KU LEUVEN

2022/839

Threshold Structure-Preserving Signatures

Elizabeth Crites, Markulf Kohlweiss, Bart Preneel,
Mahdi Sedaghat and Daniel Slamanig

KU LEUVEN

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

der Bundeswehr Universität München

COSIC Seminar, 16 November 2023

Outline:

Threshold Structure-Preserving Signatures

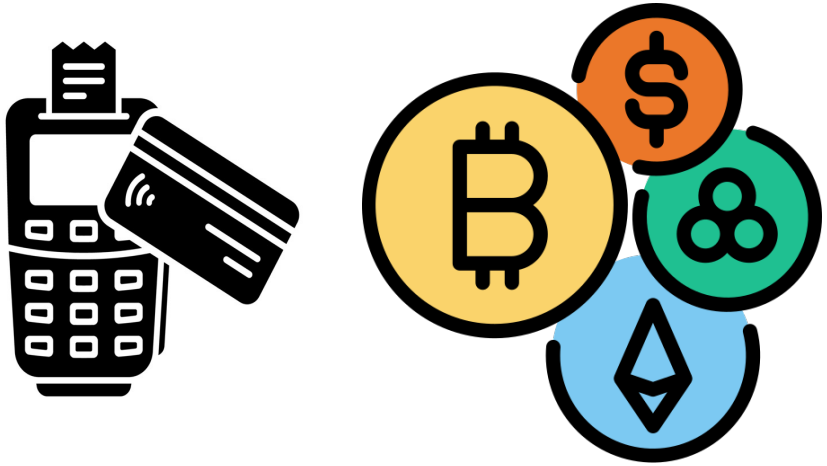
Threshold Signatures

Structure-Preserving Signatures

Digital Signatures:

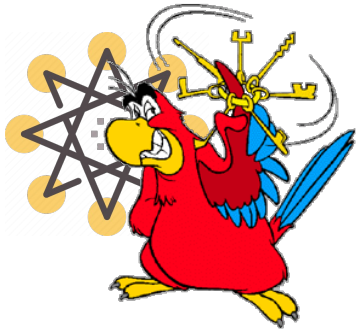
- To verify a message does really come from real person.
- The verifier accpets if the handwriting signature matchs previously seen signatures of the signer.

Digital Signatures are everywhere on the internet.



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

Single Signing key



Trusted Dealer or
Distributed Key Generation (DKG) protocols

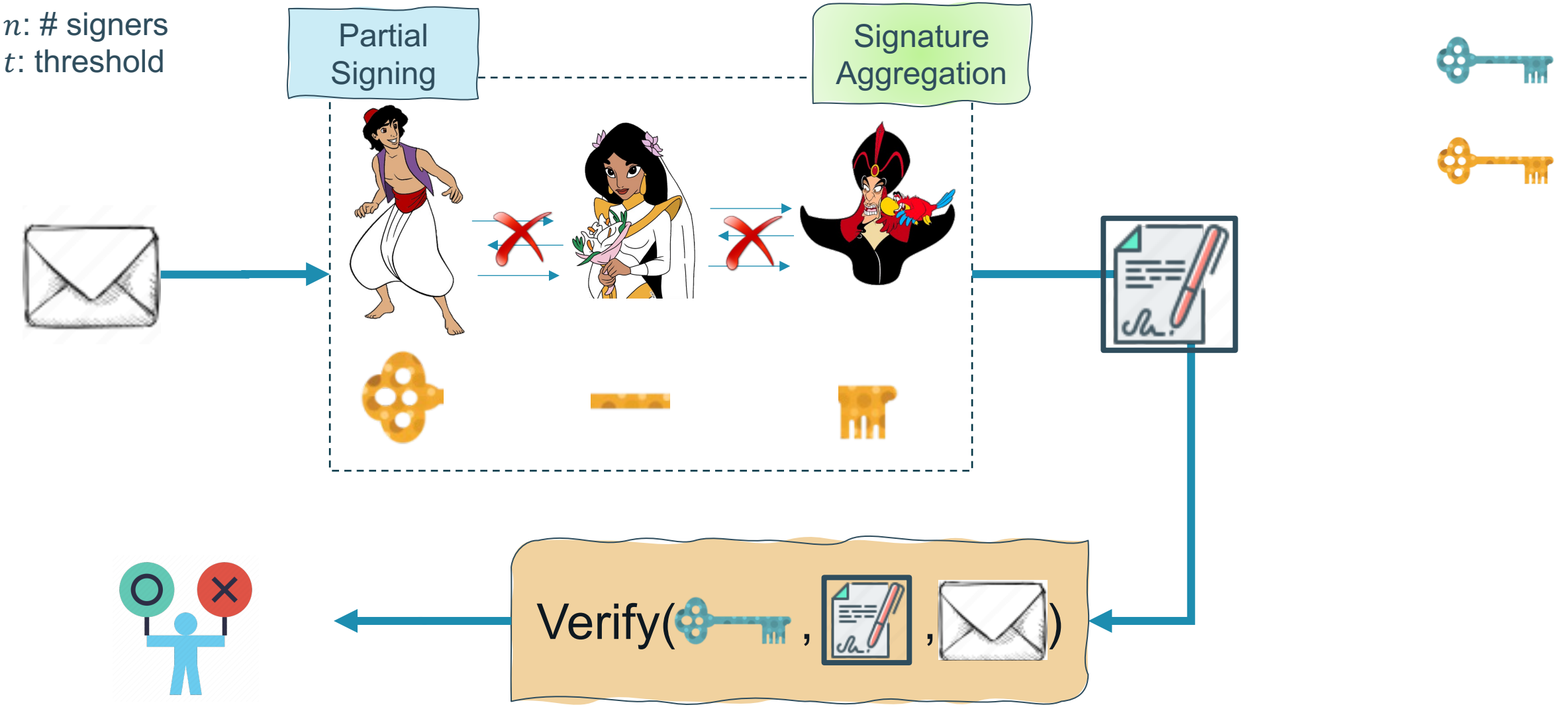
Distributed Keys

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

National Institute of Standards and Technology

Non-Interactive Threshold Signatures:

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



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.

* (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 property: $e(G_1^x, G_2^y) = e(G_1, G_2)^{xy}, \forall x, y \in \mathbb{Z}_p$
  - Non-degenerate property: $e(G_1, G_2) \neq 1_{\mathbb{G}_T}$
  - $\mathbb{G}_1 =< G_1 >, \mathbb{G}_2 =< G_2 >, \mathbb{G}_T =< e(G_1, G_2) >$

Structure-Preserving Signatures [AFG+10]:

1

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

2

Verify( ,  , ):

Done by:

- membership tests

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

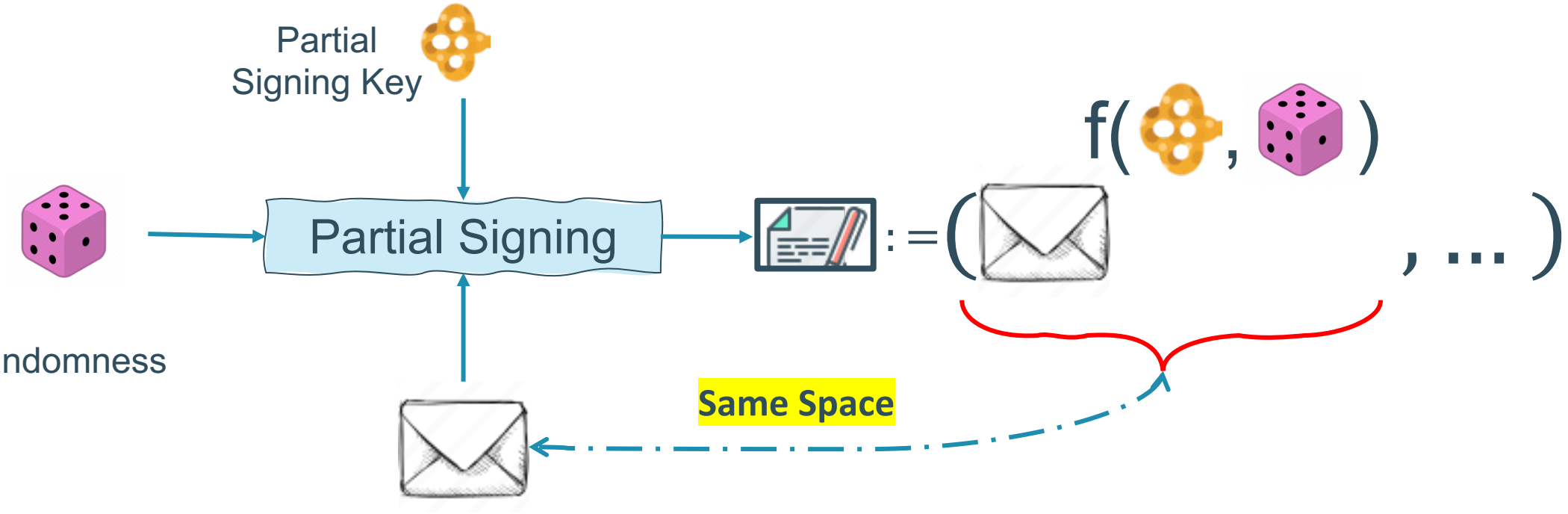
- pairing product equations

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

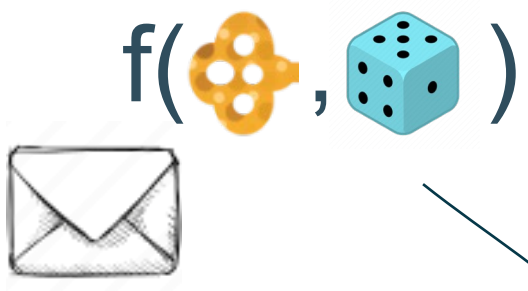
No Non-Linear operation like **Hash Functions**

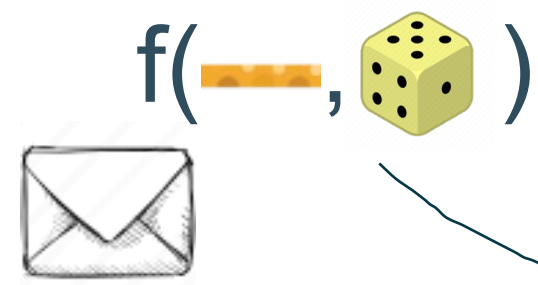
Our Main Objective and Technical Challenges:

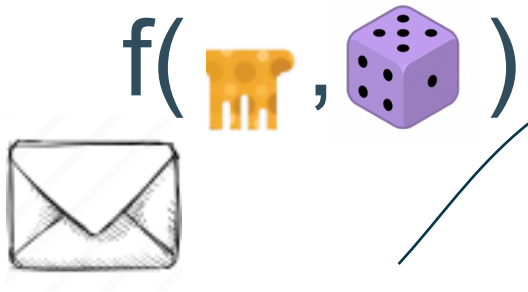
There is NO Threshold Structure-Preserving Signature Scheme (TSPS)



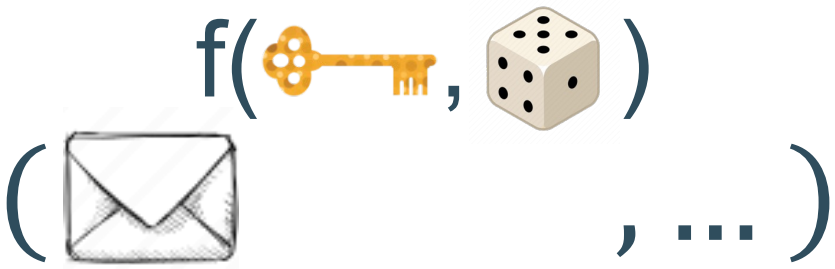
Technical Challenges:







Signature Aggregation

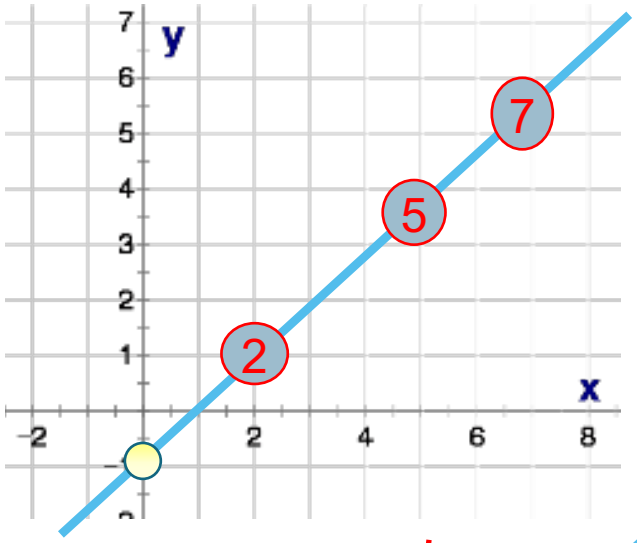


(n, t)-Shamir Secret Sharing [Sha79] over $\mathbb{Z}_p$:

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



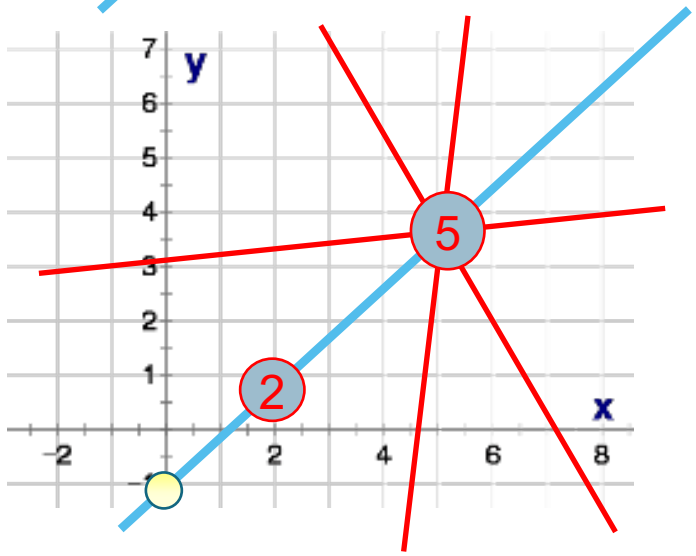
Reconstruction (in the exponent):

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

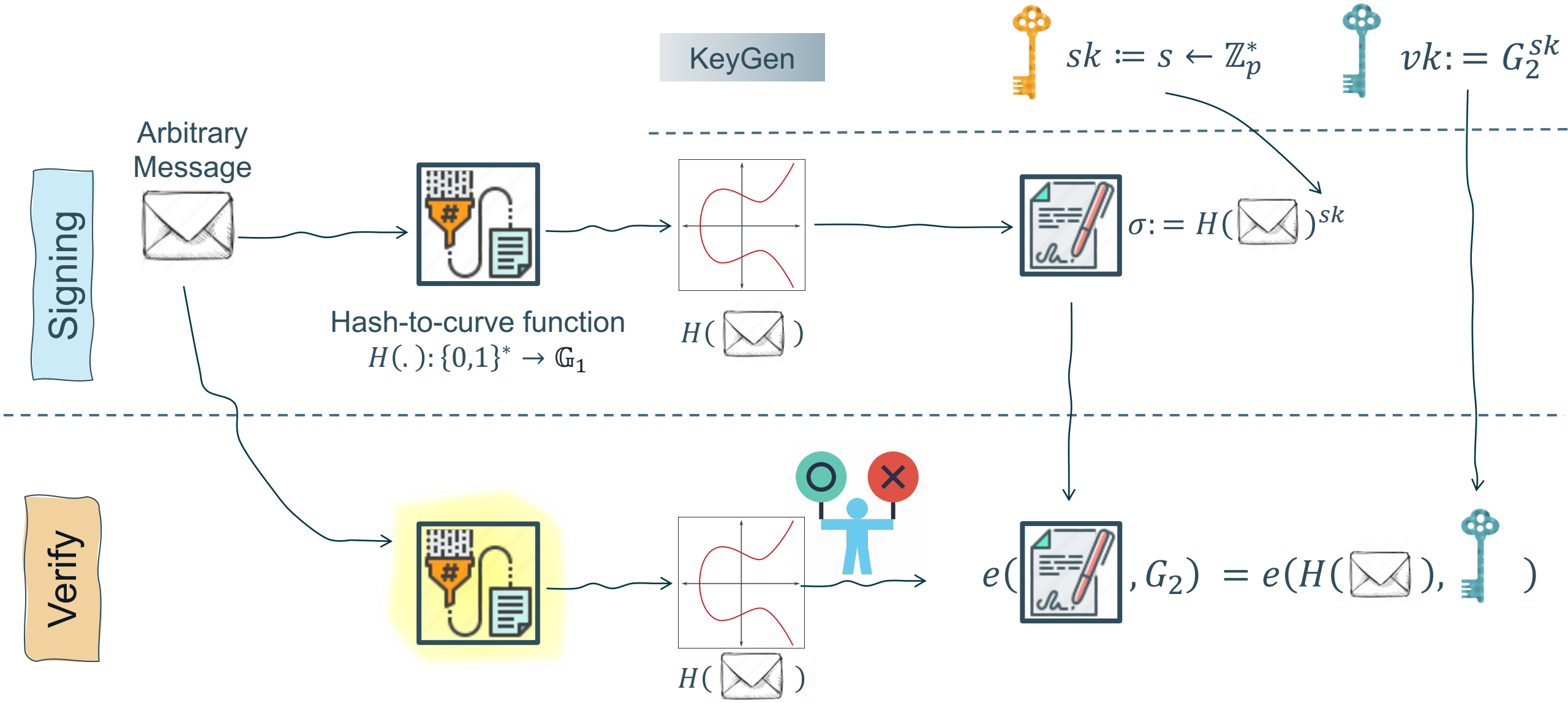
$$G_\zeta^s = \prod_{i \in T} \left(G_\zeta^{\lambda_i}\right)^{L_i^T(0)}, \qquad \zeta \in \{1,2\}$$

Where,

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



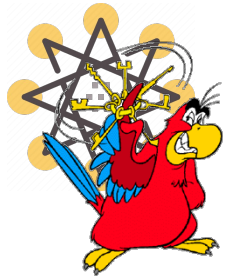
BLS signature [BLS04]:



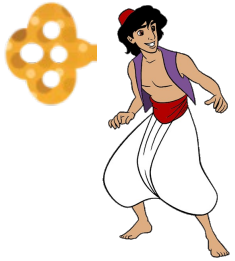
Threshold BLS signature [Bol03]: A simple example of NI-TS

KeyGen

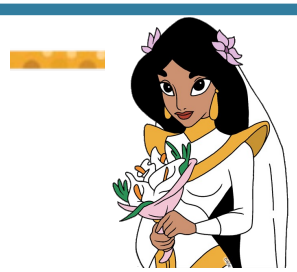
$sk := s \leftarrow \mathbb{Z}_p$



Trusted Dealer or DKG



$sk_1 := s_1$

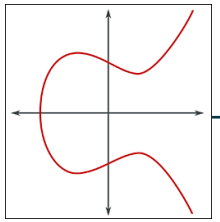


$sk_2 := s_2$

$sk_3 := s_3$

$vk := G_2^s$

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



$H($  $)$

Partial Signing

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

Signature Aggregation

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

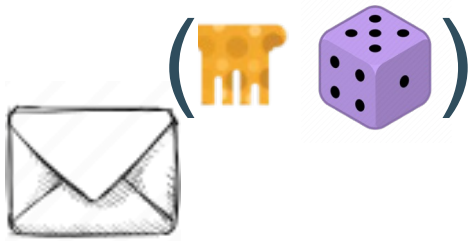
BLS is not a SPS!

Technical Challenges: Forbidden Operations in Partial Signatures

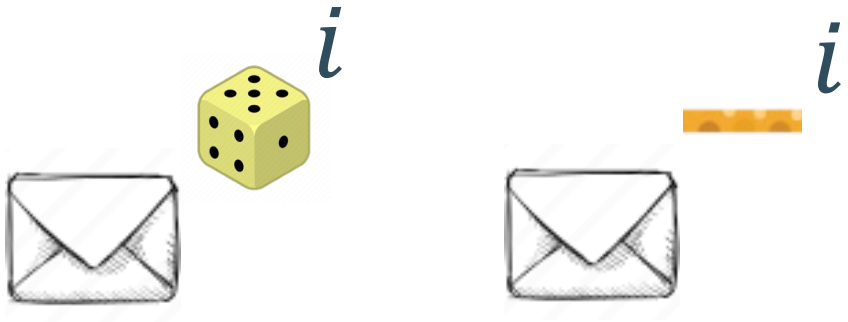
A SPS is said threshold friendly, if it avoids all these non-linear operations.

1. Randomness or secret share inverse:

2. Randomness and secret share multiplication:



3. Powers of secret share or randomness:

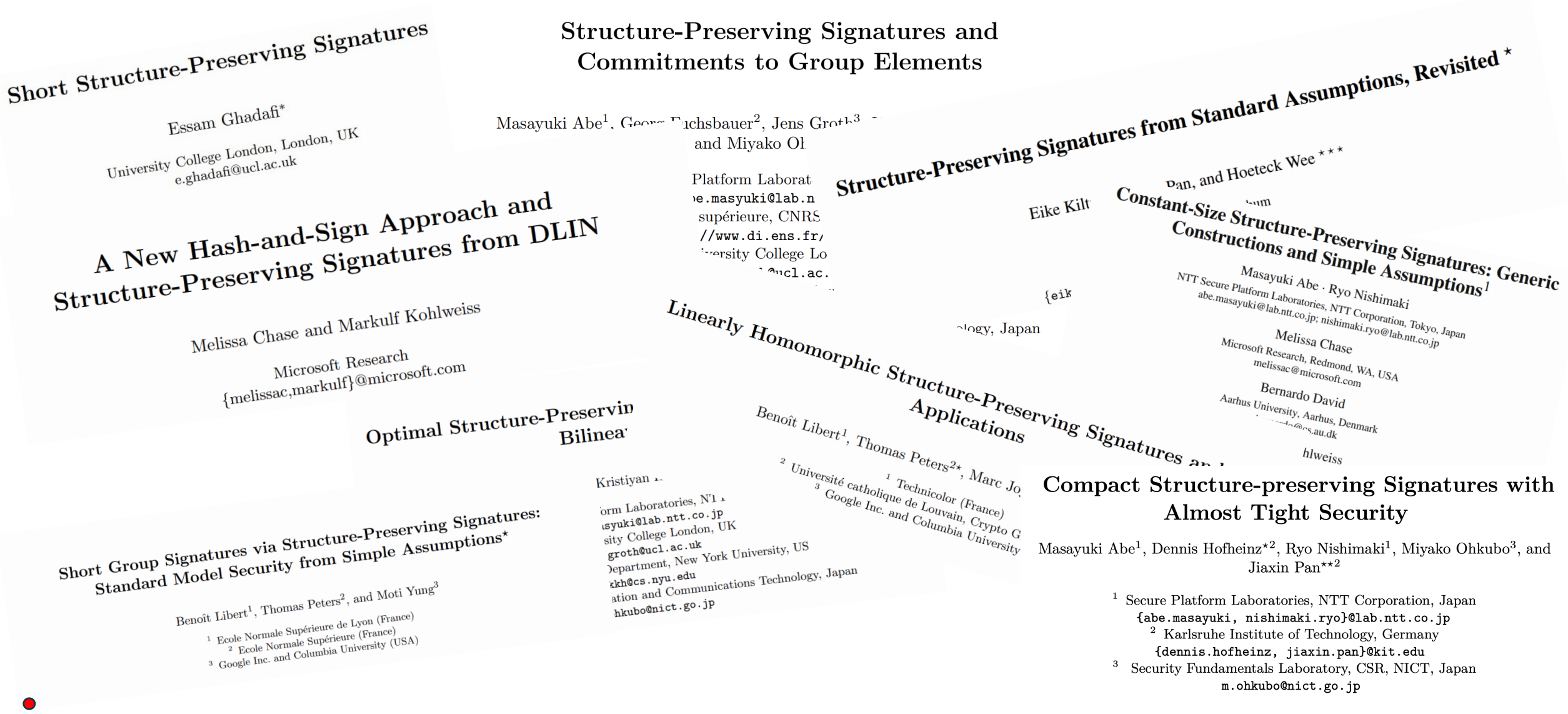


Treasure map: To look for a Non-Interactive TSPS

Threshold Signatures

Structure-Preserving Signatures

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[1]

Platform Laboratories, NTT Corporation, Japan
abe.masayuki@lab.ntt.co.jp

Structure-Preserving Signatures from Standard Assumptions, Revisited *

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

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

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-Preserving Bilinear

Linearly Homomorphic Structure-Preserving Signatures and Applications

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

[1] Technicolor (France)
[2] Université catholique de Louvain, Crypto Group
[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)

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.

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!***

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**.

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.uc
http://www-cse.ucsd.

Twinkle: Threshold Signatures from DDH with Full Adaptive Securit

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

Julian Loss [1]
Chenzhi Zhu [2]

Renas Bacho [1,3]
Benedikt Wagner [1,3]

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 Washi
{tessaro,zhucz20}@cs.washington.edu
[3] Saarland University, Saarbrücken, Germany

Better than Advertised Security for Non-interactive Threshold Signatures

[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
[5]

Practical Threshold Signature

Victor Shoup

IBM Zürich Research Lab

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

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

rg[1](✉)

Canada

USA

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
duate School of the Chinese Ac
wangho

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

Benoît Libert, Marc Joye, Moti Yung

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

Short Structure-Preserving Signatures

Essam Ghadafi*

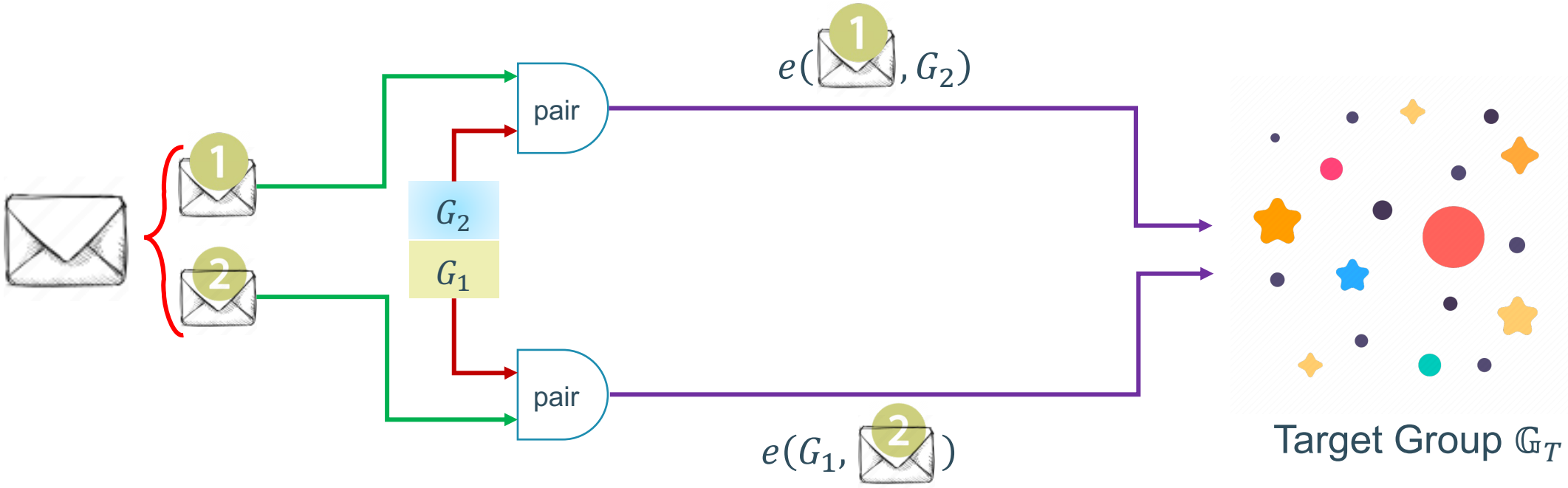
University College London, London, UK
e.ghadafi@ucl.ac.uk

Interactive TSPS

Diffie-Hellman Message Spaces [Fuc09]:

Diffie-Hellman message spaces:

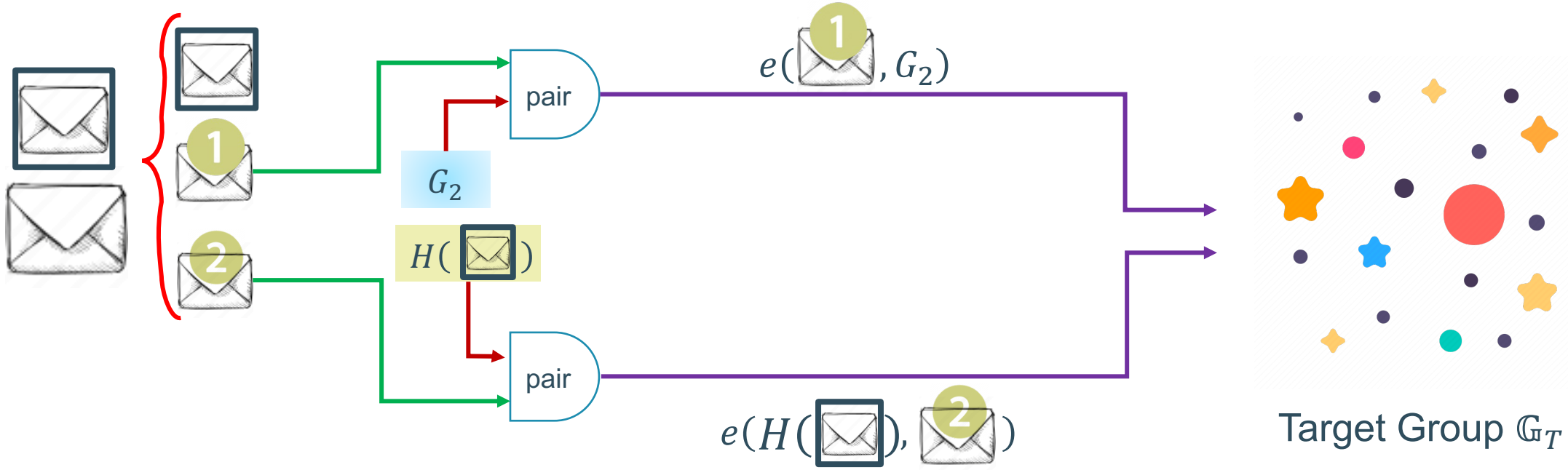
$(\mathrm{M}_1, \mathrm{M}_2) \mid \exists\, m \in \mathbb{Z}_p : e(G_1, M_2) = e(M_1, G_2)$



Indexed Diffie-Hellman Message Spaces:

Indexed Diffie-Hellman (iDH) message spaces:

$$(id, \mathrm{M}_1, \mathrm{M}_2) \mid \exists\, m \in \mathbb{Z}_p : e(H(id), M_2) = e(M_1, G_2)$$



KU LEUVEN

Our Results:

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.

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

KeyGen

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

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

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

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

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

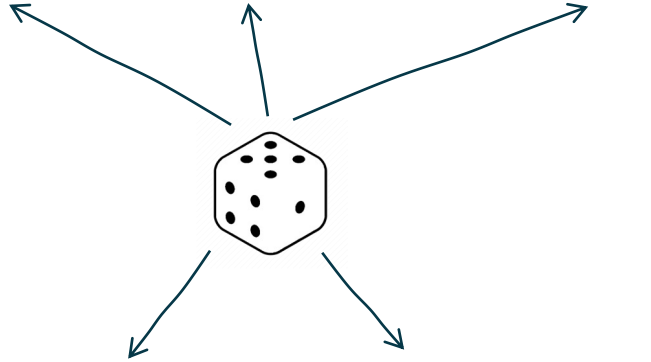
$e(h, G_2^x) e\left(M_1, G_2^y\right) = e(s, G_2)$

Is this scheme secure?

Trivial Forgery:

- The resulting iSPS is partially re-randomizable.*

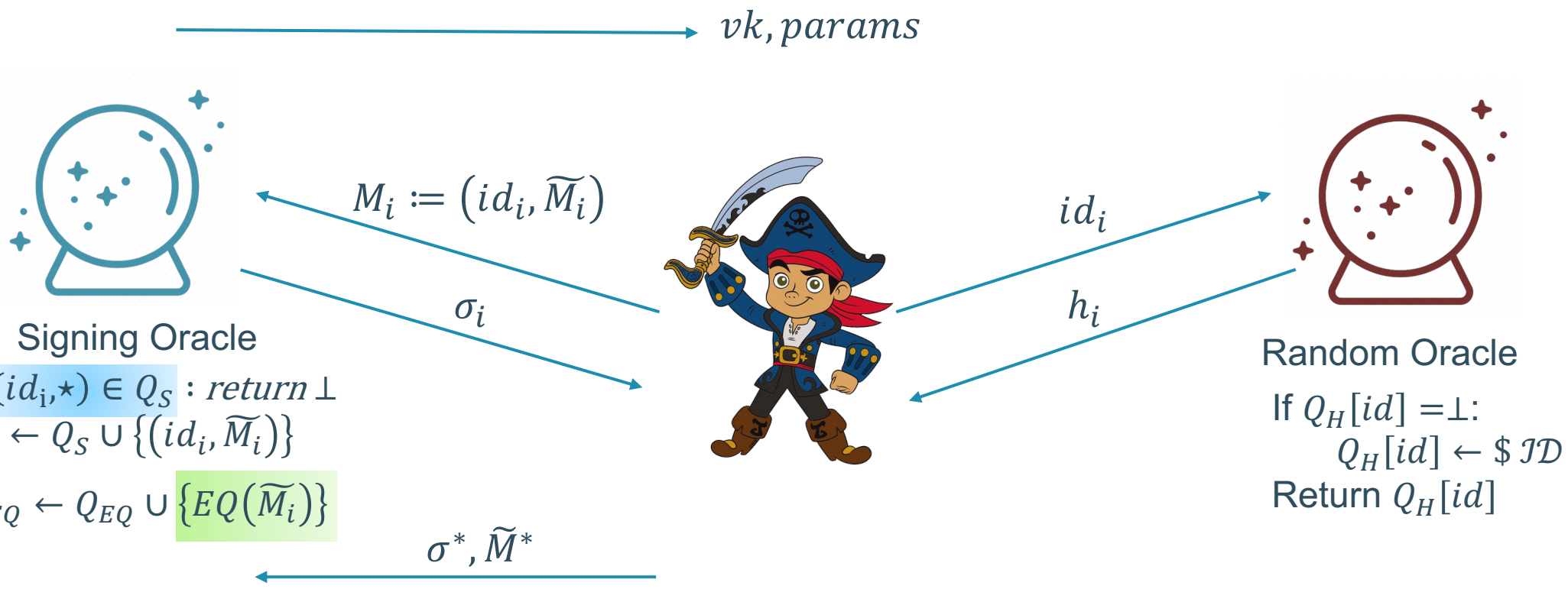
$$e(h, vk_1)e(M_1, vk_2) = e(s, G_2)$$



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

One can re-randomize the basis h and the iDH message $\tilde{M}$ and still pass the verification phase.

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



Return 1 if:

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

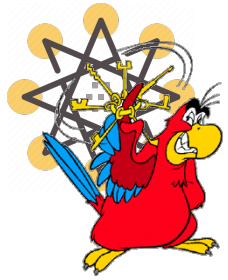
$$EQ(M_1, M_2) = \{(M_1^r, M_2) \mid r \in \mathbb{Z}_p\}$$

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

Our proposed TSPS:

KeyGen

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



Dealer (or DKG)

$sk_1 := x_1, y_1$

$sk_2 := x_2, y_2$

$sk_3 := x_3, y_3$

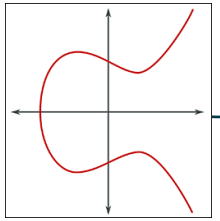
$vk := (G_2^x, G_2^y)$

iDH Message

$M = (id, M_1, M_2)$

Hash-to-Curve

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



Random Basis

h

Partial Signing

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

Signature Aggregation

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

Security Reductions:

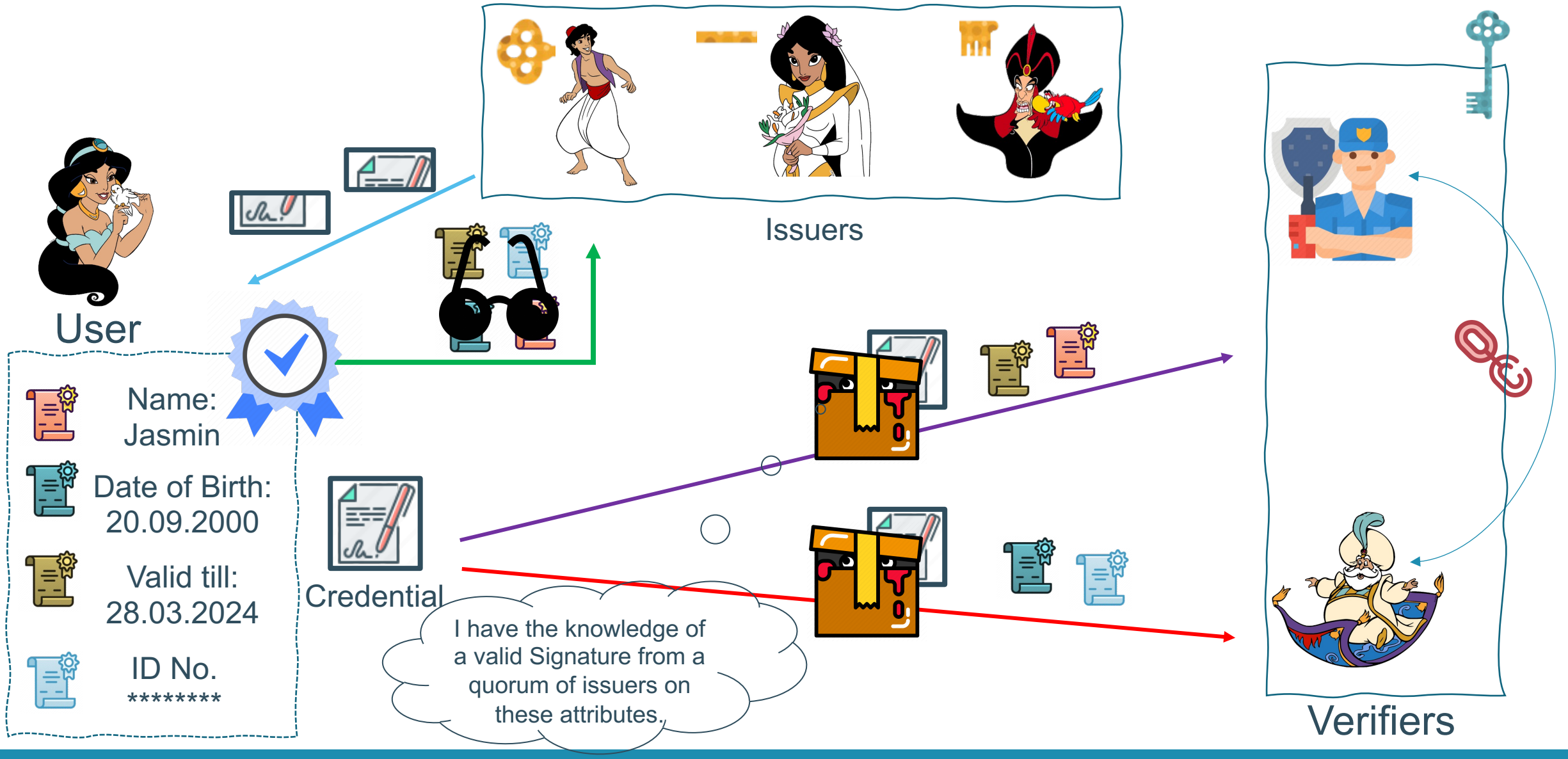
(Definition) (2,1)-DL assumption [BFL20]: Let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, p, e)$ be a type-III bilinear group. Given $\left(G_1^z, G_1^{z^2}, G_2^z\right)$, for all PPT adversaries it is infeasible to return z.

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.

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.

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) Bring the scheme to TIAC applications and measure their performance.
4) Prove the security of the scheme based on weaker assumptions (Non-Interactive).
5) Prove the threshold EUF-CiMA security with adaptive adversaries.

References

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

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. "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, Shafi, Silvio Micali, and Chales Rackoff. "The knowledge complexity of interactive proof-systems."

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. "Structure-preserving signatures and commitments to group elements.", CRYPTO 2010.

[AGHO11] Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. "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, Georg, Christian Hanser, and Daniel Slamanig. "Structure-preserving signatures on equivalence classes and constant-size anonymous credentials.", *AC'14, JoC'19.*

[BFL20] Balthazar Bauer, Georg Fuchsbauer, and Julian Loss. "A classification of computational assumptions in the algebraic group model.", CRYPTO 2020.

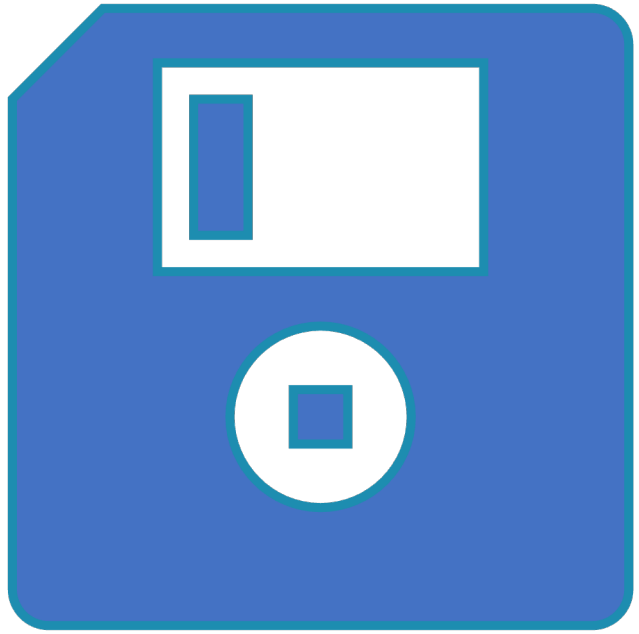
[SAB+19] Alberto Sonnino, Mustafa Al-Bassam, Shehar Bano, Sarah Meiklejohn, and George Danezis. "Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers.", NDSS 2019.

KU LEUVEN

Thank You!

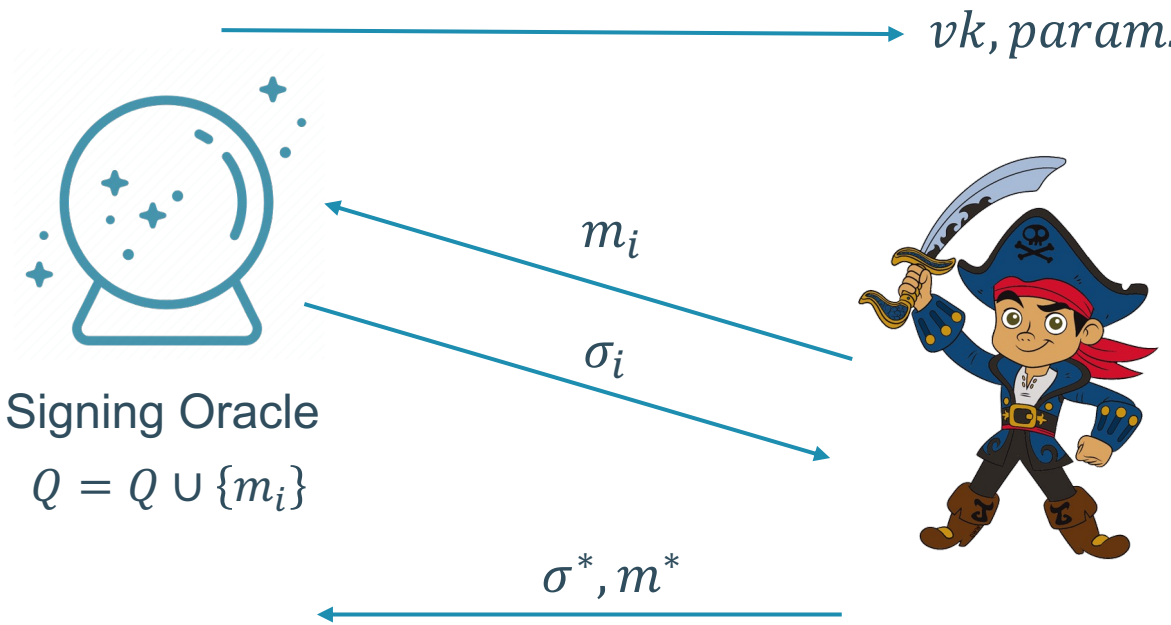
ssedagha@esat.kuleuven.be

The illustrations are credited to Disneyclips.



Backup slides

q-EUF-CMA:



Return 1 if:

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

q-EUF-CMA

Generalized Pointcheval-Sanders 3 (GPS3) Assumption:

PS Assumption

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

1 : $\mathsf{pp} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, g, \hat{g}) \leftarrow \mathcal{BG}(1^\kappa)$
2 : $x, y \leftarrow\$ \mathbb{Z}_p^*$
3 : $(m^*, h^*, s^*) \leftarrow \mathcal{A}^{\mathcal{O}^{\mathrm{PS}}}(\mathsf{pp}, \hat{g}^x, \hat{g}^y)$
4 : **return** $((1)\ h^* \neq 1_{\mathbb{G}_1} \wedge\ m^* \neq 0 \wedge$
5 : $(2)\ s^* = {h^*}^{x+m^*y} \wedge$
6 : $(3)\ m^* \notin \mathcal{Q})$

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

1 : $h \leftarrow\$ \mathbb{G}_1$
2 : $\mathcal{Q} \leftarrow \mathcal{Q} \cup \{m\}$
3 : **return** (h, h^{x+my})

GPS3 Assumption

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

1 : $\mathsf{pp} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, g, \hat{g}) \leftarrow \mathcal{BG}(1^\kappa)$
2 : $x, y \leftarrow\$ \mathbb{Z}_p^*$
3 : $(M_1^*, M_2^*, h^*, s^*) \leftarrow \mathcal{A}^{\mathcal{O}_0^{\mathrm{GPS}_3}, \mathcal{O}_1^{\mathrm{GPS}_3}}(\mathsf{pp}, \hat{g}^x, \hat{g}^y)$
4 : **return** $((1)\ M_1^* \neq 1_{\mathbb{G}_1} \wedge\ h^* \neq 1_{\mathbb{G}_1} \wedge$
5 : $(2)\ s^* = {h^*}^x {M_1^*}^y \wedge$
6 : $(3)\ \mathsf{dlog}_{h^*}(M_1^*) = \mathsf{dlog}_{\hat{g}}(M_2^*) \wedge$
7 : $(4)\ (\star, M_2^*) \notin \mathcal{Q}_1)$

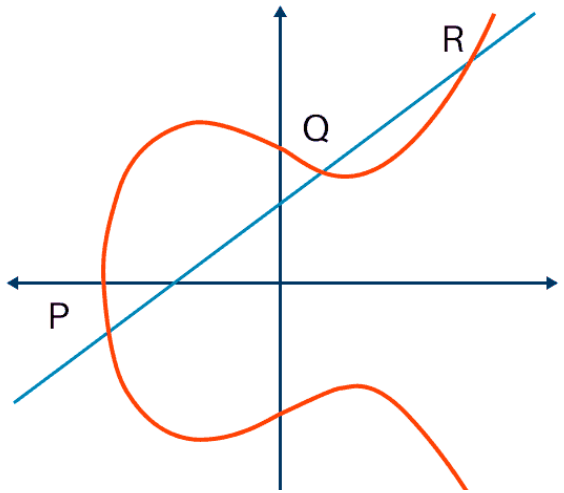
$\mathcal{O}_0^{\mathrm{GPS}_3}()$

1 : $r \leftarrow\$ \mathbb{Z}_p^*$
2 : $\mathcal{Q}_0 \leftarrow \mathcal{Q}_0 \cup \{g^r\}$
3 : **return** g^r

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

1 : **if** $(h \notin \mathcal{Q}_0 \vee \mathsf{dlog}_h(M_1) \neq \mathsf{dlog}_{\hat{g}}(M_2))$:
2 : **return** $\perp$
3 : **if** $(h, \star) \in \mathcal{Q}_1$:
4 : **return** $\perp$
5 : $\mathcal{Q}_1 \leftarrow \mathcal{Q}_1 \cup \{(h, M_2)\}$
6 : **return** $(h^x M_1^y)$

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

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