2022/839

Threshold Structure-Preserving Signatures

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

1 Web3 Foundation
2 University of Edinburgh, Edinburgh, UK
3 COSIC, KU Leuven, Leuven, Belgium
4 CODE, Universität der Bundeswehr München, Munich, Germany

Asiacrypt 2023, December 5 (Guangzhou, China)

Outline:

2022/839

Threshold Structure-Preserving Signatures

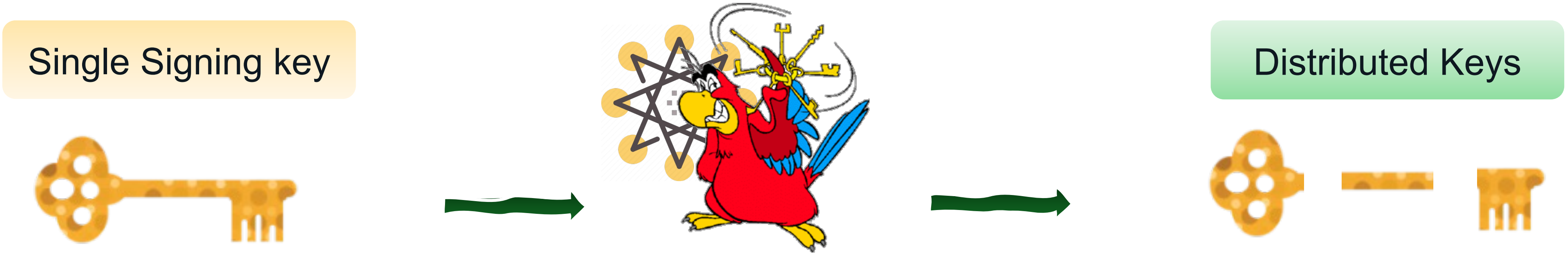
Outline:

Threshold Structure-Preserving Signatures

Threshold Signatures

Structure-Preserving Signatures

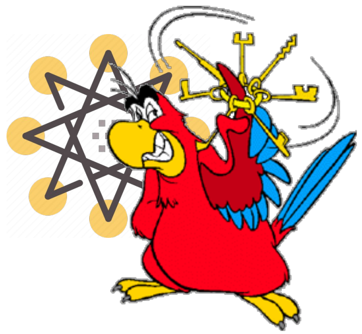
Threshold Signatures [DY90]: To tolerate some fraction of corrupt signers



Trusted Dealer or
Distributed Key Generation (DKG) protocols

Threshold Signatures [DY90]: To tolerate some fraction of corrupt signers

Single Signing key



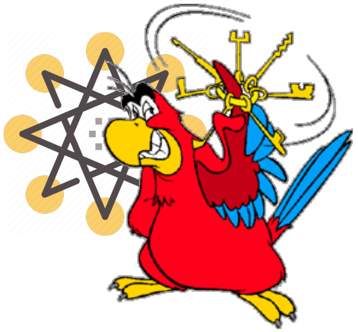
Trusted Dealer or
Distributed Key Generation (DKG) protocols

Distributed Keys

- Applications:
  1. Cryptocurrency wallets (To jointly sign and authorize a transaction)
  2. Threshold-Issuance Anonymous Credentials (To jointly authorize credentials in the system)

Threshold Signatures [DY90]: To tolerate some fraction of corrupt signers

Single Signing key



Trusted Dealer or
Distributed Key Generation (DKG) protocols

Distributed Keys

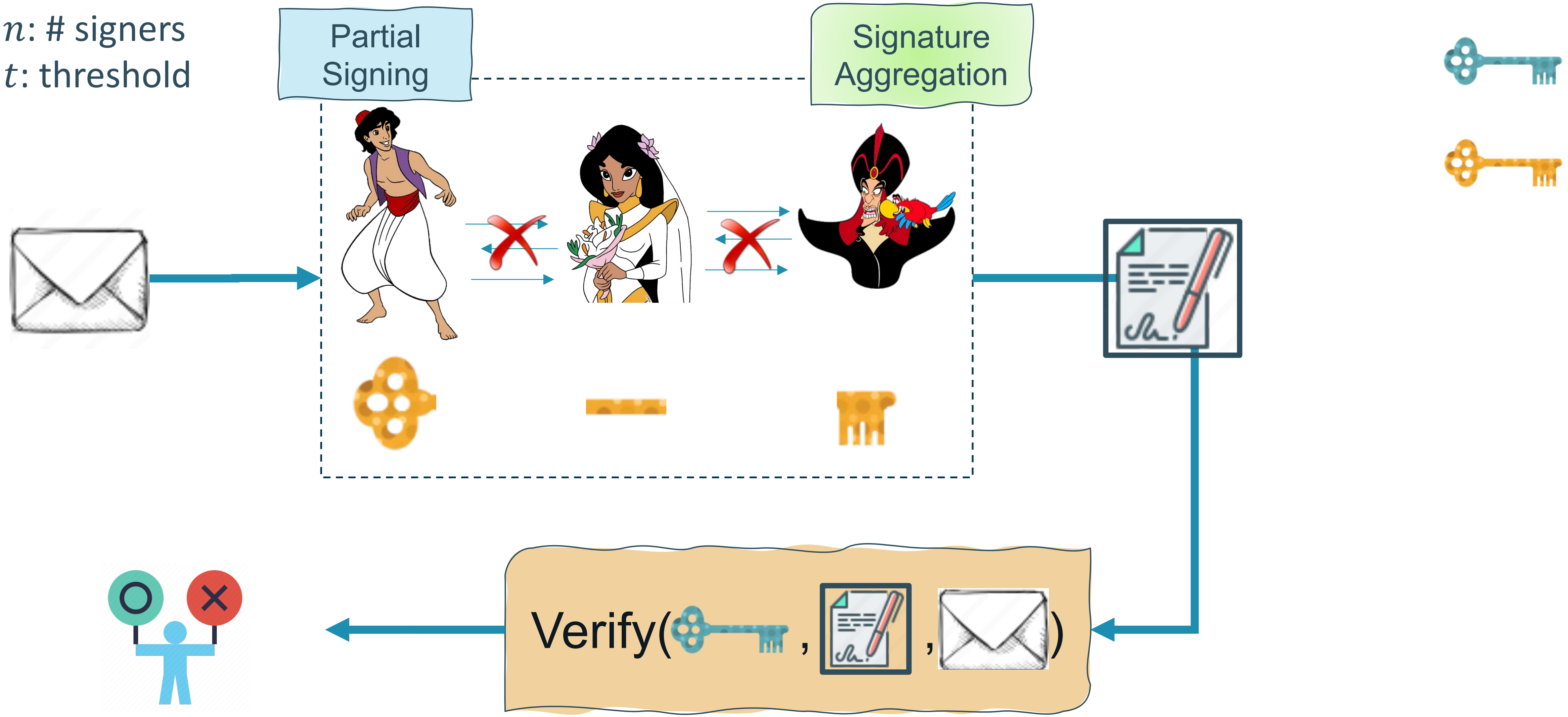
- Applications:
  1. Cryptocurrency wallets (To jointly sign and authorize a transaction)
  2. Threshold-Issuance Anonymous Credentials (To jointly authorize credentials in the system)

- Security
- Availability

NIST
National Institute of
Standards and Technology

Non-Interactive Threshold Signatures: Not one-time signature

$3 = n$: # signers
$2 = t$: threshold



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

KeyGen

$sk := s \xleftarrow{\$} \mathbb{Z}_p^*$ $vk := G_2^{sk}$

Source groups

Target group

* (Type-III) Bilinear Groups:
  - There exists an efficient map e: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$:
    - **Bilinearity**: $e\left(G_1^x, G_2^y\right) = e(G_1, G_2)^{xy}, \forall x, y \in \mathbb{Z}_p$
    - **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

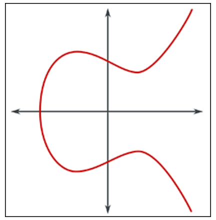
KeyGen

$sk := s \xleftarrow{\$} \mathbb{Z}_p^*$ $\qquad vk := G_2^{sk}$

Signing

Arbitrary Message

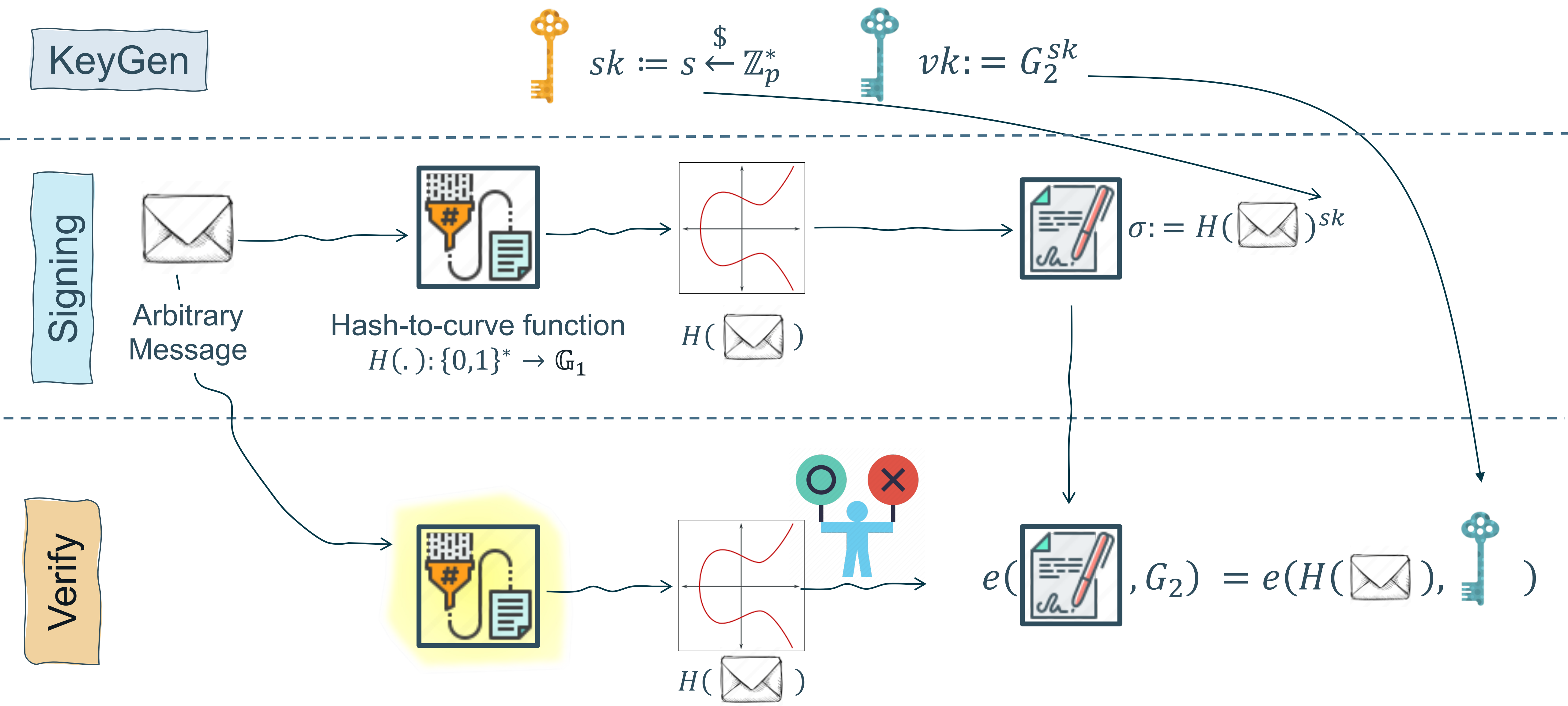
Hash-to-curve function
$H(.): \{0,1\}^* \to \mathbb{G}_1$



$H($  $)$

$\sigma := H($  $)^{sk}$

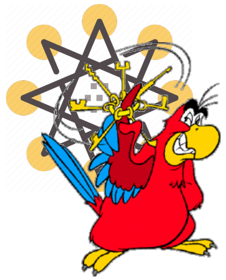
BLS signature [BLS04]: A simple not one-time NI-TS



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

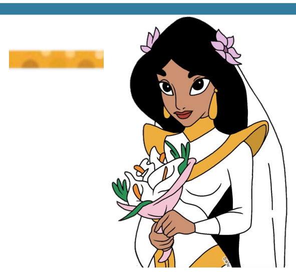
KeyGen

$sk \coloneqq s \xleftarrow{\$} \mathbb{Z}_p^*$



Trusted Dealer
or DKG

$sk_1 \coloneqq s_1$

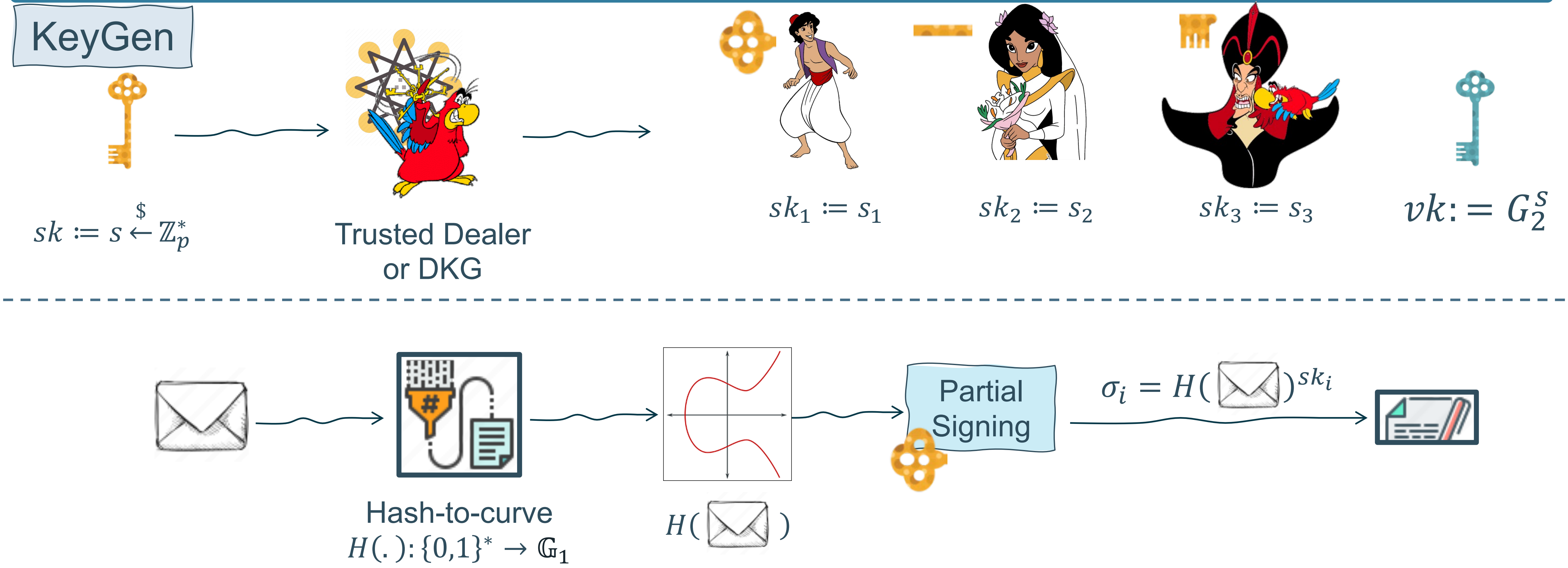


$sk_2 \coloneqq s_2$

$sk_3 \coloneqq s_3$

$vk := G_2^s$

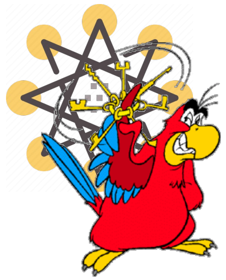
Threshold BLS signature [Bol03]: A simple example of NI-TS



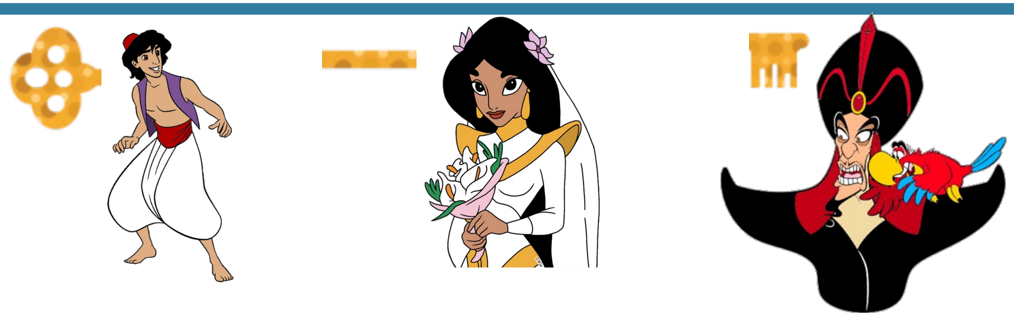
Threshold BLS signature [Bol03]: A simple example of NI-TS

KeyGen

$sk \coloneqq s \xleftarrow{\$} \mathbb{Z}_p^*$



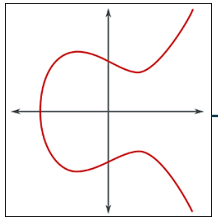
Trusted Dealer
or DKG



$sk_1 \coloneqq s_1$ $sk_2 \coloneqq s_2$ $sk_3 \coloneqq s_3$

$vk := G_2^s$

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



$H(\ )$

Partial Signing

$\sigma_i = H(\ )^{sk_i}$

Signature Aggregation

$$\sigma = \prod_{i \in T} \sigma_i^{L_i^T(0)} = \left(H(\ )^{sk_i}\right)^{L_i^T(0)} = H(\ )^{sk}, \forall\ |T| \geq t$$

Structure-Preserving Cryptography [AFG+10]:

- 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.

Structure-Preserving Signatures [AFG+10]:

1

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

Structure-Preserving Signatures [AFG+10]:

1

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

BLS is not a SPS!

No Non-Linear operation like **Hash Functions**

2

Verify(, ,):

Done by:

- membership tests

$\in \mathbb{G}_1 \vee \mathbb{G}_2$

- pairing product equations

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

Our Main Objective:

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

Our Results and Contributions:

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

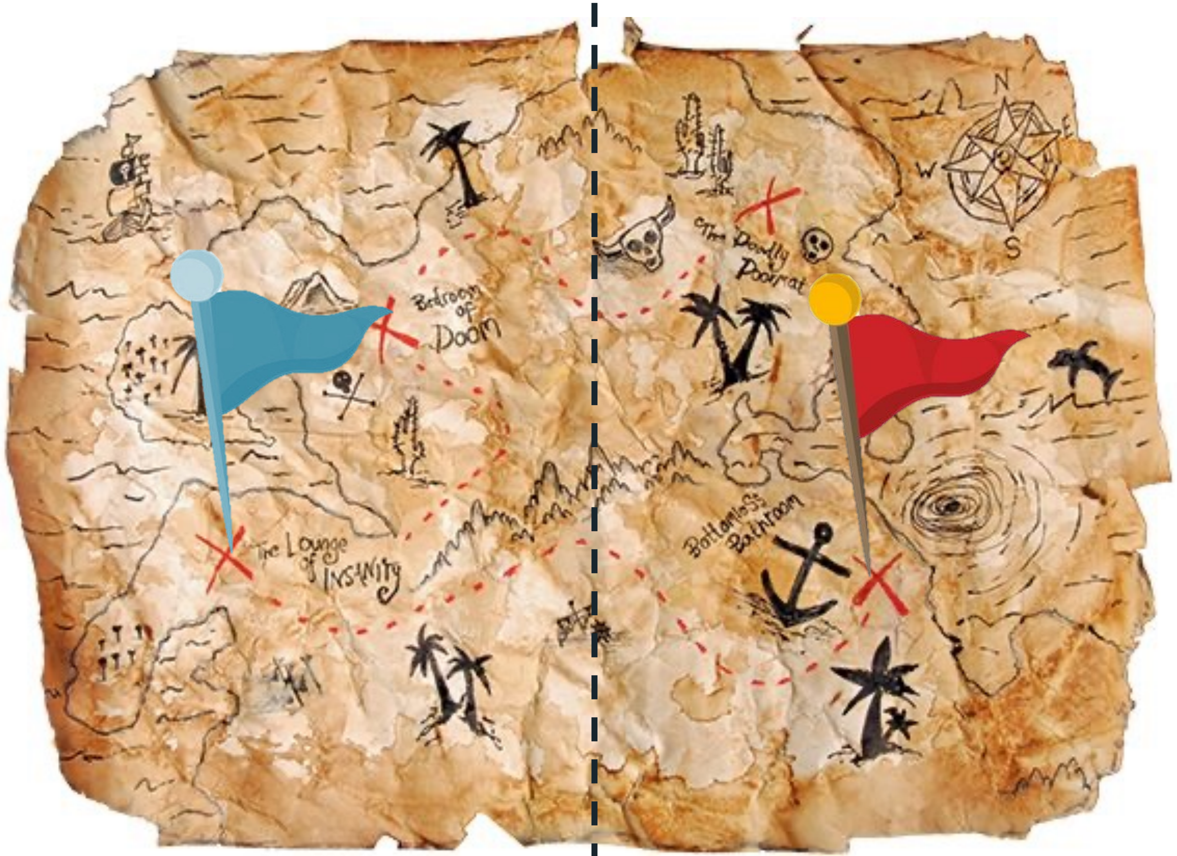
1- TSPS syntax and security definitions.

2- The first Non-Interactive TSPS over indexed Diffie-Hellman message spaces.

3- Proof of unforgeability in the AGM+ROM under the hardness of a new assumption called GPS3.

4- The shortest possible signature and the least #PPE in the verification.

Treasure map: To look for a Non-Interactive TSPS



Threshold Signatures

Structure-Preserving Signatures

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

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
.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

Existing Structure-Preserving Signatures:

Structure-Preserving Signatures and Commitments to Group Elements

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

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]

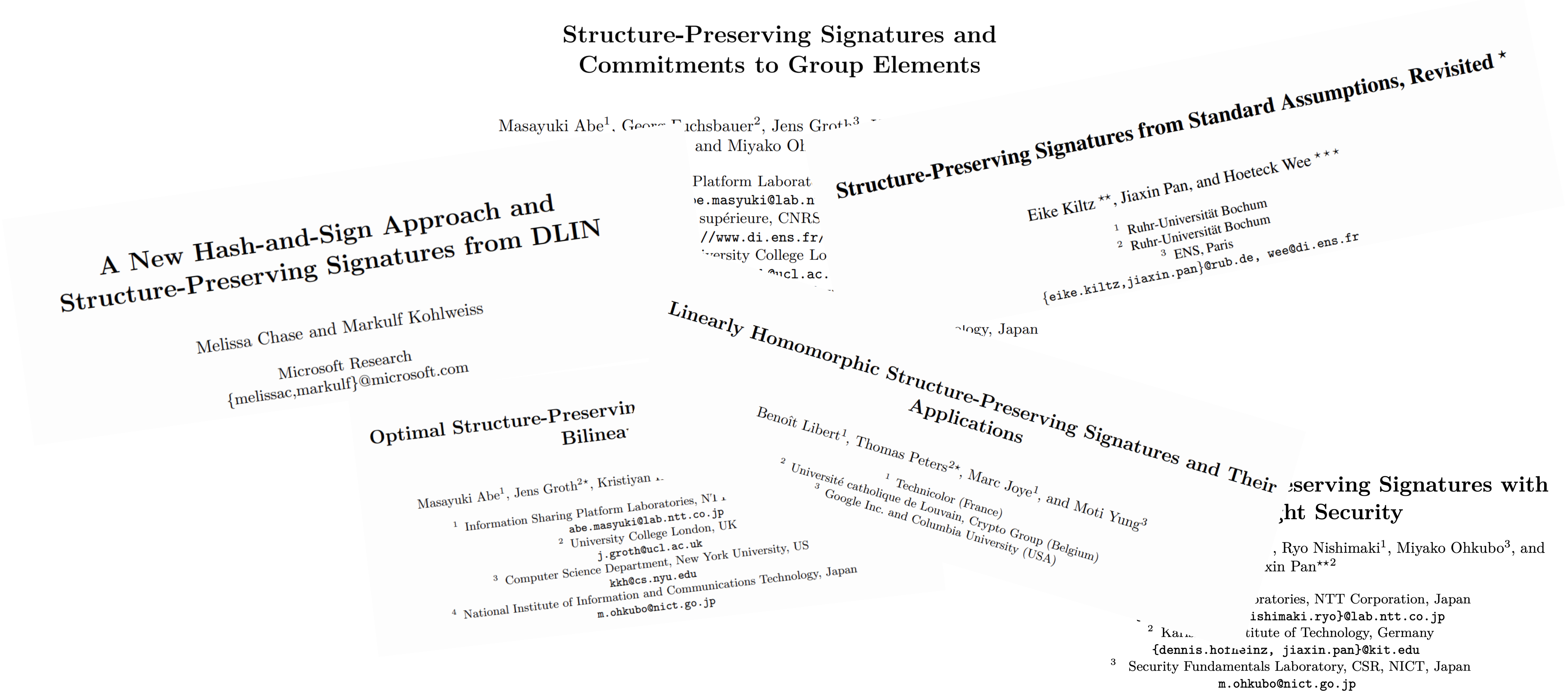
1 Information Sharing Platform Laboratories, NTT Corporation, Japan
abe.masyuki@lab.ntt.co.jp
2 University College London, UK
j.groth@ucl.ac.uk
3 Computer Science Department, New York University, US
kkh@cs.nyu.edu
4 National Institute of Information and Communications Technology, Japan
m.ohkubo@nict.go.jp

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

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...
...e.masyuki@lab.n...
... supérieure, CNRS
...//www.di.ens.fr/...
...versity College Lo...
...@ucl.ac...
...ology, Japan

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

Melissa Chase and Markulf Kohlweiss
Microsoft Research
{melissac,markulf}@microsoft.com

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 Karl... ...titute of Technology, Germany
{dennis.hofheinz, jiaxin.pan}@kit.edu
3 Security Fundamentals Laboratory, CSR, NICT, Japan
m.ohkubo@nict.go.jp

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

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 Kilt… …Pan, and Hoeteck Wee * * *
…hum
{eik…
…logy, Japan

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

Optimal Structure-Preservin… Bilinea…

Kristiyan …
…orm Laboratories, NT…
…syuki@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

Linearly Homomorphic Structure-Preserving Signatures a… 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

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)

Short Structure-Preserving Signatures

Essam Ghadafi*

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

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.

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

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

Existing Threshold Signatures:

Existing Threshold Signatures:

Finalists: 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: 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: 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

Short Structure-Preserving Signatures

Essam Ghadafi*

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

Scalar Messages

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**.

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

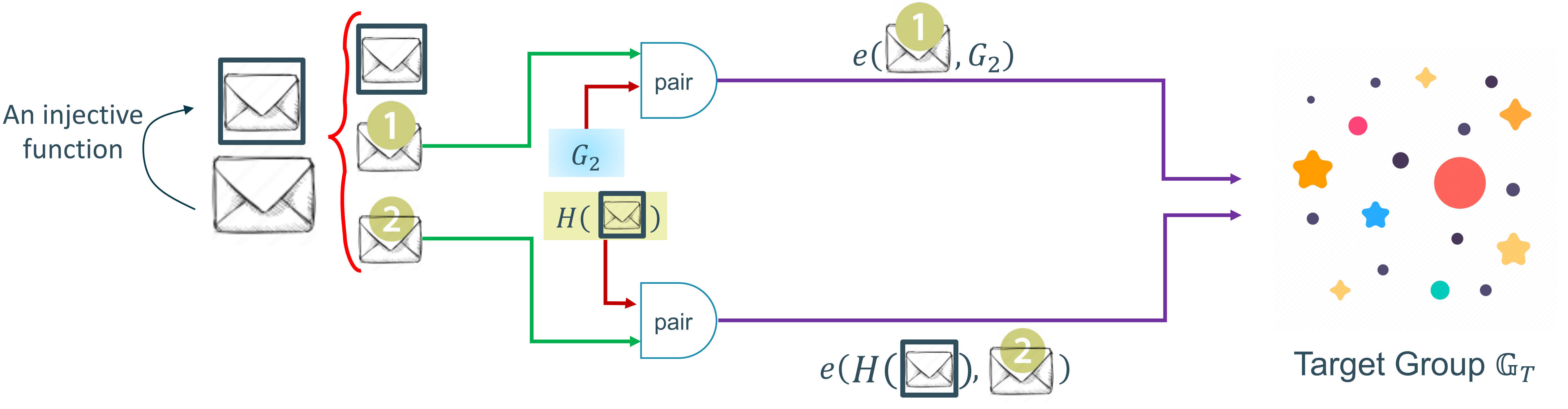
$$\text{i.e., } \exists\, m \in \mathbb{Z}_p : dlog_{G_1}(M_1) = dlog_{G_2}(M_2) = m$$

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



KU LEUVEN

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

KeyGen

$sk \coloneqq (x, y) \leftarrow {\mathbb{Z}_p^*}^2$

$vk := (G_2^x, G_2^y)$

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

KeyGen

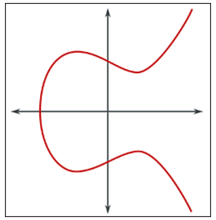
$sk := (x, y) \xleftarrow{\$} \mathbb{Z}_p^{*\,2}$

$vk := (G_2^x, G_2^y)$

Signing

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

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



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

$\sigma = (h, s) := \left(h, h^x M_1^y\right)$

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

KeyGen

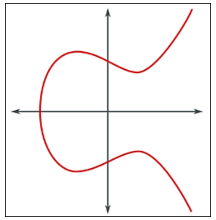
$sk := (x, y) \xleftarrow{\$} {\mathbb{Z}_p^*}^2$

$vk := (G_2^x, G_2^y)$

Signing

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

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



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

$\sigma = (h, s) := \left(h, h^x M_1^y\right)$

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

Verify

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

$e(M_1, G_2) = e(h, M_2)$

$e(h, G_2^x) e\left(M_1, G_2^y\right) = e(s, G_2)$

q-EUF-Chosen Message Attack (EUF-CMA): standard definition

$\longrightarrow vk, params$

M

σ

Signing Oracle

$Q_S \leftarrow Q_S \cup \{M\}$

q-EUF-Chosen Message Attack (EUF-CMA): standard definition

$vk, params$

σ^*, M^*

Return 1 if:

1. Verify(vk, M^*, σ^*)=1
2. $M^* \notin Q_S$
3. $|Q_S| \leq q$

M

σ

Signing Oracle

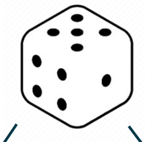
$Q_S \leftarrow Q_S \cup \{M\}$

Is this scheme EUF-CMA secure?

1 **Partial Re-randomizability**

- The resulting iSPS is partially re-randomizable.

$$e(h, vk_1)e(M_1, vk_2) = e(s, G_2)$$



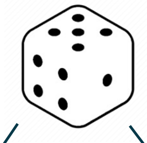
$$e(M_1, g_2) = e(h, M_2)$$

Is this scheme EUF-CMA secure?

1 Partial Re-randomizability

- The resulting iSPS is partially re-randomizable.

$$e(h, vk_1)e(M_1, vk_2) = e(s, G_2)$$



$$e(M_1, g_2) = e(h, M_2)$$

2 Repeated Index:

- The index should not repeat.

$$M^1 := (id, M_1^1, M_2^1) \qquad M^2 := (id, M_1^2, M_2^2)$$

$$(h, s^1) := \left(h, h^x {M_1^1}^y\right) \qquad (h, s^2) := \left(h, h^x {M_1^2}^y\right)$$

$$\widetilde{M}^* = \left((M_1^1 M_1^2)^{\frac{1}{2}}, (M_2^1 M_2^2)^{\frac{1}{2}}\right)$$

$$\sigma^* = (h^*, s^*) = \left(h, (s^1 s^2)^{1/2}\right)$$

q-EUF-Chosen indexed Message Attack (CiMA): Unique index

$\longrightarrow vk, params$

id_i

h_i

Random Oracle

If $Q_H[id] = \perp$:

$Q_H[id] \xleftarrow{\$} \mathcal{H}$

Return $Q_H[id]$

$M := (id, \widetilde{M})$

σ

Signing Oracle

If $(id_{\mathrm{i}}, \star) \in Q_S$: $return \perp$

$Q_S \leftarrow Q_S \cup \{(id, \widetilde{M})\}$

$Q_{EQ} \leftarrow Q_{EQ} \cup \{EQ(\widetilde{M}_i)\}$

$$EQ(M_1, M_2) = \{(M_1^r, M_2) \mid r \in \mathbb{Z}_p\}$$

q-EUF-Chosen indexed Message Attack (CiMA): Unique index

$\longrightarrow vk, params$

id_i

h_i

Random Oracle

If $Q_H[id] = \perp$:

$Q_H[id] \xleftarrow{\$} \mathcal{H}$

Return $Q_H[id]$

$\sigma^*, \widetilde{M}^*$

Return 1 if:

1. Verify($vk, \widetilde{M}^*, \sigma^*$)=1
2. $\widetilde{M}^* \notin Q_{EQ}$
3. $|Q_S| \leq q$

$M \coloneqq (id, \widetilde{M})$

σ

Signing Oracle

If $(id_i, \star) \in Q_S$: *return* $\perp$

$Q_S \leftarrow Q_S \cup \{(id, \widetilde{M})\}$

$Q_{EQ} \leftarrow Q_{EQ} \cup \{EQ(\widetilde{M}_i)\}$

Motivated by EUF-CMA definition of SPS on Equivalence Classes [FHS19].

$$EQ(M_1, M_2) = \{(M_1^r, M_2) \mid r \in \mathbb{Z}_p\}$$

Generalized Pointcheval-Sanders 3 (GPS3) assumption: Inspired by [KSAP22]

Theorem 1: GPS_3 assumption is hard in the Algebraic Group model and random oracle model as long as $(2,1)$-DL assumption is hard.

(Definition) (2,1)-DL assumption [BFL20]: Let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, p, e)$ be a type-III bilinear group. Given $\left(G_1^z, G_1^{z^2}, G_2^z\right)$, for all PPT adversaries it is infeasible to return z.

Generalized Pointcheval-Sanders 3 (GPS3) assumption: Inspired by [KSAP22]

Theorem 1: GPS_3 assumption is hard in the Algebraic Group model and random oracle model as long as $(2,1)$-DL assumption is hard.

Given $params := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, G_1, G_2)$:

$x, y \xleftarrow{\$} \mathbb{Z}_p^*$

$params, G_2^x, G_2^y$

$call$

G_1^r

Oracle $\mathcal{O}_0^{GPS_3}(.)$

$r \xleftarrow{\$} \mathbb{Z}_p^*$

$Q_0 \leftarrow Q_0 \cup \{G_1^r\}$

h, M_1, M_2

$h^x M_1^y$

Oracle $\mathcal{O}_1^{GPS_3}(.)$

If h $\notin Q_0 \vee$

$dlog_{h^*}(M_1) \neq dlog_{G_2}(M_2)$

$\vee\ (h,*) \in Q_1$:

Return $\perp$

$Q_1 \leftarrow Q_1 \cup \{(h, M_2)\}$

Generalized Pointcheval-Sanders 3 (GPS3) assumption: Inspired by [KSAP22]

Theorem 1: GPS_3 assumption is hard in the Algebraic Group model and random oracle model as long as $(2,1)$-DL assumption is hard.

Given $params := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, G_1, G_2)$:

$x, y \xleftarrow{\$} \mathbb{Z}_p^*$

$\xrightarrow{params,\, G_2^x,\, G_2^y}$

$call \rightarrow$ Oracle $\mathcal{O}_0^{GPS_3}(.)$

$r \xleftarrow{\$} \mathbb{Z}_p^*$

$Q_0 \leftarrow Q_0 \cup \{G_1^r\}$

$\leftarrow G_1^r$

$h, M_1, M_2 \rightarrow$ Oracle $\mathcal{O}_1^{GPS_3}(.)$

If h $\notin Q_0 \vee$
$dlog_{h^*}(M_1) \neq dlog_{G_2}(M_2)$
$\vee\ (h,*) \in Q_1$:
Return $\perp$
$Q_1 \leftarrow Q_1 \cup \{(h, M_2)\}$

$\leftarrow h^x M_1^y$

$\xleftarrow{(M_1^*, M_2^*, h^*, s^*)}$

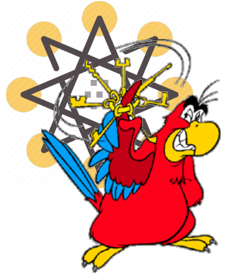
Return 1 if:

1. $h^* \neq 1_{\mathbb{G}_1} \wedge M_1^* \neq 1_{\mathbb{G}_1}$
2. $s^* = {h^*}^x {M_1^*}^y$
3. $dlog_{h^*}(M_1^*) = dlog_{G_2}(M_2^*)$
4. $(*, M_2^*) \notin Q_1$

Our proposed TSPS:

KeyGen

$sk \coloneqq (x, y) \xleftarrow{\$} {\mathbb{Z}_p^*}^2$



Dealer (or DKG)

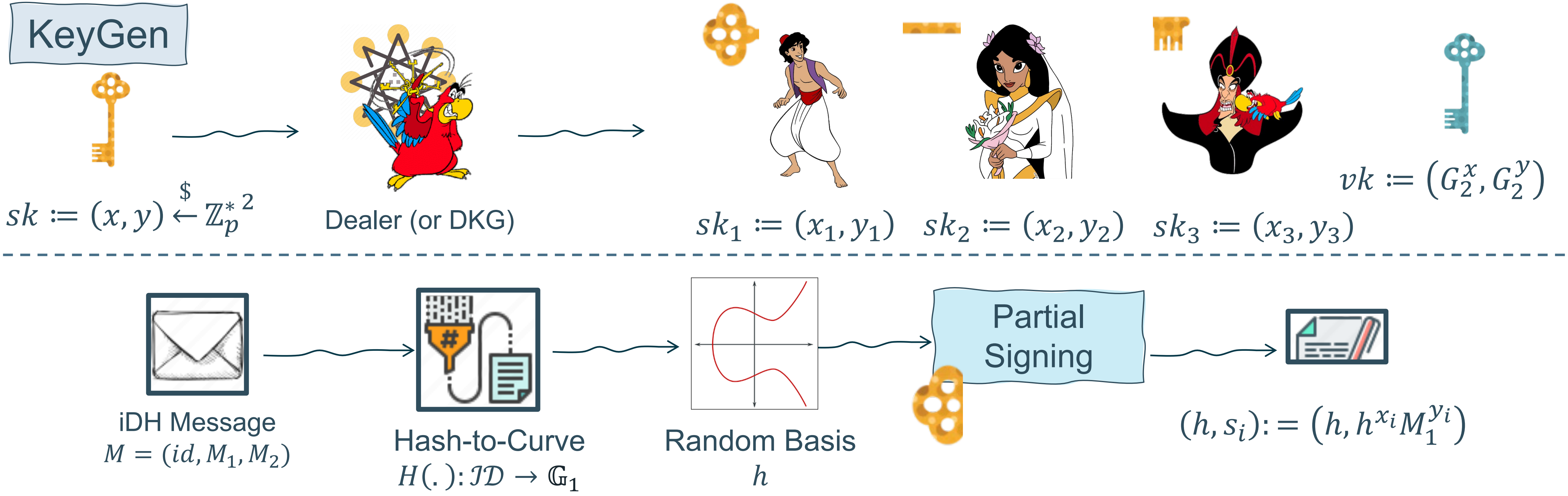
$sk_1 \coloneqq (x_1, y_1)$

$sk_2 \coloneqq (x_2, y_2)$

$sk_3 \coloneqq (x_3, y_3)$

$vk \coloneqq (G_2^x, G_2^y)$

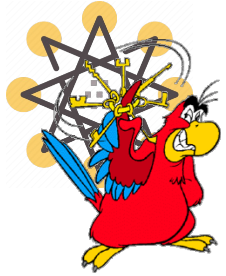
Our proposed TSPS:



Our proposed TSPS:

KeyGen

$sk \coloneqq (x, y) \overset{\$}{\leftarrow} \mathbb{Z}_p^{*\,2}$



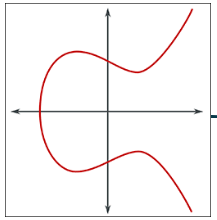
Dealer (or DKG)

$vk \coloneqq (G_2^x, G_2^y)$

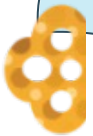
$sk_1 \coloneqq (x_1, y_1)$ $sk_2 \coloneqq (x_2, y_2)$ $sk_3 \coloneqq (x_3, y_3)$

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

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



Random Basis
h



Partial Signing

$(h, s_i) := \left(h, h^{x_i} M_1^{y_i}\right)$

Signature Aggregation

$$\sigma = \left(h, \prod_{i \in T} s_i^{L_i^T(0)}\right) = \left(h, h^x M_1^y\right), \forall\, |T| \geq t$$

Threshold EUF-CiMA: For static adversaries based on TS-UF-0 security [BCK+22]

$params$

$\mathcal{C}, |\mathcal{C}| = t - 1$

$vk, params$

id_i

h_i

Random Oracle

If $Q_H[id] = \perp$:

$Q_H[id] \xleftarrow{\$} \mathcal{H}$

Return $Q_H[id]$

$M := (k, id, \widetilde{M})$

σ_k

Partial Signing Oracle

If $(k, id_{\mathrm{i}}, \star) \in Q_S$: $return \perp$

$Q_S \leftarrow Q_S \cup \{(id, \widetilde{M})\}$

$Q_{EQ} \leftarrow Q_{EQ} \cup \{EQ(\widetilde{M}_i)\}$

$EQ(M_1, M_2) = \{(M_1^r, M_2) \mid r \in \mathbb{Z}_p\}$

Threshold EUF-CiMA: For static adversaries based on TS-UF-0 security [BCK+22]

$params$

$\mathcal{C}, |\mathcal{C}| = t - 1$

$vk, params$

id_i

h_i

Random Oracle

If $Q_H[id] = \perp$:

$Q_H[id] \xleftarrow{\$} \mathcal{H}$

Return $Q_H[id]$

$\sigma^*, \widetilde{M}^*$

Return 1 if:

1. Verify($vk, \widetilde{M}^*, \sigma^*$)=1
2. $\widetilde{M}^* \notin Q_{EQ}$
3. $|Q_S| \leq q$

$M := (k, id, \widetilde{M})$

σ_k

Partial Signing Oracle

If $(k, id_i, \star) \in Q_S$: $return \perp$

$Q_S \leftarrow Q_S \cup \{(id, \widetilde{M})\}$

$Q_{EQ} \leftarrow Q_{EQ} \cup \{EQ(\widetilde{M}_i)\}$

According to Bellare et al. [BCK+22], T-UF-0 implies that the adversary cannot query the partial signing oracle under challenge message.

$$EQ(M_1, M_2) = \{(M_1^r, M_2) \mid r \in \mathbb{Z}_p\}$$

Application: Anonymous Credentials [Cha84]

Issuer

User

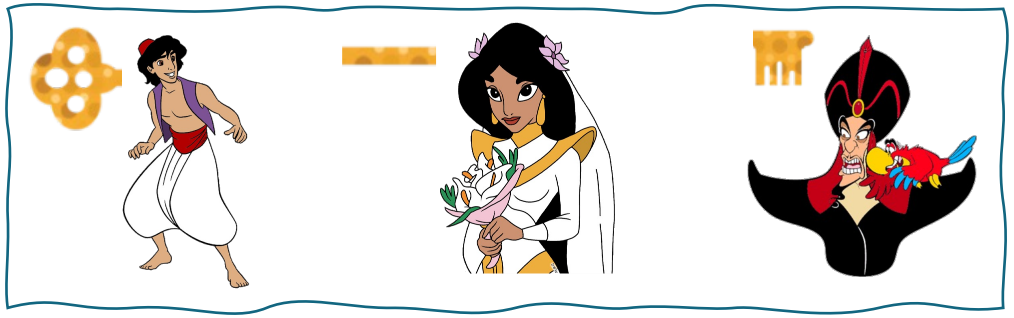
Name:
Jasmin

Date of Birth:
20.09.2000

Valid till:
30.03.2024

ID No.
****

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



Issuers

User

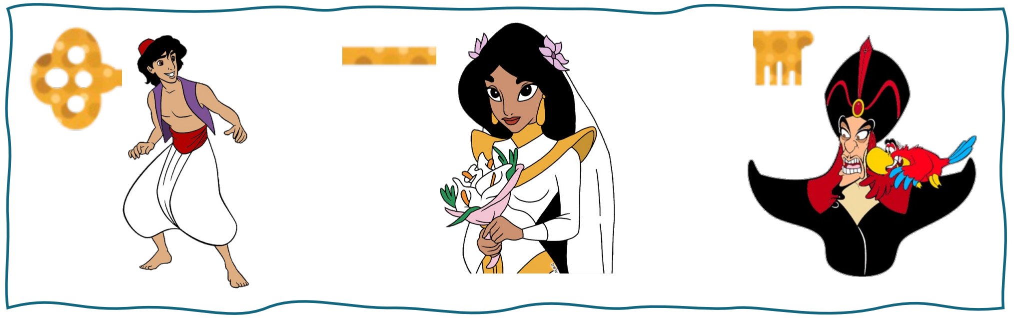
Name:
Jasmin

Date of Birth:
20.09.2000

Valid till:
30.03.2024

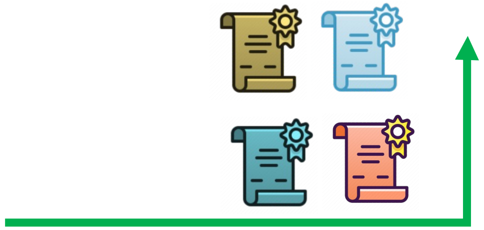
ID No.
****

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



Issuers

User



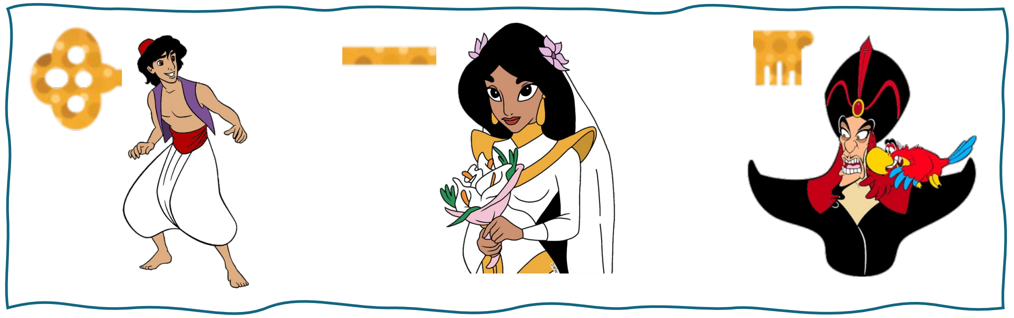
Name:
Jasmin

Date of Birth:
20.09.2000

Valid till:
30.03.2024

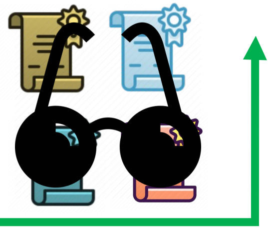
ID No.
****

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



Issuers

User



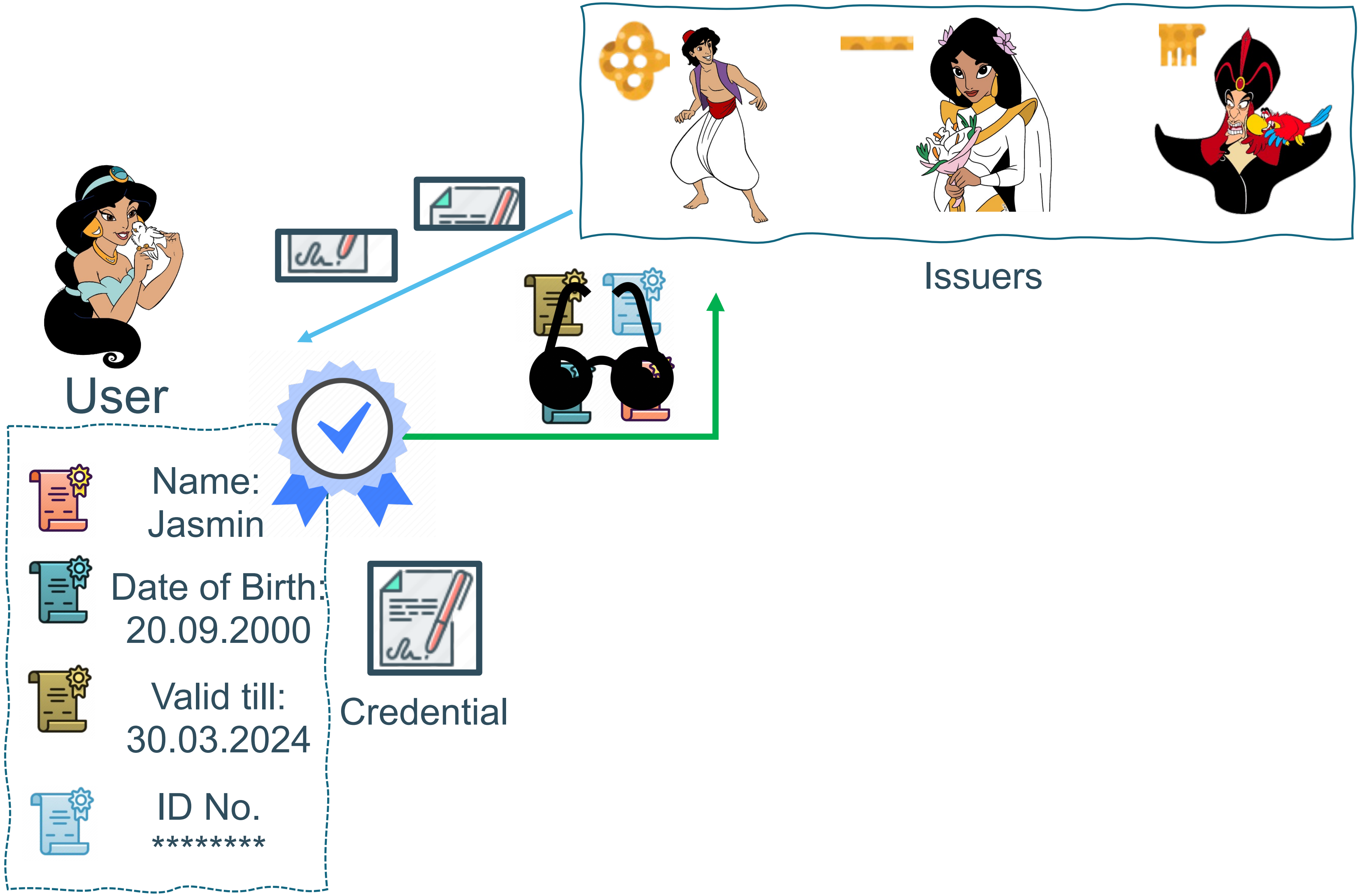
Name: Jasmin

Date of Birth: 20.09.2000

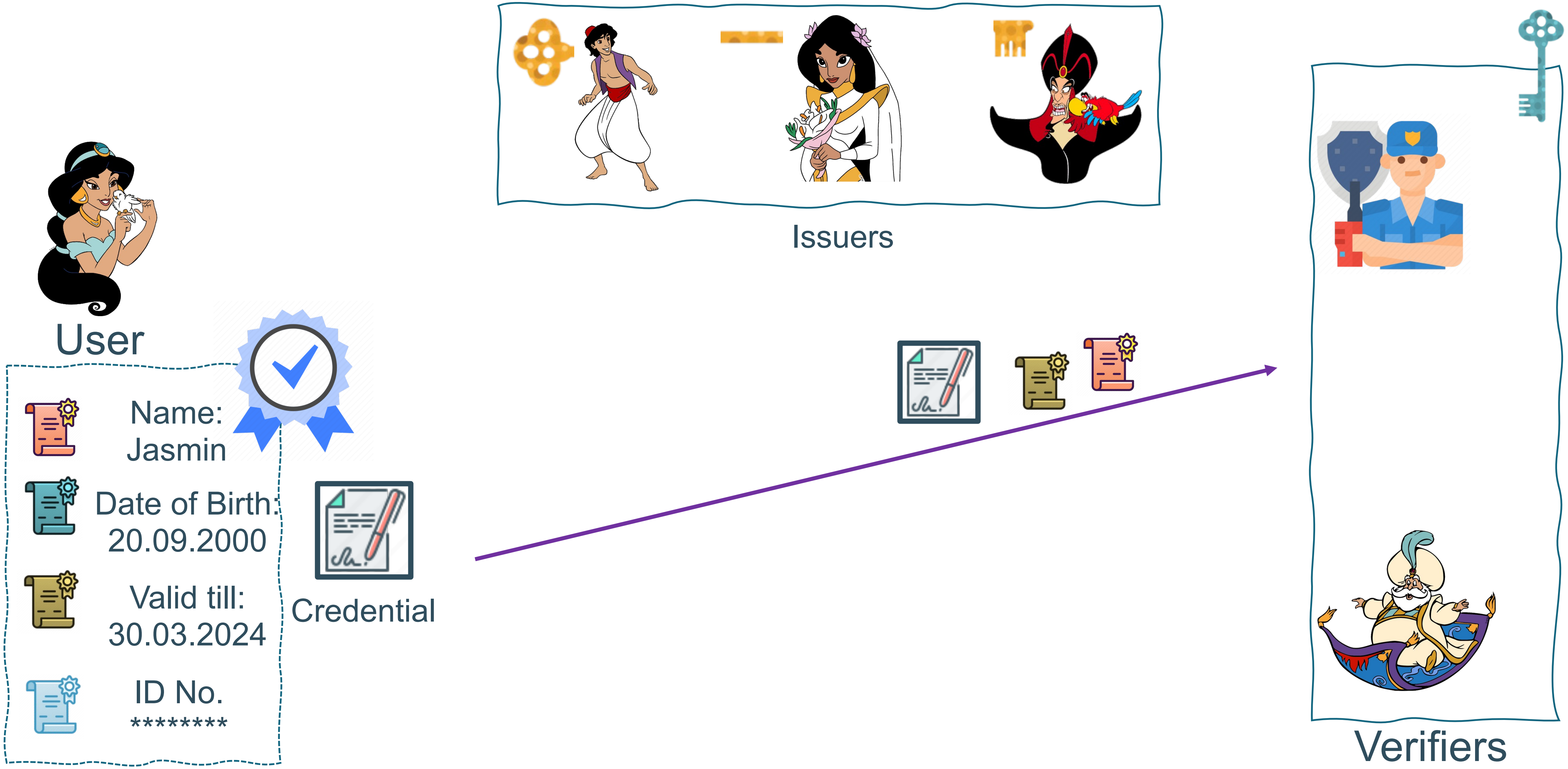
Valid till: 30.03.2024

ID No. ********

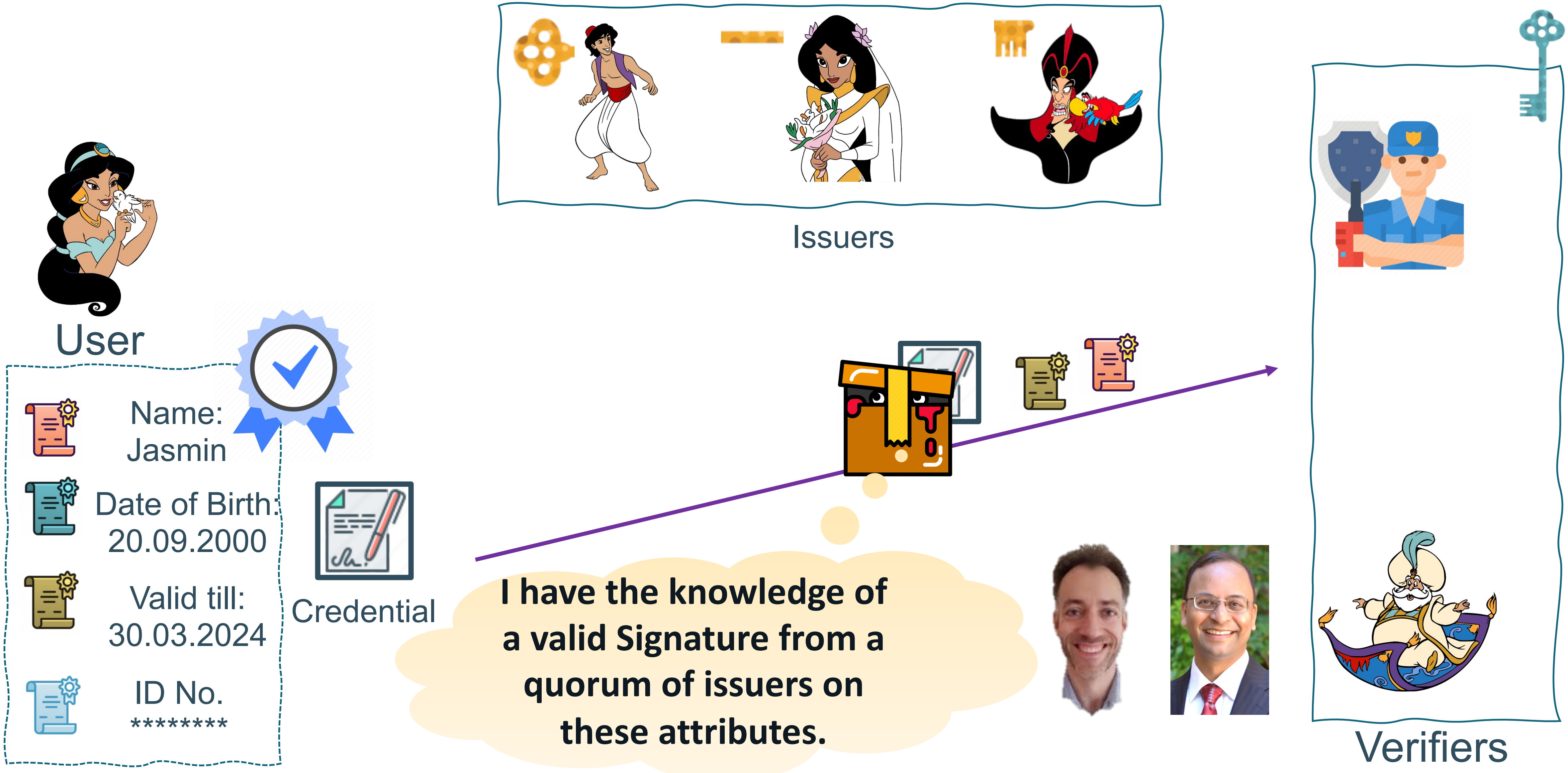
Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



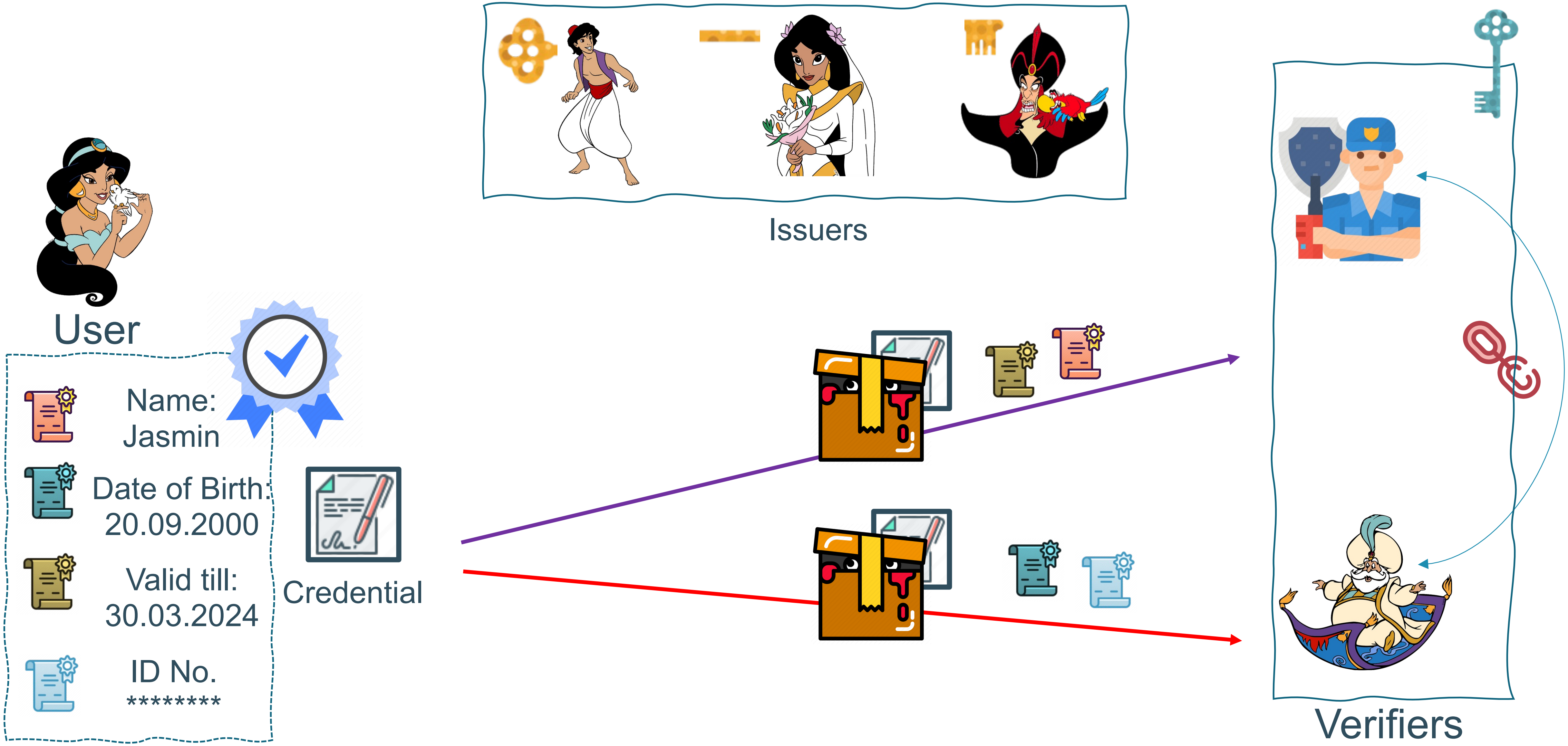
Application: Threshold-Issuance Anonymous Credential systems [SAB+19]



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



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



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.
- We proposed the first (Non-Interactive) TSPS over indexed Diffie-Hellman message spaces.
- We proved its EUF-CiMA security under the hardness of GPS3 assumption in AGM+ROM.
- We discussed TIAC as a primary application of this scheme.

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.
- We proposed the first (Non-Interactive) TSPS over indexed Diffie-Hellman message spaces.
- We proved its EUF-CiMA security under the hardness of GPS3 assumption in AGM+ROM.
- We discussed TIAC as a primary application of this scheme.

Potential open questions and subsequent works:

1) Improve the space of messages from indexed DH message spaces to arbitrary.
2) Remove the indexing method and achieve EUF-CMA security.
3) Prove the security of the scheme based on Non-Interactive assumptions.
4) Prove the threshold EUF-CiMA security with adaptive adversaries and under TS-UF-1

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.*

[BFL20] Bauer et al. "A classification of computational assumptions in the algebraic group model.", CRYPTO 2020.

[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.

[KSAP22] Kim et al. "Practical Dynamic Group Signatures Without Knowledge Extractors". Designs, Codes and Cryptography, Oct 2022.

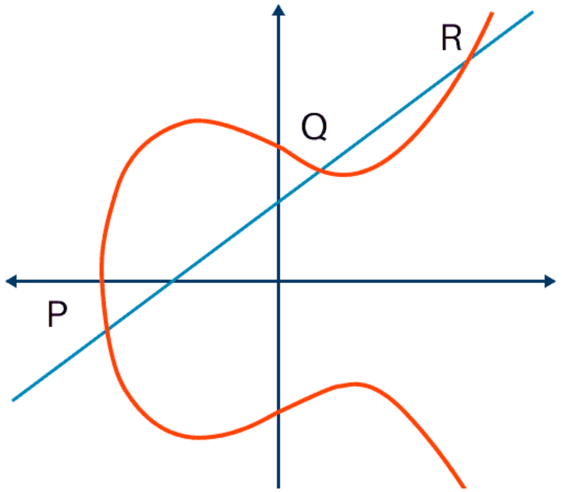
Thank You!

ssedagha@esat.kuleuven.be

The illustrations are credited to Disneyclips.

Backup slides

Bilinear Pairings:



$y^2 = x^3 + ax + b$

- It is symmetric
- Any line intersects the curve no more than 3 points.
- Dot function:

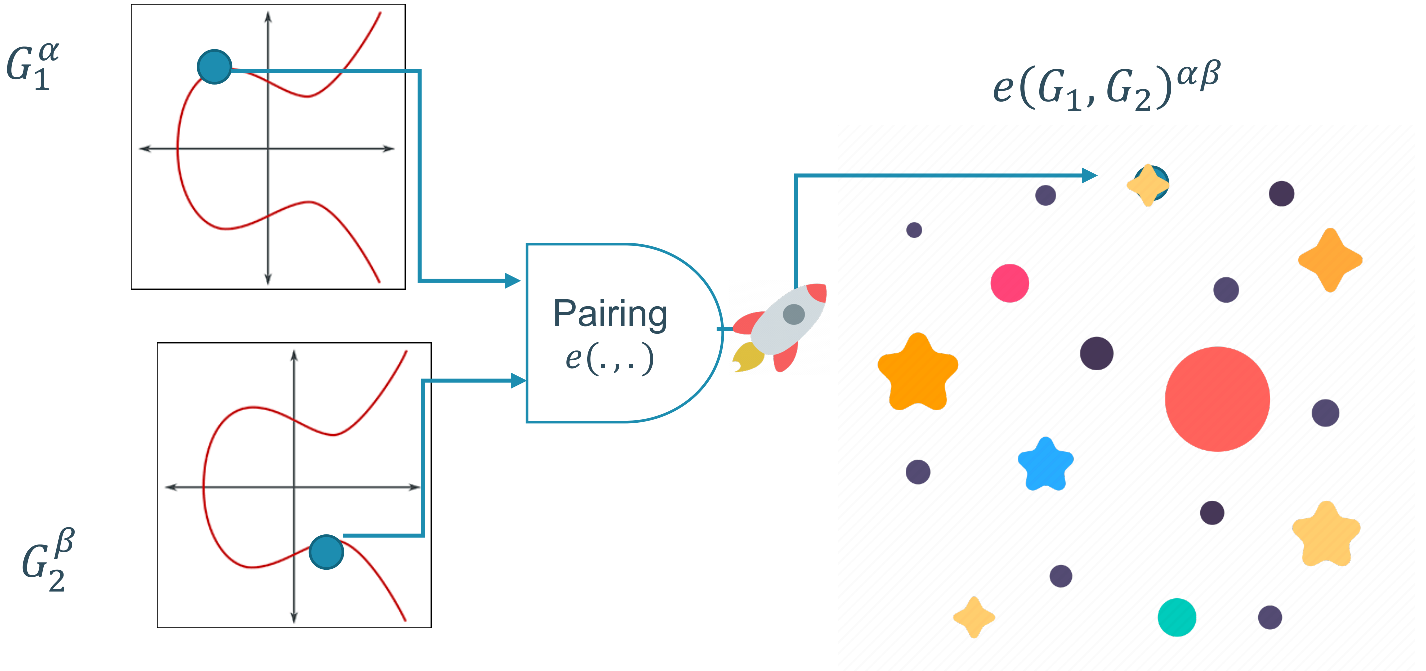
$$P \circ Q \rightarrow R$$

BN-254

$y^2 = x^3 + 4x + 20$

BLS12-381

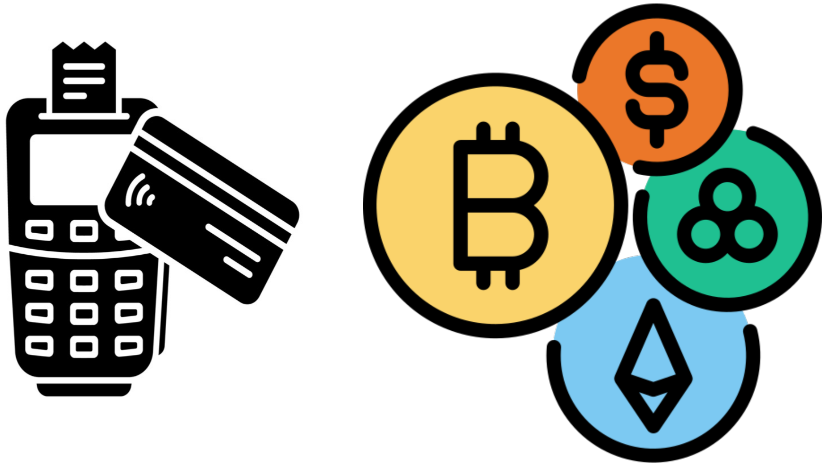
$y^2 = x^3 + 4$



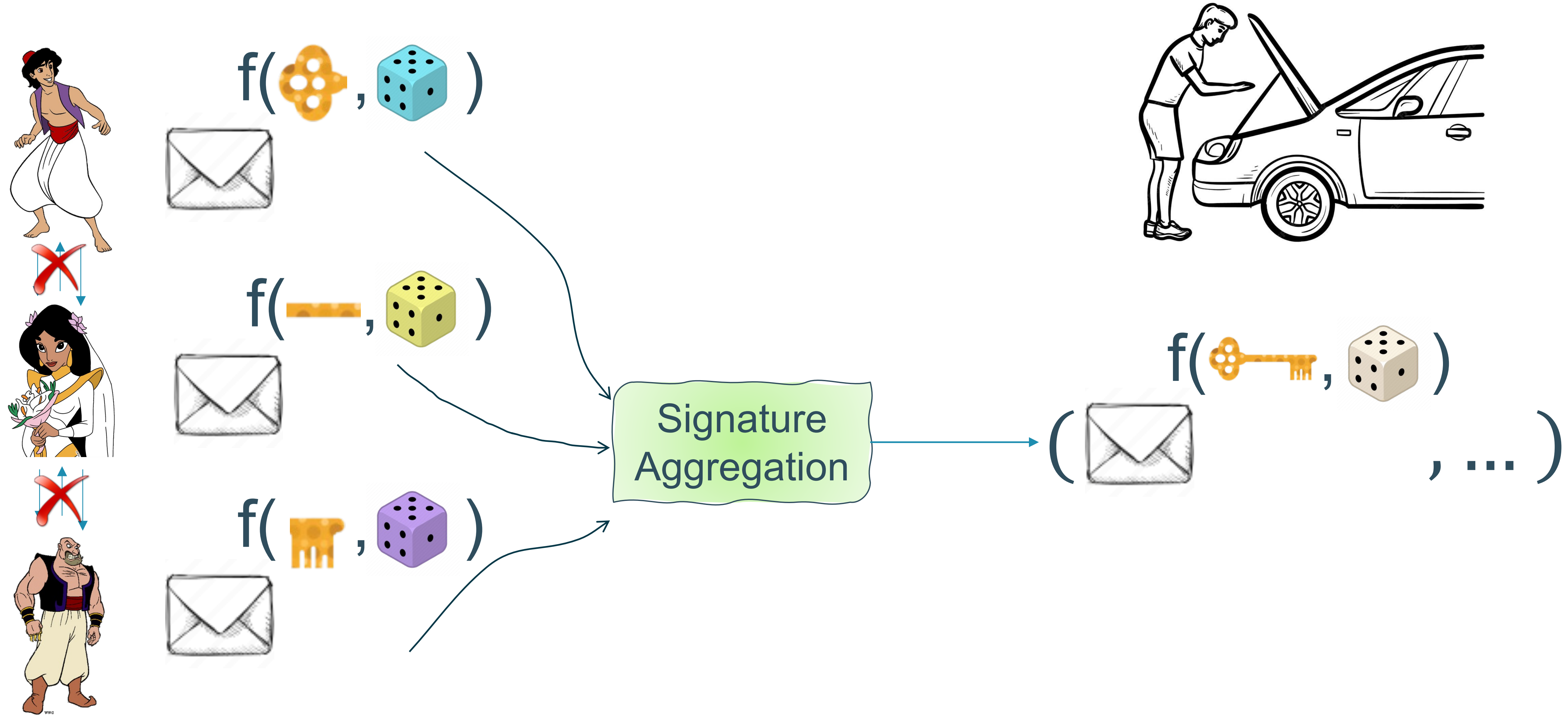
Digital Signatures:

- To verify a message does really come from real person.
- The verifier accpets if the handwriting signature matchs previously seen signatures of the signer.

Digital Signatures are everywhere on the internet.



Technical Challenges:

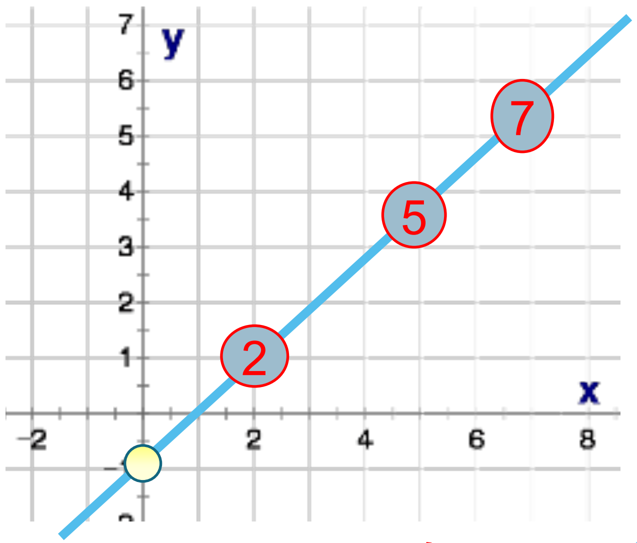


(n,t)-Shamir Secret Sharing [Sha79] over $\mathbb{Z}_p$:

Sharing:

Trusted Dealer

- To share a secret $s \in \mathbb{Z}_p$ amongst n parties:
  - Sample random $f(x) = s + \sum_{k=1}^{t-1} r_k x^k$
  - Give $\lambda_i = f(i)$ to P_i



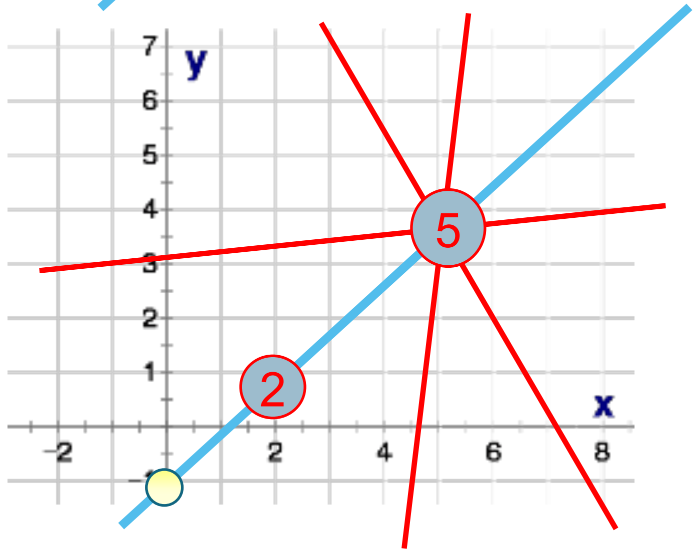
Reconstruction (in the exponent):

- Given $|T| \geq t$ shares:

$$G_\zeta^s = \prod_{i \in T} \left(G_\zeta^{\lambda_i}\right)^{L_i^T(0)}, \qquad \zeta \in \{1,2\}$$

Where,

$$L_i^T(x) = \prod_{i \in T, j \neq i} \frac{j - x}{j - i}$$

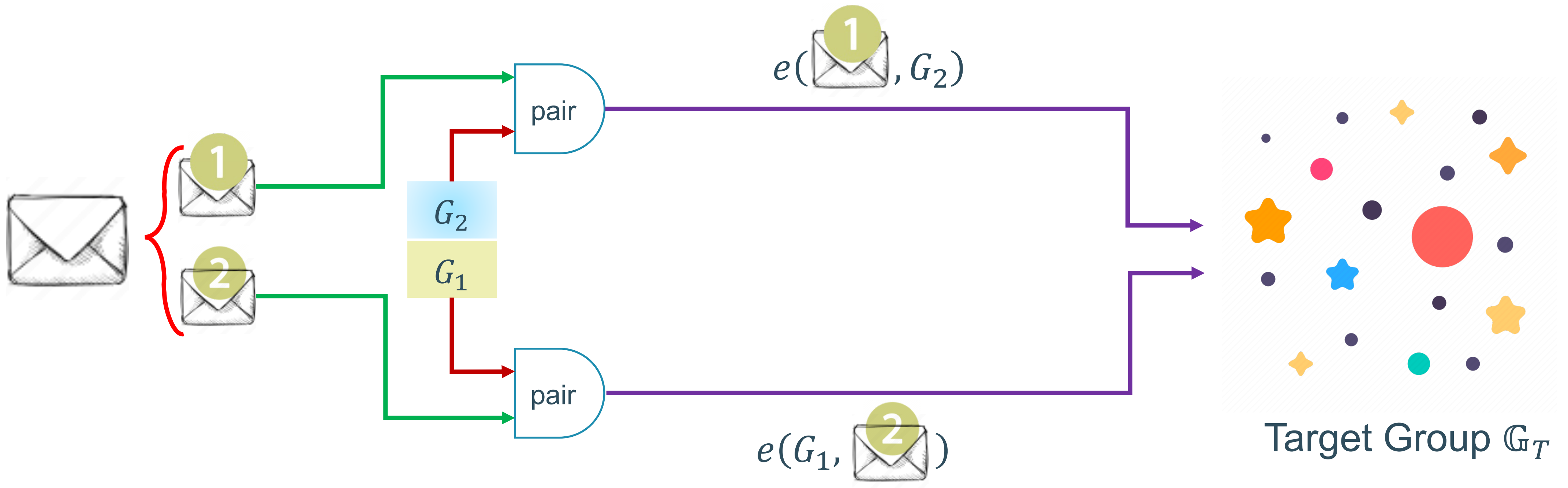


Diffie-Hellman Message Spaces [Fuc09]:

Diffie-Hellman message spaces:

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

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



KU LEUVEN

Pointcheval-Sanders (PS) assumption [PS16]:

Theorem 2: The proposed iSPS is <u>EUF-CiMA secure</u> under the hardness of GPS_3 assumption.

Given $params := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, G_1, G_2)$:

$x, y \xleftarrow{\$} \mathbb{Z}_p^*$

$\xrightarrow{params,\, G_2^x,\, G_2^y}$

$\xleftarrow{(m^*, h^*, s^*)}$

$m \in \mathbb{Z}_p$

out

PS Oracle

$h \xleftarrow{\$} \mathbb{G}_1$
$Q \leftarrow Q \cup \{m\}$
$out = (h, h^{x+my})$

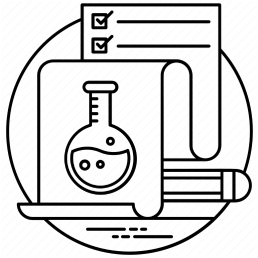
Return 1 if:

1. $h^* \neq 1_{\mathbb{G}_1} \wedge m^* \neq 0$
2. $s^* = {h^*}^{x+m^*y}$
3. $m^* \notin Q$

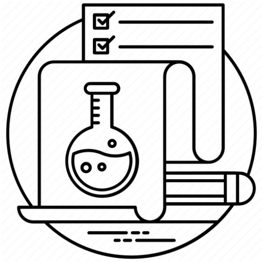
Security Reductions:

(Definition) (2,1)-DL assumption [BFL20]: Let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, p, e)$ be a type-III bilinear group. Given $\left(G_1^z, G_1^{z^2}, G_2^z\right)$, for all PPT adversaries it is infeasible to return z.

Theorem 1:
GPS_3 assumption is hard in the Algebraic adversary model and random oracle model as long as $(2,1)$-DL assumption is hard.



Theorem 2:
The proposed iSPS is EUF-CiMA secure under the hardness of GPS_3 assumption.



Theorem 3:
The proposed TSPS is Threshold EUF-CiMA secure under the security of iSPS.

Generalized Pointcheval-Sanders 3 (GPS3) Assumption:

PS Assumption

$\mathbf{G}^{\mathrm{PS}}(1^\kappa)$

$\mathsf{pp} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, g, \hat{g}) \leftarrow \mathcal{BG}(1^\kappa)$

$x, y \leftarrow\!\$\ \mathbb{Z}_p^*$

$(m^*, h^*, s^*) \leftarrow \mathcal{A}^{\mathcal{O}^{\mathrm{PS}}}(\mathsf{pp}, \hat{g}^x, \hat{g}^y)$

$\textbf{return}\ ((1)\ h^* \neq 1_{\mathbb{G}_1} \wedge\ m^* \neq 0 \wedge$

$(2)\ s^* = h^{*^{x+m^*y}}\ \wedge$

$(3)\ m^* \notin \mathcal{Q})$

$\mathcal{O}^{\mathrm{PS}}(m) //\ m \in \mathbb{Z}_p$

$h \leftarrow\!\$\ \mathbb{G}_1$

$\mathcal{Q} \leftarrow \mathcal{Q} \cup \{m\}$

$\textbf{return}\ (h, h^{x+my})$

GPS3 Assumption

$\mathbf{G}^{\mathrm{GPS}_3}(1^\kappa)$

$\mathsf{pp} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, g, \hat{g}) \leftarrow \mathcal{BG}(1^\kappa)$

$x, y \leftarrow\!\$\ \mathbb{Z}_p^*$

$(M_1^*, M_2^*, h^*, s^*) \leftarrow \mathcal{A}^{\mathcal{O}_0^{\mathrm{GPS}_3}, \mathcal{O}_1^{\mathrm{GPS}_3}}(\mathsf{pp}, \hat{g}^x, \hat{g}^y)$

$\textbf{return}\ ((1)\ M_1^* \neq 1_{\mathbb{G}_1} \wedge\ h^* \neq 1_{\mathbb{G}_1}\ \wedge$

$(2)\ s^* = h^{*^x} M_1^{*^y}\ \wedge$

$(3)\ \mathsf{dlog}_{h^*}(M_1^*) = \mathsf{dlog}_{\hat{g}}(M_2^*) \wedge$

$(4)\ (\star, M_2^*) \notin \mathcal{Q}_1)$

$\mathcal{O}_0^{\mathrm{GPS}_3}()$

$r \leftarrow\!\$\ \mathbb{Z}_p^*$

$\mathcal{Q}_0 \leftarrow \mathcal{Q}_0 \cup \{g^r\}$

$\textbf{return}\ g^r$

$\mathcal{O}_1^{\mathrm{GPS}_3}(h, M_1, M_2) // M_1 \in \mathbb{G}_1, M_2 \in \mathbb{G}_2$

$\textbf{if}\ (h \notin \mathcal{Q}_0 \vee \mathsf{dlog}_h(M_1) \neq \mathsf{dlog}_{\hat{g}}(M_2)) :$

$\quad \textbf{return}\ \perp$

$\textbf{if}\ (h, \star) \in \mathcal{Q}_1 :$

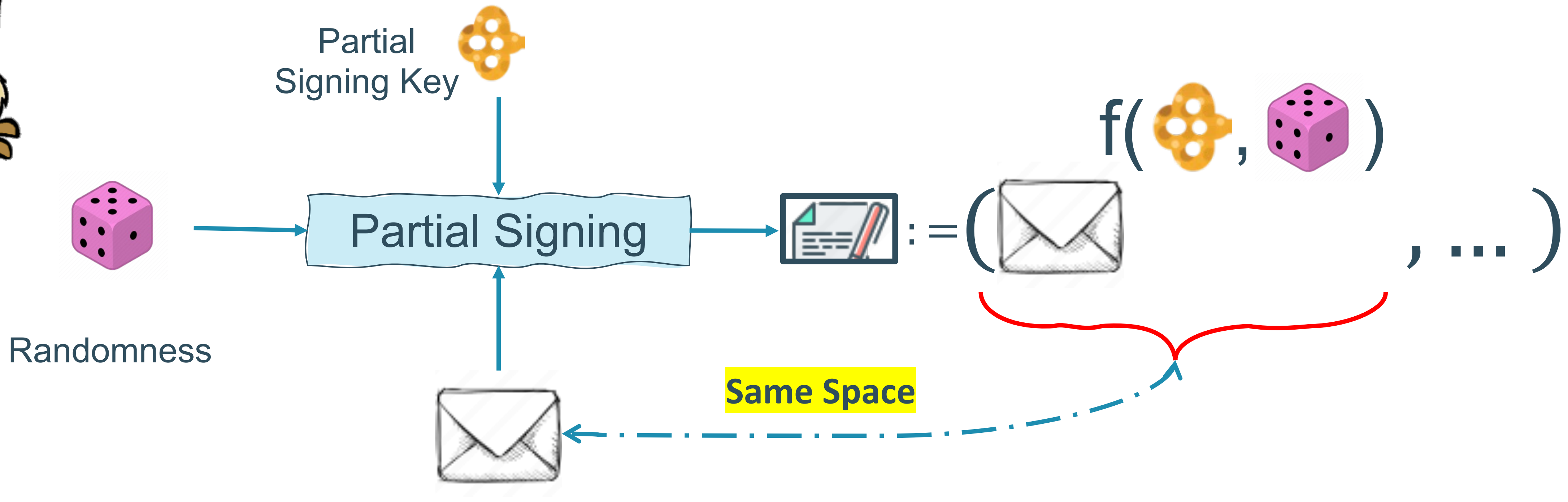
$\quad \textbf{return}\ \perp$

$\mathcal{Q}_1 \leftarrow \mathcal{Q}_1 \cup \{(h, M_2)\}$

$\textbf{return}\ (h^x M_1^y)$

Our Main Objective and Technical Challenges:

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

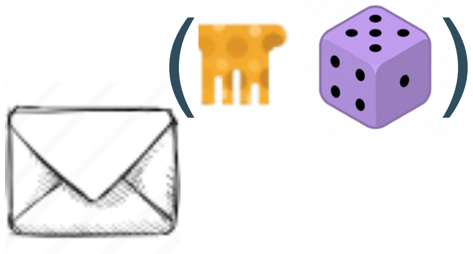


Technical Challenges: Forbidden Operations in Partial Signatures

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: