KU LEUVEN

FACULTY OF
ENGINEERING SCIENCE

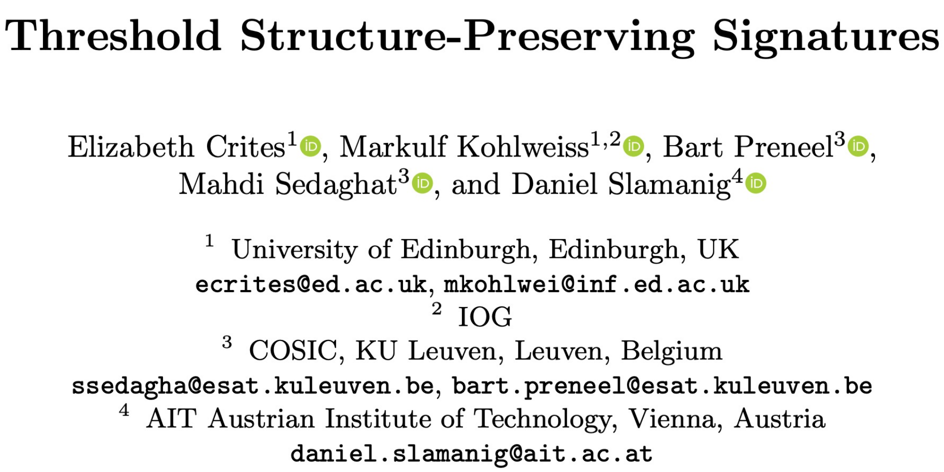
COSIC

Threshold Structure-Preserving Signatures: Done and Ongoing Projects

Mahdi Sedaghat

June 4 (Zurich, Switzerland)

Outline:

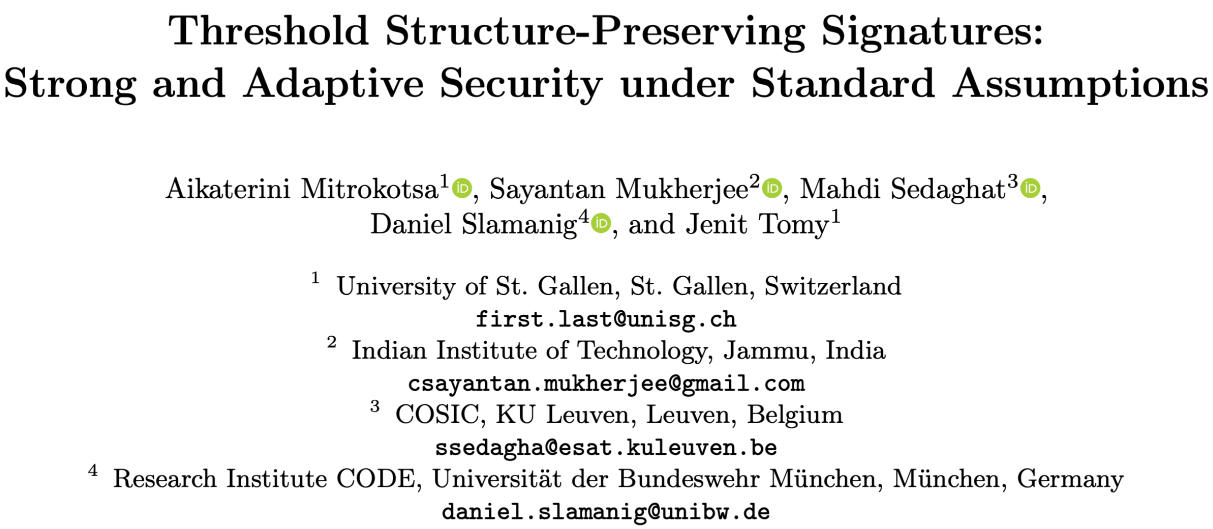


Threshold Structure-Preserving Signatures

Elizabeth Crites[1], Markulf Kohlweiss[1,2], Bart Preneel[3],
Mahdi Sedaghat[3], and Daniel Slamanig[4]

[1] University of Edinburgh, Edinburgh, UK
ecrites@ed.ac.uk, mkohlwei@inf.ed.ac.uk
[2] IOG
[3] COSIC, KU Leuven, Leuven, Belgium
ssedagha@esat.kuleuven.be, bart.preneel@esat.kuleuven.be
[4] AIT Austrian Institute of Technology, Vienna, Austria
daniel.slamanig@ait.ac.at

eprint/2022/839



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

Aikaterini Mitrokotsa[1], Sayantan Mukherjee[2], Mahdi Sedaghat[3],
Daniel Slamanig[4], and Jenit Tomy[1]

[1] University of St. Gallen, St. Gallen, Switzerland
first.last@unisg.ch
[2] Indian Institute of Technology, Jammu, India
csayantan.mukherjee@gmail.com
[3] COSIC, KU Leuven, Leuven, Belgium
ssedagha@esat.kuleuven.be
[4] Research Institute CODE, Universität der Bundeswehr München, München, Germany
daniel.slamanig@unibw.de

eprint/2024/445

Outline:

Threshold Structure-Preserving Signatures

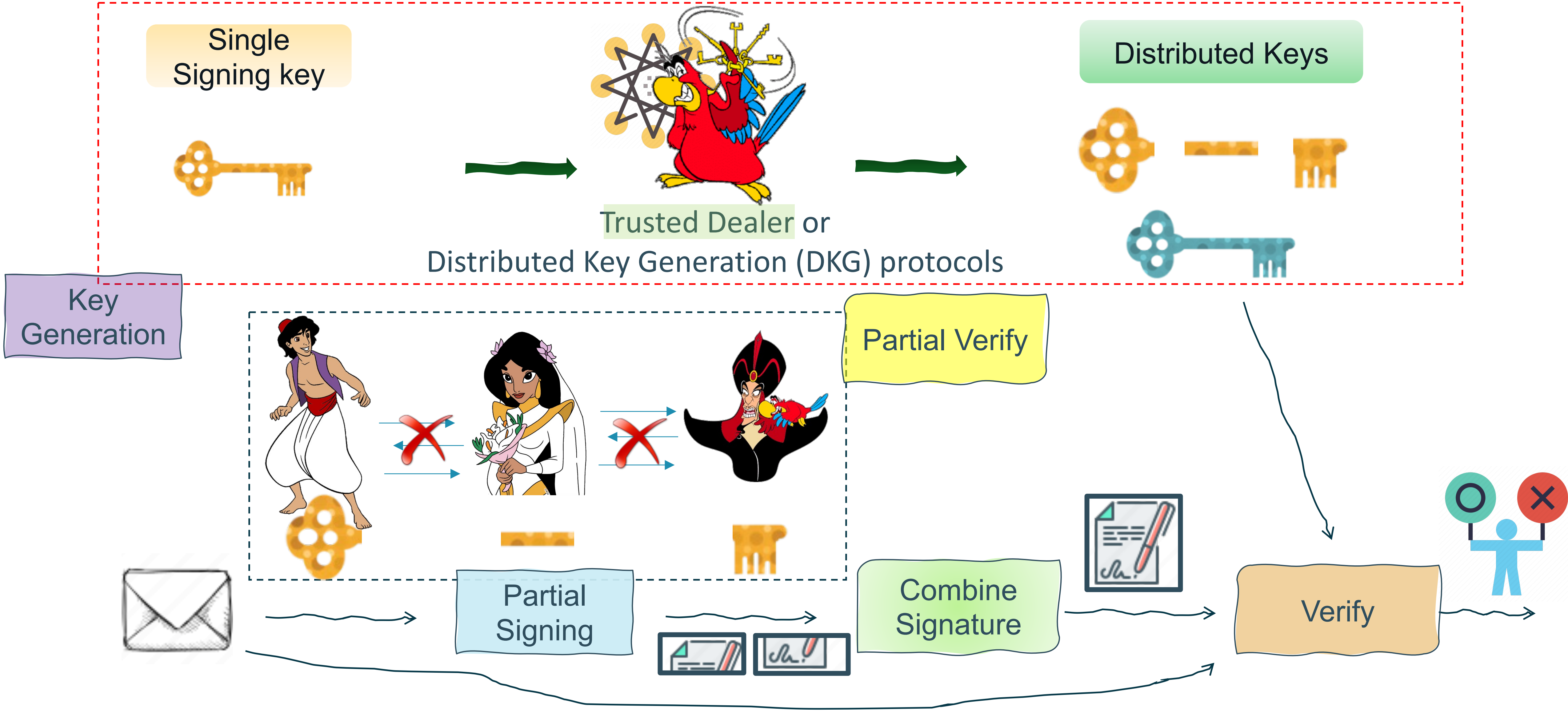
Outline:

Threshold Structure-Preserving Signatures

Threshold Signatures

Structure-Preserving Signatures

(Non-Interactive) Threshold Signatures: To Tolerate Some Fraction of Corrupt Signers



Single Signing key

Trusted Dealer or
Distributed Key Generation (DKG) protocols

Distributed Keys

Key Generation

Partial Verify

Partial Signing

Combine Signature

Verify

BLS signature [BLS04]: A simple not one-time NI-TS over bilinear groups*

Key Generation

$sk := x \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ $vk := [x]_2$

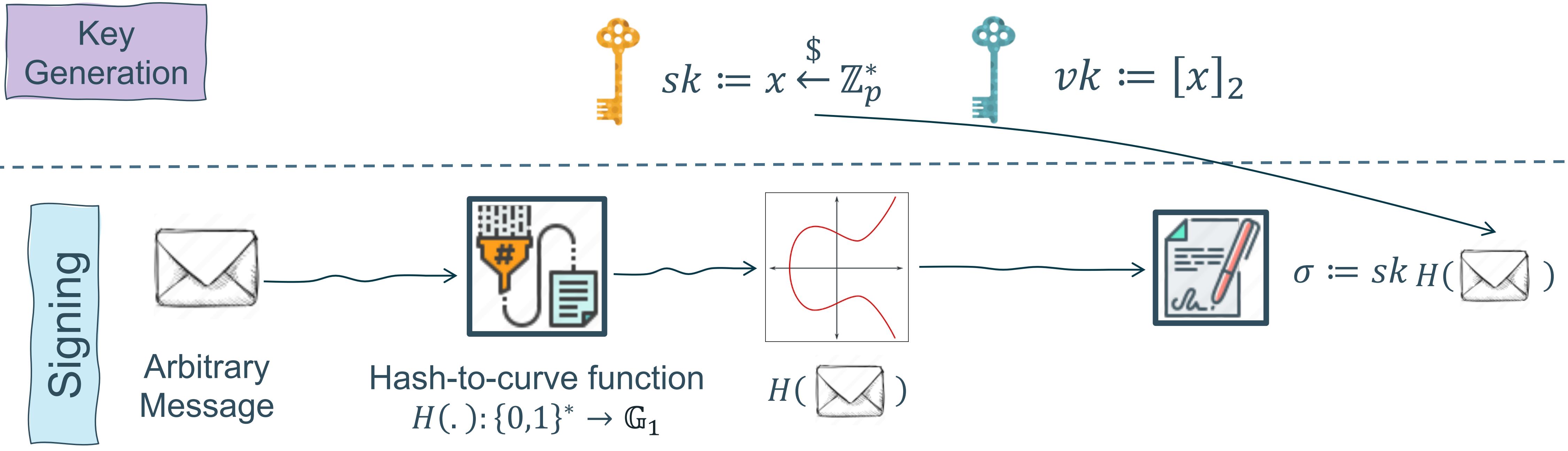
* (Type-III) Bilinear Groups:

Source groups

Target group

- There exists an efficient map e: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$:
  - **Bilinearity**: $e([x]_1, [y]_2) = [xy]_T\,,\ \forall\, x, y \in \mathbb{Z}_p$
  - **Non-degenerate**: $e(G_1, G_2) \neq 1_{\mathbb{G}_T}$
  - $\mathbb{G}_1 =< G_1 >, \mathbb{G}_2 =< G_2 >, \mathbb{G}_T =< e(G_1, G_2) >$

BLS signature [BLS04]: A simple not one-time NI-TS



Key Generation

$sk := x \xleftarrow{\$} \mathbb{Z}_p^*$

$vk := [x]_2$

Signing

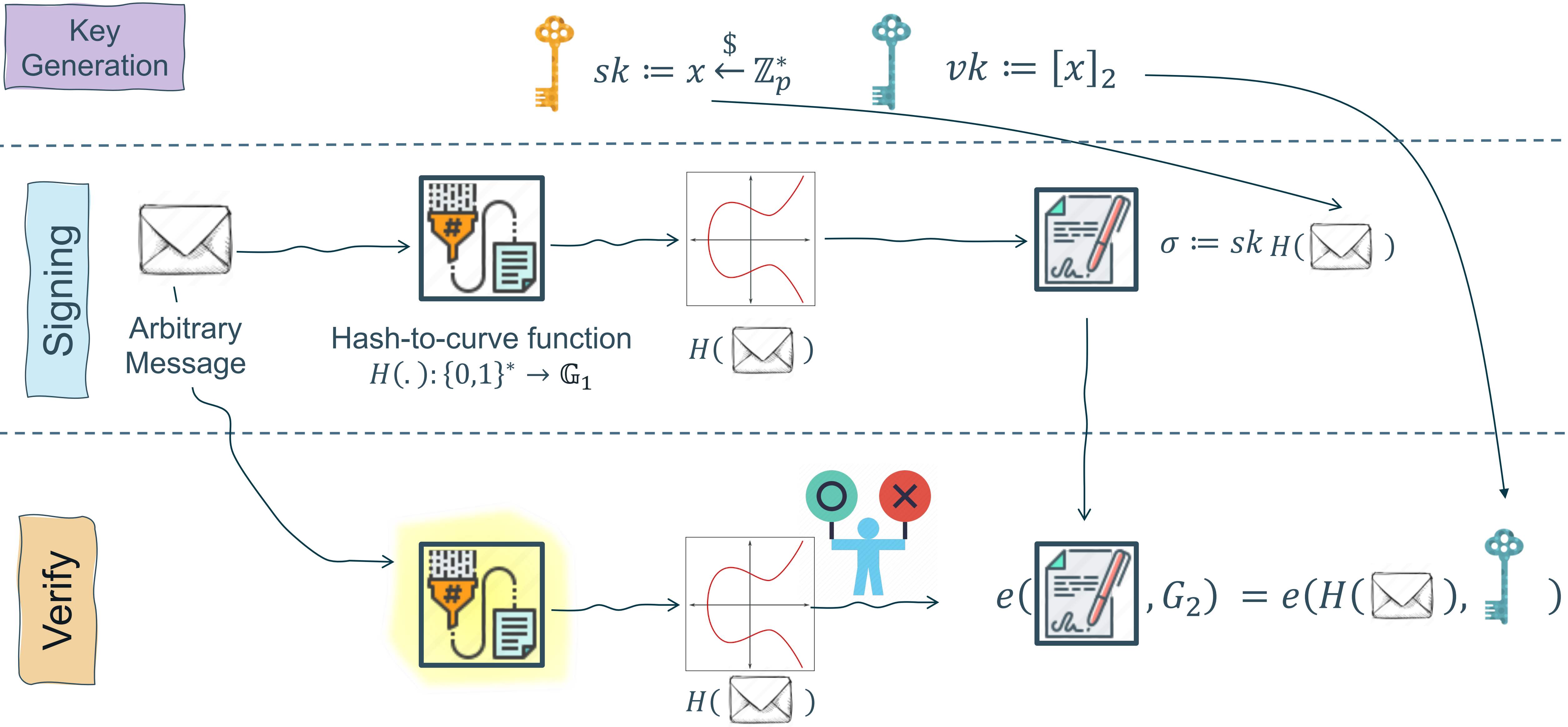
Arbitrary Message

Hash-to-curve function
$H(.) : \{0,1\}^* \rightarrow \mathbb{G}_1$

$H($✉$)$

$\sigma := sk\; H($✉$)$

BLS signature [BLS04]: A simple not one-time NI-TS



Key Generation

$sk := x \xleftarrow{\$} \mathbb{Z}_p^*$

$vk := [x]_2$

Signing

Arbitrary Message

Hash-to-curve function

$H(.): \{0,1\}^* \rightarrow \mathbb{G}_1$

$H($✉$)$

$\sigma := sk\, H($✉$)$

Verify

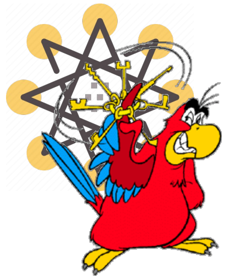
$H($✉$)$

$e($📝$, G_2) = e(H($✉$),$ 🔑 $)$

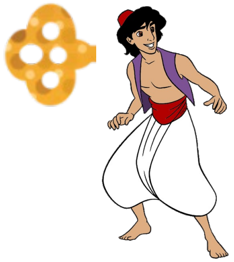
Threshold BLS signature [Bol03]: A simple example of NI-TS

Key Generation

$sk := x \overset{\$}{\leftarrow} \mathbb{Z}_p^*$



Trusted Dealer or DKG



$sk_1 := x_1$

$vk_1 := [x_1]_2$

$sk_2 := x_2$

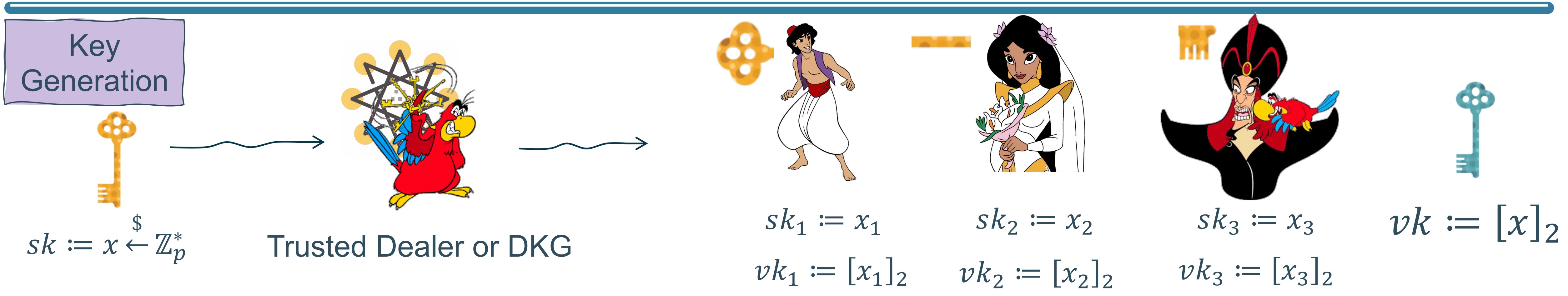
$vk_2 := [x_2]_2$

$sk_3 := x_3$

$vk_3 := [x_3]_2$

$vk := [x]_2$

Threshold BLS signature [Bol03]: A simple example of NI-TS



Key Generation

$sk := x \xleftarrow{\$} \mathbb{Z}_p^*$

Trusted Dealer or DKG

$sk_1 := x_1$

$vk_1 := [x_1]_2$

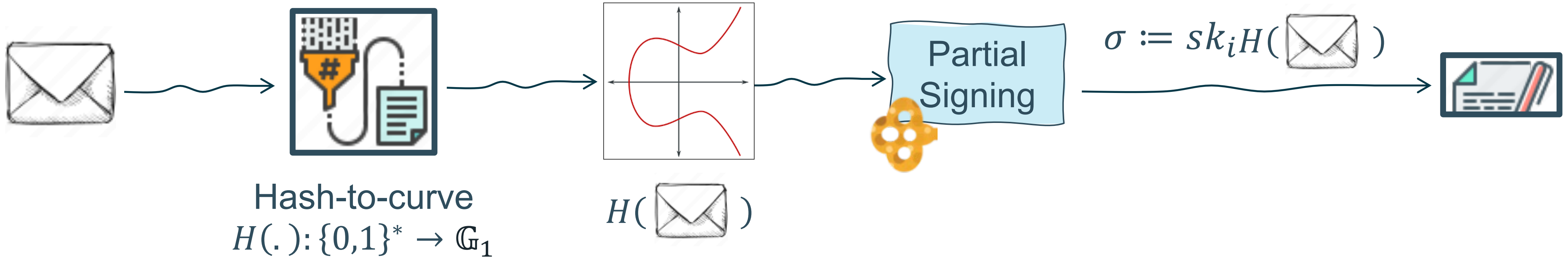
$sk_2 := x_2$

$vk_2 := [x_2]_2$

$sk_3 := x_3$

$vk_3 := [x_3]_2$

$vk := [x]_2$



Hash-to-curve

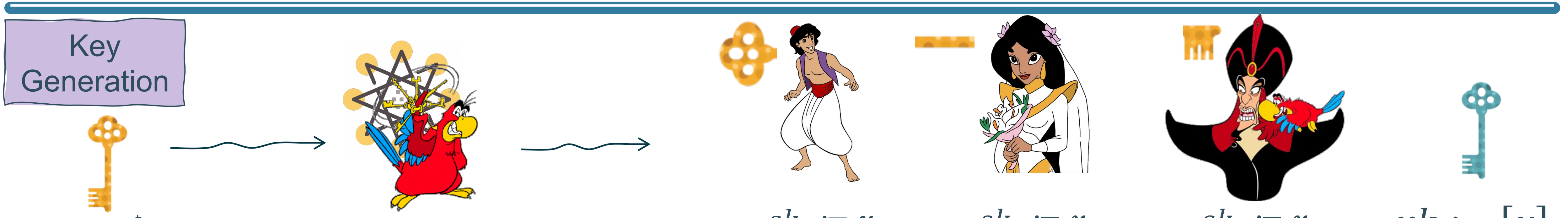
$H(.): \{0,1\}^* \to \mathbb{G}_1$

$H($ ✉ $)$

Partial Signing

$\sigma := sk_i H($ ✉ $)$

Threshold BLS signature [Bol03]: A simple example of NI-TS



Key Generation

$sk := x \overset{\$}{\leftarrow} \mathbb{Z}_p^*$

Trusted Dealer or DKG

$sk_1 := x_1$

$vk_1 := [x_1]_2$

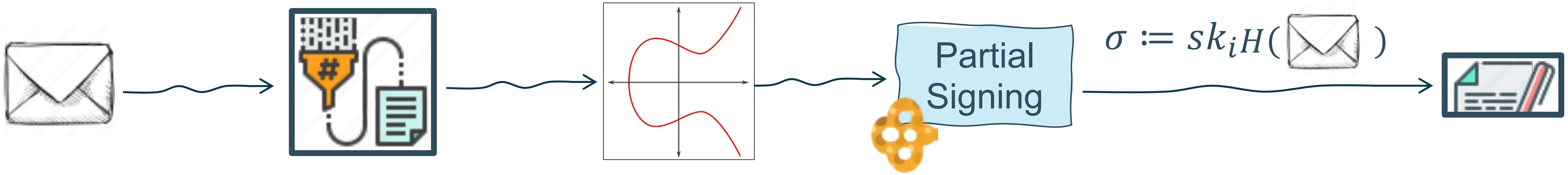
$sk_2 := x_2$

$vk_2 := [x_2]_2$

$sk_3 := x_3$

$vk_3 := [x_3]_2$

$vk := [x]_2$



Hash-to-curve

$H(.) : \{0,1\}^* \rightarrow \mathbb{G}_1$

$H($✉$)$

Partial Signing

$\sigma := sk_i H($✉$)$

Combine Signature

$\sigma = \sum_i L_i^T(0)\sigma_i = sk\, H($✉$)$ $\quad |T| \geq t$

Structure-Preserving Signatures [AFG+10]: To Preserve an Algebraic Structure Over Bilinear Groups

1 🔑 📝 ✉

Source group elements of either $\mathbb{G}_1$ or $\mathbb{G}_2$

No Non-Li e Hash Functions

BLS is not a SPS!

2 To verify a signature of this type only do:

- ❖ membership tests

🔑 📝 ✉ $\in \mathbb{G}_1 \vee \mathbb{G}_2$

- ❖ pairing product equations

$e($✉, 🔑$)e($📝$, G_2) = 1_{\mathbb{G}_T}$

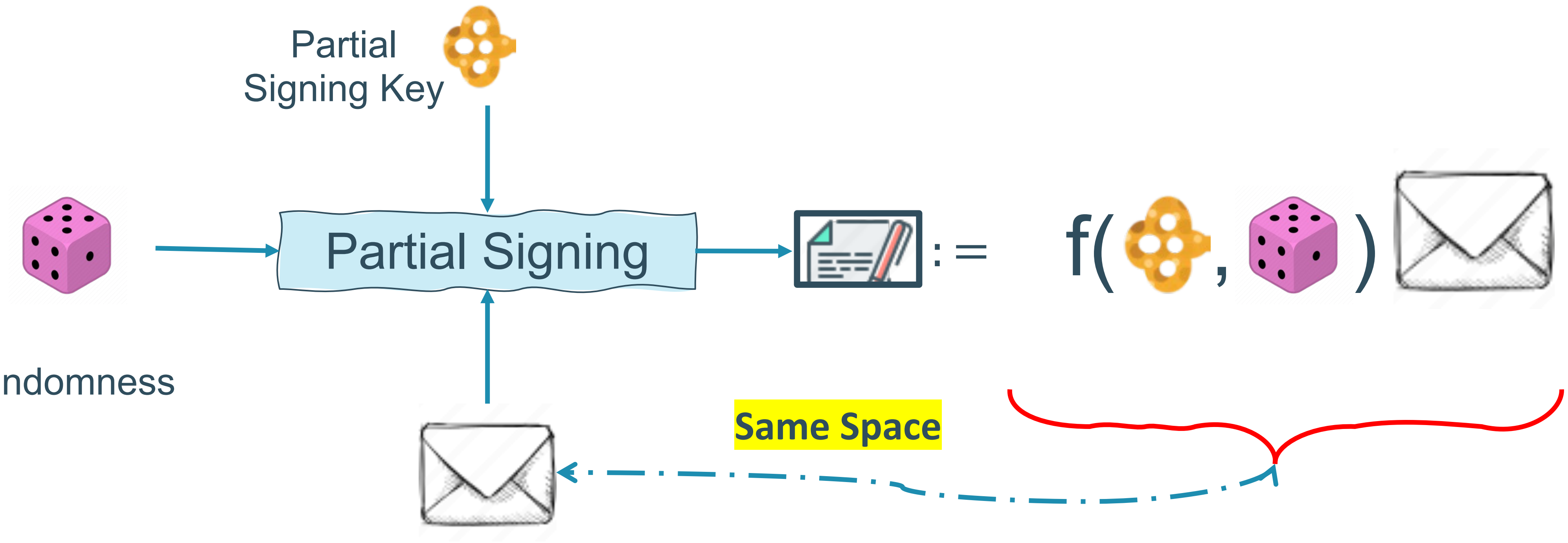
A general framework for efficient generic constructions of cryptographic primitives over bilinear groups.

1. **Groth-Sahai [GS08] proof system friendly**
   - ➢ Straight-line extraction.
   - ➢ Standard Model.
   - ➢ Applications: group signatures, blind signatures, etc.
2. **Enabling Modular Design in complex systems**
   - ➢ Makes easy to combine building blocks.

Our Main Objective and Technical Challenges:

There is NO Threshold Structure-Preserving Signature Scheme (TSPS).

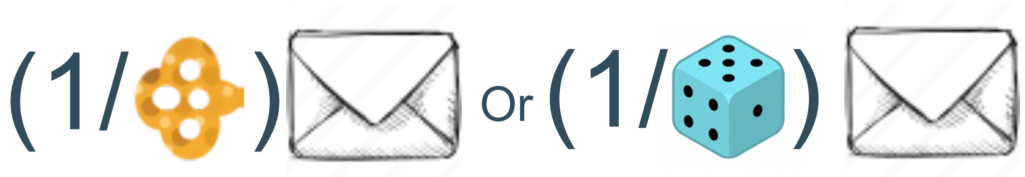
Non-Interactive and not one-time TSPS.



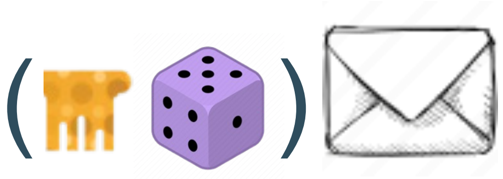
Technical Challenges: Forbidden Operations in Partial Signatures

An SPS is said threshold friendly, if it avoids all these non-linear operations.

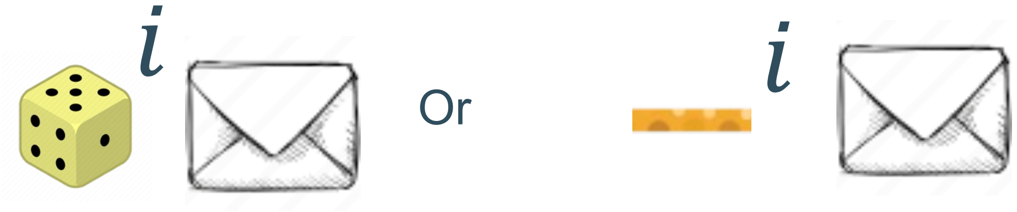
1 Randomness or secret share inverse:



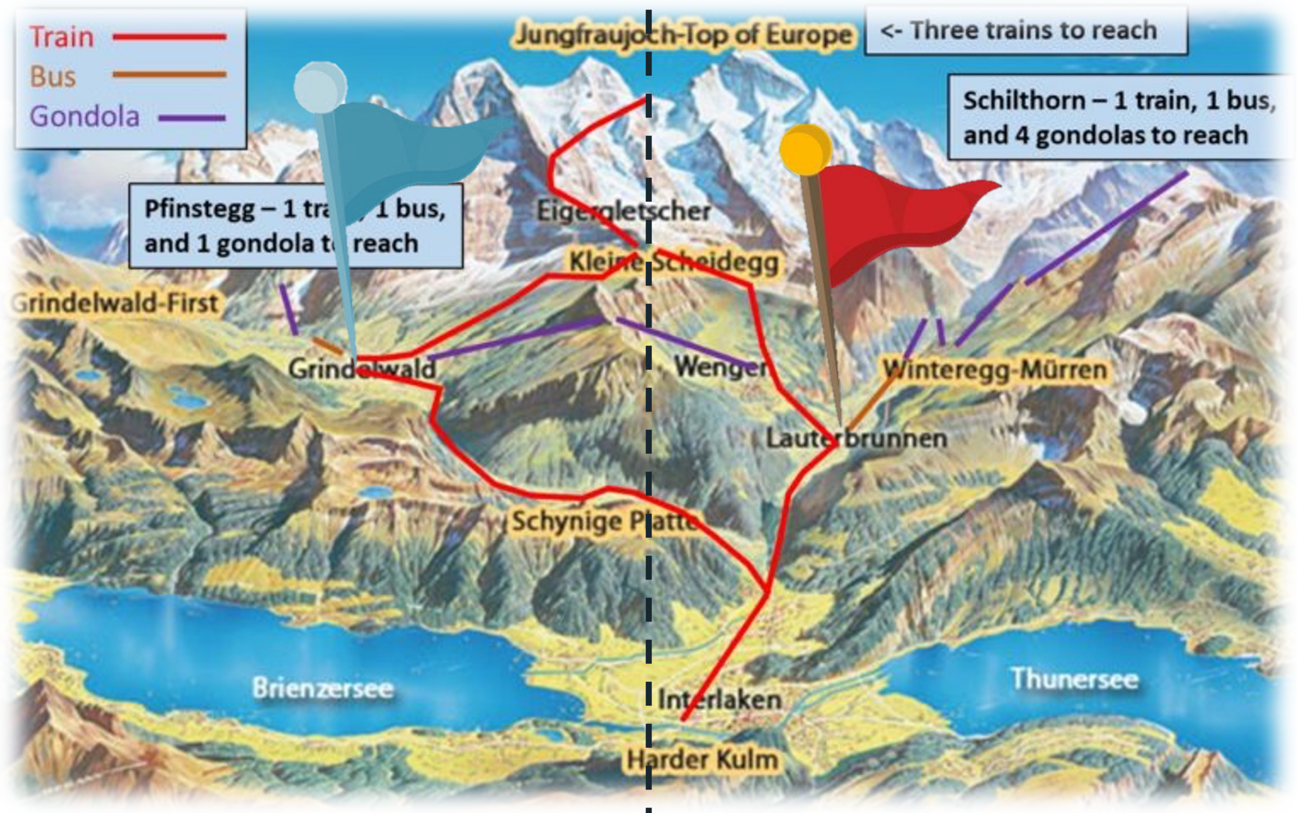
2 Randomness and secret share multiplication:



3 Powers of secret share or randomness:



Treasure map: To look for a Non-Interactive TSPS



<- Three trains to reach

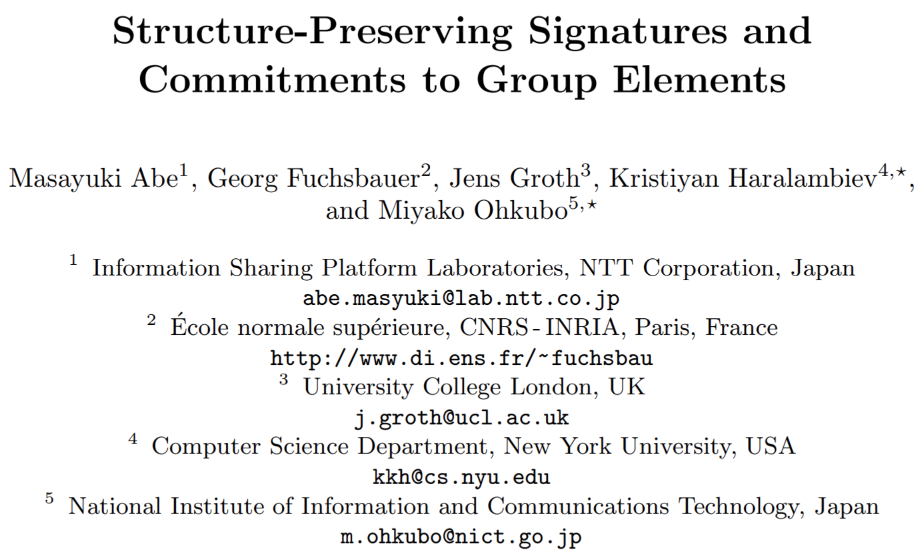
Schilthorn – 1 train, 1 bus, and 4 gondolas to reach

Pfinstegg – 1 tra 1 bus, and 1 gondola t reach

Threshold Signatures

Structure-Preserving Signatures

Some Existing Structure-Preserving Signatures:

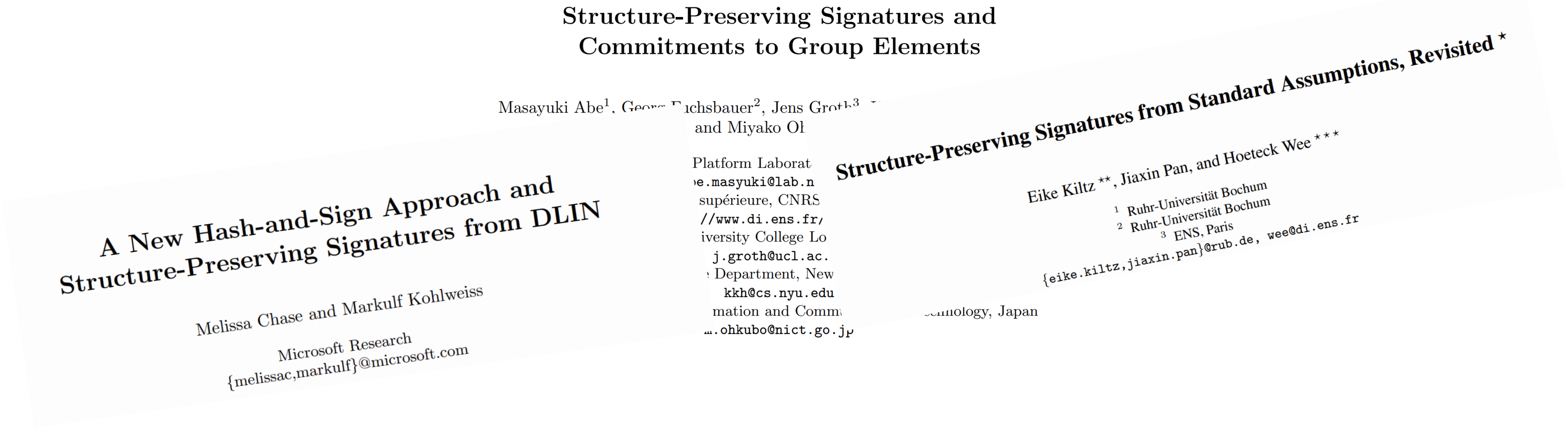


Structure-Preserving Signatures and Commitments to Group Elements

Masayuki Abe[1], Georg Fuchsbauer[2], Jens Groth[3], Kristiyan Haralambiev[4,⋆],
and Miyako Ohkubo[5,⋆]

[1] Information Sharing Platform Laboratories, NTT Corporation, Japan
abe.masyuki@lab.ntt.co.jp
[2] École normale supérieure, CNRS - INRIA, Paris, France
http://www.di.ens.fr/~fuchsbau
[3] University College London, UK
j.groth@ucl.ac.uk
[4] Computer Science Department, New York University, USA
kkh@cs.nyu.edu
[5] National Institute of Information and Communications Technology, Japan
m.ohkubo@nict.go.jp

Some Existing Structure-Preserving Signatures:



Structure-Preserving Signatures and
Commitments to Group Elements

Masayuki Abe[1], Georg Fuchsbauer[2], Jens Groth[3],
and Miyako Oh

Platform Laborat
be.masyuki@lab.n
supérieure, CNRS
//www.di.ens.fr/
iversity College Lo
j.groth@ucl.ac.
Department, New
kkh@cs.nyu.edu
mation and Comm
m.ohkubo@nict.go.jp
chnology, Japan

A New Hash-and-Sign Approach and
Structure-Preserving Signatures from DLIN

Melissa Chase and Markulf Kohlweiss

Microsoft Research
{melissac,markulf}@microsoft.com

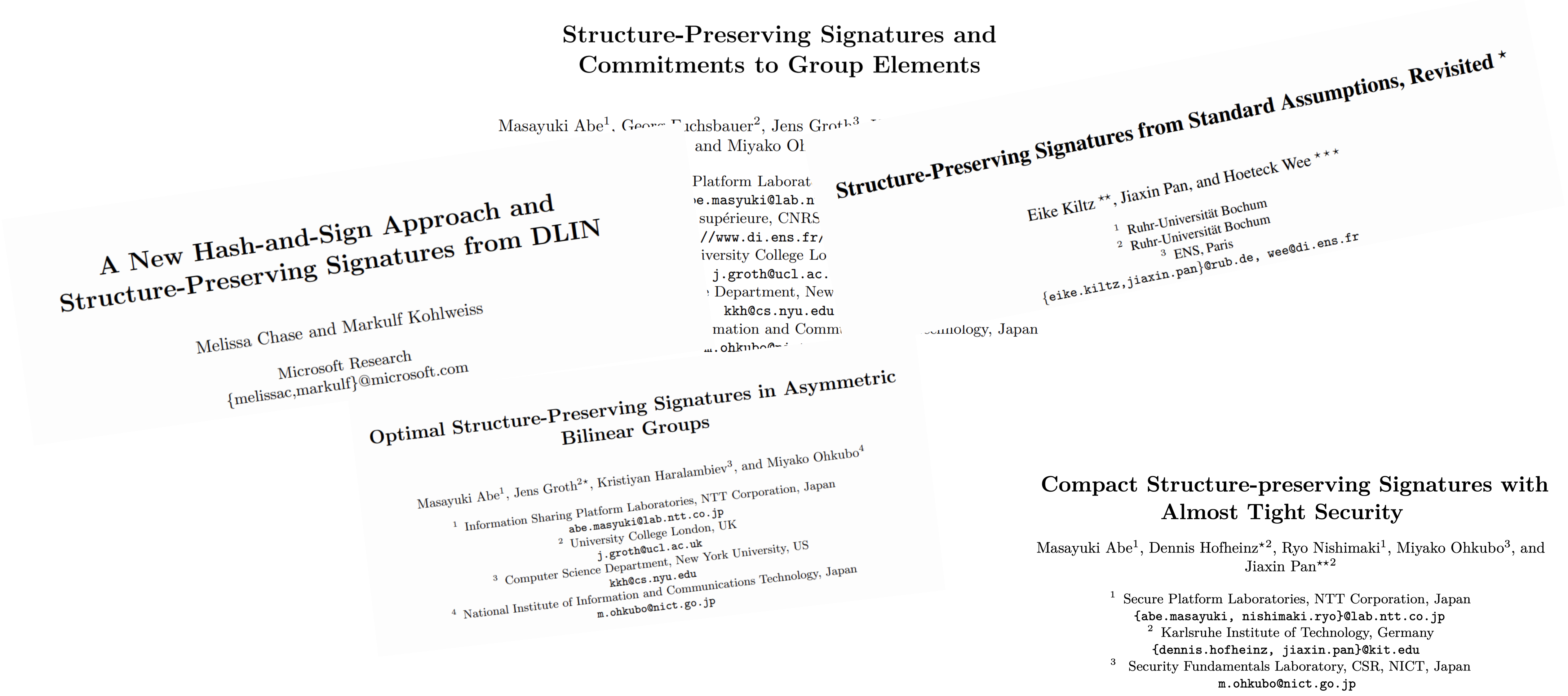
Structure-Preserving Signatures from Standard Assumptions, Revisited *

Eike Kiltz **, Jiaxin Pan, and Hoeteck Wee ***

[1] Ruhr-Universität Bochum
[2] Ruhr-Universität Bochum
[3] ENS, Paris

{eike.kiltz,jiaxin.pan}@rub.de, wee@di.ens.fr

Some Existing Structure-Preserving Signatures:



Structure-Preserving Signatures and
Commitments to Group Elements

Masayuki Abe[1], Georg Fuchsbauer[2], Jens Groth[3],
and Miyako Oh

Platform Laborat
be.masyuki@lab.n
supérieure, CNRS
//www.di.ens.fr/
iversity College Lo
j.groth@ucl.ac.
Department, New
kkh@cs.nyu.edu
mation and Comm
m.ohkubo@n
chnology, Japan

A New Hash-and-Sign Approach and
Structure-Preserving Signatures from DLIN

Melissa Chase and Markulf Kohlweiss

Microsoft Research
{melissac,markulf}@microsoft.com

Structure-Preserving Signatures from Standard Assumptions, Revisited *

Eike Kiltz **, Jiaxin Pan, and Hoeteck Wee ***

[1] Ruhr-Universität Bochum
[2] Ruhr-Universität Bochum
[3] ENS, Paris

{eike.kiltz,jiaxin.pan}@rub.de, wee@di.ens.fr

Optimal Structure-Preserving Signatures in Asymmetric
Bilinear Groups

Masayuki Abe[1], Jens Groth[2*], Kristiyan Haralambiev[3], and Miyako Ohkubo[4]

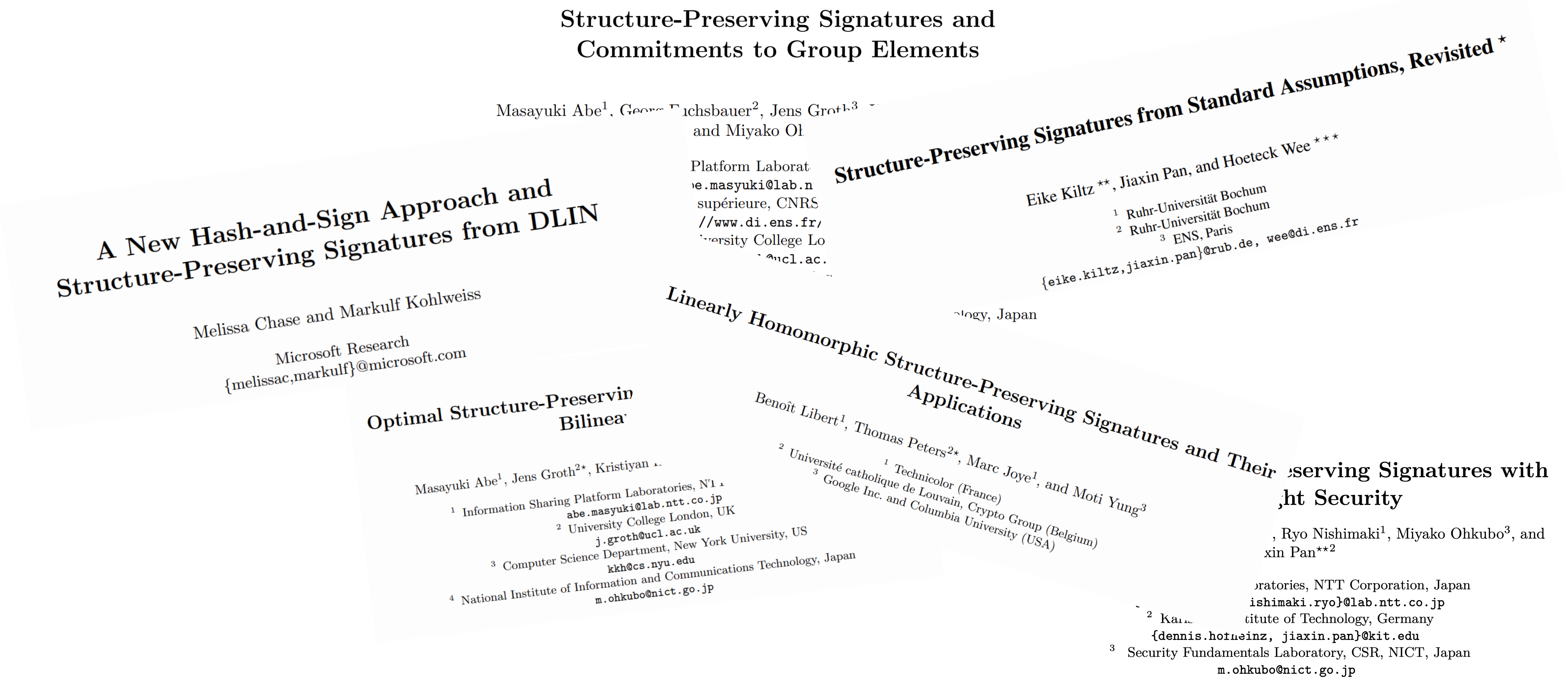
[1] Information Sharing Platform Laboratories, NTT Corporation, Japan
abe.masyuki@lab.ntt.co.jp
[2] University College London, UK
j.groth@ucl.ac.uk
[3] Computer Science Department, New York University, US
kkh@cs.nyu.edu
[4] National Institute of Information and Communications Technology, Japan
m.ohkubo@nict.go.jp

Compact Structure-preserving Signatures with
Almost Tight Security

Masayuki Abe[1], Dennis Hofheinz[*2], Ryo Nishimaki[1], Miyako Ohkubo[3], and
Jiaxin Pan[**2]

[1] Secure Platform Laboratories, NTT Corporation, Japan
{abe.masayuki, nishimaki.ryo}@lab.ntt.co.jp
[2] Karlsruhe Institute of Technology, Germany
{dennis.hofheinz, jiaxin.pan}@kit.edu
[3] Security Fundamentals Laboratory, CSR, NICT, Japan
m.ohkubo@nict.go.jp

Some Existing Structure-Preserving Signatures:



Structure-Preserving Signatures and
Commitments to Group Elements

Masayuki Abe[1], Georg Fuchsbauer[2], Jens Groth[3],
and Miyako Oh

Platform Laborat
abe.masyuki@lab.n
supérieure, CNRS
//www.di.ens.fr/
University College Lo
@ucl.ac.
ology, Japan

A New Hash-and-Sign Approach and
Structure-Preserving Signatures from DLIN

Melissa Chase and Markulf Kohlweiss

Microsoft Research
{melissac,markulf}@microsoft.com

Structure-Preserving Signatures from Standard Assumptions, Revisited *

Eike Kiltz **, Jiaxin Pan, and Hoeteck Wee * * *

[1] Ruhr-Universität Bochum
[2] Ruhr-Universität Bochum
[3] ENS, Paris
{eike.kiltz,jiaxin.pan}@rub.de, wee@di.ens.fr

Optimal Structure-Preservin
Bilinea

Masayuki Abe[1], Jens Groth[2]*, Kristiyan

[1] Information Sharing Platform Laboratories, NT
abe.masyuki@lab.ntt.co.jp
[2] University College London, UK
j.groth@ucl.ac.uk
[3] Computer Science Department, New York University, US
kkh@cs.nyu.edu
[4] National Institute of Information and Communications Technology, Japan
m.ohkubo@nict.go.jp

Linearly Homomorphic Structure-Preserving Signatures and Their
Applications

Benoît Libert[1], Thomas Peters[2]*, Marc Joye[1], and Moti Yung[3]

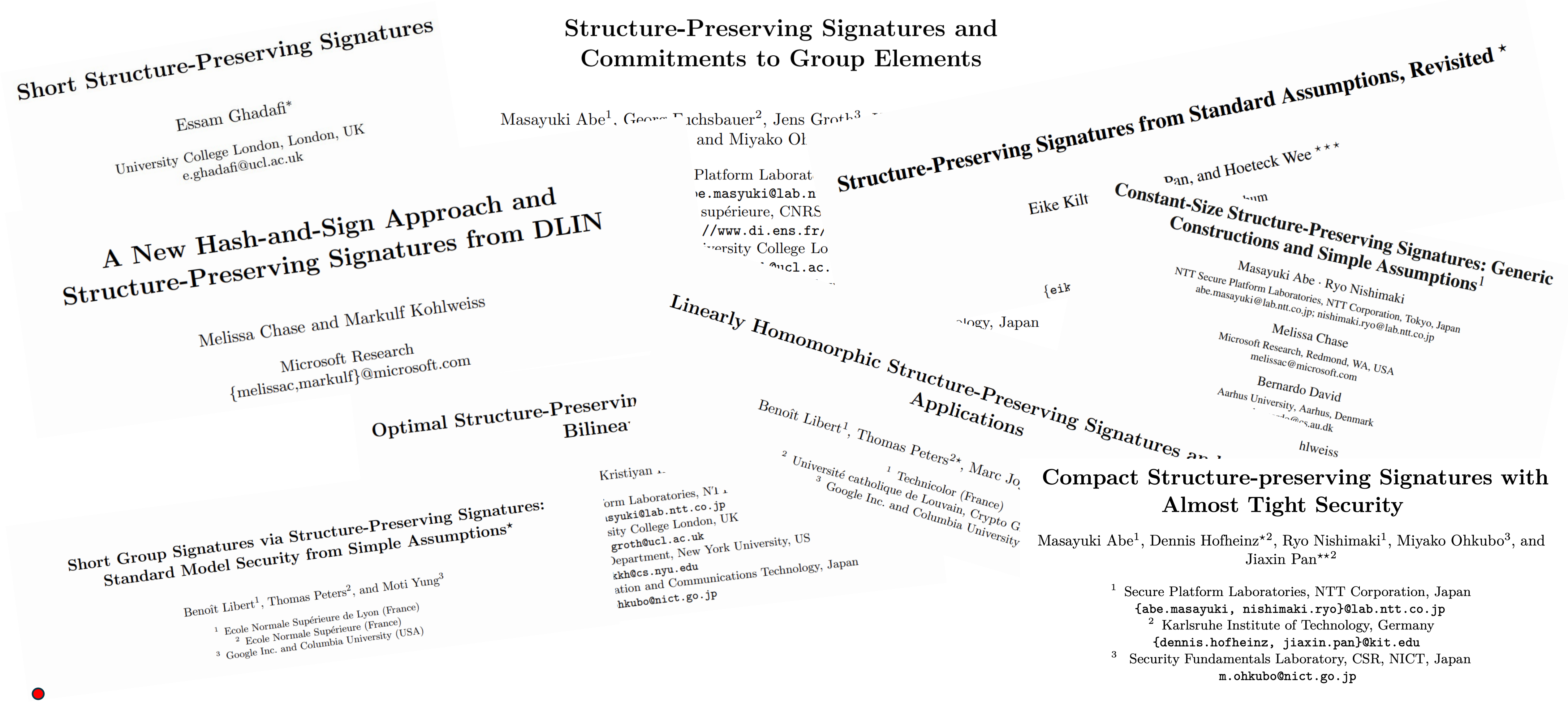
[1] Technicolor (France)
[2] Université catholique de Louvain, Crypto Group (Belgium)
[3] Google Inc. and Columbia University (USA)

serving Signatures with
ht Security

, Ryo Nishimaki[1], Miyako Ohkubo[3], and
xin Pan**2

oratories, NTT Corporation, Japan
ishimaki.ryo}@lab.ntt.co.jp
[2] Kar titute of Technology, Germany
{dennis.hofheinz, jiaxin.pan}@kit.edu
[3] Security Fundamentals Laboratory, CSR, NICT, Japan
m.ohkubo@nict.go.jp

Some Existing Structure-Preserving Signatures:



Short Structure-Preserving Signatures

Essam Ghadafi*

University College London, London, UK
e.ghadafi@ucl.ac.uk

Structure-Preserving Signatures and Commitments to Group Elements

Masayuki Abe[1], Georg Fuchsbauer[2], Jens Groth[3], and Miyako Oh

Platform Laborat
be.masyuki@lab.n
supérieure, CNRS
//www.di.ens.fr/
versity College Lo
@ucl.ac.

Structure-Preserving Signatures from Standard Assumptions, Revisited *

Eike Kilt
Pan, and Hoeteck Wee * * *

{eik

logy, Japan

A New Hash-and-Sign Approach and Structure-Preserving Signatures from DLIN

Melissa Chase and Markulf Kohlweiss

Microsoft Research
{melissac,markulf}@microsoft.com

Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions[1]

Masayuki Abe · Ryo Nishimaki
NTT Secure Platform Laboratories, NTT Corporation, Tokyo, Japan
abe.masayuki@lab.ntt.co.jp; nishimaki.ryo@lab.ntt.co.jp

Melissa Chase
Microsoft Research, Redmond, WA, USA
melissac@microsoft.com

Bernardo David
Aarhus University, Aarhus, Denmark
@cs.au.dk

hlweiss

Linearly Homomorphic Structure-Preserving Signatures an Applications

Benoît Libert[1], Thomas Peters[2]*, Marc Jo

[1] Technicolor (France)
[2] Université catholique de Louvain, Crypto G
[3] Google Inc. and Columbia University

Optimal Structure-Preservin Bilinea

Kristiyan

orm Laboratories, NT
asyuki@lab.ntt.co.jp
sity College London, UK
groth@ucl.ac.uk
Department, New York University, US
kkh@cs.nyu.edu
ation and Communications Technology, Japan
hkubo@nict.go.jp

Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions*

Benoît Libert[1], Thomas Peters[2], and Moti Yung[3]

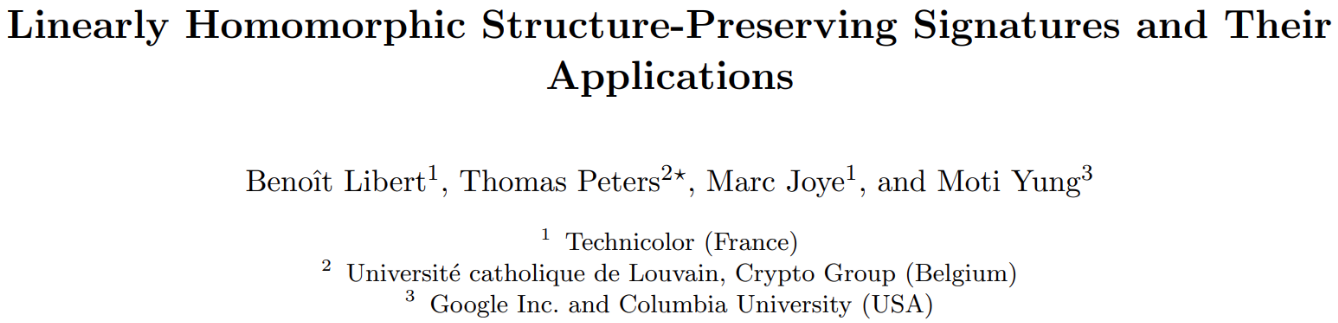
[1] Ecole Normale Supérieure de Lyon (France)
[2] Ecole Normale Supérieure (France)
[3] Google Inc. and Columbia University (USA)

Compact Structure-preserving Signatures with Almost Tight Security

Masayuki Abe[1], Dennis Hofheinz*[2], Ryo Nishimaki[1], Miyako Ohkubo[3], and Jiaxin Pan**[2]

[1] Secure Platform Laboratories, NTT Corporation, Japan
{abe.masayuki, nishimaki.ryo}@lab.ntt.co.jp
[2] Karlsruhe Institute of Technology, Germany
{dennis.hofheinz, jiaxin.pan}@kit.edu
[3] Security Fundamentals Laboratory, CSR, NICT, Japan
m.ohkubo@nict.go.jp

Structure-Preserving Signatures: Some Candidates

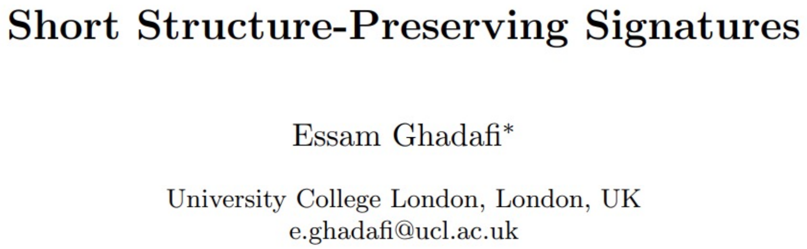


Linearly Homomorphic Structure-Preserving Signatures and Their Applications

Benoît Libert[1], Thomas Peters[2]⋆, Marc Joye[1], and Moti Yung[3]

[1] Technicolor (France)
[2] Université catholique de Louvain, Crypto Group (Belgium)
[3] Google Inc. and Columbia University (USA)

One-time Threshold SPS *



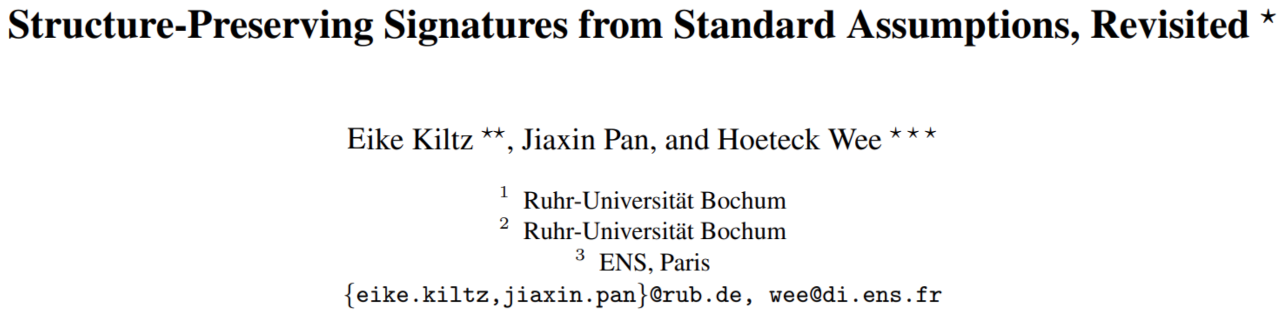
Short Structure-Preserving Signatures

Essam Ghadafi*

University College London, London, UK
e.ghadafi@ucl.ac.uk

Interactive Threshold SPS *
At least two rounds of communication

* This has not been discussed in any previous research or studies.



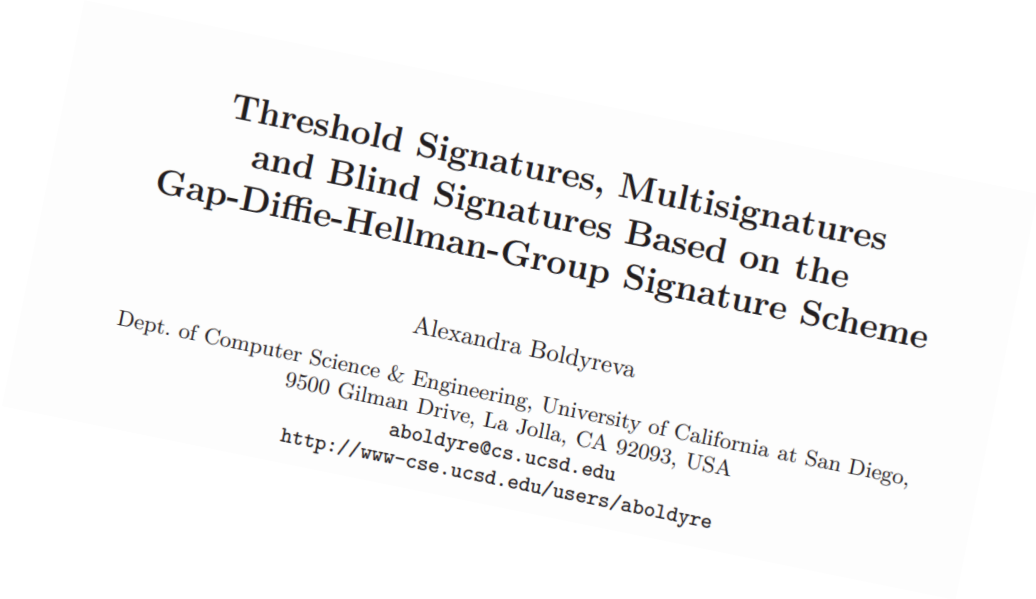
Structure-Preserving Signatures from Standard Assumptions, Revisited ⋆

Eike Kiltz ⋆⋆, Jiaxin Pan, and Hoeteck Wee ⋆⋆⋆

[1] Ruhr-Universität Bochum
[2] Ruhr-Universität Bochum
[3] ENS, Paris
{eike.kiltz,jiaxin.pan}@rub.de, wee@di.ens.fr

A NI-TSPS based on Standard Assumptions.

Some Existing Threshold Signatures:

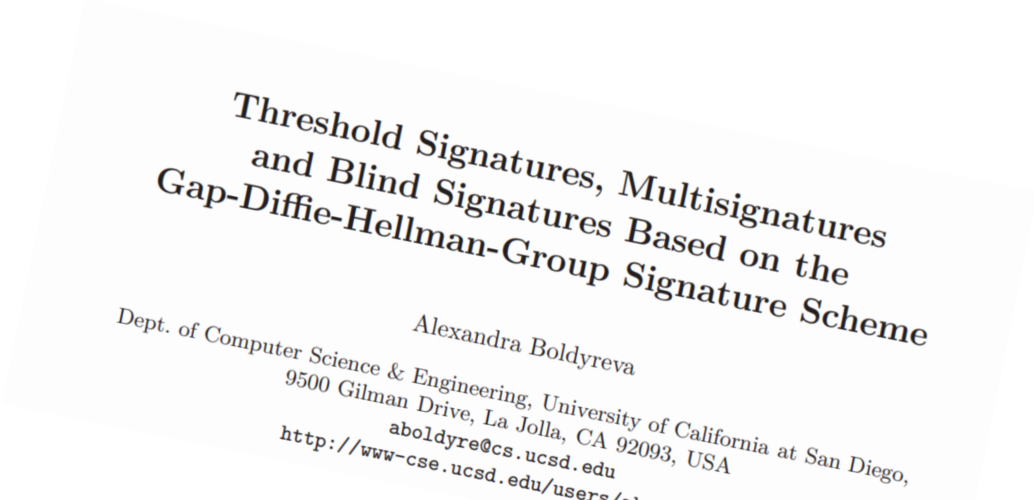


Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme

Alexandra Boldyreva

Dept. of Computer Science & Engineering, University of California at San Diego,
9500 Gilman Drive, La Jolla, CA 92093, USA
aboldyre@cs.ucsd.edu
http://www-cse.ucsd.edu/users/aboldyre

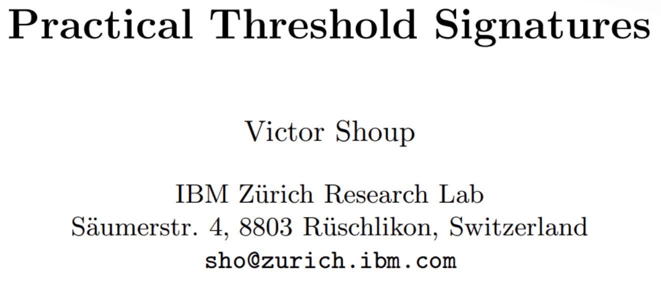
Some Existing Threshold Signatures:



Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme

Alexandra Boldyreva

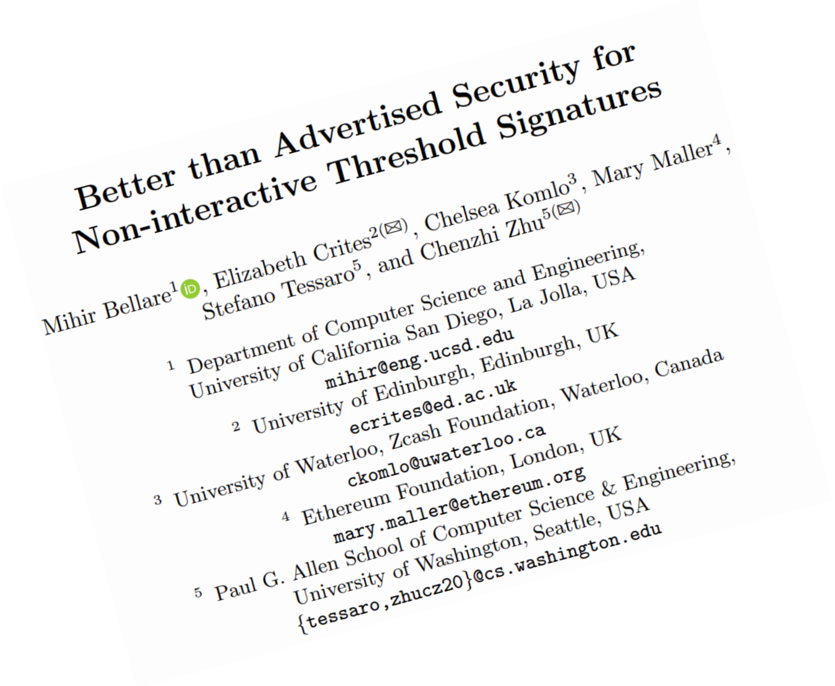
Dept. of Computer Science & Engineering, University of California at San Diego,
9500 Gilman Drive, La Jolla, CA 92093, USA
aboldyre@cs.ucsd.edu
http://www-cse.ucsd.edu/users/aboldyre



Practical Threshold Signatures

Victor Shoup

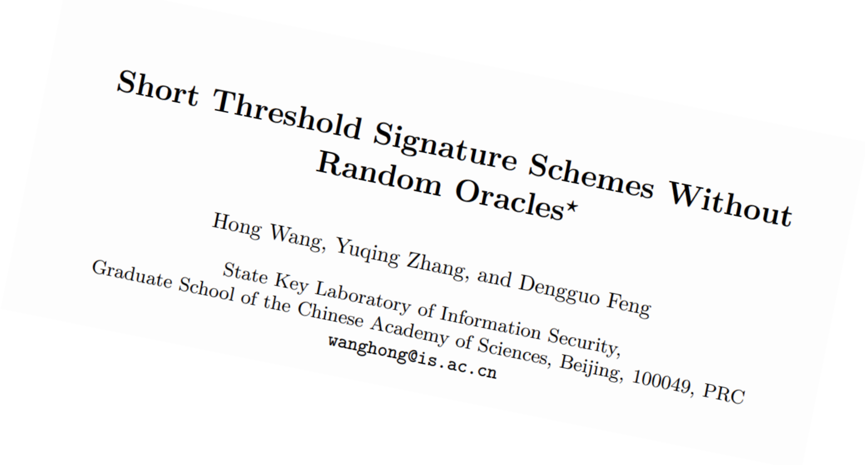
IBM Zürich Research Lab
Säumerstr. 4, 8803 Rüschlikon, Switzerland
sho@zurich.ibm.com



Better than Advertised Security for Non-interactive Threshold Signatures

Mihir Bellare[1], Elizabeth Crites[2](✉), Chelsea Komlo[3], Mary Maller[4], Stefano Tessaro[5], and Chenzhi Zhu[5](✉)

[1] Department of Computer Science and Engineering,
University of California San Diego, La Jolla, USA
mihir@eng.ucsd.edu
[2] University of Edinburgh, Edinburgh, UK
ecrites@ed.ac.uk
[3] University of Waterloo, Zcash Foundation, Waterloo, Canada
ckomlo@uwaterloo.ca
[4] Ethereum Foundation, London, UK
mary.maller@ethereum.org
[5] Paul G. Allen School of Computer Science & Engineering,
University of Washington, Seattle, USA
{tessaro,zhucz20}@cs.washington.edu



Short Threshold Signature Schemes Without Random Oracles*

Hong Wang, Yuqing Zhang, and Dengguo Feng

State Key Laboratory of Information Security,
Graduate School of the Chinese Academy of Sciences, Beijing, 100049, PRC
wanghong@is.ac.cn

Some Existing Threshold Signatures:

Threshold Signatures with Private Accountability

Dan Boneh[1] and Chelsea Komlo[2](✉)

[1] Stanford University, Stanford, USA
[2] University of Waterloo, Waterloo, Canada
ckomlo@uwaterloo.ca

Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme

Alexandra Boldyreva

of Computer Science & Engineering, University of California at San Diego,
9500 Gilman Drive, La Jolla, CA 92093, USA
aboldyre@cs.ucsd.edu
http://www-cse.ucsd.edu/users/aboldyre

Practical Threshold Signatures

Victor Shoup

IBM Zürich Research Lab

Better than Advertised Security for Non-interactive Threshold Signatures

Mihir Bellare[1], Elizabeth Crites[2](✉), Chelsea Komlo[3], Mary Maller[4], Stefano Tessaro[5], and Chenzhi Zhu[5](✉)

[1] Department of Computer Science and Engineering, University of California San Diego, La Jolla, USA
mihir@eng.ucsd.edu
[2] University of Edinburgh, Edinburgh, UK
ecrites@ed.ac.uk
[3] University of Waterloo, Zcash Foundation, Waterloo, Canada
ckomlo@uwaterloo.ca
[4] Ethereum Foundation

Fully Adaptive Schnorr Threshold Signatures*

Elizabeth Crites[1], Chelsea Komlo[2], and Mary Maller[3]

[1] University of Edinburgh, UK
[2] University of Waterloo & Zcash Foundation
[3] Ethereum Foundation & PQShield, UK
ecrites@ed.ac.uk, ckomlo@uwaterloo.ca, mary.maller@ethereum.org

FROST: Flexible Round-Optimized Schnorr Threshold Signatures

Chelsea Komlo[1,2] and Ian Goldberg[1](✉)

[1] University of Waterloo, Waterloo, Canada
iang@uwaterloo.ca
[2] Zcash Foundation, New York, USA

Short Threshold Signature
Random Orac

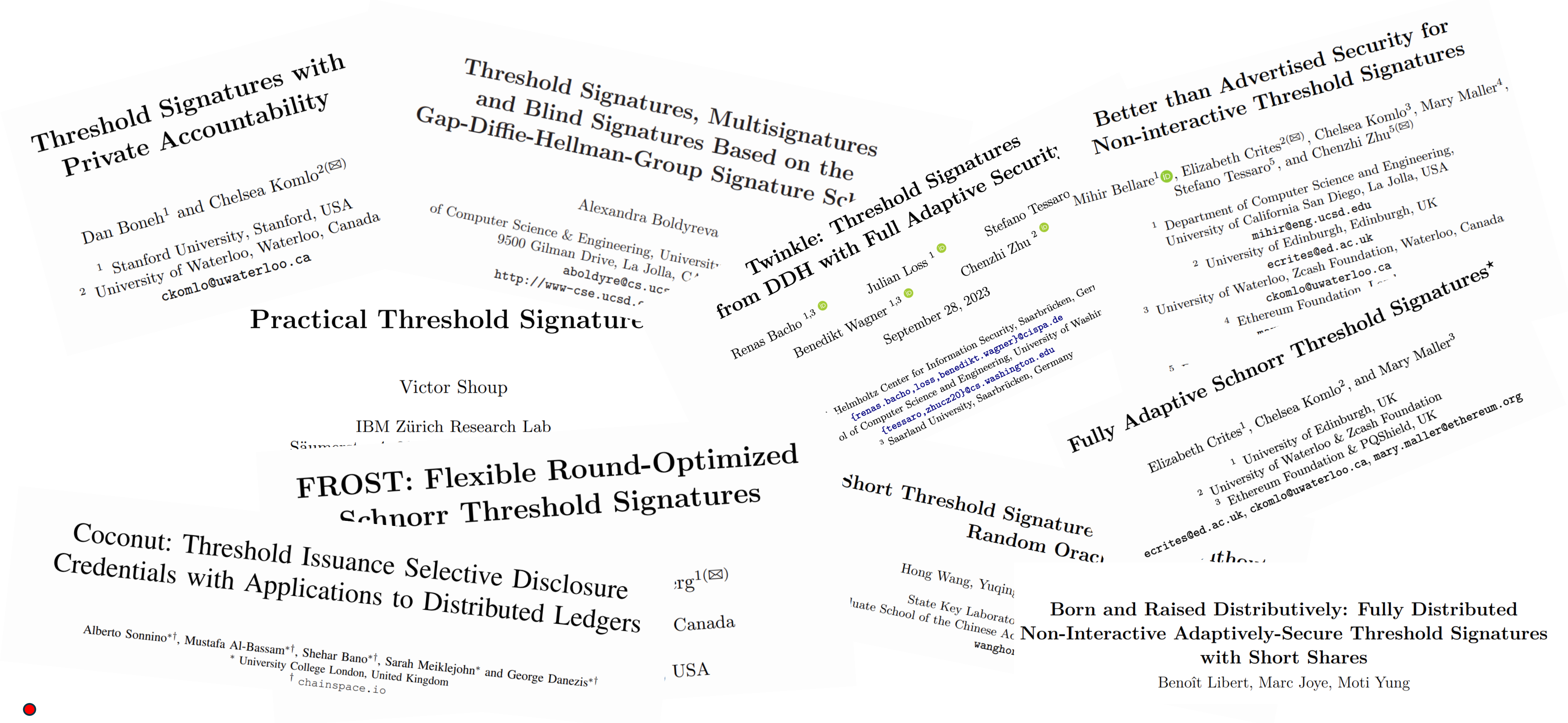
Hong Wang, Yuqin

State Key Laborato
luate School of the Chinese Ac
wanghor

Born and Raised Distributively: Fully Distributed Non-Interactive Adaptively-Secure Threshold Signatures with Short Shares

Benoît Libert, Marc Joye, Moti Yung

Some Existing Threshold Signatures:



Threshold Signatures with Private Accountability

Dan Boneh[1] and Chelsea Komlo[2(✉)]

[1] Stanford University, Stanford, USA
[2] University of Waterloo, Waterloo, Canada
ckomlo@uwaterloo.ca

Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Sc

Alexandra Boldyreva

of Computer Science & Engineering, Universit
9500 Gilman Drive, La Jolla, C
aboldyre@cs.ucs
http://www-cse.ucsd.

Practical Threshold Signatur

Victor Shoup

IBM Zürich Research Lab

Twinkle: Threshold Signatures from DDH with Full Adaptive Securit

Renas Bacho[1,3] Julian Loss[1] Stefano Tessaro
Benedikt Wagner[1,3] Chenzhi Zhu[2]

September 28, 2023

Helmholtz Center for Information Security, Saarbrücken, Ger
{renas.bacho,loss,benedikt.wagner}@cispa.de
ol of Computer Science and Engineering, University of Washin
{tessaro,zhucz20}@cs.washington.edu
[3] Saarland University, Saarbrücken, Germany

Better than Advertised Security for Non-interactive Threshold Signatures

Mihir Bellare[1], Elizabeth Crites[2(✉)], Chelsea Komlo[3], Mary Maller[4], Stefano Tessaro[5], and Chenzhi Zhu[5(✉)]

[1] Department of Computer Science and Engineering, University of California San Diego, La Jolla, USA
mihir@eng.ucsd.edu
[2] University of Edinburgh, Edinburgh, UK
ecrites@ed.ac.uk
[3] University of Waterloo, Zcash Foundation, Waterloo, Canada
ckomlo@uwaterloo.ca
[4] Ethereum Foundation, L
[5]

Fully Adaptive Schnorr Threshold Signatures*

Elizabeth Crites[1], Chelsea Komlo[2], and Mary Maller[3]

[1] University of Edinburgh, UK
[2] University of Waterloo & Zcash Foundation
[3] Ethereum Foundation & PQShield, UK
ecrites@ed.ac.uk, ckomlo@uwaterloo.ca, mary.maller@ethereum.org

FROST: Flexible Round-Optimized Schnorr Threshold Signatures

rg[1(✉)]
Canada
USA

Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers

Alberto Sonnino*†, Mustafa Al-Bassam*†, Shehar Bano*†, Sarah Meiklejohn* and George Danezis*†
* University College London, United Kingdom
† chainspace.io

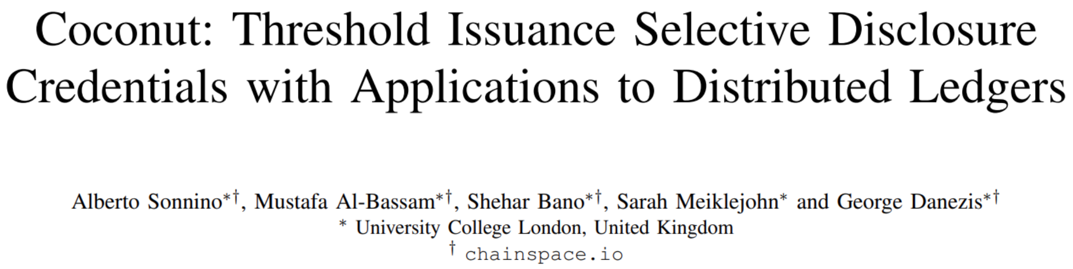
Short Threshold Signature
Random Orac

Hong Wang, Yuqin
State Key Laborato
luate School of the Chinese Ac
wanghon

Born and Raised Distributively: Fully Distributed Non-Interactive Adaptively-Secure Threshold Signatures with Short Shares

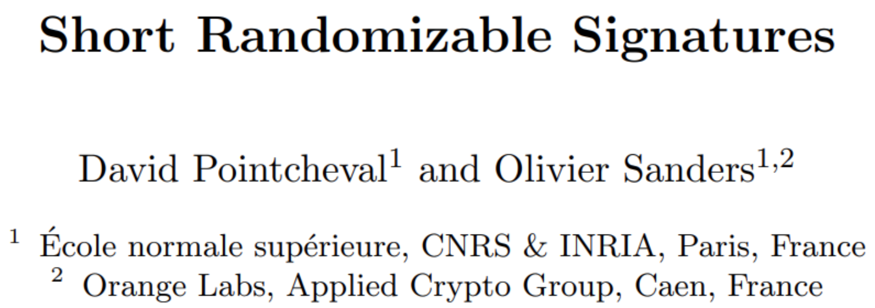
Benoît Libert, Marc Joye, Moti Yung

Finalists for the Initial Work: To Build a Threshold-Friendly SPS



Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers

Alberto Sonnino*†, Mustafa Al-Bassam*†, Shehar Bano*†, Sarah Meiklejohn* and George Danezis*†
* University College London, United Kingdom
† chainspace.io



Short Randomizable Signatures

David Pointcheval[1] and Olivier Sanders[1,2]

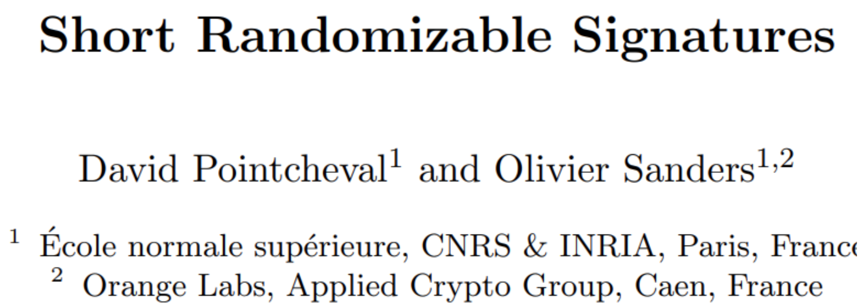
[1] École normale supérieure, CNRS & INRIA, Paris, France
[2] Orange Labs, Applied Crypto Group, Caen, France

Scalar Messages

Finalists for the Initial Work: To Build a Threshold-Friendly SPS

Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers

Alberto Sonnino*†, Mustafa Al-Bassam*†, Shehar Bano*†, Sarah Meiklejohn* and George Danezis*†
* University College London, United Kingdom
† chainspace.io



Short Randomizable Signatures

David Pointcheval[1] and Olivier Sanders[1,2]

[1] École normale supérieure, CNRS & INRIA, Paris, Franc
[2] Orange Labs, Applied Crypto Group, Caen, France

Scalar Messages

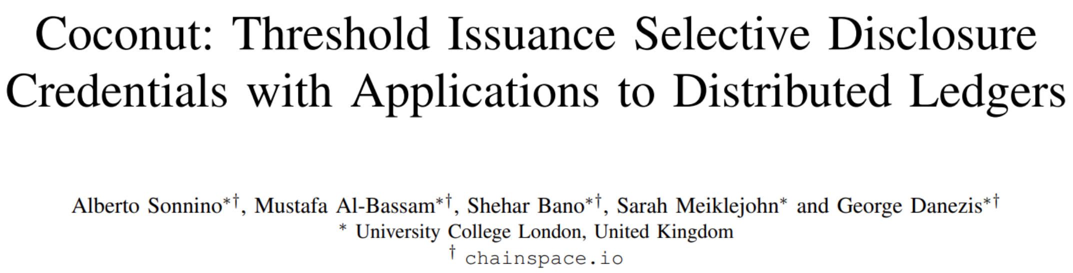
Short Structure-Preserving Signatures

Essam Ghadafi*

University College London, London, UK
e.ghadafi@ucl.ac.uk

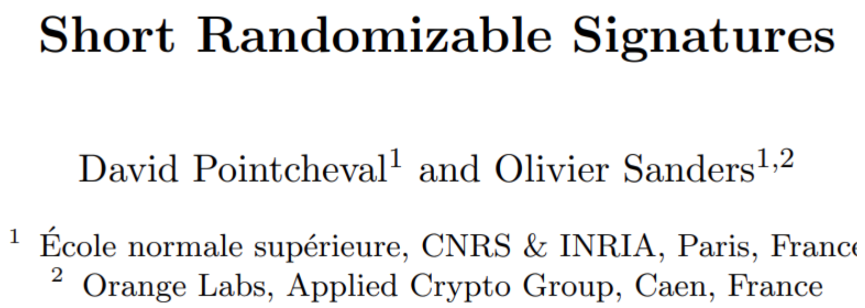
Interactive TSPS

Finalists for the Initial Work: To Build a Threshold-Friendly SPS



Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers

Alberto Sonnino*†, Mustafa Al-Bassam*†, Shehar Bano*†, Sarah Meiklejohn* and George Danezis*†
* University College London, United Kingdom
† chainspace.io

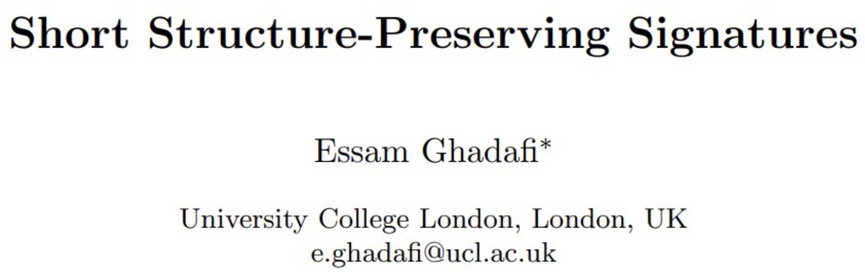


Short Randomizable Signatures

David Pointcheval[1] and Olivier Sanders[1,2]

[1] École normale supérieure, CNRS & INRIA, Paris, Franc
[2] Orange Labs, Applied Crypto Group, Caen, France

Scalar Messages



Short Structure-Preserving Signatures

Essam Ghadafi*

University College London, London, UK
e.ghadafi@ucl.ac.uk

Interactive TSPS

SPS Impossibility Results [AGHO11]:

1. **No unilateral SPS (respectively TSPS) exists!***
   - Both message and Signature components belong to the same source group.
2. **No SPS with signature of fewer than 3 group elements exists!***

Ghadafi [Gha16] has shown both these impossibility results are possible over **Diffie-Hellman message space**.

$$(\mathrm{M}_1, \mathrm{M}_2): e(G_1, M_2) = e(M_1, G_2\ )$$

i.e., $\exists\ m \in \mathbb{Z}_p: dlog_{G_1}(M_1) = dlog_{G_2}(M_2) = m$

SPS Impossibility Results [AGHO11]:

1 **No unilateral SPS (respectively TSPS) exists!***

- Both message and Signature components belong to the same source group.

2 **No SPS with signature of fewer than ~~3 group elements~~ exists!***

2 group elements

3 **No SPS with fewer than 2 pairing product equations to be verified exists!**

Ghadafi [Gha16] has shown both these impossibility results are possible over **Diffie-Hellman message space**.

$$(\mathrm{M}_1, \mathrm{M}_2): e(G_1, M_2) = e(M_1, G_2\ )$$

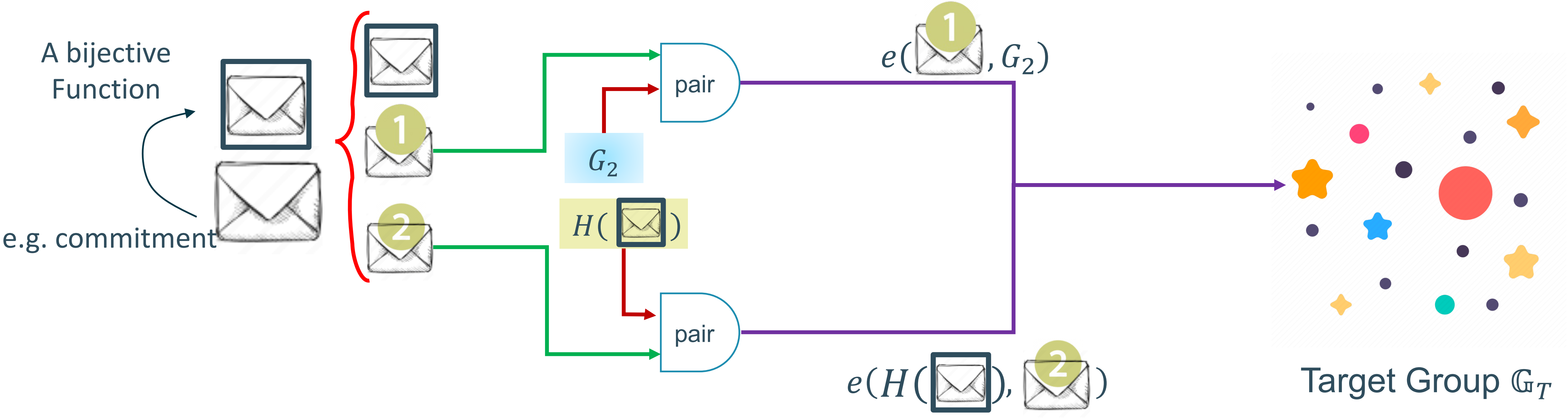
$$\text{i.e., } \exists\ m \in \mathbb{Z}_p : dlog_{G_1}(M_1) = dlog_{G_2}(M_2) = m$$

Indexed Diffie-Hellman Message Spaces:

Indexed Diffie-Hellman (iDH) message spaces:

$$(id, \mathrm{M}_1, \mathrm{M}_2): e(H(id), M_2) = e(M_1, G_2)$$

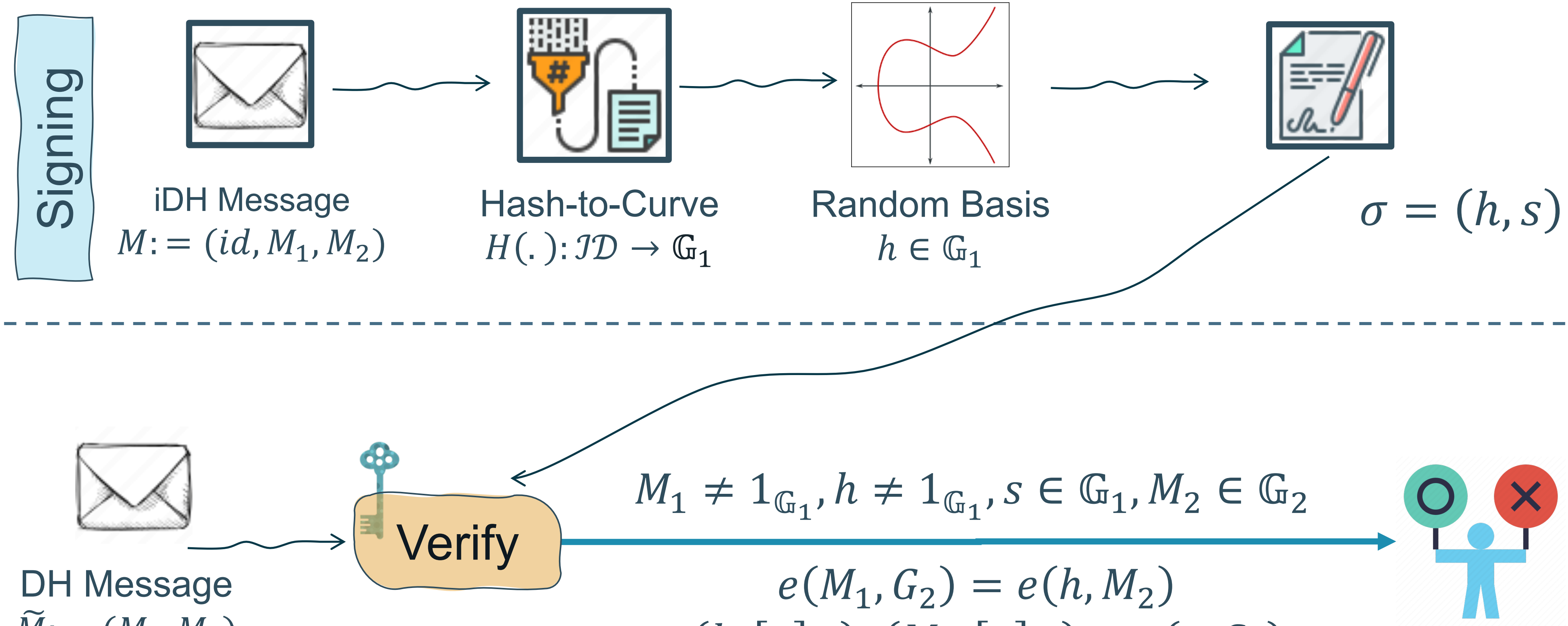
i.e., $\exists\, m \in \mathbb{Z}_p: dlog_{H(id)}(M_1) = dlog_{G_2}(M_2) = m$



Our proposed message-indexed SPS (iSPS): A Threshold-Friendly SPS

KeyGen

$sk := (x, y) \overset{\$}{\leftarrow} {\mathbb{Z}_p^*}^2$ $\quad vk := ([x]_2, [y]_2)$



iDH Message
$M := (id, M_1, M_2)$

Hash-to-Curve
$H(.) : \mathcal{ID} \to \mathbb{G}_1$

Random Basis
$h \in \mathbb{G}_1$

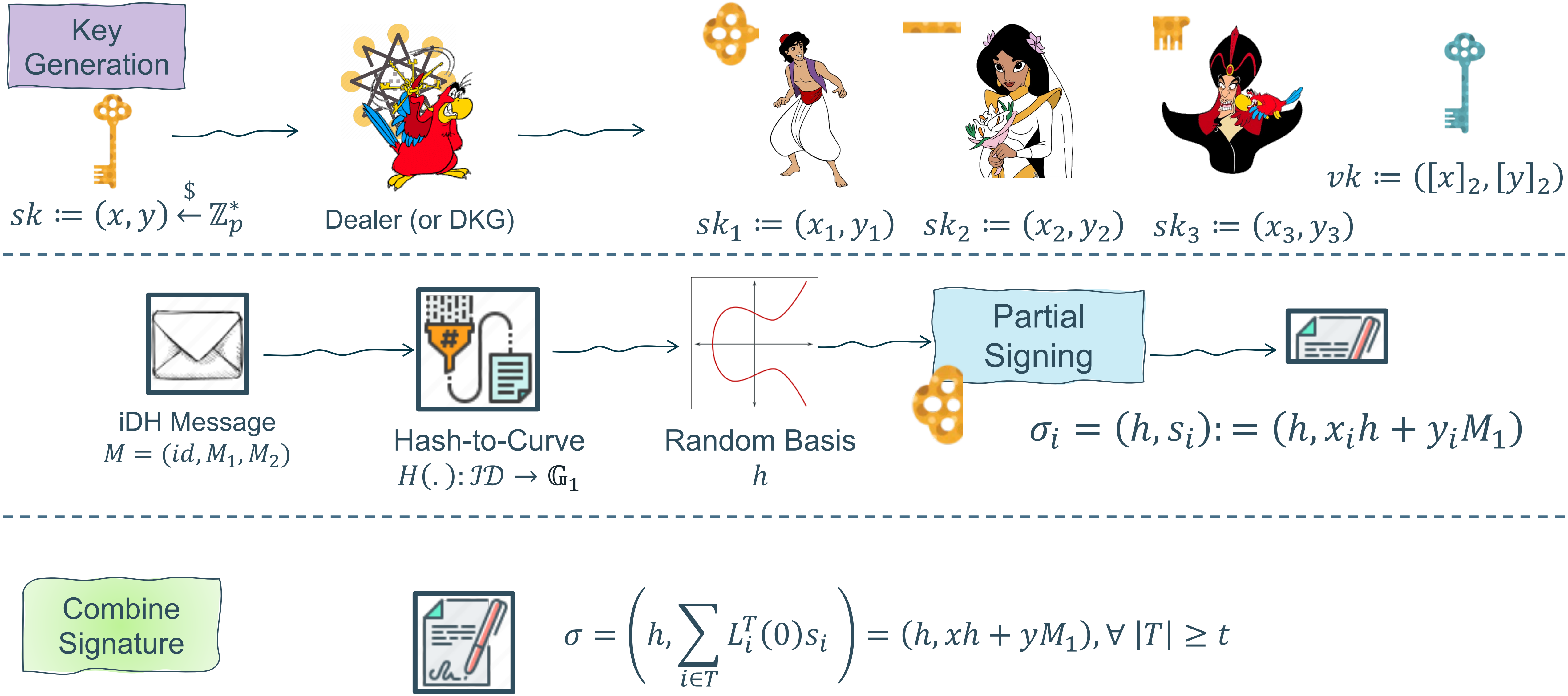
$\sigma = (h, s) := (h, xh + yM_1)$

DH Message
$\tilde{M} := (M_1, M_2)$

$M_1 \neq 1_{\mathbb{G}_1}, h \neq 1_{\mathbb{G}_1}, s \in \mathbb{G}_1, M_2 \in \mathbb{G}_2$

$e(M_1, G_2) = e(h, M_2)$
$e(h, [x]_2)e(M_1, [y]_2) = e(s, G_2)$

Our proposed TSPS: The first TSPS [CKPSS23]



Key Generation

$sk := (x, y) \xleftarrow{\$} \mathbb{Z}_p^*$

Dealer (or DKG)

$sk_1 := (x_1, y_1)$ $sk_2 := (x_2, y_2)$ $sk_3 := (x_3, y_3)$

$vk := ([x]_2, [y]_2)$

iDH Message

$M = (id, M_1, M_2)$

Hash-to-Curve

$H(.): \mathcal{ID} \to \mathbb{G}_1$

Random Basis

h

Partial Signing

$$\sigma_i = (h, s_i) := (h, x_i h + y_i M_1)$$

Combine Signature

$$\sigma = \left(h, \sum_{i \in T} L_i^T(0) s_i\right) = (h, xh + yM_1), \forall\, |T| \geq t$$

Security Notions: EUF-CMA

$G^{\mathrm{CMA}}_{\mathrm{DS},\mathcal{A}}(\kappa)$

```
$G^{\text{TS-UF-0}}_{\text{TS},\mathcal{A}}(\kappa)$, $G^{\text{TS-UF-1}}_{\text{TS},\mathcal{A}}(\kappa)$, $G^{\text{adp-TS-UF-0}}_{\text{TS},\mathcal{A}}(\kappa)$, $G^{\text{adp-TS-UF-1}}_{\text{TS},\mathcal{A}}(\kappa)$:
$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\kappa)$
$(n, t, \mathsf{CS}, \mathsf{st}_0) \leftarrow \mathcal{A}(\mathsf{pp})$
$\mathsf{HS} := [1, n] \setminus \mathsf{CS}$
$(\mathsf{vk}, \{\mathsf{sk}_i\}_{i\in[1,n]}, \{\mathsf{vk}_i\}_{i\in[1,n]}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}, n, t)$
$([\mathbf{m}^*], \Sigma^*, \mathsf{st}_1) \leftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{PSign}}(.),\, \mathcal{O}^{\mathsf{Corrupt}}(.)}(\mathsf{st}_0, \mathsf{vk}, \{\mathsf{sk}_i\}_{i\in\mathsf{CS}}, \{\mathsf{vk}_i\}_{i\in[1,n]})$
return $\Big(\mathsf{Verify}(\mathsf{pp}, \mathsf{vk}, [\mathbf{m}^*], \Sigma^*) \wedge |\mathsf{CS}| < t \wedge [\mathbf{m}^*]$ is fresh
        $(S_1([\mathbf{m}^*]) = \emptyset \vee |S_1([\mathbf{m}^*])| < t - |\mathsf{CS}|)\Big)$

$\mathcal{O}^{\mathsf{PSign}}(i, [\mathbf{m}])$:
Assert $([\mathbf{m}] \in \mathcal{M} \wedge i \in \mathsf{HS})$
$\Sigma_i \leftarrow \mathsf{ParSign}(\mathsf{pp}, \mathsf{sk}_i, [\mathbf{m}])$
if $\Sigma_i \neq \perp$:
    $S_1([\mathbf{m}]) \leftarrow S_1([\mathbf{m}]) \cup \{i\}$
return $(\Sigma_i)$

$\mathcal{O}^{\mathsf{Corrupt}}(k)$:
if $k \in \mathsf{CS}$:
    return $\perp$
else: $\mathsf{CS} \leftarrow \mathsf{CS} \cup \{k\}$
    $\mathsf{HS} \leftarrow \mathsf{HS} \setminus \{k\}$
    return $(\mathsf{sk}_k)$
```

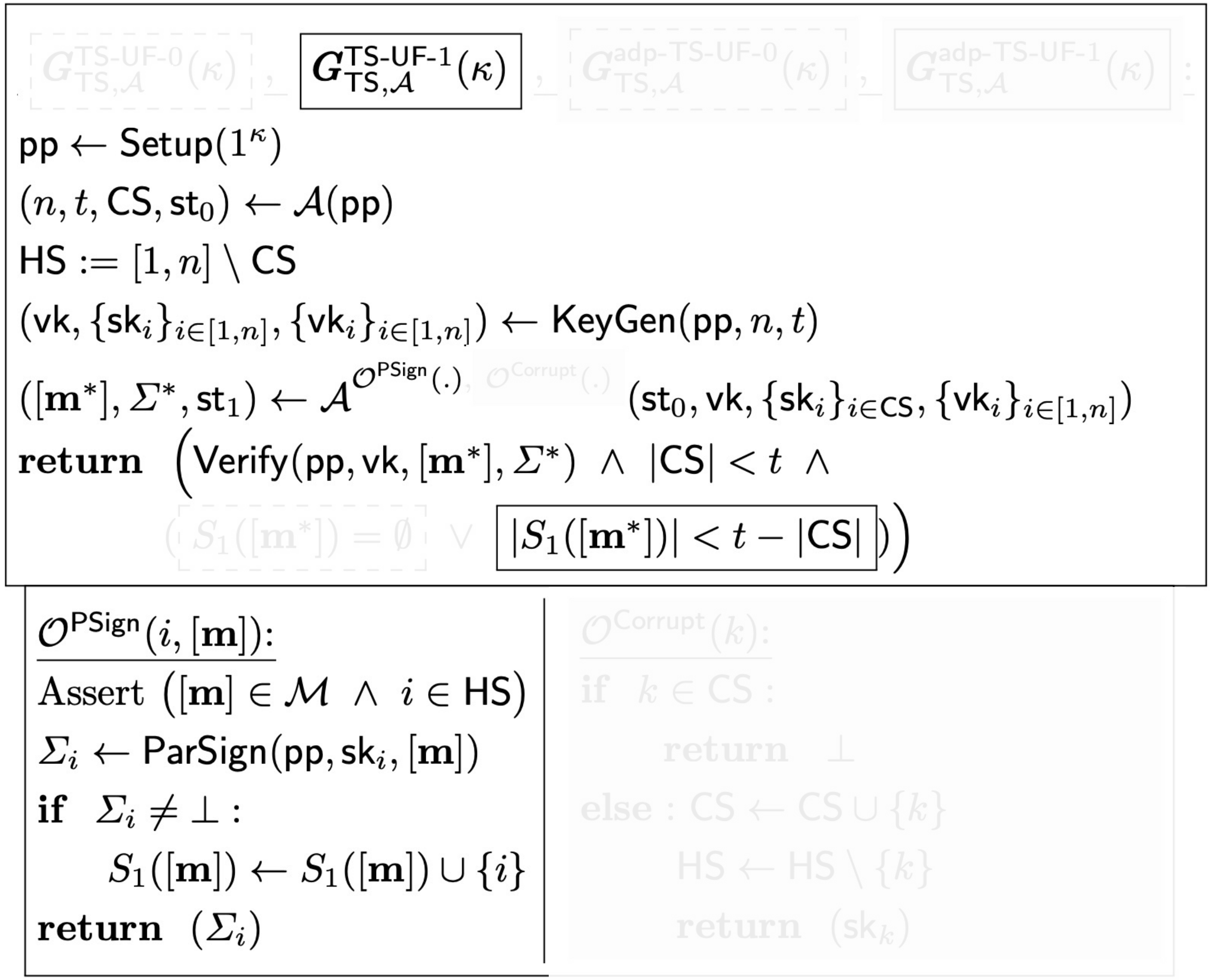
Security Notions: Bellare et al. [BCK+22]

```
$\boxed{G^{\text{TS-UF-0}}_{\text{TS},\mathcal{A}}(\kappa)}$, $\boxed{G^{\text{TS-UF-1}}_{\text{TS},\mathcal{A}}(\kappa)}$, $\boxed{G^{\text{adp-TS-UF-0}}_{\text{TS},\mathcal{A}}(\kappa)}$, $\boxed{G^{\text{adp-TS-UF-1}}_{\text{TS},\mathcal{A}}(\kappa)}$:
$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\kappa)$
$(n, t, \mathsf{CS}, \mathsf{st}_0) \leftarrow \mathcal{A}(\mathsf{pp})$
$\mathsf{HS} := [1, n] \setminus \mathsf{CS}$
$(\mathsf{vk}, \{\mathsf{sk}_i\}_{i \in [1,n]}, \{\mathsf{vk}_i\}_{i \in [1,n]}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}, n, t)$
$([\mathbf{m}^*], \Sigma^*, \mathsf{st}_1) \leftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{PSign}}(.),\ \mathcal{O}^{\mathsf{Corrupt}}(.)}(\mathsf{st}_0, \mathsf{vk}, \{\mathsf{sk}_i\}_{i \in \mathsf{CS}}, \{\mathsf{vk}_i\}_{i \in [1,n]})$
return $\Big(\mathsf{Verify}(\mathsf{pp}, \mathsf{vk}, [\mathbf{m}^*], \Sigma^*) \ \wedge\ |\mathsf{CS}| < t \ \wedge$
        $(\boxed{S_1([\mathbf{m}^*]) = \emptyset} \ \vee\ \boxed{|S_1([\mathbf{m}^*])| < t - |\mathsf{CS}|})\Big)$
```

```
$\mathcal{O}^{\mathsf{PSign}}(i, [\mathbf{m}])$:
Assert $([\mathbf{m}] \in \mathcal{M} \ \wedge\ i \in \mathsf{HS})$
$\Sigma_i \leftarrow \mathsf{ParSign}(\mathsf{pp}, \mathsf{sk}_i, [\mathbf{m}])$
if $\Sigma_i \neq \perp$ :
    $S_1([\mathbf{m}]) \leftarrow S_1([\mathbf{m}]) \cup \{i\}$
return $(\Sigma_i)$
```

```
$\mathcal{O}^{\mathsf{Corrupt}}(k)$:
if $k \in \mathsf{CS}$ :
    return $\perp$
else : $\mathsf{CS} \leftarrow \mathsf{CS} \cup \{k\}$
    $\mathsf{HS} \leftarrow \mathsf{HS} \setminus \{k\}$
    return $(\mathsf{sk}_k)$
```

Security Notions: Bellare et al. [BCK+22]

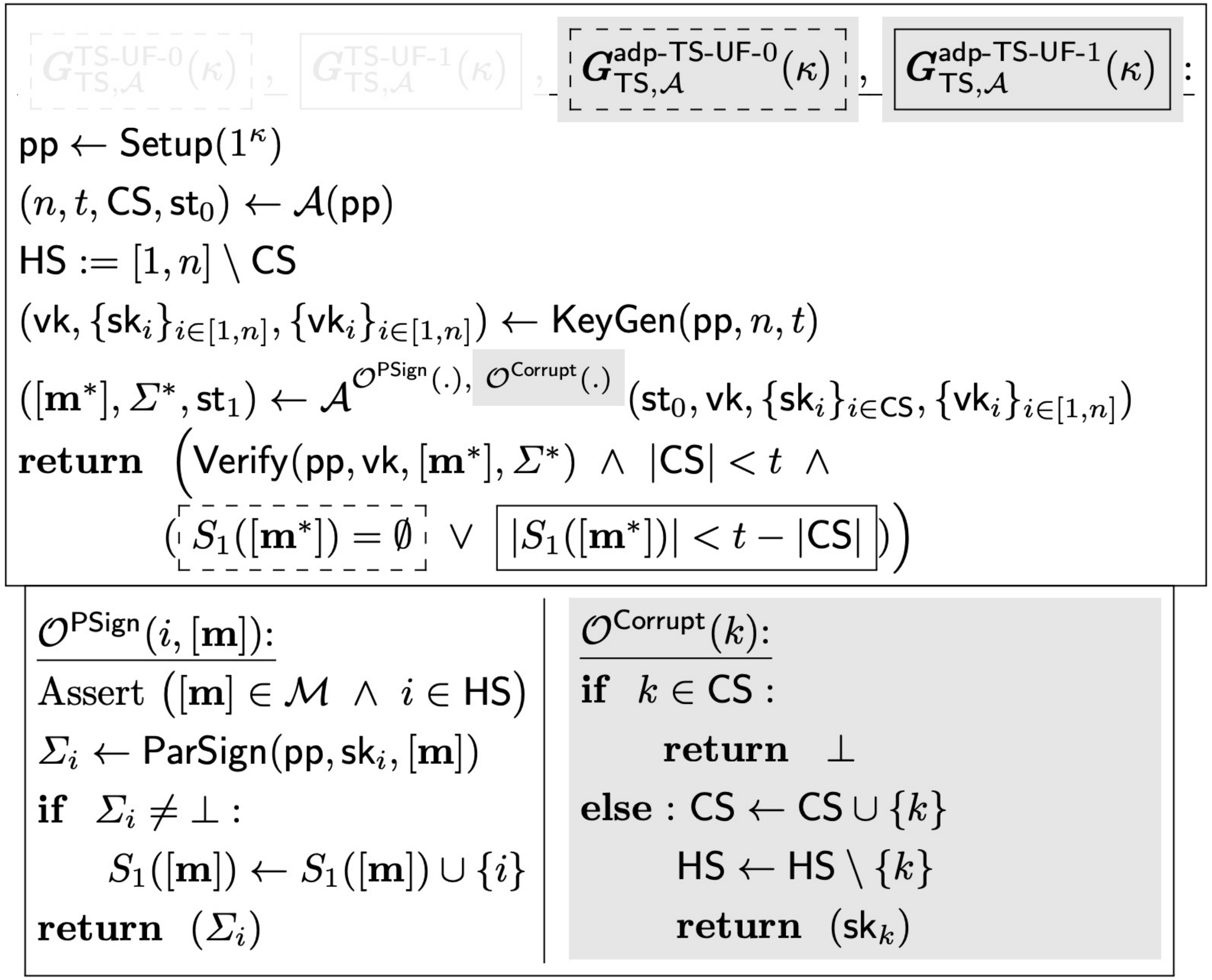


```
$G^{\text{TS-UF-0}}_{\text{TS},\mathcal{A}}(\kappa)$ , $\boxed{G^{\text{TS-UF-1}}_{\text{TS},\mathcal{A}}(\kappa)}$ , $G^{\text{adp-TS-UF-0}}_{\text{TS},\mathcal{A}}(\kappa)$ , $G^{\text{adp-TS-UF-1}}_{\text{TS},\mathcal{A}}(\kappa)$ :
$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\kappa)$
$(n, t, \mathsf{CS}, \mathsf{st}_0) \leftarrow \mathcal{A}(\mathsf{pp})$
$\mathsf{HS} := [1, n] \setminus \mathsf{CS}$
$(\mathsf{vk}, \{\mathsf{sk}_i\}_{i\in[1,n]}, \{\mathsf{vk}_i\}_{i\in[1,n]}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}, n, t)$
$([\mathbf{m}^*], \Sigma^*, \mathsf{st}_1) \leftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{PSign}}(.),\ \mathcal{O}^{\mathsf{Corrupt}}(.)}(\mathsf{st}_0, \mathsf{vk}, \{\mathsf{sk}_i\}_{i\in\mathsf{CS}}, \{\mathsf{vk}_i\}_{i\in[1,n]})$
return $\Big(\mathsf{Verify}(\mathsf{pp}, \mathsf{vk}, [\mathbf{m}^*], \Sigma^*) \ \wedge \ |\mathsf{CS}| < t \ \wedge$
    $(\ S_1([\mathbf{m}^*]) = \emptyset \ \vee \ \boxed{|S_1([\mathbf{m}^*])| < t - |\mathsf{CS}|}\ )\Big)$

$\mathcal{O}^{\mathsf{PSign}}(i, [\mathbf{m}])$:
Assert $([\mathbf{m}] \in \mathcal{M} \ \wedge \ i \in \mathsf{HS})$
$\Sigma_i \leftarrow \mathsf{ParSign}(\mathsf{pp}, \mathsf{sk}_i, [\mathbf{m}])$
if $\Sigma_i \neq \perp$ :
    $S_1([\mathbf{m}]) \leftarrow S_1([\mathbf{m}]) \cup \{i\}$
return $(\Sigma_i)$

$\mathcal{O}^{\mathsf{Corrupt}}(k)$:
if $k \in \mathsf{CS}$ :
    return $\perp$
else : $\mathsf{CS} \leftarrow \mathsf{CS} \cup \{k\}$
    $\mathsf{HS} \leftarrow \mathsf{HS} \setminus \{k\}$
    return $(\mathsf{sk}_k)$
```

Security Notions: Bellare et al. [BCK+22]



```
$G^{\mathsf{TS\text{-}UF\text{-}0}}_{\mathsf{TS},\mathcal{A}}(\kappa)$, $G^{\mathsf{TS\text{-}UF\text{-}1}}_{\mathsf{TS},\mathcal{A}}(\kappa)$, $G^{\mathsf{adp\text{-}TS\text{-}UF\text{-}0}}_{\mathsf{TS},\mathcal{A}}(\kappa)$, $\boxed{G^{\mathsf{adp\text{-}TS\text{-}UF\text{-}1}}_{\mathsf{TS},\mathcal{A}}(\kappa)}$:
$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\kappa)$
$(n, t, \mathsf{CS}, \mathsf{st}_0) \leftarrow \mathcal{A}(\mathsf{pp})$
$\mathsf{HS} := [1, n] \setminus \mathsf{CS}$
$(\mathsf{vk}, \{\mathsf{sk}_i\}_{i \in [1,n]}, \{\mathsf{vk}_i\}_{i \in [1,n]}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}, n, t)$
$([\mathbf{m}^*], \Sigma^*, \mathsf{st}_1) \leftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{PSign}}(.),\ \mathcal{O}^{\mathsf{Corrupt}}(.)}(\mathsf{st}_0, \mathsf{vk}, \{\mathsf{sk}_i\}_{i \in \mathsf{CS}}, \{\mathsf{vk}_i\}_{i \in [1,n]})$
return $\Big(\mathsf{Verify}(\mathsf{pp}, \mathsf{vk}, [\mathbf{m}^*], \Sigma^*) \ \wedge \ |\mathsf{CS}| < t \ \wedge$
        $(S_1([\mathbf{m}^*]) = \emptyset \ \vee \ \boxed{|S_1([\mathbf{m}^*])| < t - |\mathsf{CS}|})\Big)$
```

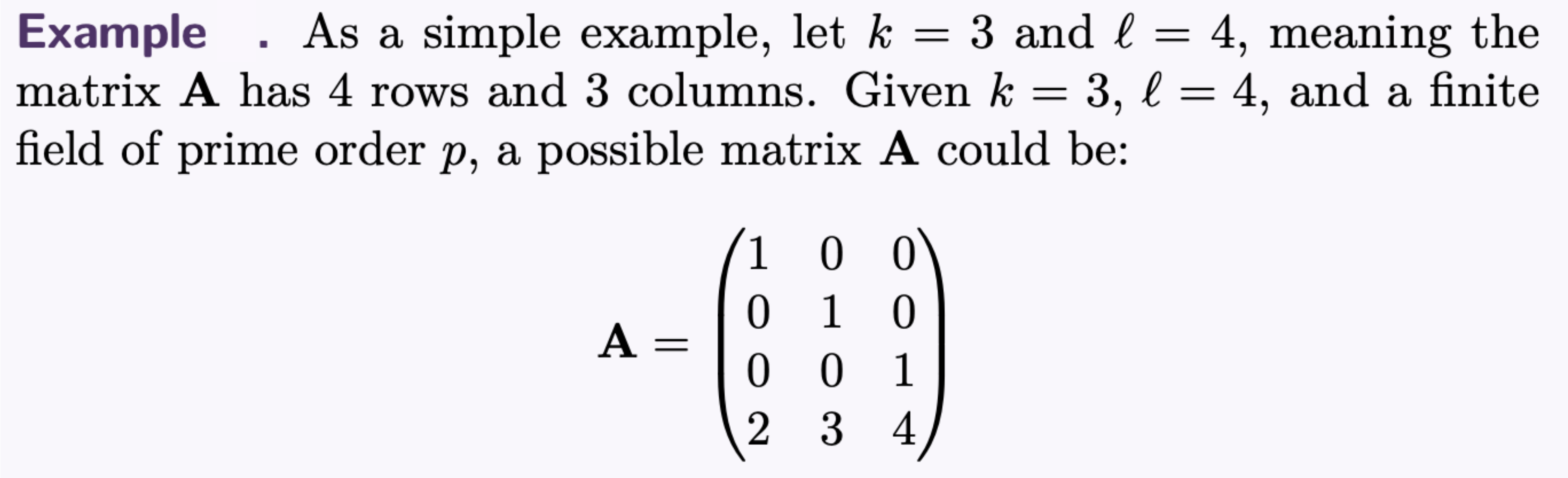
```
$\mathcal{O}^{\mathsf{PSign}}(i, [\mathbf{m}])$:
Assert $([\mathbf{m}] \in \mathcal{M} \ \wedge \ i \in \mathsf{HS})$
$\Sigma_i \leftarrow \mathsf{ParSign}(\mathsf{pp}, \mathsf{sk}_i, [\mathbf{m}])$
if $\Sigma_i \neq \perp$ :
    $S_1([\mathbf{m}]) \leftarrow S_1([\mathbf{m}]) \cup \{i\}$
return $(\Sigma_i)$
```

```
$\mathcal{O}^{\mathsf{Corrupt}}(k)$:
if $k \in \mathsf{CS}$ :
    return $\perp$
else : $\mathsf{CS} \leftarrow \mathsf{CS} \cup \{k\}$
    $\mathsf{HS} \leftarrow \mathsf{HS} \setminus \{k\}$
    return $(\mathsf{sk}_k)$
```

Supplementary Notations:

$$e([\mathbf{A}]_1, [\mathbf{B}]_2) = e\left(\begin{pmatrix} \alpha_{1,1}\mathsf{G}_1 & \cdots & \alpha_{1,n}\mathsf{G}_1 \\ \alpha_{2,1}\mathsf{G}_1 & \cdots & \alpha_{2,n}\mathsf{G}_1 \\ \vdots & \ddots & \vdots \\ \alpha_{m,1}\mathsf{G}_1 & \cdots & \alpha_{m,n}\mathsf{G}_1 \end{pmatrix}, \begin{pmatrix} \beta_{1,1}\mathsf{G}_2 & \cdots & \beta_{1,n}\mathsf{G}_2 \\ \beta_{2,1}\mathsf{G}_2 & \cdots & \beta_{2,n}\mathsf{G}_2 \\ \vdots & \ddots & \vdots \\ \beta_{m,1}\mathsf{G}_2 & \cdots & \beta_{m,n}\mathsf{G}_2 \end{pmatrix}\right) = [\mathbf{AB}]_{\mathbf{T}} \in \mathbb{G}_T$$

$\mathcal{D}_{\ell,k}$ is called a matrix distribution. It produces matrices from $\mathbb{Z}_p^{\ell \times k}$ of full rank k. W.l.o.g. we let the first k rows of $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$ forms an invertible matrix. When $\ell = k + 1$, we refer to the distribution as $\mathcal{D}_k$



Example . As a simple example, let $k = 3$ and $\ell = 4$, meaning the matrix $\mathbf{A}$ has 4 rows and 3 columns. Given $k = 3$, $\ell = 4$, and a finite field of prime order p, a possible matrix $\mathbf{A}$ could be:

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 3 & 4 \end{pmatrix}$$

Matrix Assumptions:

Decisional Diffie-Hellman Assumption $x, y, z \leftarrow_{\$} \mathbb{Z}_p^*$

$Adv^{\mathsf{DDH}}_{\mathcal{A}}(\kappa) := |\varepsilon_1 - \varepsilon_0| \leq \nu(\kappa)$ $\varepsilon_\beta := \Pr[\mathcal{A}([x], [y], [xy + \beta z]) = 1]$

$\mathcal{D}_{\ell,k}$-Matrix Decisional Diffie-Hellman ($\mathcal{D}_{\ell,k}$-MDDH) $\mathbf{A} \leftarrow_{\$} \mathcal{D}_{\ell,k}, \mathbf{r} \leftarrow_{\$} \mathbb{Z}_p^k, \mathbf{u} \leftarrow_{\$} \mathbb{Z}_p^\ell$

$Adv^{\mathsf{MDDH}}_{\mathcal{D}_{\ell,k},\mathbb{G}_\zeta,\mathcal{A}}(\kappa) := |\varepsilon_{\mathbf{1}} - \varepsilon_{\mathbf{0}}| \leq \nu(\kappa)$ $\varepsilon_\beta := \Pr\left[\mathcal{A}(\mathcal{BG}, [\mathbf{A}]_\zeta, [\mathbf{Ar} + \beta\mathbf{u}]_\zeta) = 1\right]$

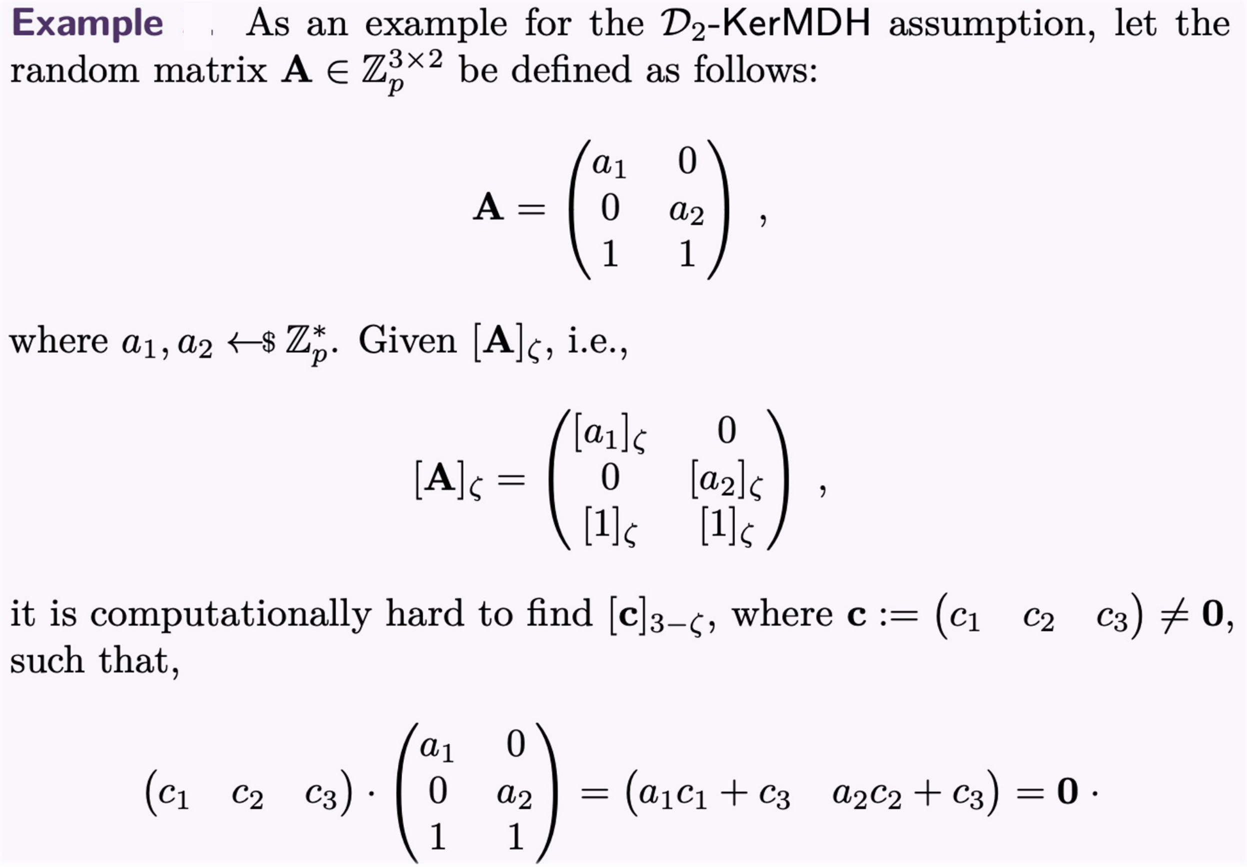
$\mathcal{D}_k$-Kernel Matrix Diffie-Hellman ($\mathcal{D}_k$-KerMDH) $\mathbf{A} \leftarrow_{\$} \mathcal{D}_k$

$Adv^{\mathsf{KerMDH}}_{\mathcal{D}_k,\mathbb{G}_\zeta,\mathcal{A}}(\kappa) = \Pr\left[\mathbf{c} \in \mathsf{orth}(\mathbf{A}) \mid [\mathbf{c}]_{3-\zeta} \leftarrow \mathcal{A}(\mathcal{BG}, [\mathbf{A}]_\zeta))\right] \leq \nu(\kappa)$ $\zeta = \{1, 2\}$

Matrix Assumptions:

$\mathcal{D}_k$-Kernel Matrix Diffie-Hellman ($\mathcal{D}_k$-KerMDH) $\quad \mathbf{A} \leftarrow\$ \mathcal{D}_k$

$$Adv^{\mathsf{KerMDH}}_{\mathcal{D}_k,\mathbb{G}_\zeta,\mathcal{A}}(\kappa) = \Pr\left[\mathbf{c} \in \mathsf{orth}(\mathbf{A}) \mid [\mathbf{c}]_{3-\zeta} \leftarrow \mathcal{A}(\mathcal{BG}, [\mathbf{A}]_\zeta))\right] \leq \nu(\kappa) \qquad \zeta = \{1,2\}$$



Example As an example for the $\mathcal{D}_2$-KerMDH assumption, let the random matrix $\mathbf{A} \in \mathbb{Z}_p^{3\times 2}$ be defined as follows:

$$\mathbf{A} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix},$$

where $a_1, a_2 \leftarrow\$ \mathbb{Z}_p^*$. Given $[\mathbf{A}]_\zeta$, i.e.,

$$[\mathbf{A}]_\zeta = \begin{pmatrix} [a_1]_\zeta & 0 \\ 0 & [a_2]_\zeta \\ [1]_\zeta & [1]_\zeta \end{pmatrix},$$

it is computationally hard to find $[\mathbf{c}]_{3-\zeta}$, where $\mathbf{c} := \begin{pmatrix} c_1 & c_2 & c_3 \end{pmatrix} \neq \mathbf{0}$, such that,

$$\begin{pmatrix} c_1 & c_2 & c_3 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a_1 c_1 + c_3 & a_2 c_2 + c_3 \end{pmatrix} = \mathbf{0}\,.$$

Kiltz, Pan and Wee SPS [KPW15]:

Key Generation

$$\mathbf{A}, \mathbf{B} \leftarrow_\$ \mathcal{D}_k$$

$$\mathbf{K} \leftarrow_\$ \mathbb{Z}_p^{(\ell+1)\times(k+1)}$$

$$\mathbf{U}, \mathbf{V} \leftarrow_\$ \mathbb{Z}_p^{(k+1)\times(k+1)}$$

$$\left(\mathbf{K}, [\mathbf{B}^\top \mathbf{U}]_1, [\mathbf{B}^\top \mathbf{V}]_1, [\mathbf{B}]_1\right)$$

$$\left([\mathbf{A}]_2, [\mathbf{U}\mathbf{A}]_2, [\mathbf{V}\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2\right)$$

Signing

$$[\text{✉}]$$

$$\mathbf{r} \leftarrow_\$ \mathbb{Z}_p^k$$

$$\tau \leftarrow_\$ \mathbb{Z}_p$$

$$\sigma_1 := \left[\begin{pmatrix}1 & \mathbf{m}^\top\end{pmatrix}\right]_1 \mathbf{K} + \mathbf{r}^\top \left[\mathbf{B}^\top(\mathbf{U} + \tau\mathbf{V})\right]_1 \in \mathbb{G}_1^{1\times(k+1)}$$

$$\sigma_2 := [\mathbf{r}^\top \mathbf{B}^\top]_1 \in \mathbb{G}_1^{1\times(k+1)}$$

$$\sigma_3 := [\mathbf{r}^\top \mathbf{B}^\top \tau]_1 \in \mathbb{G}_1^{1\times(k+1)}$$

$$\sigma_4 := [\tau]_2 \in \mathbb{G}_2$$

Verify

$$e(\sigma_1, [\mathbf{A}]_2) = e\left(\left[\begin{pmatrix}1 & \mathbf{m}^\top\end{pmatrix}\right]_1, [\mathbf{K}\mathbf{A}]_2\right)\ e(\sigma_2, [\mathbf{U}\mathbf{A}]_2)\ e(\sigma_3, [\mathbf{V}\mathbf{A}]_2)$$

$$e(\sigma_2, \sigma_4) = e(\sigma_3, \mathsf{G}_2)$$

Modified KPW15:

Setup

$\mathbf{A}, \mathbf{B} \leftarrow_{\$} \mathcal{D}_k$

$\mathbf{U}, \mathbf{V} \leftarrow_{\$} \mathbb{Z}_p^{(k+1)\times(k+1)}$

$(\mathcal{BG}, [\mathbf{A}]_2, [\mathbf{U}\mathbf{A}]_2, [\mathbf{V}\mathbf{A}]_2, [\mathbf{B}^\top\mathbf{U}]_1, [\mathbf{B}^\top\mathbf{V}]_1, [\mathbf{B}]_1)$

Key Generation

$\mathbf{K} \leftarrow_{\$} \mathbb{Z}_p^{(\ell+1)\times(k+1)}$

$[\mathbf{K}\mathbf{A}]_2$

Signing

$\mathbf{r} \leftarrow_{\$} \mathbb{Z}_p^k$

$\tau := \mathsf{H}([\mathbf{m}]_1)$

$\sigma_1 := [(1 \quad \mathbf{m}^\top)]_1 \mathbf{K} + \mathbf{r}^\top [\mathbf{B}^\top(\mathbf{U} + \tau\mathbf{V})]_1 \quad \in \mathbb{G}_1^{1\times(k+1)}$

$\sigma_2 := [\mathbf{r}^\top\mathbf{B}^\top]_1 \quad \in \mathbb{G}_1^{1\times(k+1)}$

$\sigma_3 := [\mathbf{r}^\top\mathbf{B}^\top\tau]_1 \quad \in \mathbb{G}_1^{1\times(k+1)}$

$\sigma_4 := [\tau]_2 \quad \in \mathbb{G}_2$

Verify

$e(\sigma_1, [\mathbf{A}]_2) = e\left([(1 \quad \mathbf{m}^\top)]_1, [\mathbf{K}\mathbf{A}]_2\right) \; e(\sigma_2, [\mathbf{U}\mathbf{A}]_2) \; e(\sigma_3, [\mathbf{V}\mathbf{A}]_2)$

$e(\sigma_2, \sigma_4) = e(\sigma_3, \mathsf{G}_2)$

TSPS Under Standard Assumptions: adp-T-UF-1 [MMSST24]

We start from a SPS proposed by Kiltz et al. [KPW15], where the first and second signature components are as follows:

$$\text{KPW15}:\ (\sigma_1, \sigma_2) := \left(\underbrace{\left[\left(1\ \mathbf{m}^\top\right)\right]_1}_{\text{SP-OTS}} \mathbf{K} + \overbrace{\mathbf{r}^\top \left[\mathbf{B}^\top(\mathbf{U} + \tau \cdot \mathbf{V})\right]_1, \left[\mathbf{r}^\top \mathbf{B}^\top\right]_1}^{\text{randomized PRF}} \right)$$

We slightly modify the scheme such that the tag τ is obtained from a collision-resistant hash function.

$$(\sigma_1, \sigma_2) = \left(\left[\left(1\ \mathbf{m}^\top\right)\right]_1 \mathbf{K}_i + \mathbf{r}_i^\top \left[\mathbf{B}^\top(\mathbf{U} + \tau \cdot \mathbf{V})\right]_1, \left[\mathbf{r}_i^\top \mathbf{B}^\top\right]_1 \right)$$

Finally, the partial signature is defined as:

```
$\mathbf{r}_i \leftarrow \mathbb{Z}_p^k$.
$\tau := \mathcal{H}([\mathbf{m}]_1)$.
Output $\Sigma_i := (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ s.t.
$\sigma_1 := \left[\left(1\ \mathbf{m}^\top\right)\right]_1 \mathbf{K}_i + \mathbf{r}_i^\top \left[\mathbf{B}^\top(\mathbf{U} + \tau\mathbf{V})\right]_1$ ,
  $\sigma_2 := \left[\mathbf{r}_i^\top \mathbf{B}^\top\right]_1$ ,
  $\sigma_3 := \left[\tau \mathbf{r}_i^\top \mathbf{B}^\top\right]_1$ ,
  $\sigma_4 := [\tau]_2$ .
```

Application: Anonymous Credentials [Cha84]

Issuer

User

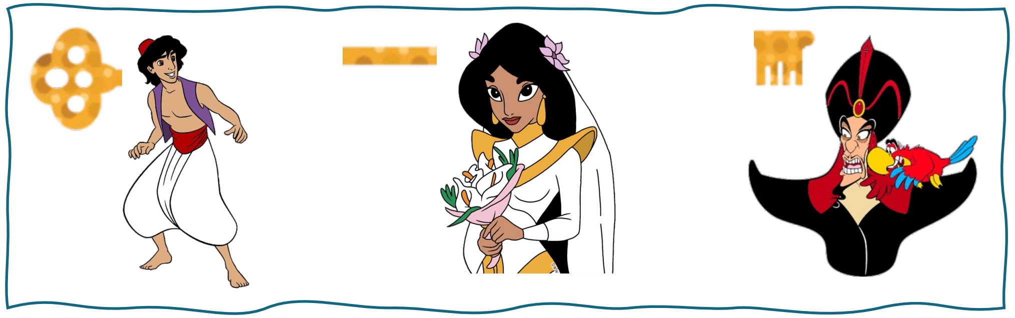
Name:
Jasmin

Date of Birth:
20.09.2000

Valid till:
30.03.2024

ID No.
****

Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



Issuers

User

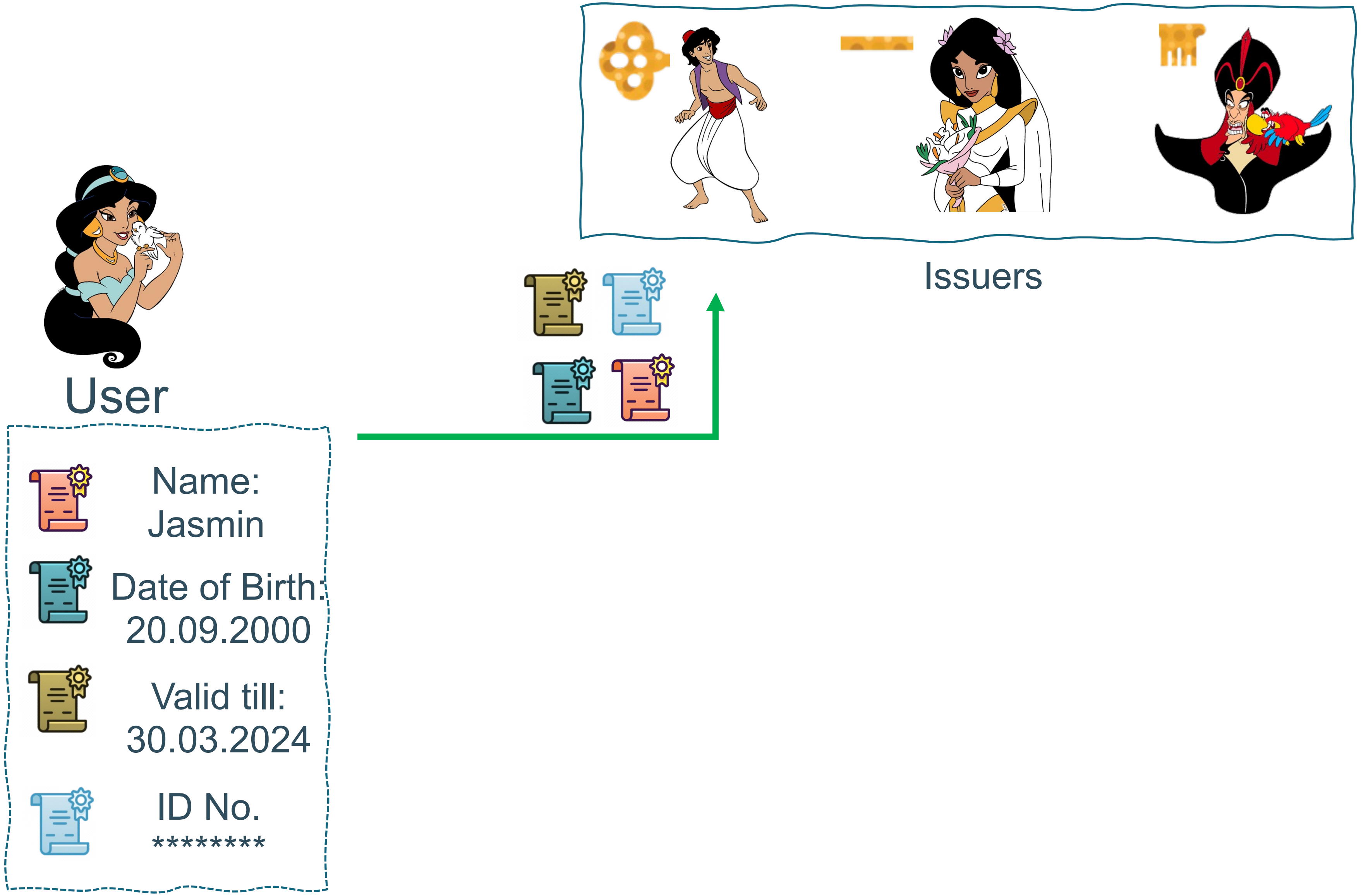
Name:
Jasmin

Date of Birth:
20.09.2000

Valid till:
30.03.2024

ID No.
****

Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



Issuers

User

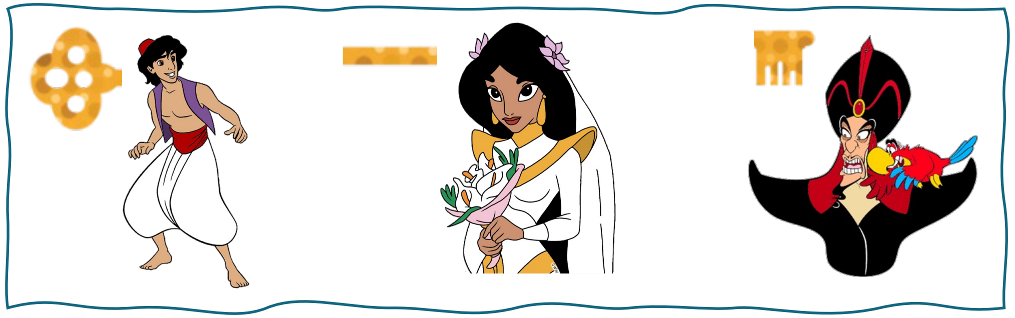
Name:
Jasmin

Date of Birth:
20.09.2000

Valid till:
30.03.2024

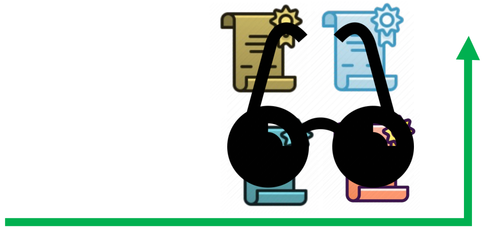
ID No.
****

Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



Issuers

User



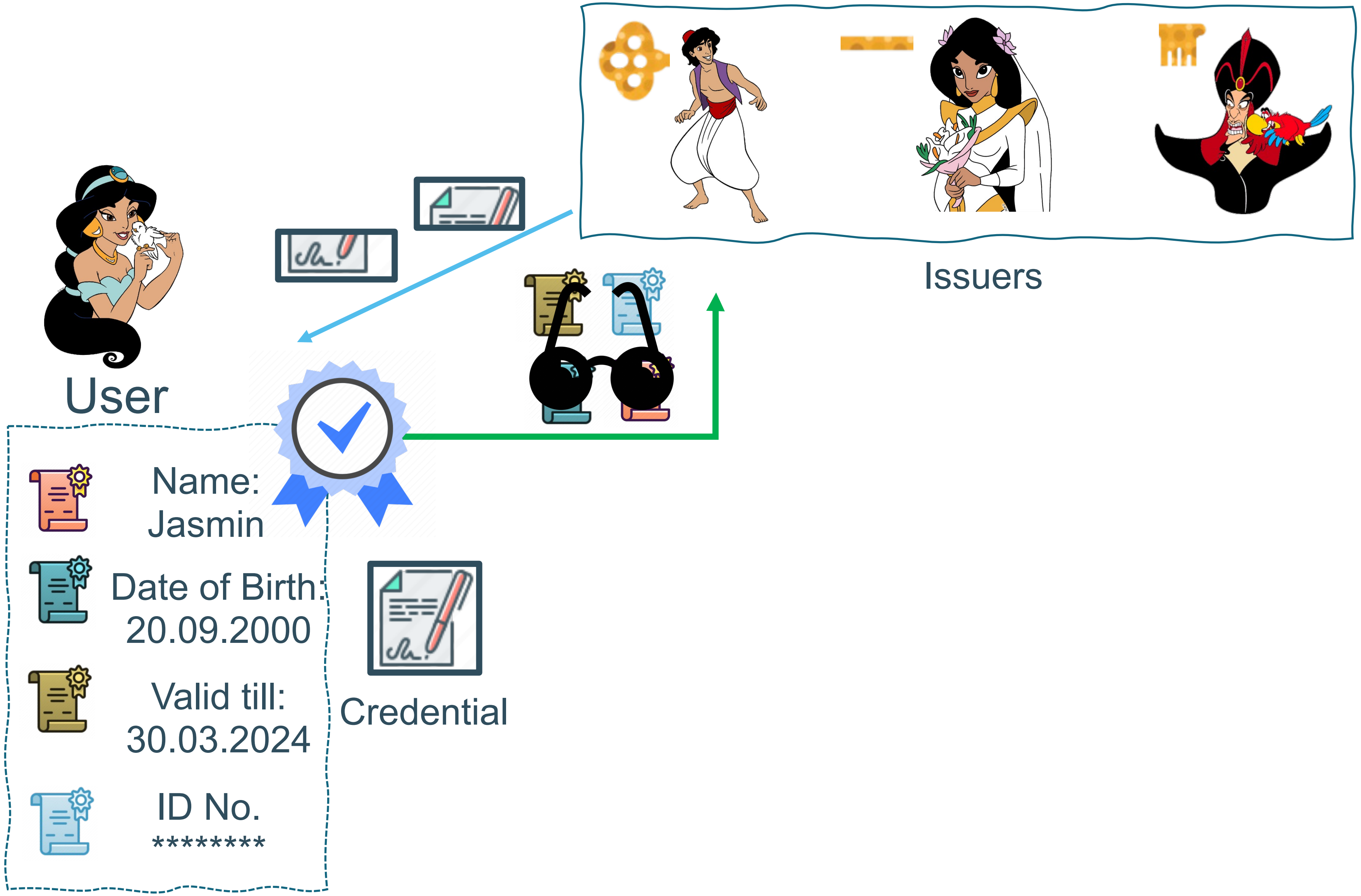
Name:
Jasmin

Date of Birth:
20.09.2000

Valid till:
30.03.2024

ID No.
****

Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



Issuers

User

Name:
Jasmin

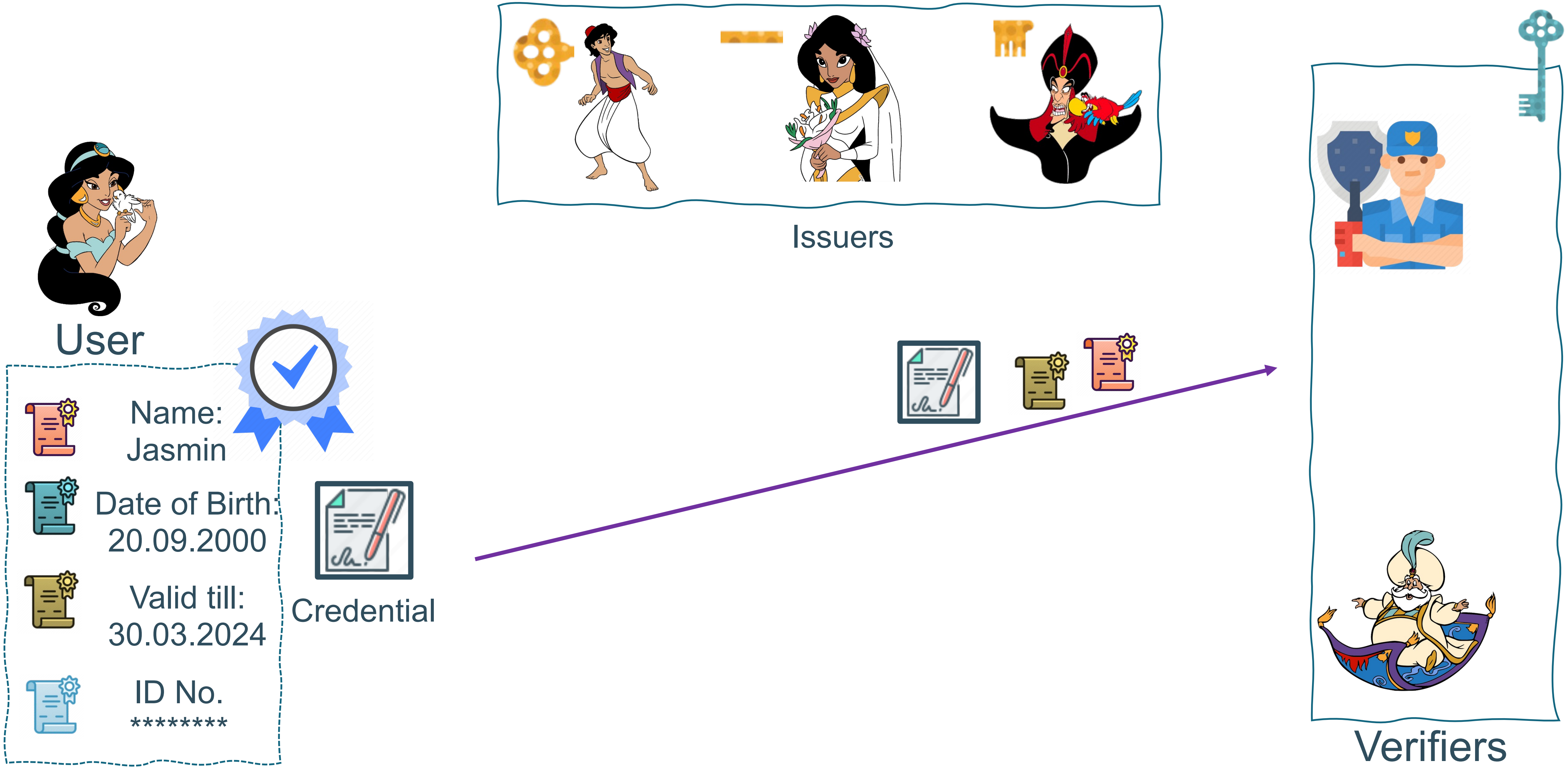
Date of Birth:
20.09.2000

Valid till:
30.03.2024

ID No.
****

Credential

Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



Issuers

User

Name:
Jasmin

Date of Birth:
20.09.2000

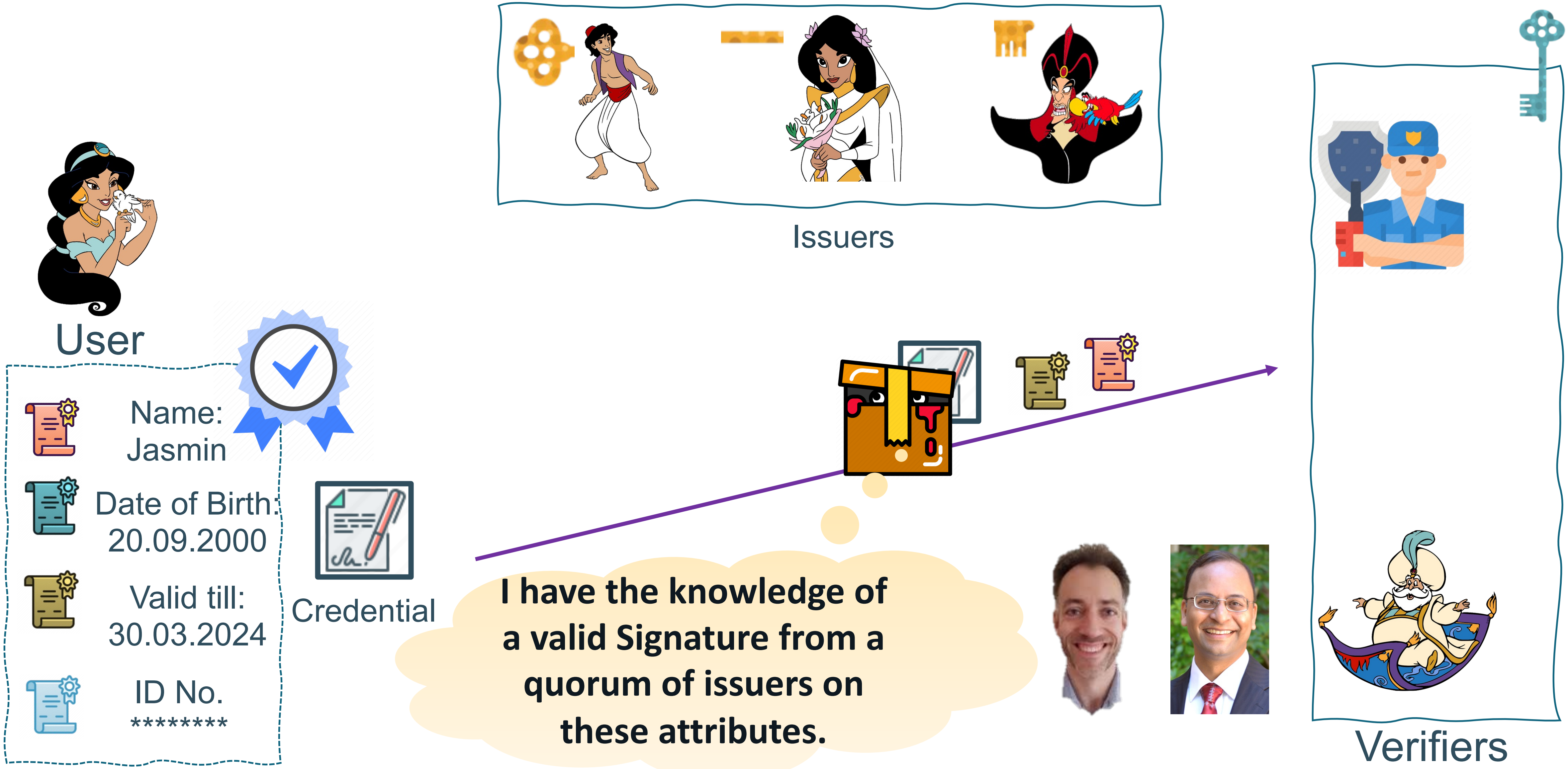
Valid till:
30.03.2024

ID No.
****

Credential

Verifiers

Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



Issuers

User

Name: Jasmin

Date of Birth: 20.09.2000

Valid till: 30.03.2024

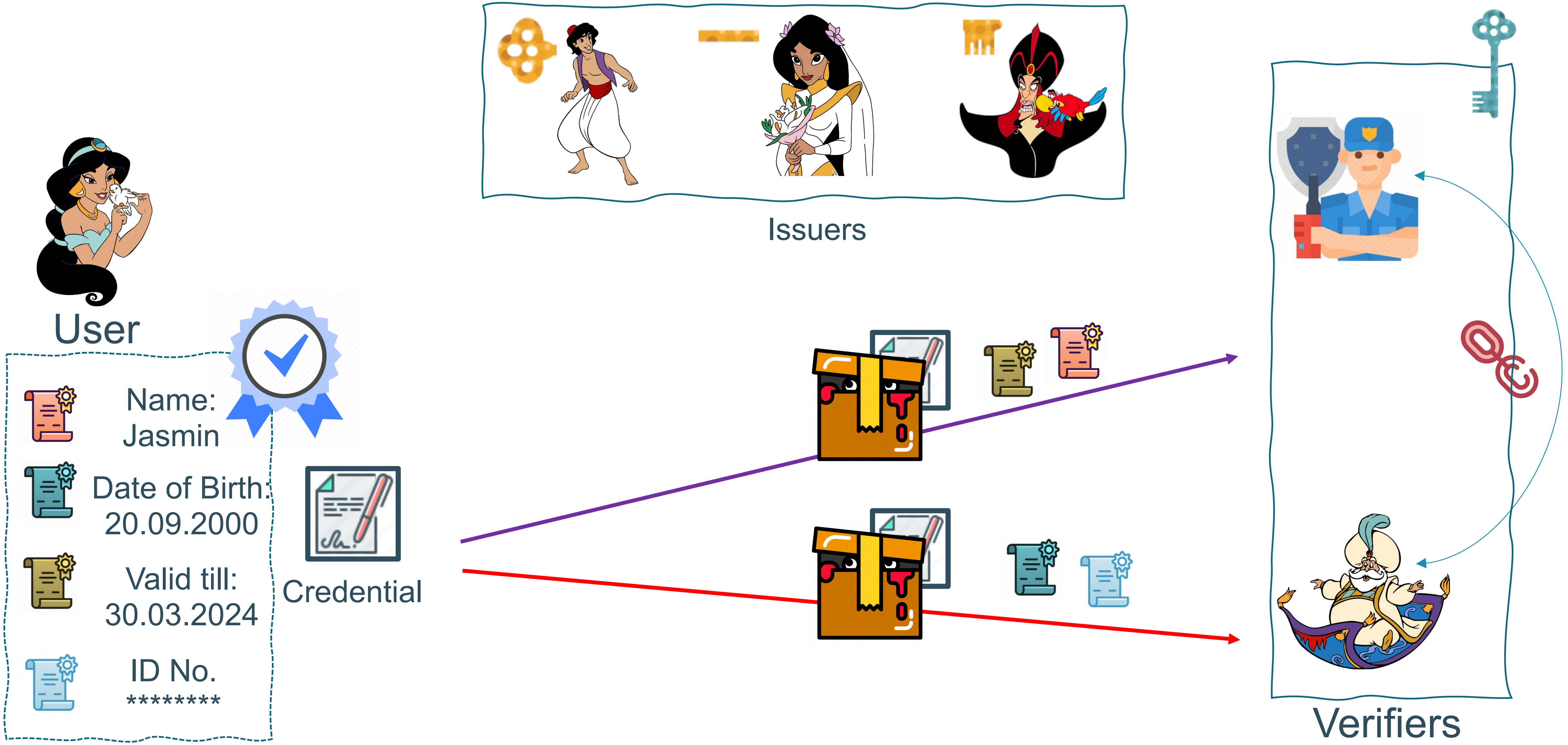
ID No. ********

Credential

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

Verifiers

Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



Issuers

User

Name: Jasmin

Date of Birth: 20.09.2000

Valid till: 30.03.2024

ID No. ********

Credential

Verifiers

Conclusion and Open questions:

Conclusion:

- Threshold signatures tolerate some fraction of of corrupted signers.
- SPS enable a modular framework to design complex systems more efficiently.
- No Threshold SPS exists.
- The first (Non-Interactive) TSPS over indexed Diffie-Hellman message spaces.
- A TSPS based on standard assumptions.
- We discussed TIAC as a primary application of this scheme.

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) Tightly secure TSPS.

References

[Cha84] David Chaum. “A new paradigm for individuals in the information age.” In *IEEE Symposium on Security and Privacy* 1984.

[BLS04] Boneh et al. “Short signatures from the Weil pairing.”, Journal of Cryptology, 2004.

[Sha79] Adi Shamir. “How to share a secret.”, Communications of the Association for Computing Machinery, November 1979.

[Bol03] Alexandra Boldyreva. “Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme.”, PKC 2003.

[GMR89] Goldwasser et al. “The knowledge complexity of interactive proof-systems.”

[AFG+10] Abe et al. “Structure-preserving signatures and commitments to group elements.”, CRYPTO 2010.

[AGHO11] Abe et al. “Optimal structure-preserving signatures in asymmetric bilinear groups.”, CRYPTO 2011.

[Fuc09] Georg Fuchsbauer. “Automorphic signatures in bilinear groups and an application to round-optimal blind signatures.” Cryptology ePrint Archive, Report 2009/320, 2009.

[PS16] David Pointcheval and Olivier Sanders. “Short randomizable signatures.”, CT-RSA 2016.

[Gha16] Essam Ghadafi. “Short structure-preserving signatures”, CT-RSA 2016.

[GS08] Jens Groth and Amit Sahai. “Efficient non-interactive proof systems for bilinear groups.”, EUROCRYPT 2008.

[FHS19] Fuchsbauer et al. “Structure-preserving signatures on equivalence classes and constant-size anonymous credentials.”, AC’14, JoC’19.

[SAB+19] Sonnino et al. “Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers.”, NDSS 2019.

[BCK+22] Bellare et al. “Better than advertised security for non-interactive threshold signatures.”, CRYPTO 2022.

[KPW15] Eike Kiltz, Jiaxin Pan, and Hoeteck Wee. "Structure-preserving signatures from standard assumptions, revisited.”, Crypto 2015.

Thank You!

ssedagha@esat.kuleuven.be

The illustrations are credited to Disneyclips.