical challenges such as those related to understanding and quantifying disclosure risks, scalability and efficiency, and verification and validation approaches to ensure the correctness of design, implementation, and deployment present barriers to broader adoption. Furthermore, in many application scenarios, the integration of various techniques will be needed to support end-to-end privacy. Additional work is also needed to determine how issues of fairness, transparency, and accountability can be assured while achieving privacy guarantees.

- PPDSA technologies will be trustworthy, and will be created and used in a manner that upholds accountability.
- PPDSA technologies will be created and used to minimize the risk of harm to individuals and society arising from data sharing and analytics, with explicit consideration of impacts on underserved, marginalized, and vulnerable communities.

Based on the guiding principles, this Strategy identifies the following strategic priorities for the public and private sectors to progress toward the vision of a future data ecosystem that effectively incorporates PPDSA technologies:

- **Advance governance and responsible adoption** through the establishment of a multi-partner steering group to help develop and maintain a healthy PPDSA ecosystem, greater clarity on the use of PPDSA technologies within the statutory and regulatory environments, and proactive risk mitigation measures.
- **Elevate and promote foundational and use-inspired research** through investments in multidisciplinary research that will advance practical deployment of PPDSA approach and exploratory research to develop the next generation of PPDSA technologies.
- **Accelerate translation to practice** through pilot implementations, development of consensus technical standards, and creation of user-focused tools, decision aids, and testbeds.
- **Build expertise and promote training and education** through concerted efforts to expand PPDSA expertise across the public and private sector and foster privacy education opportunities from K-12 through higher education, with particular attention to capacity building in underserved communities.
- **Foster international collaboration on PPDSA** through promotion of partnerships and an international policy environment that furthers the development and adoption of PPDSA technologies and supports common values while protecting national and economic security.

PPDSA technologies have the potential to catalyze American innovation and creativity by facilitating data sharing and analytics while protecting sensitive information and individuals' privacy. Leveraging data at scale holds the power to drive transformative innovation to address climate change, financial crime, public health, human trafficking, social equity, and other challenges, yet it also holds the potential to violate privacy and undercut the fundamental rights of individuals and communities. PPDSA technologies, coupled with strong governance, can play a critical role in protecting democratic values and mitigating privacy risks and harms while enabling data sharing and analytics that will contribute to improvements in the quality of life of the American people. This Strategy serves as a roadmap for both the public and private sectors to responsibly harness the potential of PPDSA technologies and move together toward the vision that anchors this Strategy.

OSTP, in partnership with the National Economic Council, will focus and coordinate Federal activities to advance the priorities put forward in this Strategy.

JUNE 14, 2024

# Executive Order on White House Council on Supply Chain Resilience



By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. As described in Executive Order 14017 of February 24, 2021 (America's Supply Chains), it is the policy of my Administration to strengthen the enduring resilience of America's supply chains. The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity, public health, and national security. Pandemics and other biological threats, cyber attacks, climate stressors and extreme weather events, transnational corruption, terrorist attacks, geopolitical disputes, unfair economic competition, and other disruptive conditions can reduce critical infrastructure, manufacturing, and processing capacity and the availability of critical goods, materials, and services. Building resilient American supply chains will necessitate enhancing domestic manufacturing capacity, supporting America's competitive edge in research and development, encouraging innovation, reinforcing critical infrastructure, and creating well-paying jobs. Building resilient American supply chains will also provide a foundation to strengthen prosperity, advance the fight against climate change, enhance national emergency preparedness, and encourage economic growth across the Nation.

More resilient supply chains are secure and diverse. Characteristics of resilient supply chains include greater domestic production; a diverse and agile supplier base; built-in redundancies; a reliable transportation system; secure critical infrastructure; adequate stockpiles; safe and secure data networks; reliable food systems; and a world-class, globally competitive American manufacturing base and workforce. Close cooperation on building global supply chain resilience with allies and partners who share our values will foster collective economic and national security, encourage innovation, and strengthen the capacity to respond to and recover from international disasters and emergencies.

Sec. 2. Definitions. For purposes of this order:

(a) "Agency" has the meaning given to that term in Executive Order 14017.

(b) "Critical goods and materials" has the meaning given to that term in Executive Order 14017.

(c) "Other essential goods, materials, and services" means goods, materials, and services that are essential to national and economic security, emergency preparedness, or to advance the policy set forth in section 1 of this order, but not included within the definition of "critical goods and materials."

(d) "Critical infrastructure" means assets, systems, and networks, whether physical or virtual, that are so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, national public health or safety, or any combination thereof.

Sec. 3. Coordination. (a) This order supplements and reaffirms the principles governing America's supply chains established in Executive Order 14017. Any provisions of Executive Order 14017 not amended in this order shall remain in effect.

(b) Notwithstanding section 2 of Executive Order 14017, the Assistant to the President for National Security Affairs (APNSA) and the Assistant to the President for Economic Policy (APEP) shall coordinate, as appropriate, the executive branch actions necessary to implement this order through the White House Council on Supply Chain Resilience (Council) established on November 27, 2023, and further described in section 4 of this order. In coordinating the work of the Council on issues related to national security, and on other issues as they deem appropriate, the APNSA and the APEP shall work with the Council in conformance with the interagency process identified in National Security Memorandum 2 of February 4, 2021 (Renewing the National Security Council System).

Sec. 4. White House Council on Supply Chain Resilience.

(a) The White House Council on Supply Chain Resilience residing within the Executive Office of the President is led by the APNSA and the APEP, who serve as Co-Chairs of the Council. In addition to the Co-Chairs, the membership of the Council consists of the following members:

(i) the Secretary of State;
(ii) the Secretary of the Treasury;
(iii) the Secretary of Defense;
(iv) the Attorney General;
(v) the Secretary of the Interior;
(vi) the Secretary of Agriculture;
(vii) the Secretary of Commerce;
(viii) the Secretary of Labor;
(ix) the Secretary of Health and Human Services;

MAY 12, 2021

# Executive Order on Improving the Nation's Cybersecurity



By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

Sec. 2. Removing Barriers to Sharing Threat Information.

(a) The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.

(b) Within 60 days of the date of this order, the Director of the Office of Management and Budget (OMB), in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, shall review the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement contract requirements and language for contracting with IT and OT service providers and recommend updates to such requirements and language to the FAR Council and other appropriate agencies. The recommendations shall include descriptions of contractors to be covered by the proposed contract language.

(c) The recommended contract language and requirements described in subsection (b) of this section shall be designed to ensure that:

(i) service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies' requirements;

(ii) service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with

# Securing Defense-Critical Supply Chains

An action plan developed in response to
President Biden's Executive Order 14017

**February 2022**

# Table of Contents

# Foreword from the Deputy Secretary of Defense

The Department of Defense (DoD) is aligning its priorities and capabilities to enhance our readiness. By modernizing our approach to supply chain resilience, DoD can deliver decisive advantages to our Warfighters in a dynamic threat landscape.

In an effort to improve supply chain resilience and protect against material shortages, President Joseph R. Biden Jr. signed Executive Order (E.O.) 14017, America's Supply Chains. In response to the EO, this report provides DoD's assessment of defense critical supply chains in order to improve our capacity to defend the Nation.

Our recommendations focus on how we can increase domestic production capacity and renew the sources of our economic security. We will continue investing in the production and manufacturing capabilities that will enable a modern, technology-enabled defense industrial base. Because we know that workers animate supply chains, we will foster development of an industrial workforce to ensure the right skillsets are available as needed to meet our requirements. We will also contribute to our national defense stockpile and utilize it to provide flexibility in the case of disruptions or emergencies.

This report reinforces our commitment to American values and underscores the importance of a free, open, and rules-based market. We will prioritize collaboration with our allies and partners to build a network of secure global supply chains. Further, we will safeguard global market integrity to ensure that industry can continue to provide superior products and services to our force.

Our plans include a strong commitment to cooperation with all who have a stake in our national security: our interagency collaborators, Congress, private industry, the American people, and our allies and international partners. By emphasizing teamwork, this report delivers a whole-of-Nation approach to national security and invites greater industrial collaboration with our friends across the globe.

Our work to build resilient, competitive, and sustainable supply chains will be a longterm campaign. Given the complexities of our defense supply chains, the plans in this report are bold and ambitious in their scope. We will continue to iterate on our approach. Our prioritization of expanded and new supply chain capabilities will help us face the challenges of the 21st century with fortitude.

**Dr. Kathleen H. Hicks**

United States Deputy
Secretary of Defense

# Executive Summary

The Department of Defense (DoD) requires healthy, resilient, diverse, and secure supply chains to ensure the development and sustainment of capabilities critical to national security. The ongoing COVID-19 pandemic highlighted vulnerabilities in complex global supply chains in very real ways to the public, government, and industry. Beyond COVID-19, supply chain disruptions have become more frequent and severe overall.

In order to strengthen the national industrial base during times of disruption, President Joseph R. Biden, Jr. signed Executive Order (E.O.) 14017, *America's Supply Chains,* on February 24, 2021. The E.O. calls for a comprehensive review of supply chains in critical sectors, including the defense industrial base (DIB). This report provides DoD's assessment of supply chains in the DIB and articulates the Department's plans to ensure security of supply for items vital to national security.

The national resolve to strengthen America's supply chains is not limited to the Executive Branch. Congress has demonstrated a commitment to renewing and strengthening U.S. manufacturing through the Bipartisan Infrastructure Law (BIL) and the House Armed Services Committee (HASC) critical supply chain task force. The DIB and related trade associations have outlined myriad actions and are actively engaging with government at all levels to build resiliency.[1] The DoD is committed to strengthening the industrial base and establishing a network of domestic and allied supply chains to meet national security needs.

Given the breadth and scale of defense supply chains, the one-year effort prioritized four areas in which critical vulnerabilities pose the most pressing threat to national security. These focus areas are:

- **Kinetic capabilities:** current missiles systems and advanced and developing missile capabilities, including hypersonic weapons technology, as well as directed energy weapons
- **Energy storage and batteries:** high-capacity batteries, with a particular focus on lithium batteries
- **Castings and forgings:** metals or composites developed into key parts and manufacturing tools through high-intensity processes
- **Microelectronics:** State-of-the-Practice (SOTP) and legacy microelectronics, as well as State-of-the-Art (SOTA) microelectronics

1. National Defense Industrial Association, *The Health and Readiness of the Defense Industrial Base.* February 2022. https://safe.menlosecurity.com/doc/docview/viewer/docNCFF7F14465DBf21220840d3330e2a40ffe2aa8a8a1606143d25262da1d46a8be6a685f2e24e7.

This report also provides an update on the implementation of recommendations in DoD's Review of Critical Minerals and Materials, included in the 100-day response to E.O. 14017 published on June 8, 2021.[2]

Underpinning all four key focus areas are strategic enablers that are required for mission success. Fragility or gaps in these enablers create operational and strategic risk, and addressing the challenges in each is critical to building overall supply chain resilience. The strategic enablers are:

- **Workforce:** trade skills through doctoral-level engineering skills
- **Cyber posture:** industrial security, counterintelligence, and cybersecurity
- **Manufacturing:** current manufacturing practices, as well as advanced technology like additive manufacturing
- **Small business:** the role of key members of DoD supply chains

This report provides a strategic assessment of these focus areas and enablers, as well as the steps that can be taken to mitigate identified threats and vulnerabilities and build resilience.

Across all focus areas and enablers, the Department identified certain foundational recommendations to enhance and grow the industrial base. These cross-cutting recommendations underpin the sector specific recommendations outlined in subsequent sections of this report and are critical to the Department's overall ability to make strategic informed acquisition and sustainment decisions. These recommendations are:

- **Build domestic production capacity:** For those supply chains that are critical for national defense, the U.S. is committed to ensuring reliable production access within the defense industrial base, both domestic and allied.
- **Engage with partners and allies:** The U.S. is collaborating with its international partners and allies to develop policies and arrangements that strengthen our defense industrial bases and improve supply chain resilience.
- **Mitigate Foreign Ownership, Control, or Influence (FOCI) and safeguard markets:** The Department is committed to protecting its supply chains and the defense industrial base from adversarial FOCI by scaling efforts to identify and mitigate FOCI concerns.
- **Conduct data analysis:** DoD will continue to build on previous efforts to expand its visibility into supply chains by collecting and organizing key data.
- **Aggregate demand:** The Department will signal to industry what the likely total demand is across multiple programs, so industry can better anticipate number of orders from year to year.
- **Develop common standards:** To leverage commercial sector innovations, and to embed modernizing technologies in weapon systems, the DoD will work, where possible, to limit its use of military-unique requirements when developing performance requirements.
- **Update acquisition policies:** DoD should engage in efforts to develop a whole-of-government strategy and implementation plan to engage with industry and Congress to determine which policy and regulatory changes would encourage expansion of capabilities.

The above actions and sector specific recommendations will provide DoD with a strategic roadmap to renew the DIB and maintain its position as the world leader in innovation well into the 21st Century.

2. United States, White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*, 1*00-Day Reviews Under Executive Order 14017.* June 2021.

PRESIDENTIAL ACTIONS

# STRENGTHENING AMERICAN LEADERSHIP IN DIGITAL FINANCIAL TECHNOLOGY

EXECUTIVE ORDER

January 23, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote United States leadership in digital assets and financial technology while protecting economic liberty, it is hereby ordered as follows:

Section 1. Purpose and Policies. (a) The digital asset industry plays a crucial role in innovation and economic development in the United States, as well as our Nation's international leadership. It is therefore the policy of my Administration to support the responsible growth and use of digital assets, blockchain technology, and related technologies across all sectors of the economy, including by:

(i) protecting and promoting the ability of individual citizens and private-sector entities alike to access and use for lawful purposes open public blockchain networks without persecution, including the ability to develop and deploy software, to participate in mining and validating, to transact with other persons without unlawful censorship, and to maintain self-custody of digital assets;

(ii) promoting and protecting the sovereignty of the United States dollar, including through actions to promote the development and growth of lawful and legitimate dollar-backed stablecoins worldwide;

(iii) protecting and promoting fair and open access to banking services for all law-abiding individual citizens and private-sector entities alike;

(iv) providing regulatory clarity and certainty built on technology-neutral regulations, frameworks that account for emerging technologies, transparent decision making, and well-defined jurisdictional regulatory boundaries, all of which are essential to supporting a vibrant and inclusive digital economy and innovation in digital assets, permissionless blockchains, and distributed ledger technologies; and

(v) taking measures to protect Americans from the risks of Central Bank Digital Currencies (CBDCs), which threaten the stability of the financial system, individual privacy, and the sovereignty of the United States, including by prohibiting the establishment, issuance, circulation, and use of a CBDC within the jurisdiction of the United States.

Sec. 2. Definitions. (a) For the purpose of this order, the term "digital asset" refers to any digital representation of value that is recorded on a distributed ledger, including cryptocurrencies, digital tokens, and stablecoins.

(b) The term "blockchain" means any technology where data is:

(i) shared across a network to create a public ledger of verified transactions or information among network participants;

(ii) linked using cryptography to maintain the integrity of the public ledger and to execute other functions;

(iii) distributed among network participants in an automated fashion to concurrently update network participants on the state of the public ledger and any other functions; and

(iv) composed of source code that is publicly available.

(c) "Central Bank Digital Currency" means a form of digital money or monetary value, denominated in the national unit of account, that is a direct liability of the central bank.