

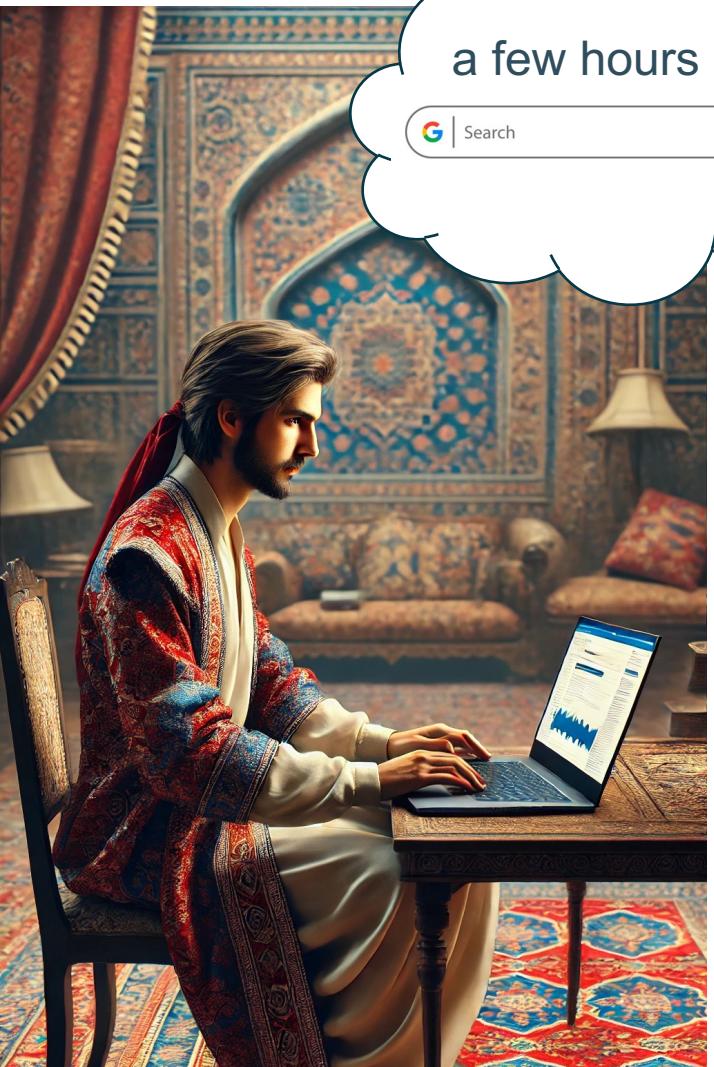
# Privacy-Enhancing Techniques in Distributed Systems

Mahdi Sedaghat

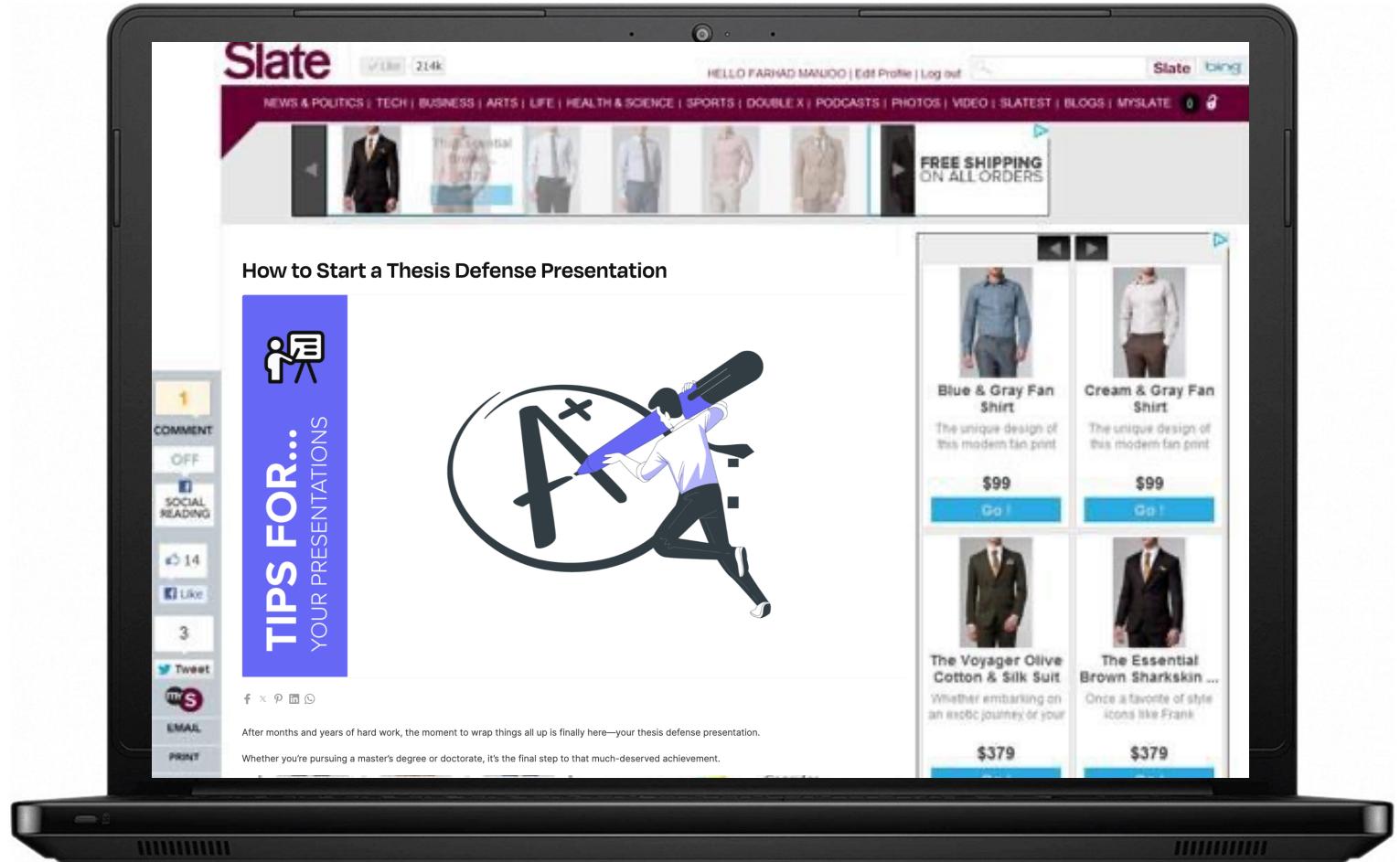
Supervisor: Prof. dr. ir. Bart Preneel

Public Defense -- 09 July 2024





a few hours ago:



Why did this happen to me?  
Have I been hacked?

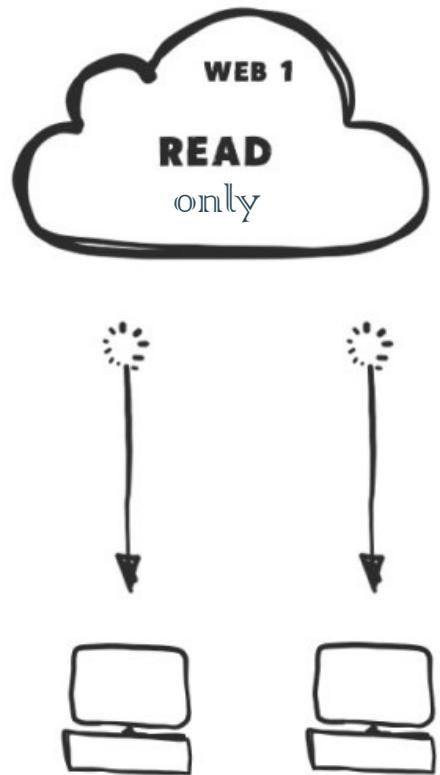
Oh! I am now more confused!

This is because we are all in  
the era of Web 2.0!

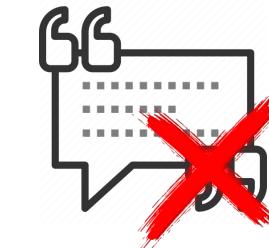


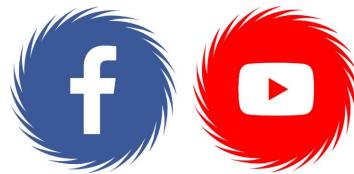
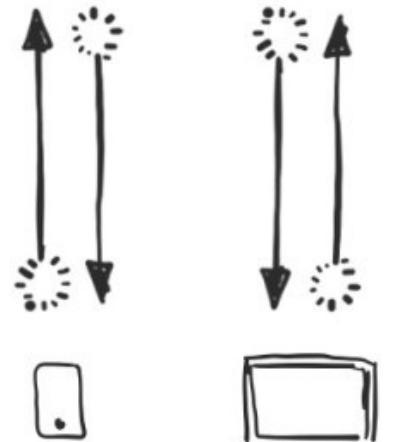


This website were Read-only content and not interactable.



Everything got started from Web 1.0, introduced in 1993.





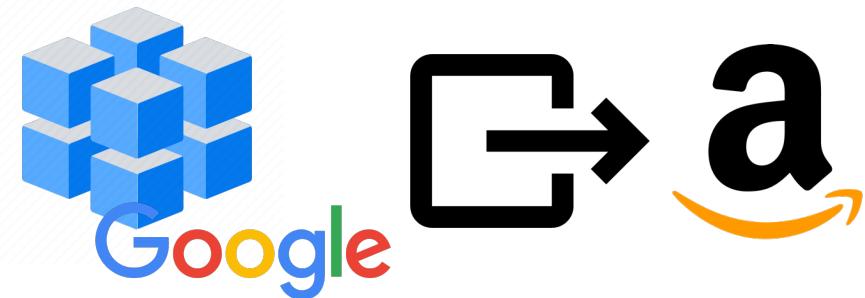
In 2004, Web 2.0 came to the picture.

They started collecting data from us to keep us on their websites longer.





We don't read and even fewer understand how they allow their personal data is being used.



Purposes

- Store and/or acc...
- Select basic ads...
- Create a person...
- Select personali...
- Create a person...
- Select personali...
- Measure ad perf...
- Measure content...
- Apply market res...
- Develop and imp...

Special Purposes

- Ensure security...
- Technically deliv...

Features

- Match and combi...
- Link different dev...
- Receive and use...

Special Features

- Use precise geolocation data



## We use cookies

This website uses cookies to ensure you get the best experience on our website.

ACCEPT
Save Settings & Exit
Continue with Recommended Cookies

Consent

8 / 50

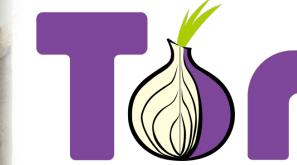
COSIC (Computer Security and Industrial Cryptography) group

KU LEUVEN



Is there any permanent solution?

Yes! Use Tor or Brave browsers.



Yes, Distributed  
Systems!

# Internet Usage Statistics In 2024



By Lexie Pelchen  
Editor



Reviewed By  
Samantha Allen  
Home Improvement, Gardening,  
Home Design

Published: Mar 1, 2024, 9:32pm

We earn a commission from partner links on Forbes Home. Commissions do not affect our editors' opinions or evaluations.

**There are 5.35 billion internet users worldwide.**

around 66% of the world's population

**On average, users spend 6.5 hours online every day.**

People spend 4 hours daily, on their mobile devices.

2024

# Read Write Own

## Building the Next Era of the Internet

### Chris Dixon

**The internet was created to give an equal access to everyone.**

**The internet wasn't immediately monetized.**  
It was designed to be permissionless and democratically governed.

1993

**And then everything changed!!!!**



**Mega-corporations like Google, Meta (Facebook), Apple, Amazon, and Microsoft seized control**

The top 1% of social networks:

95% of social web traffic

86% of social mobile app usage

The top 1% of search engines:

97% of search traffic



2004

**The internet became permissioned and centralized.**

The centralized internet weakened the data privacy by the ads-based companies

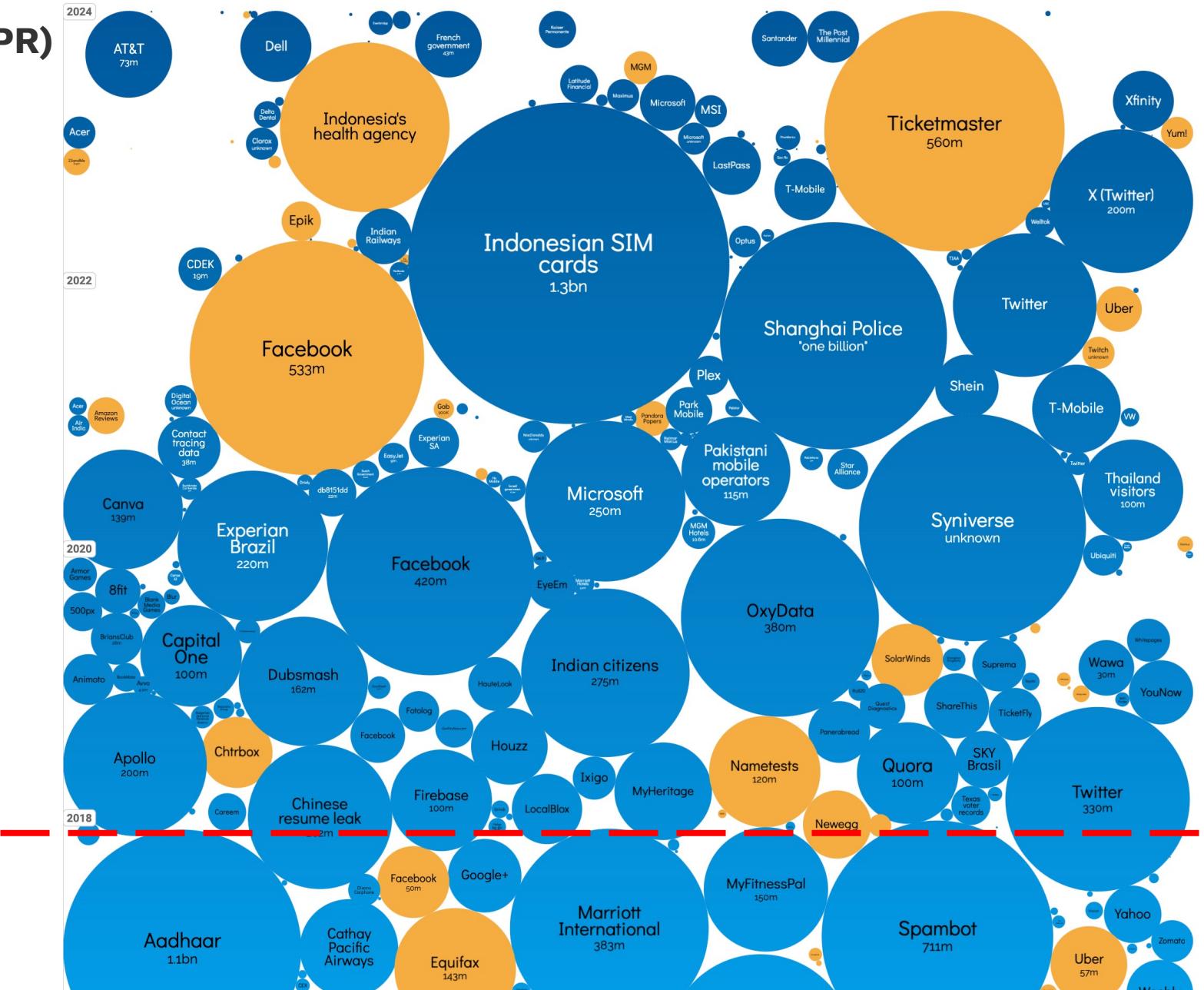
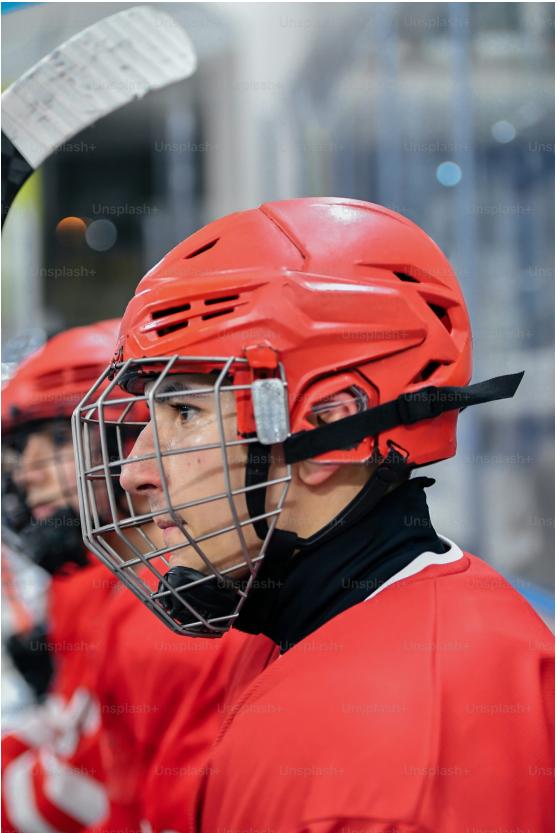
**Regulations came to rescue, but ...!**



# General Data Protection Regulation (GDPR) the use of personal data!

It started on 25 May 2018

World's biggest data Breaches:



Centralized systems have full access to users' data.





Reduce the risk of data breach by distributing the trust.

Conclusion and Future Work



## Privacy-Enhancing Techniques in Distributed Systems

Privacy-Enhancing Techniques  
As cryptographic solution

Distributed Systems  
No Trust

Cryptographical Primitives

Threshold Signatures

Non-Interactive Zero-Knowledge Proofs



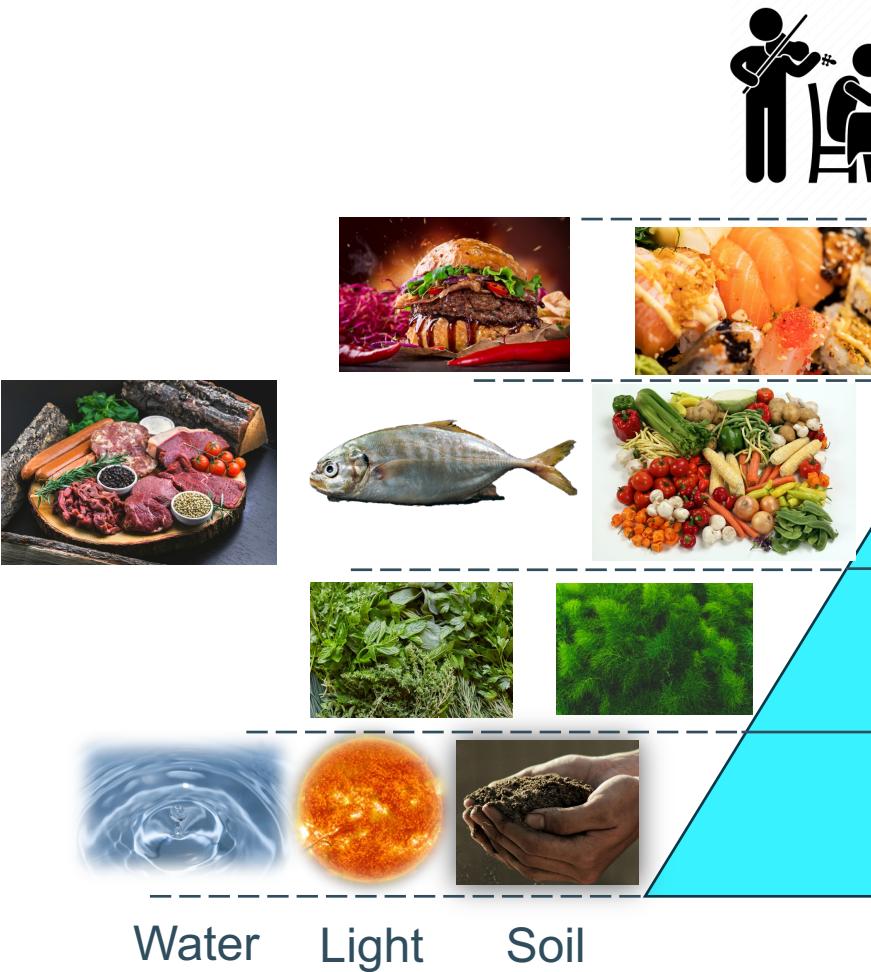
Cryptographers are either the farmers  
or the chefs of the digital world.

Many people consider cryptographers to  
be the digital world's security guards.

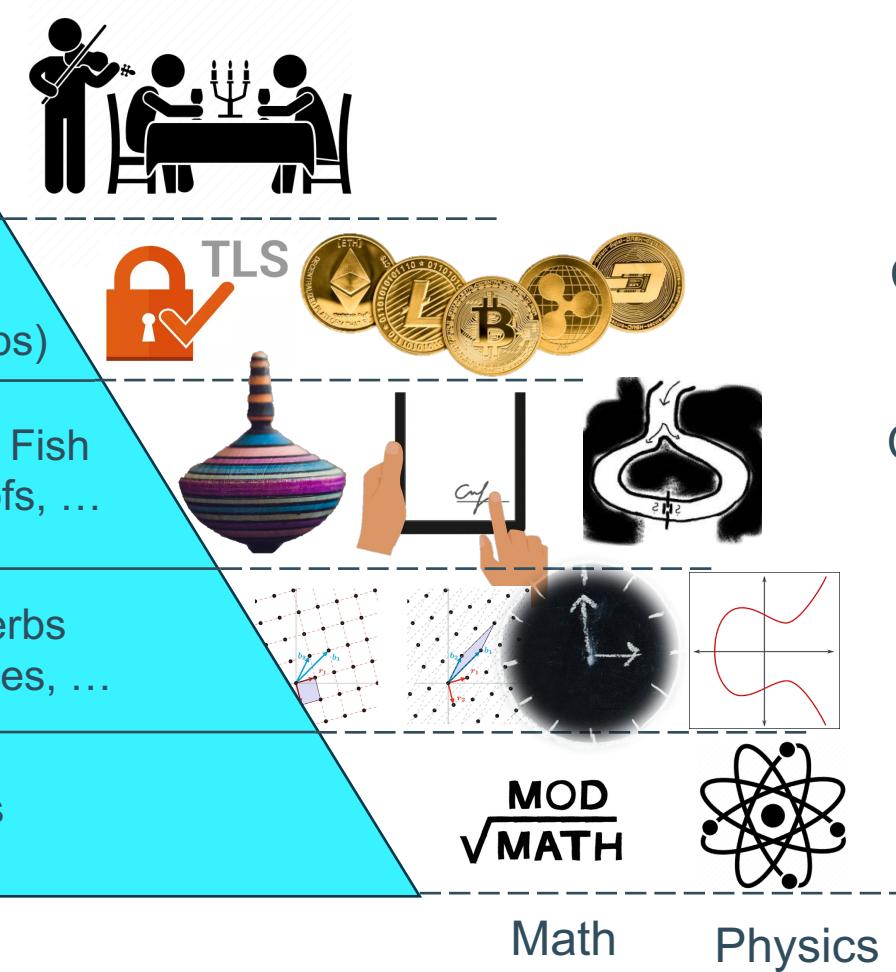
Source: Unsplash

# Cryptography: Human Food Chain vs. Cryptography Chain

Human Food Chain



Cryptography Chain



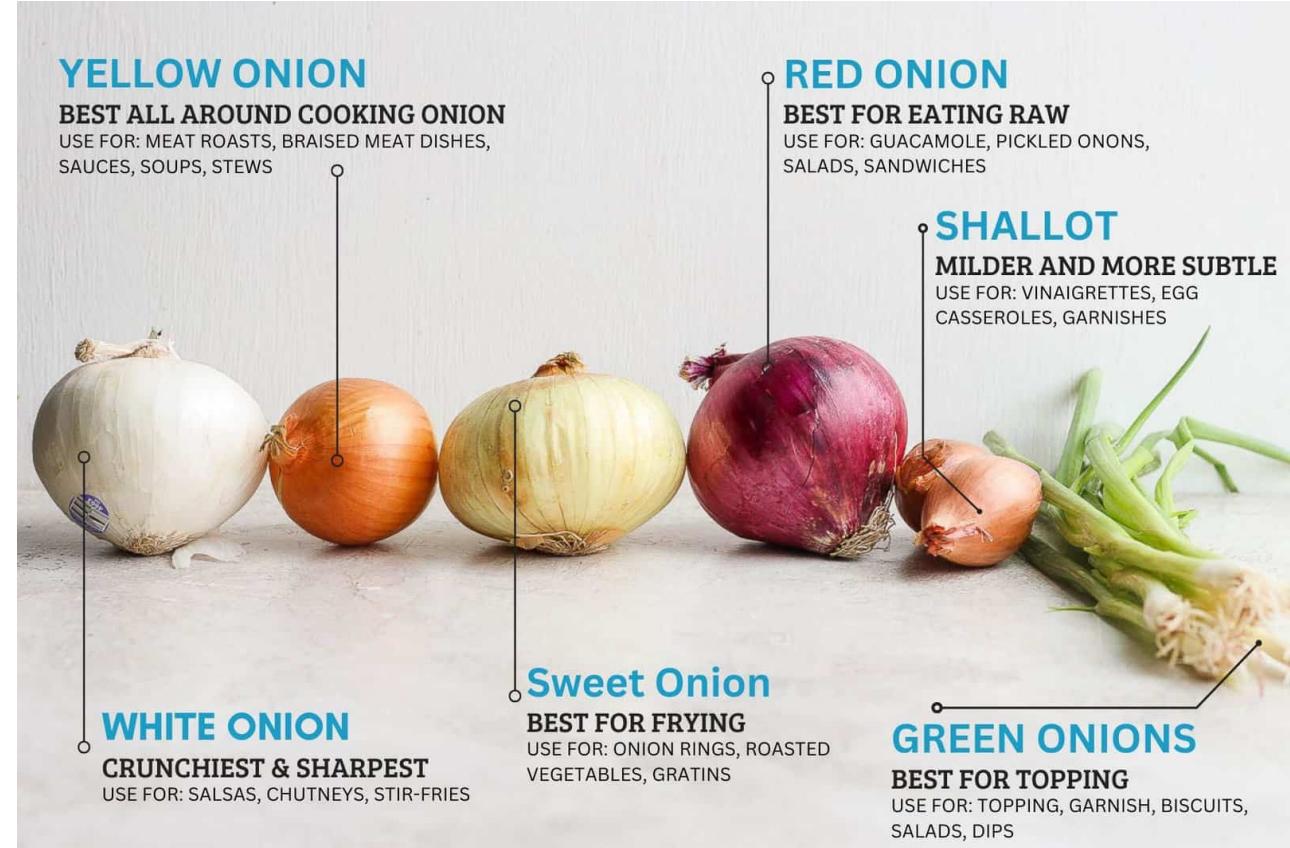
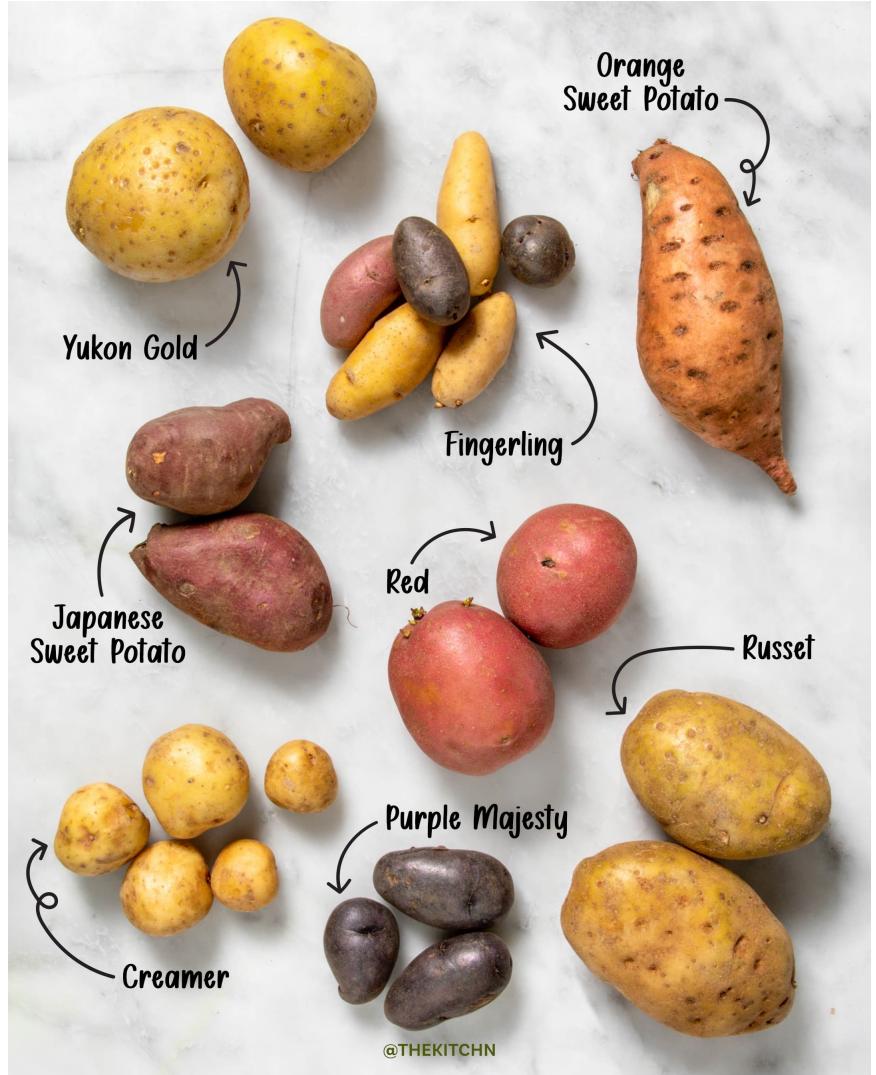
Cryptographic  
Protocols

Cryptographic  
Primitives

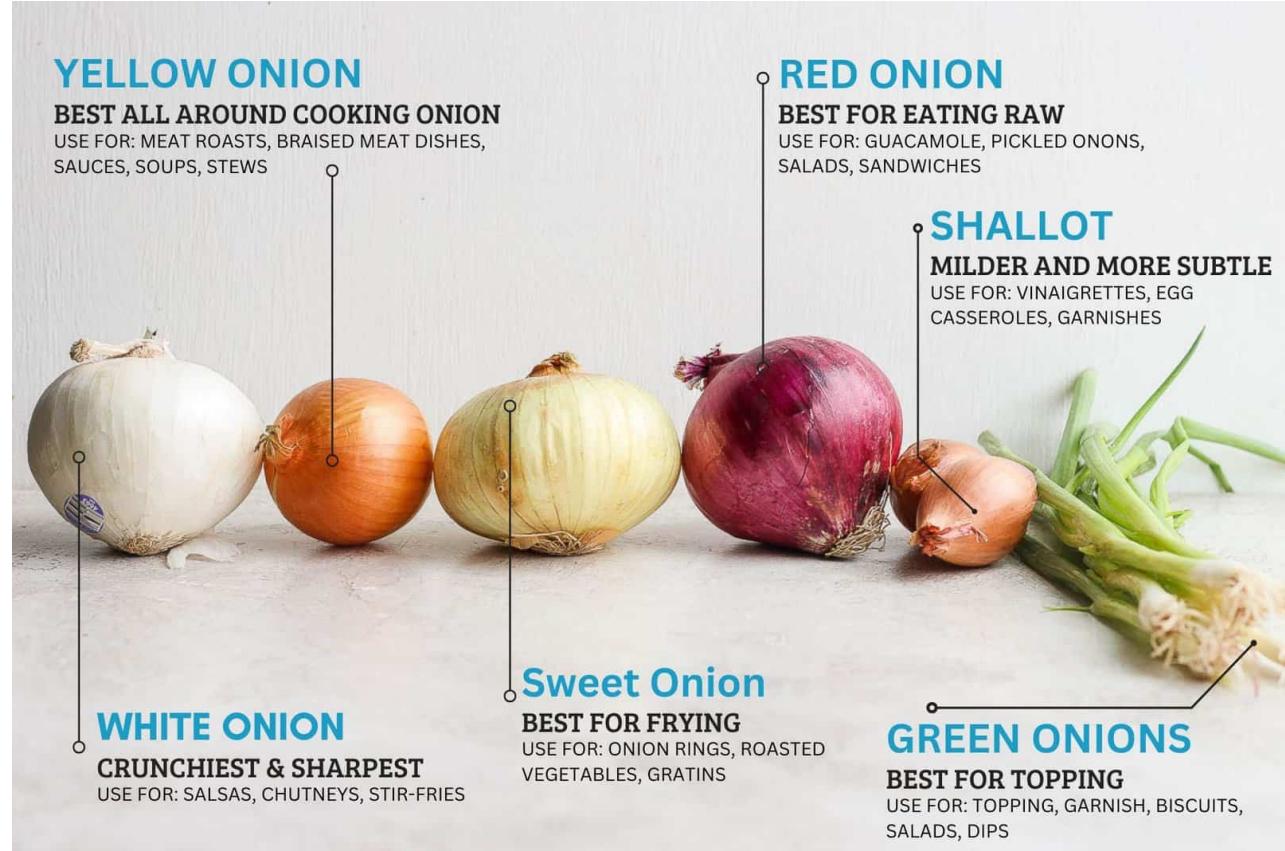
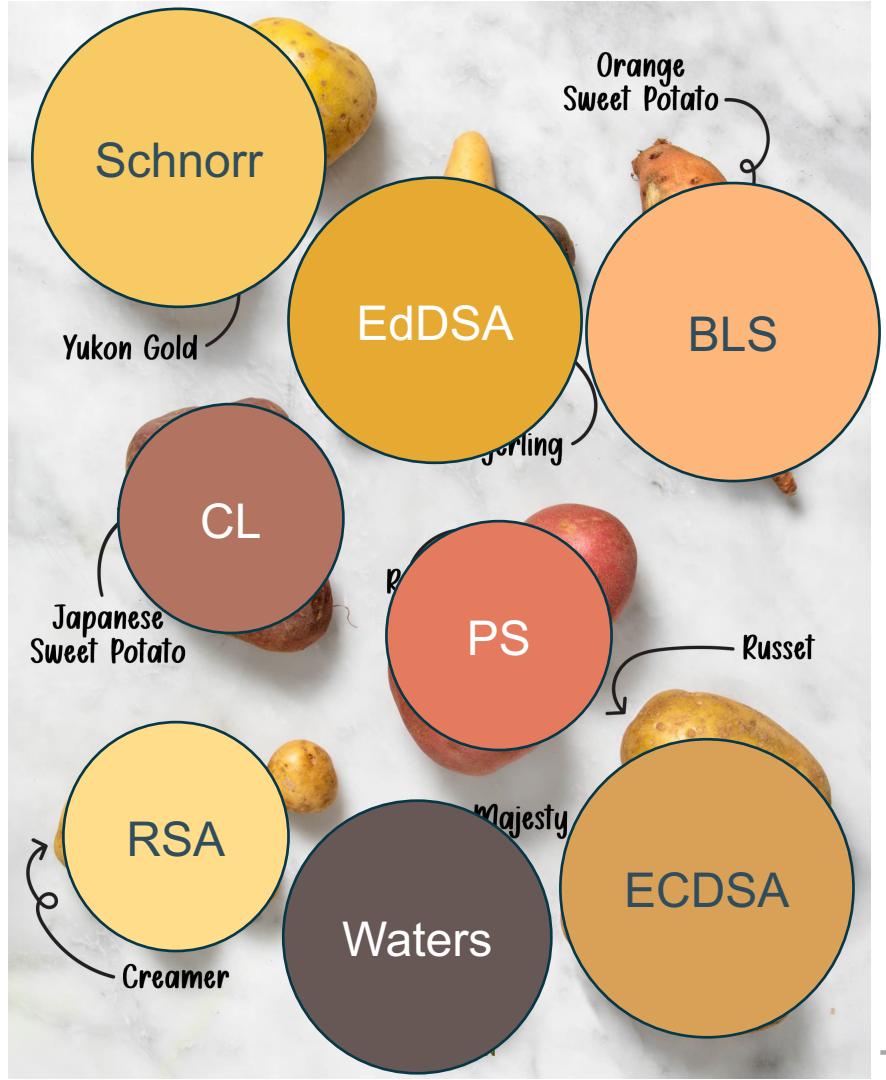
Hardness  
assumptions

Pure  
Science

# Cryptography: Primitives vs. Ingredients

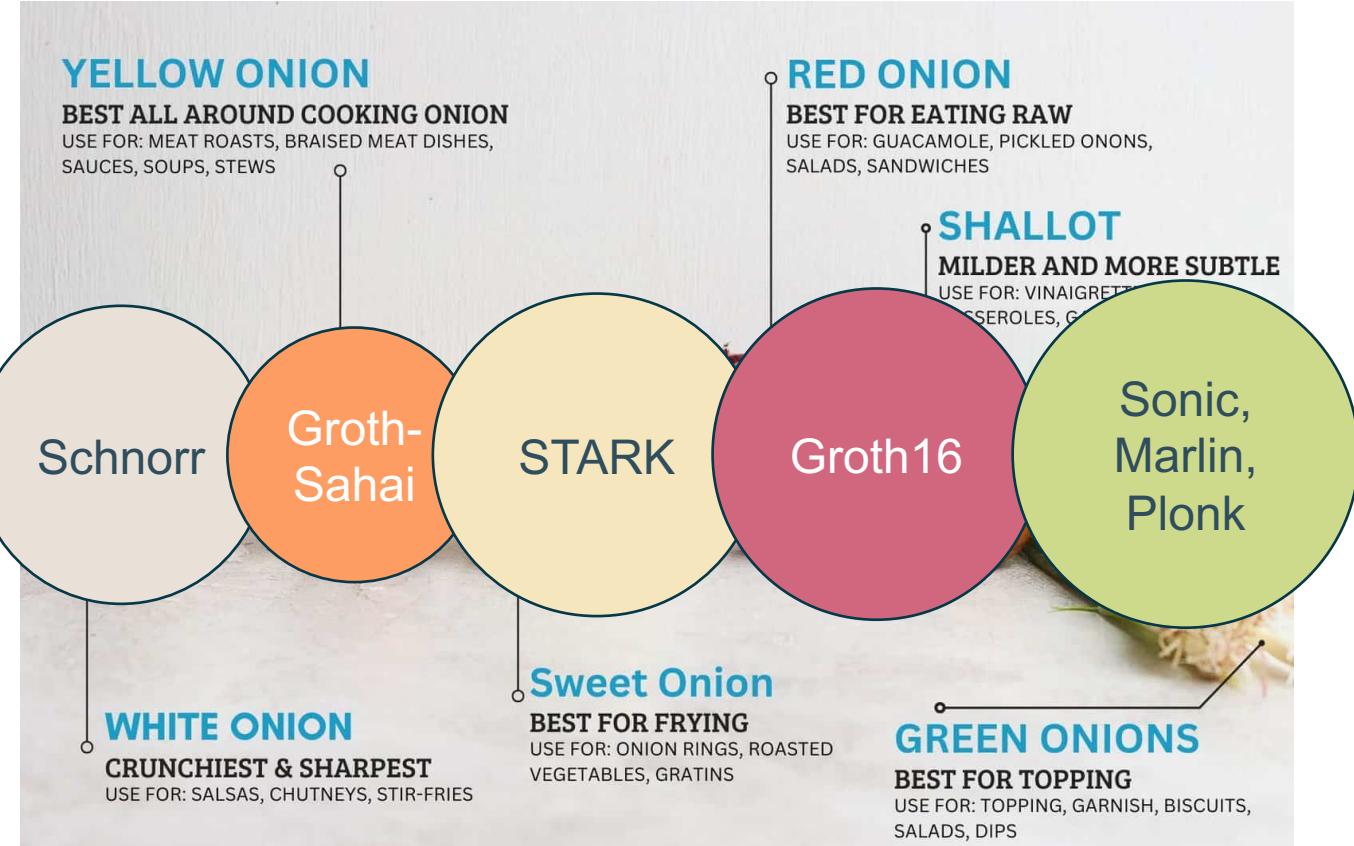
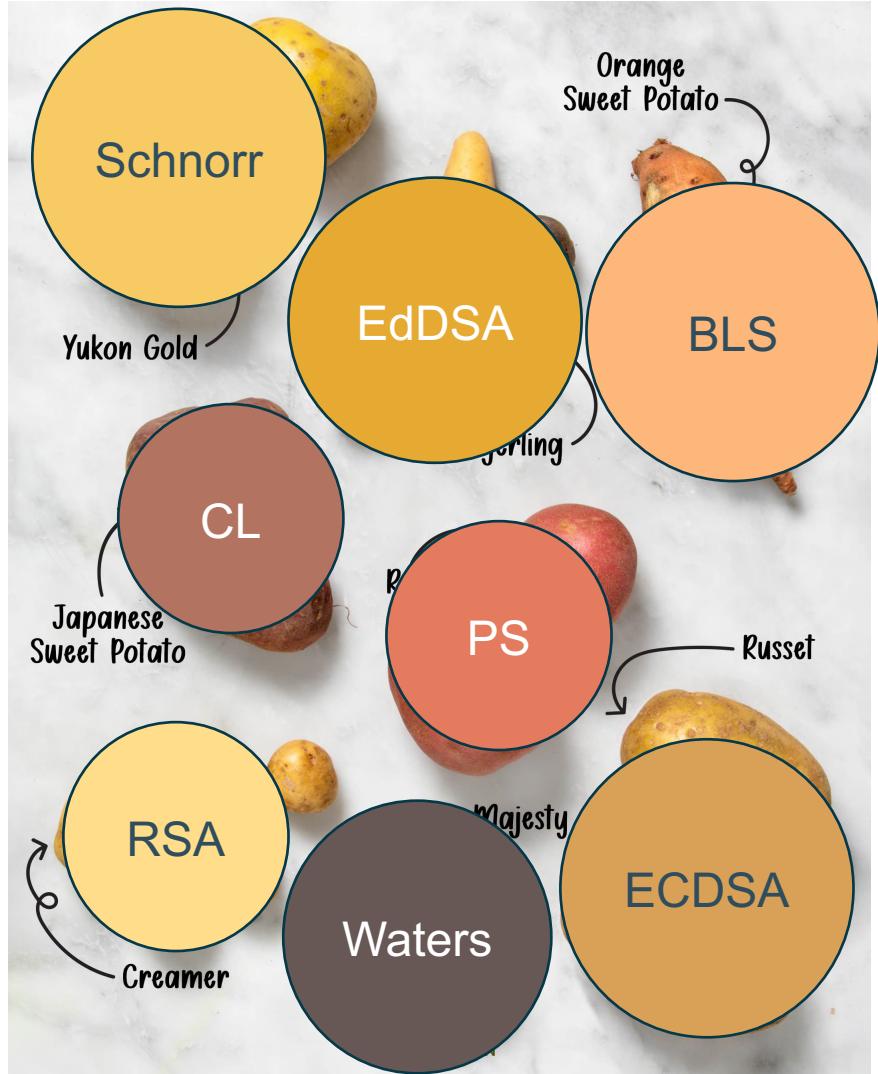


# Cryptography: Primitives vs. Ingredients



Digital Signatures  
To bind a message to its author.

# Cryptography: Primitives vs. Ingredients



Zero-Knowledge Proofs

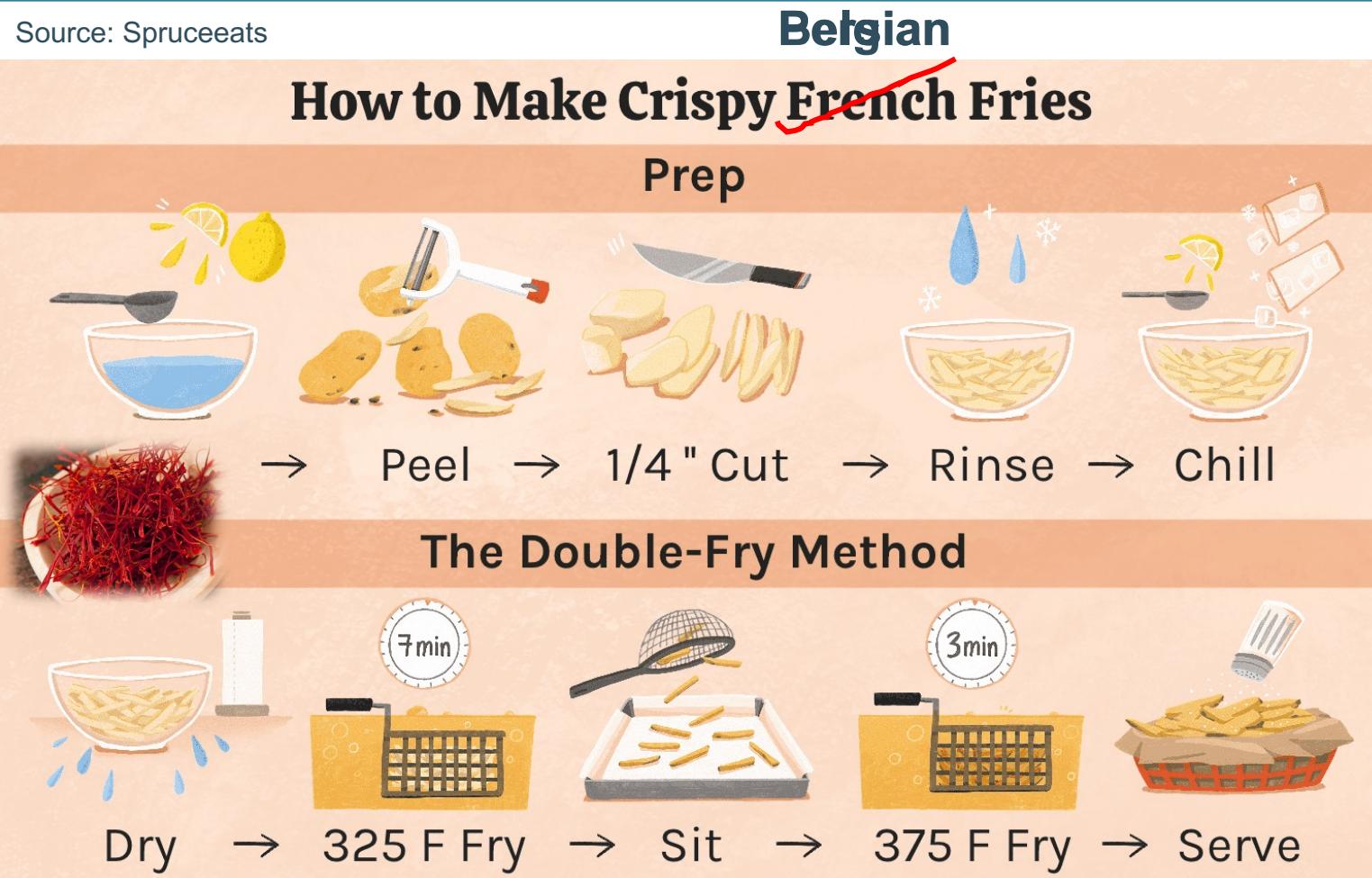
Digital Signatures

To bind a message to its author.

To prove the validity of a claim to a verifier, w/o extra leakage.

# TLS 1.3: A famous Cryptographical Recipe for Hand Shaking Protocols

Source: Spruceeats

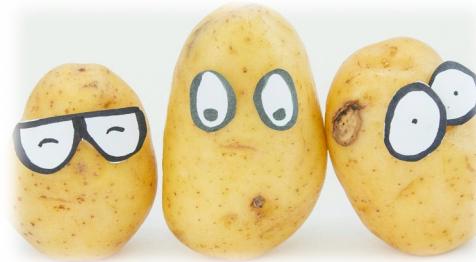


TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_BGV

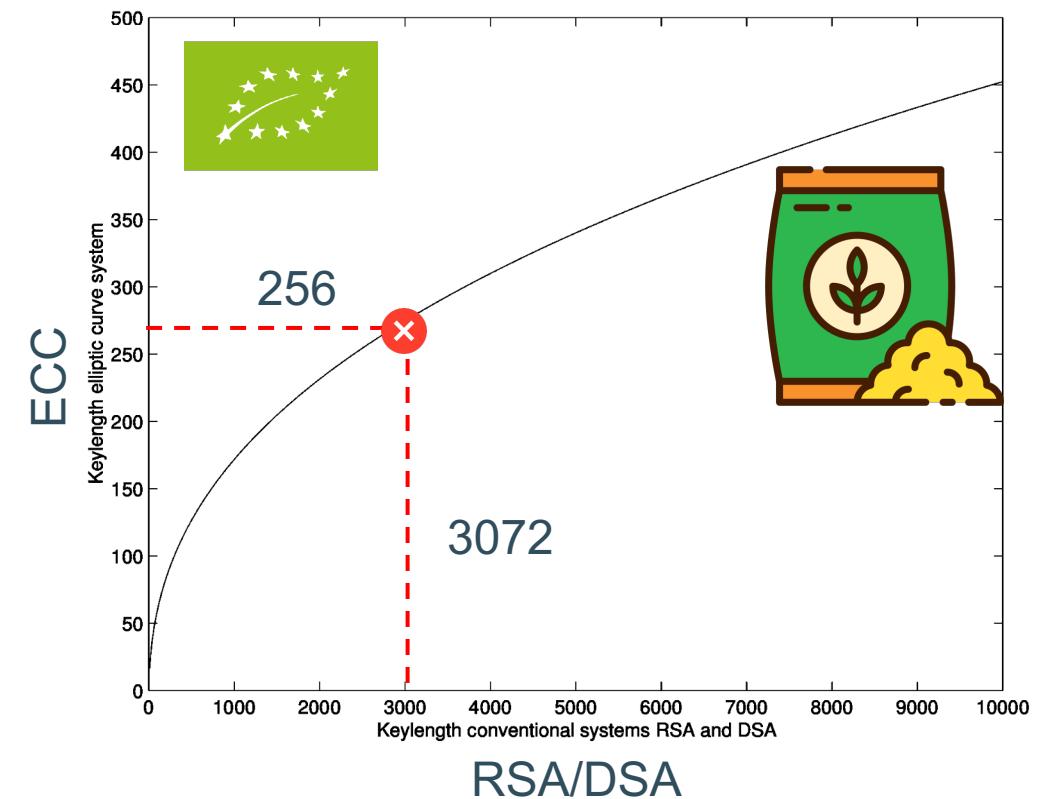
**TLS 1.3:**  
Signature:

ECDSA  
EdDSA  
RSA

Key exchange protocol:  
DHE  
ECDHE



# Security Models: From Weak to Strong Adversaries



Breaking Rainbow Takes a Weekend on a Laptop,  
Ward Beullens

# Summary of Results

Live fully  
work passionately  
create endlessly



# Publications:

MLS-ABAC: Efficient Multi-Level Security Attribute Based Access Control scheme. [FGCS'22]

Cross-Domain Attribute-Based Access Control Encryption. [CANS'21]

Reusable, instant and private payment guarantees for cryptocurrencies. [ACISP'23]

Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments. [PETS'24, CTB'24]

zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials. [CCS'24, SBC'24]

Subset-optimized BLS Multi-signature with Key Aggregation. [FC'24]

Tiramisu: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model. [CANS'21]

Benchmarking the setup of updatable zk-SNARK. [Latincrypt'23]

Threshold Structure-Preserving Signatures. [Asiacrypt'23]

Threshold Structure Preserving Signatures: Strong and Adaptive Security under Standard Assumptions. [PKC'24]

## Access Control

## Applications in Blockchain

## Non-Interactive Zero-Knowledge

## Threshold Signatures



# Publications:

2020    2021    2022    2023    2024

- 
- MLS-ABAC: Efficient Multi-Level Security Attribute Based Access Control scheme. [FGCS'22]
- Cross-Domain Attribute-Based Access Control Encryption. [CANS'21]
- Reusable, instant and private payment guarantees for cryptocurrencies. [ACISP'23]
- Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments. [PETS'24, CTB'24]
- zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials. [CCS'24, SBC'24]
- Subset-optimized BLS Multi-signature with Key Aggregation. [FC'24]
- Tiramisu: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model. [CANS'21]
- Benchmarking the setup of updatable zk-SNARK. [Latincrypt'23]
- Threshold Structure-Preserving Signatures. [Asiacrypt'23]
- Threshold Structure Preserving Signatures: Strong and Adaptive Security under Standard Assumptions. [PKC'24]



# Threshold Signatures

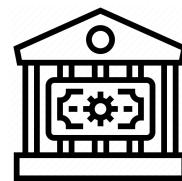
---

To enhance the availability and build trust

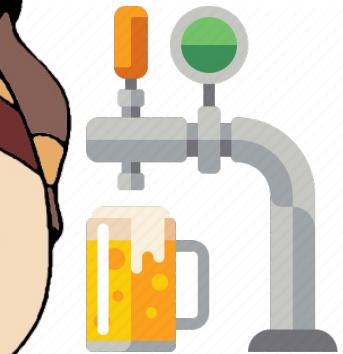
# Let's Have a Beer:



	Name: Aladdin
	Date of birth: 20.09.2000
	Nationality: *****
	ID number: *****



City hall



Bar

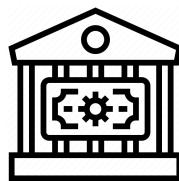
Is the person with this photo older than 18 years old?



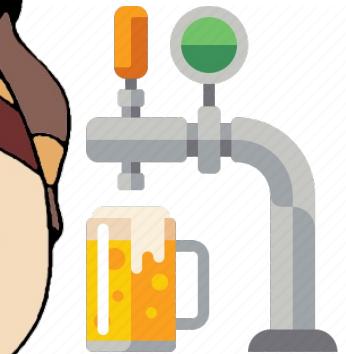
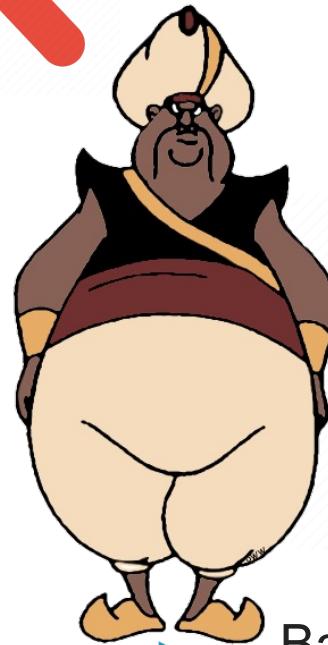
# Let's have a beer:



	Name: Aladdin
	Date of birth: 20.09.2000
	Nationality: *****
	ID number: *****



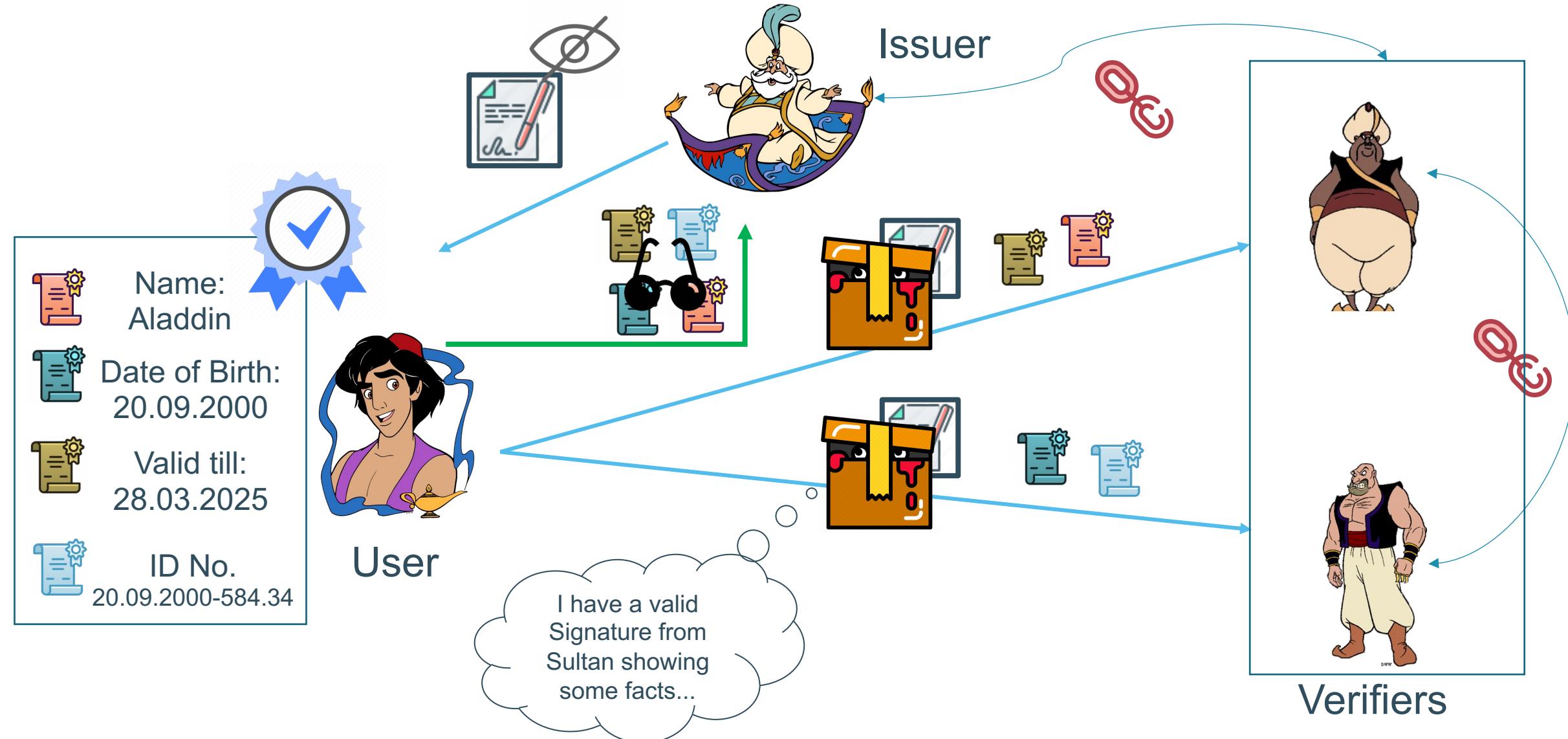
City hall



Is the person with this photo older  
than 18 years old?



# Anonymous Credentials [Cha84]: A well-known cryptographical technique

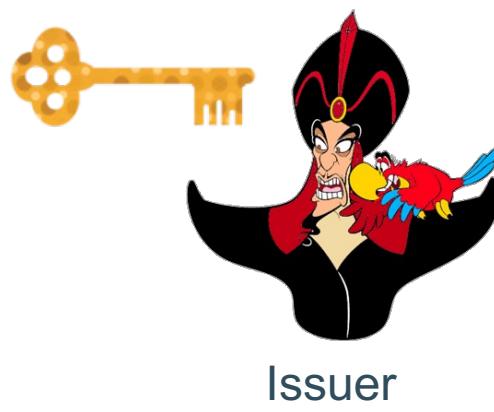


# Anonymous Credentials: Single Point of Failure



User

	Name: Aladdin
	Date of Birth: 20.09.2000
	Valid till: 28.03.2025
	ID No. 20.09.2000-584.34



Issuer

# Threshold-Issuance Anonymous Credential systems:



User

	Name: Aladdin
	Date of Birth: 20.09.2000
	Valid till: 28.03.2025
	ID No. 20.09.2000-584.34



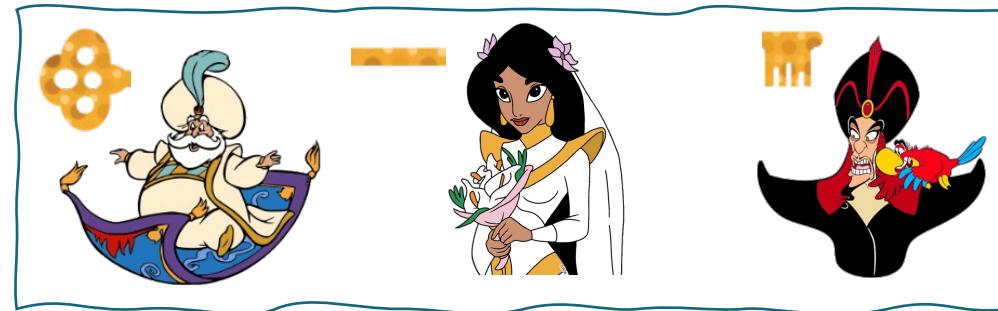
Issuers

# Threshold-Issuance Anonymous Credential systems:



User

	Name: Aladdin
	Date of Birth: 20.09.2000
	Valid till: 28.03.2025
	ID No. 20.09.2000-584.34



Issuers

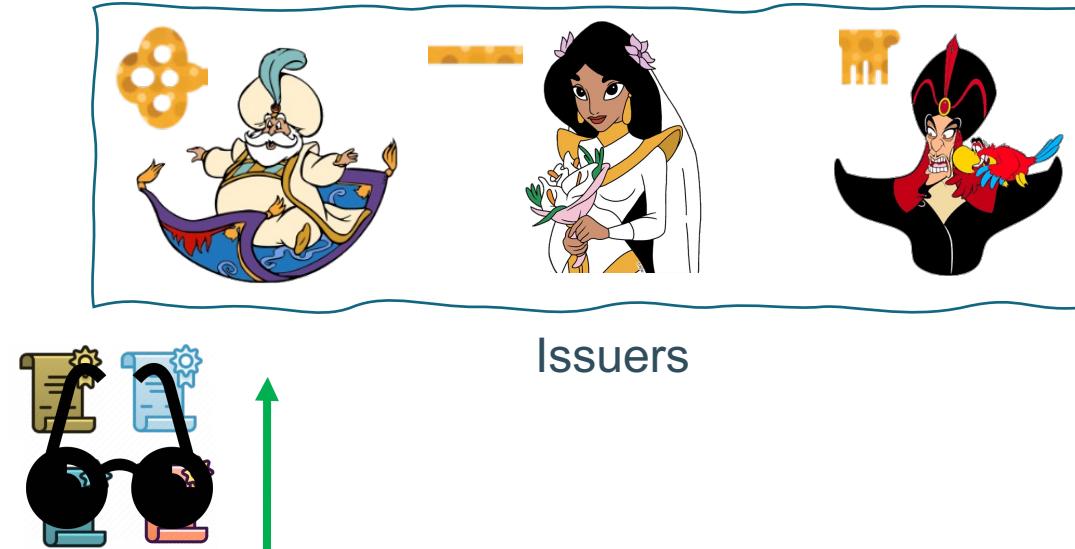


# Threshold-Issuance Anonymous Credential systems:

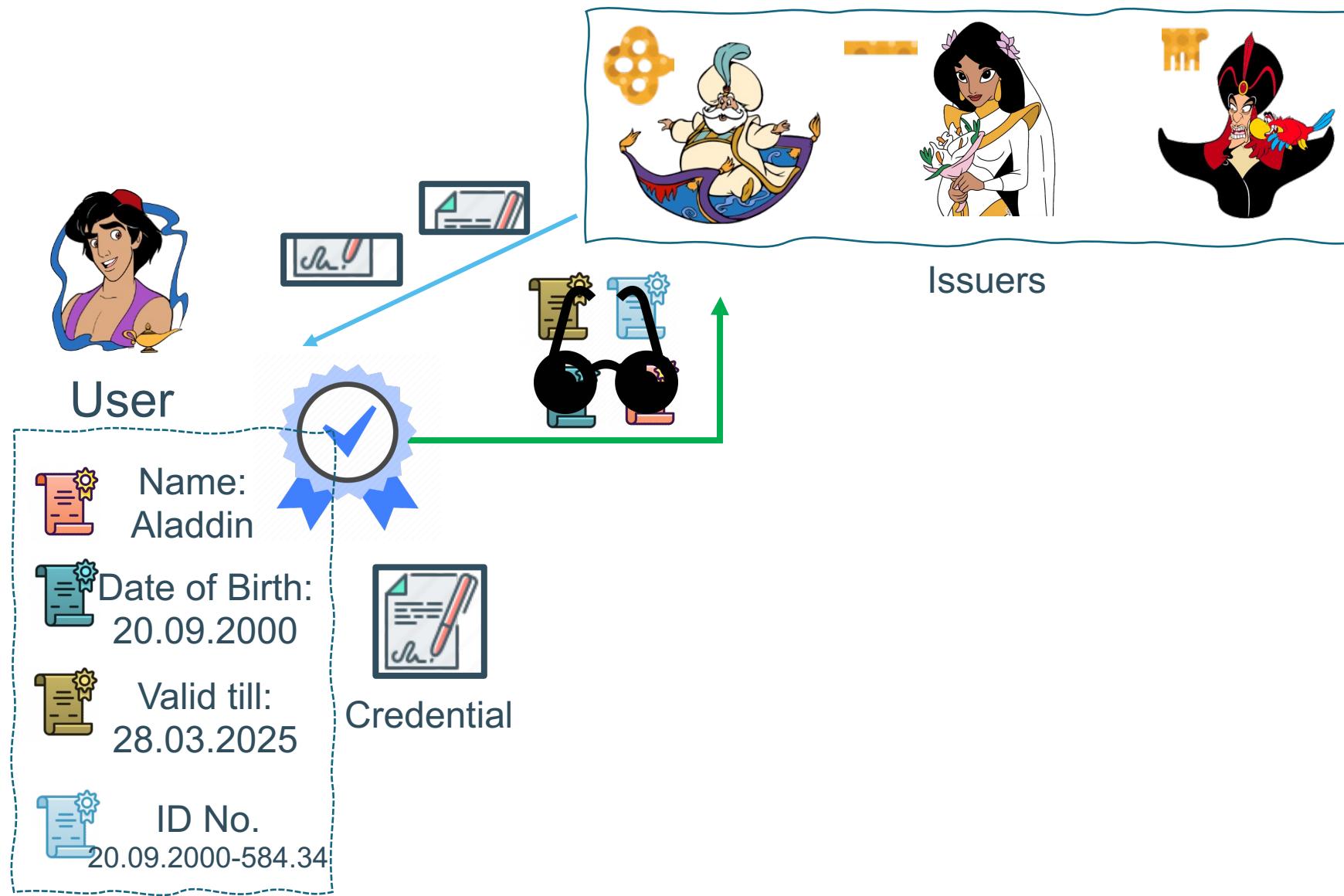


User

	Name: Aladdin
	Date of Birth: 20.09.2000
	Valid till: 28.03.2025
	ID No. 20.09.2000-584.34



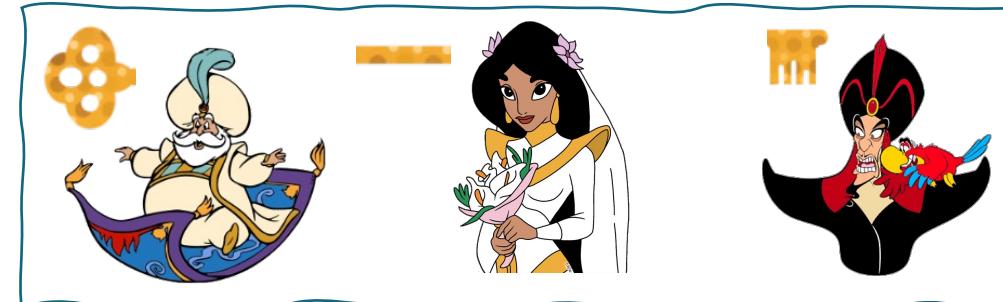
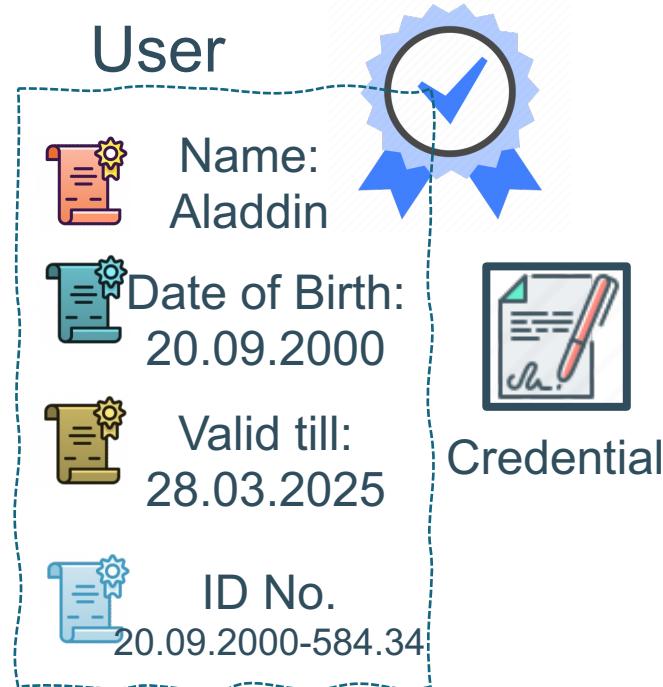
# Threshold-Issuance Anonymous Credential systems:



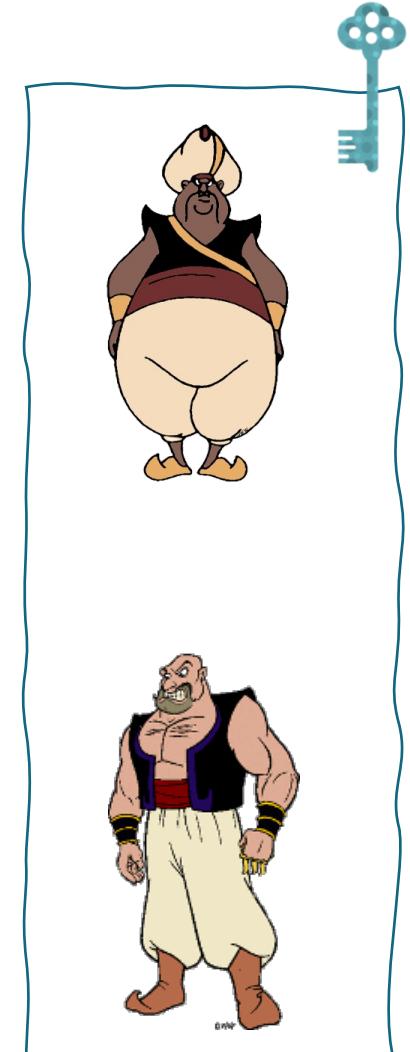
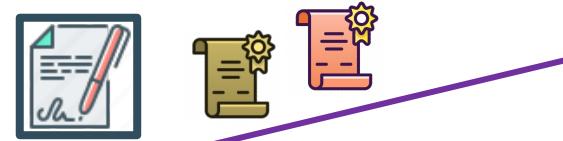
# Threshold-Issuance Anonymous Credential systems:



User



Issuers

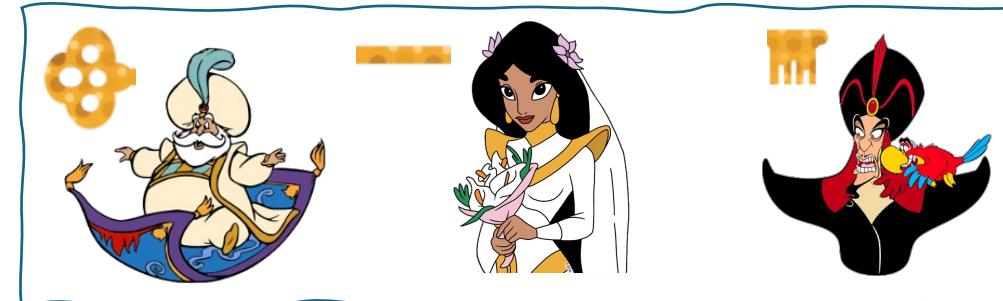
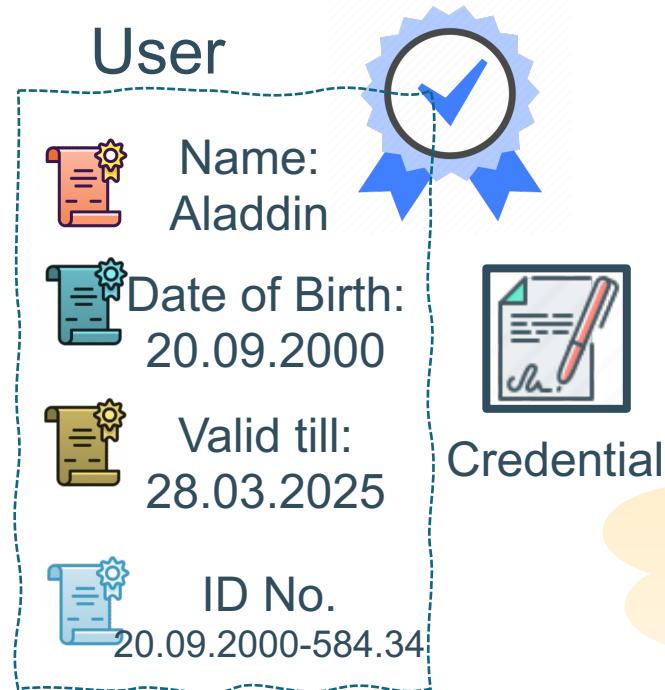


Verifiers

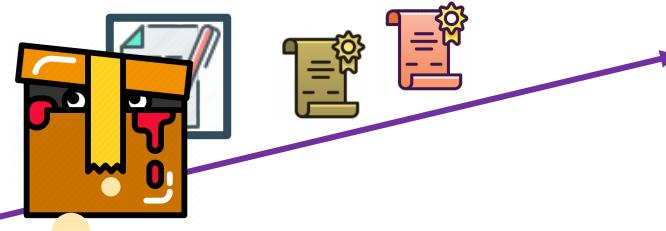
# Threshold-Issuance Anonymous Credential systems:



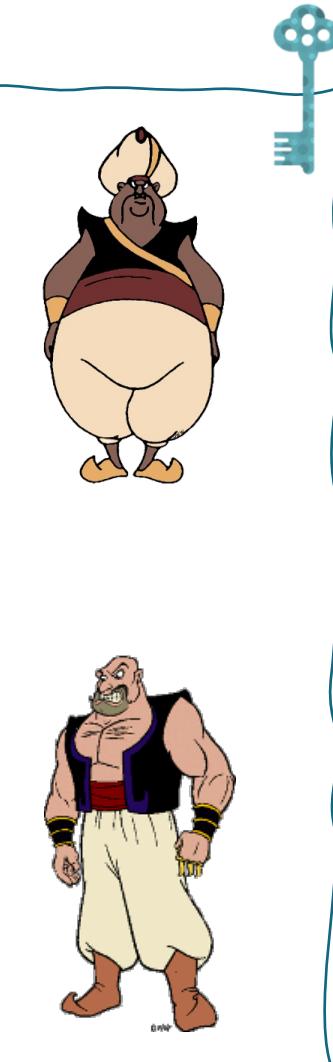
User



Issuers



I have the knowledge of  
a valid Signature from a  
quorum of issuers on  
these attributes.



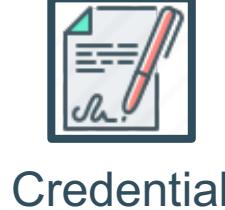
Verifiers

# Threshold-Issuance Anonymous Credential systems:

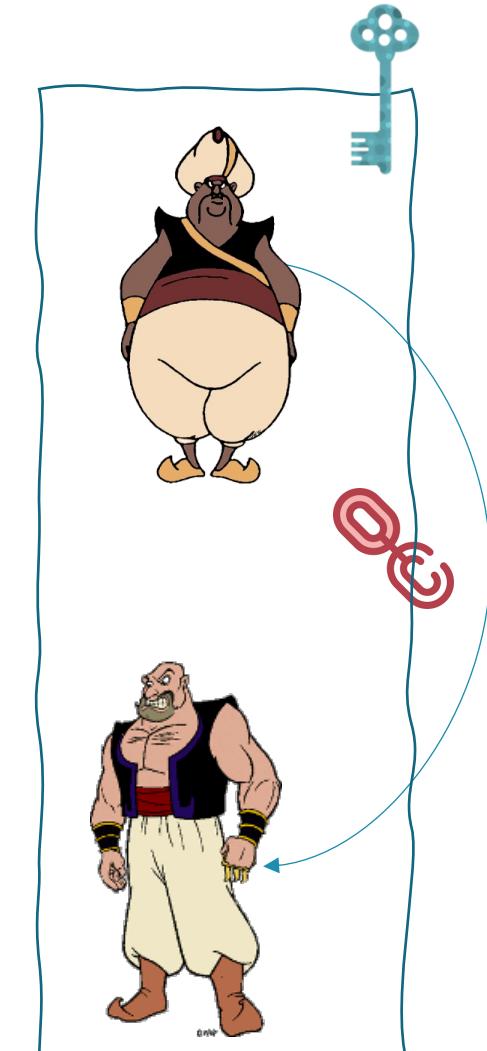
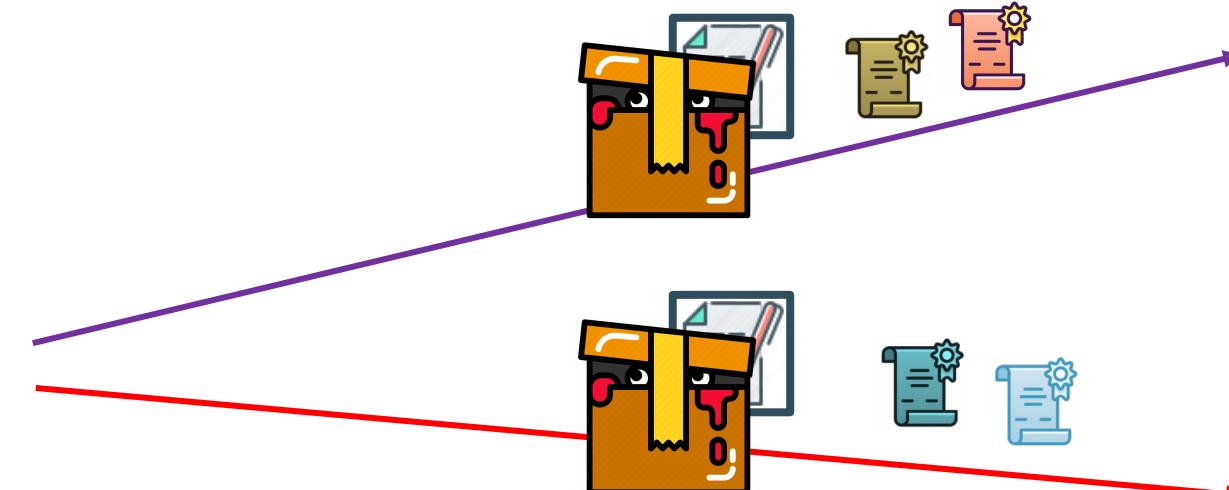


User

	Name: Aladdin
	Date of Birth: 20.09.2000
	Valid till: 28.03.2025
	ID No. 20.09.2000-584.34

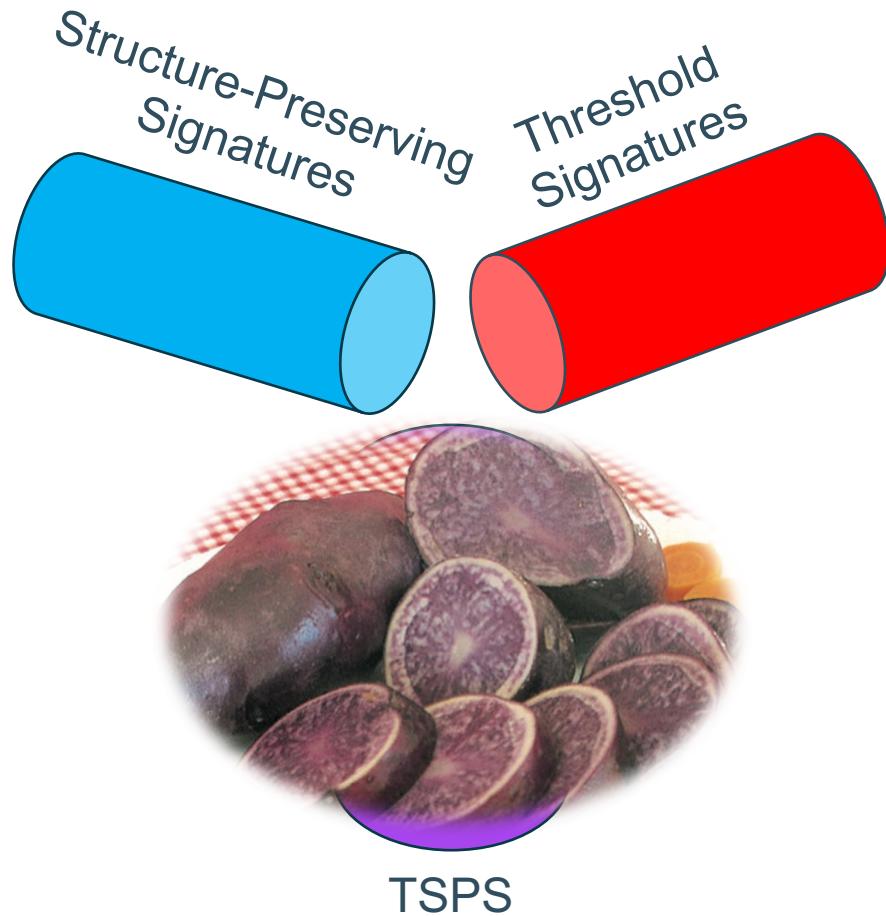


Issuers



Verifiers

# Threshold Structure-Preserving Signatures: To define a new ingredient



## Threshold Structure-Preserving Signatures

Elizabeth Crites<sup>1</sup>, Markulf Kohlweiss<sup>1,2</sup>, Bart Preneel<sup>3</sup>,  
Mahdi Sedaghat<sup>3</sup>, and Daniel Slamanig<sup>4</sup>

<sup>1</sup> University of Edinburgh, Edinburgh, UK  
[ecrites@ed.ac.uk](mailto:ecrites@ed.ac.uk), [mkohlwei@inf.ed.ac.uk](mailto:mkohlwei@inf.ed.ac.uk)

<sup>2</sup> IOG

<sup>3</sup> COSIC, KU Leuven, Leuven, Belgium  
[ssedagha@esat.kuleuven.be](mailto:ssedagha@esat.kuleuven.be), [bart.preneel@esat.kuleuven.be](mailto:bart.preneel@esat.kuleuven.be)

<sup>4</sup> AIT Austrian Institute of Technology, Vienna, Austria  
[daniel.slamanig@ait.ac.at](mailto:daniel.slamanig@ait.ac.at)

## Threshold Structure-Preserving Signatures: Strong and Adaptive Security under Standard Assumptions

Aikaterini Mitrokotsa<sup>1</sup>, Sayantan Mukherjee<sup>2</sup>, Mahdi Sedaghat<sup>3</sup>,  
Daniel Slamanig<sup>4</sup>, and Jenit Tomy<sup>1</sup>

<sup>1</sup> University of St. Gallen, St. Gallen, Switzerland  
[first.last@unisg.ch](mailto:first.last@unisg.ch)

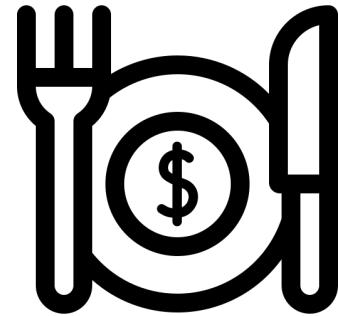
<sup>2</sup> Indian Institute of Technology, Jammu, India  
[csayantan.mukherjee@gmail.com](mailto:csayantan.mukherjee@gmail.com)

<sup>3</sup> COSIC, KU Leuven, Leuven, Belgium  
[ssedagha@esat.kuleuven.be](mailto:ssedagha@esat.kuleuven.be)

<sup>4</sup> Research Institute CODE, Universität der Bundeswehr München, München, Germany  
[daniel.slamanig@unibw.de](mailto:daniel.slamanig@unibw.de)

# Existing TSPS Comparison:

---



Short Signature  
& fast verification



Group Vector  
messages



Adaptive  
Security



Standard  
Assumption

---

Initial TSPS [AC'23]



---

Follow-up work [PKC'24]



# Publications

MLS-ABAC: Efficient Multi-Level Security Attribute Based Access Control scheme. [FGCS'22]

Cross-Domain Attribute-Based Access Control Encryption. [CANS'21]

## Access Control

Reusable, instant and private payment guarantees for cryptocurrencies. [ACISP'23]

Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments. [PETS'24, CTB'24]

## Applications in Blockchain

zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials. [CCS'24, SBC'24]

Subset-optimized BLS Multi-signature with Key Aggregation. [FC'24]

Tiramisu: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model. [CANS'21]

Benchmarking the setup of updatable zk-SNARK. [Latincrypt'23]

Threshold Structure-Preserving Signatures. [Asiacrypt'23]

Threshold Structure Preserving Signatures: Strong and Adaptive Security under Standard Assumptions. [PKC'24]

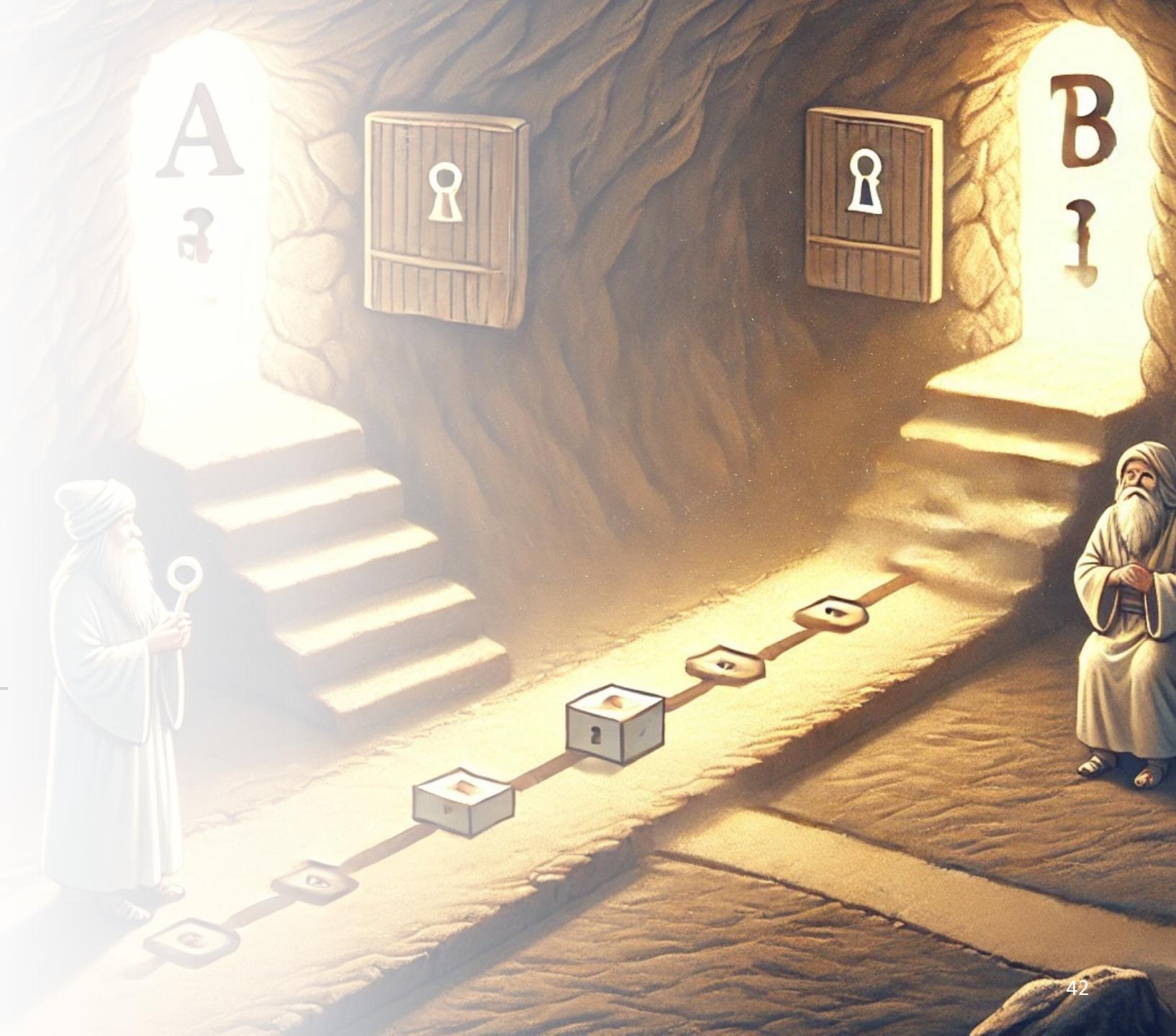
## Non-Interactive Zero-Knowledge



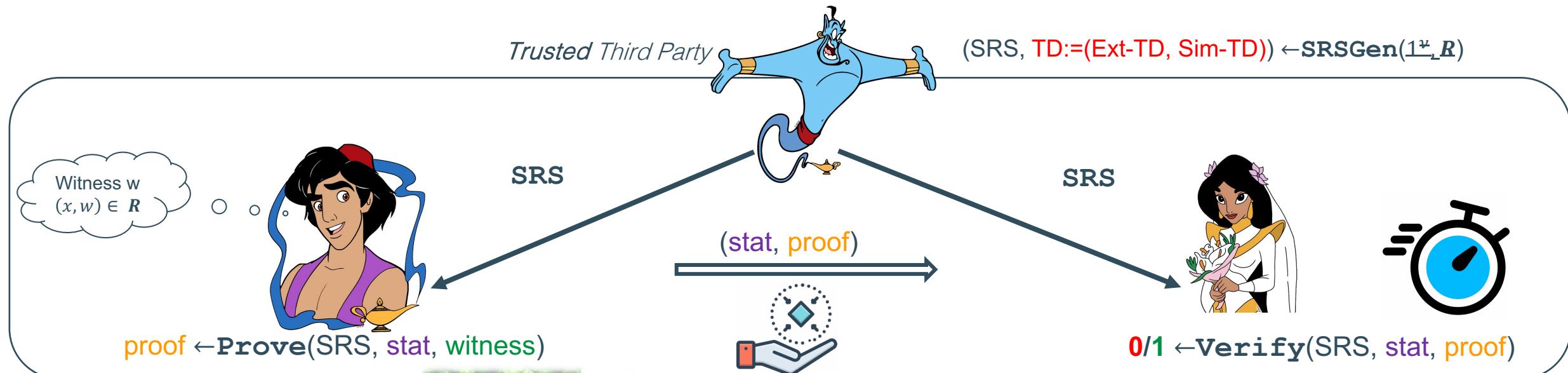
## Threshold Signatures

# Non-Interactive Zero- Knowledge Proofs

To prove the knowledge of secret values without extra leakage



# zk-SNARKs in the SRS Model: Basic Security requirements



- **Zero-Knowledge (ZK)**
- **Knowledge Soundness**
- **Simulation Knowledge Soundness** (a.k.a. Simulation Extractable)



$\text{Ext}(\text{proof}, \text{Ext-TD}) \rightarrow \text{witness}: (\text{stat}, \text{witness}) \in R$

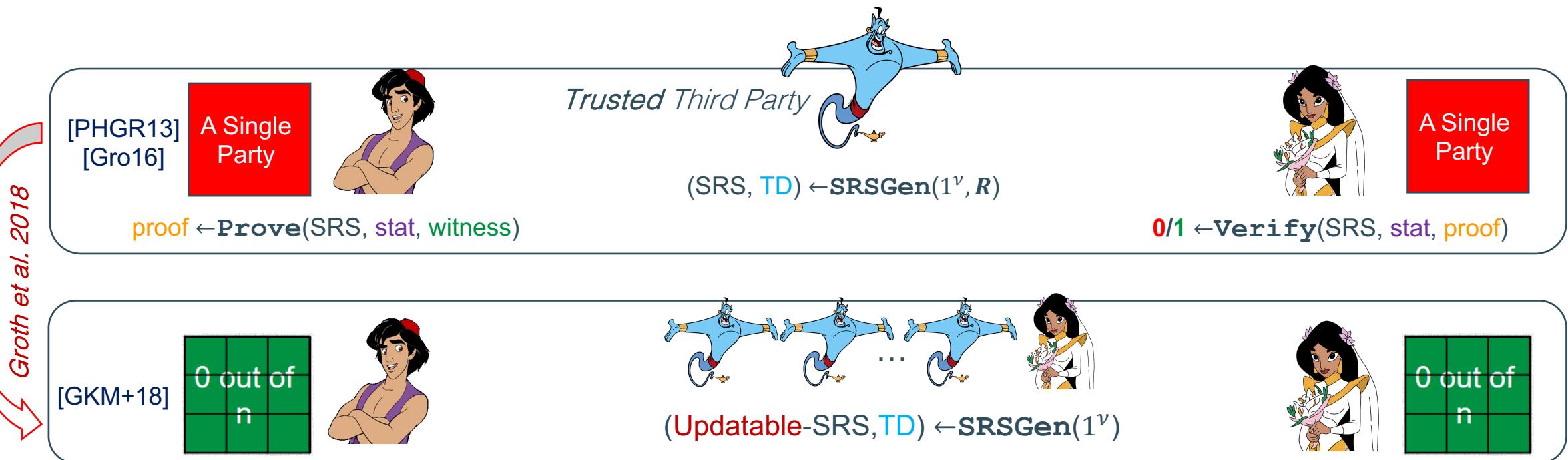
Black-Box and non Black-Box (white-box)



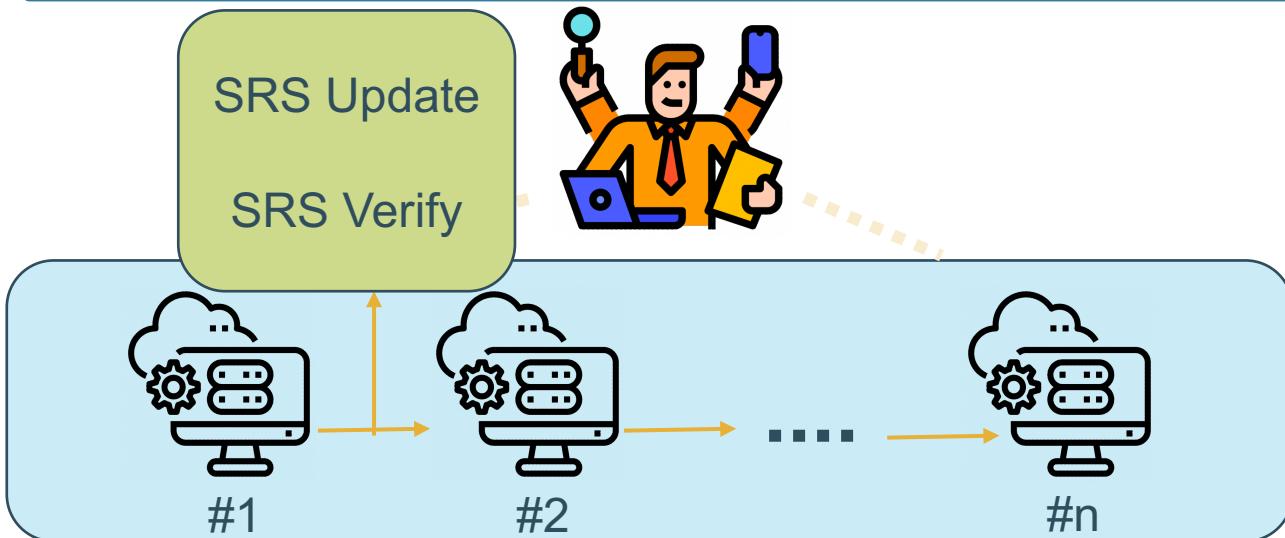
$\text{Sim}(\text{stat}, \text{Sim-TD}) \rightarrow \text{proof}' \approx_c \text{proof}$

# On the setup of NIZKs in the Universal and Updatable SRS-Model: Trust or Update

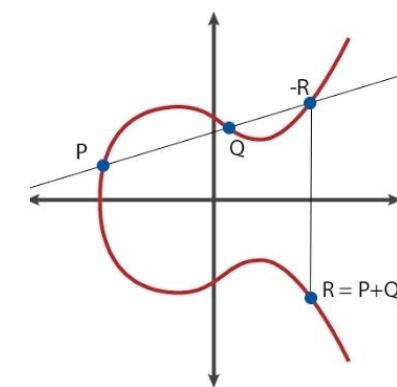
Updatability



# On the setup of NIZKs in the Universal and Updatable SRS-Model: Trust or Update



Ubuntu 20.4.2 LTS,  
Intel Core i9-9900, 3.1 GHz  
128 GB of RAM

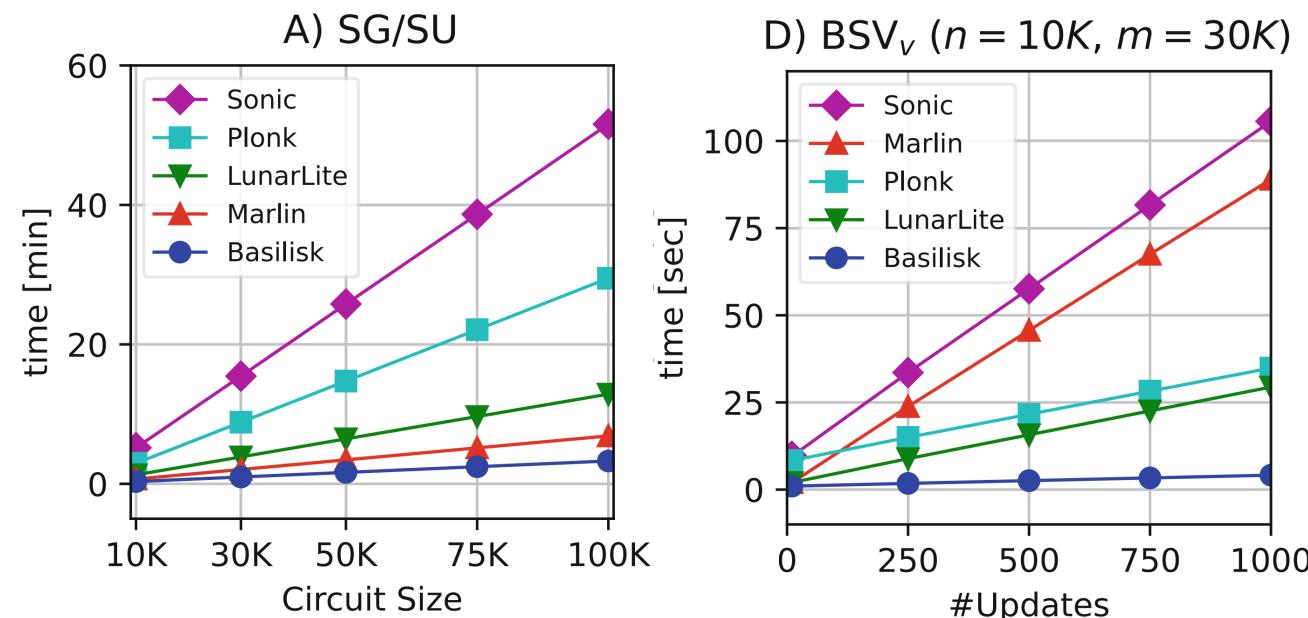


BLS12-381 curve with  
117-120 bits of security

## Benchmarking the Setup of Updatable Zk-SNARKs

Karim Baghery<sup>(✉)</sup> , Axel Mertens , and Mahdi Sedaghat 

COSIC, KU Leuven, Leuven, Belgium  
{karim.baghery,axel.mertens}@kuleuven.be, ssedagha@esat.kuleuven.be



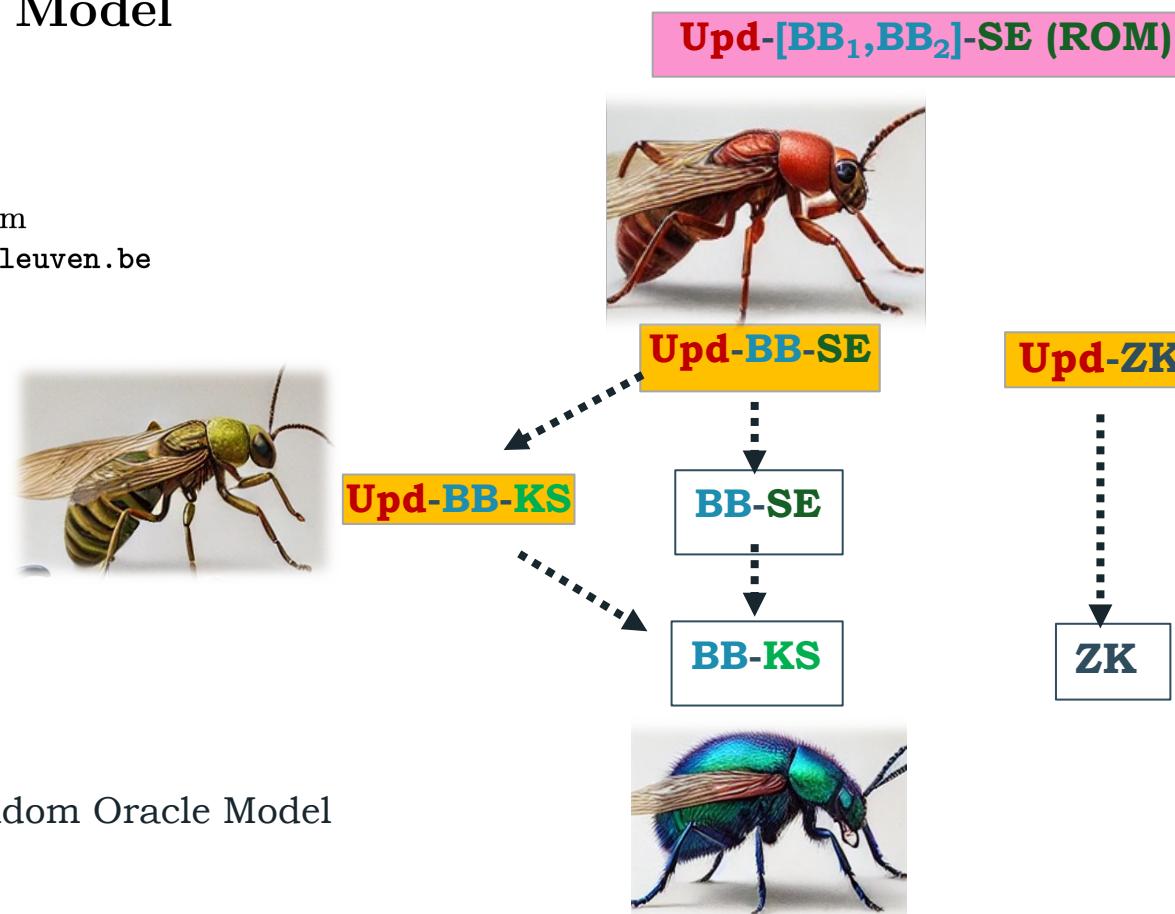
# Upd-BB-SE: Tiramisu as a General Framework to Lift (Upd-nBB-SE or Upd-BB-KS) to Upd-BB-SE

## TIRAMISU: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model

Karim Baghery and Mahdi Sedaghat

imec-COSIC, KU Leuven, Leuven, Belgium  
karim.baghery@kuleuven.be, ssedagha@esat.kuleuven.be

Tiramisu [BS21]  
[GKO+23]  
[AGRS24]  
[CF24,724]



**Sub:** Subversion | **Upd:** Updatable | **ROM:** Random Oracle Model

**BB:** Black-Box | **nBB:** non-Black-Box

**ZK:** Zero-knowledge | **SND:** Soundness | **KS:** Knowledge Sound | **SE:** Simulation Extractable

# Conclusion and Future Work

Still A Long Journey Ahead!

## CONCLUSION AND FUTURE WORK

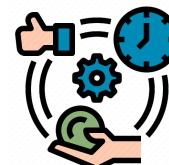
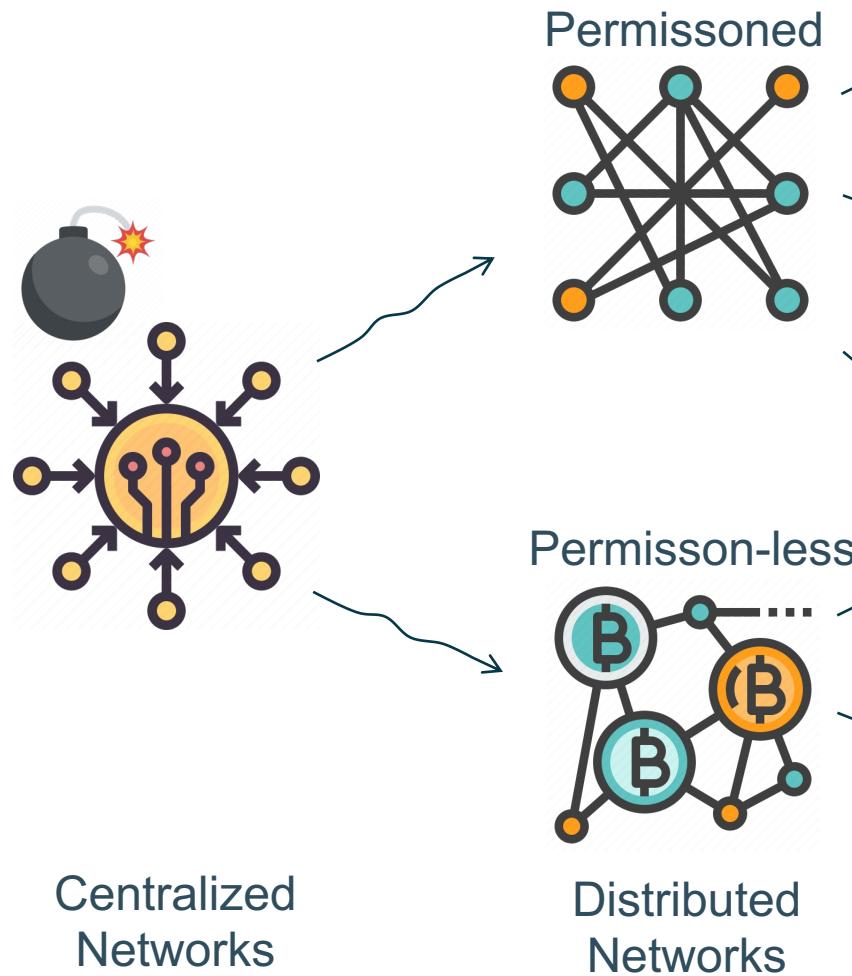
Dr. Pradeep Kumar Jayaraman, M.Tech (Mechanical Engineering),  
Tata Consultancy Services, Mumbai, India. Presented by Jayaraman  
and Suresh Bhambhani at the International Conference on  
Energy Efficient Technologies.

- The research work has been conducted on the basis of the  
existing literature and the results obtained from the  
existing literature have been used to validate the  
research work.



# Discussed Papers in a Nutshell!

Disclaimer: None are secure if adversary has access to a QC! :)



Compatibility



Regulation-Friendly



Privacy



Scalability

AC'23 Threshold Structure-Preserving Signatures

PKC'24 Threshold Structure-Preserving Signatures:  
Strong and Adaptive Security under Standard Assumptions

PETS'24 Unlinkable Policy-Compliant Signatures for Compliant  
and Decentralized Anonymous Payments

CANS'21 Cross-Domain Attribute-Based  
Access Control Encryption\*

LatinCrypt'23 Benchmarking the Setup of Updatable  
zk-SNARKs

TIRAMISU: Black-Box Simulation Extractable  
NIZKs in the Updatable CRS Model

FC'24 Subset-optimized BLS Multi-signature  
with Key Aggregation

Reusable, Instant and Private Payment Guarantees for  
ACISP'23 Cryptocurrencies

# Conclusion:

---

- Distributed Systems reduce the trust to single party.
- Privacy-Enhancing Techniques enable privacy by design.
- Threshold signatures tolerate some fraction of corrupted signers.
- SPS enable a modular framework to design complex systems more efficiently.
- No Threshold SPS exists.
- NIZK is an important privacy-enhancing tool.
- Pre-processing NIZKs., i.e. in the CRS model, require a trusted setup.
- Universal and updatable NIZKs are reducing this trust.
- To model these schemes in the universal composable frameworks we need stronger notions of security such as Upd-BB-SE.

**Disclaimer:** None of the discussed primitives are secure if adversary has access to a QC! /:

# Future Work:

---

## Potential open questions and subsequent works:

- 1) Achieve a TSPS as efficient as the initial work while as secure as the latter TSPS.
- 2) Extend NI-TSPS to NI-TSPS on Equivalence-Classes [2024/625].
- 3) How we can achieve Accountable NI-TSPS.
- 4) Achieve Upd-BB-SE with witness-succinct proofs [2024/724].
- 5) Prove the Sub-ZK of existing UU-SNARKs under AGMOS [TCC'23].





Thank You!

[ssedagha@esat.kuleuven.be](mailto:ssedagha@esat.kuleuven.be)

The illustrations are credited to Disneyclips, Unsplash, DALL.E, iconfinder and google.