Improved Constructions of Anonymous Credentials From Structure-Preserving Signatures on Equivalence Classes

Aisling Connolly[1†] Pascal Lafourcade [‡]
Octavio Perez Kempner [§,¶]

[†]DFINITY

[‡]University Clermont Auvergne, LIMOS, France

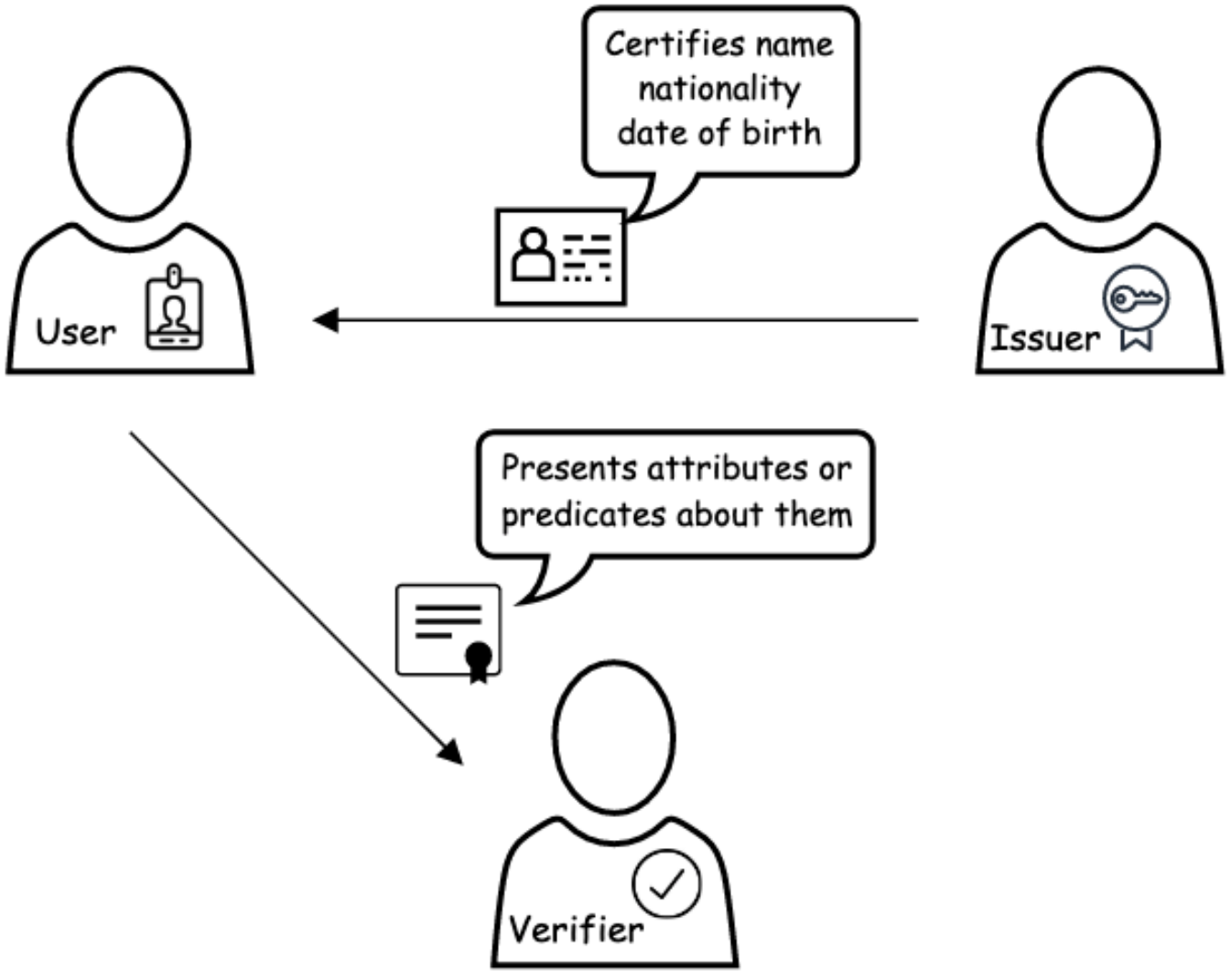
[§]DIENS, École normale supérieure, CNRS, PSL University, Paris, France

[¶]be-ys Research, France

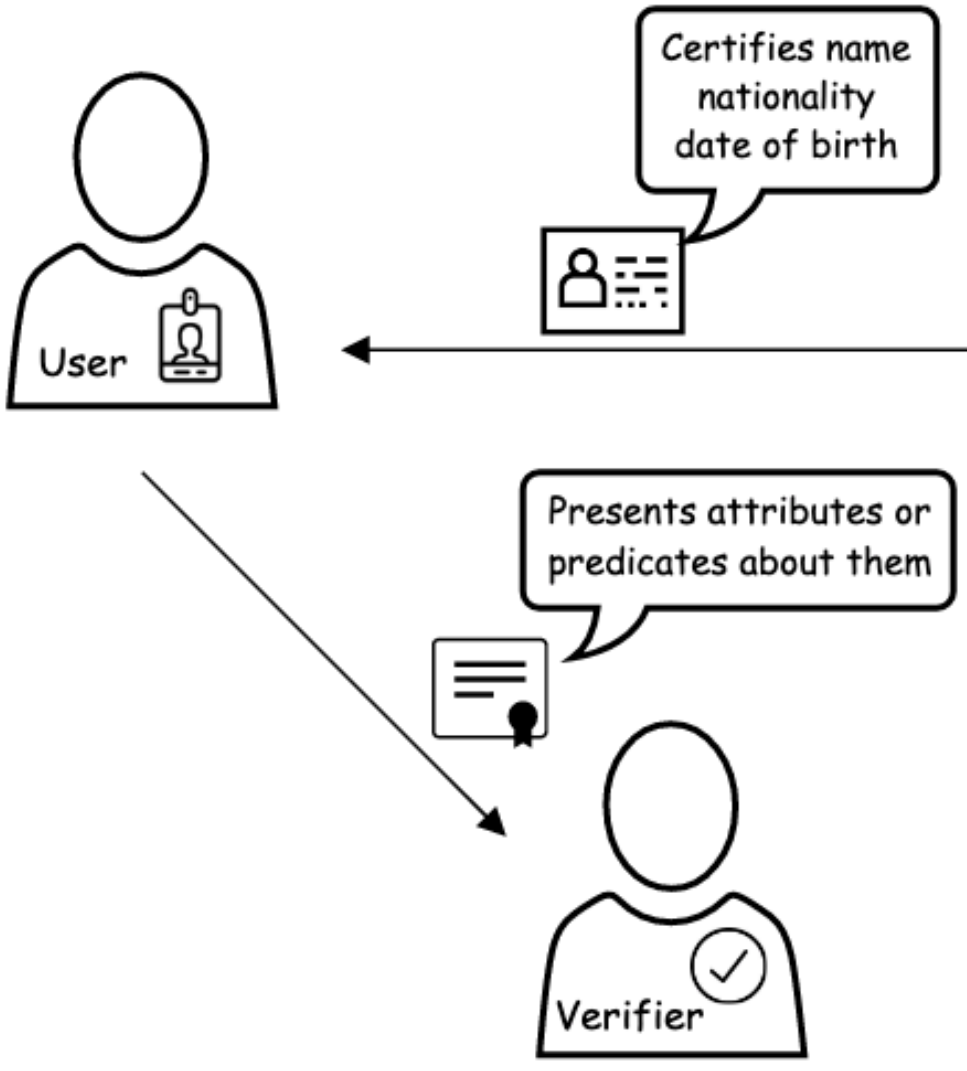
[1]Work done while the author was at Wordline Global.

Agenda

Attribute-based credentials

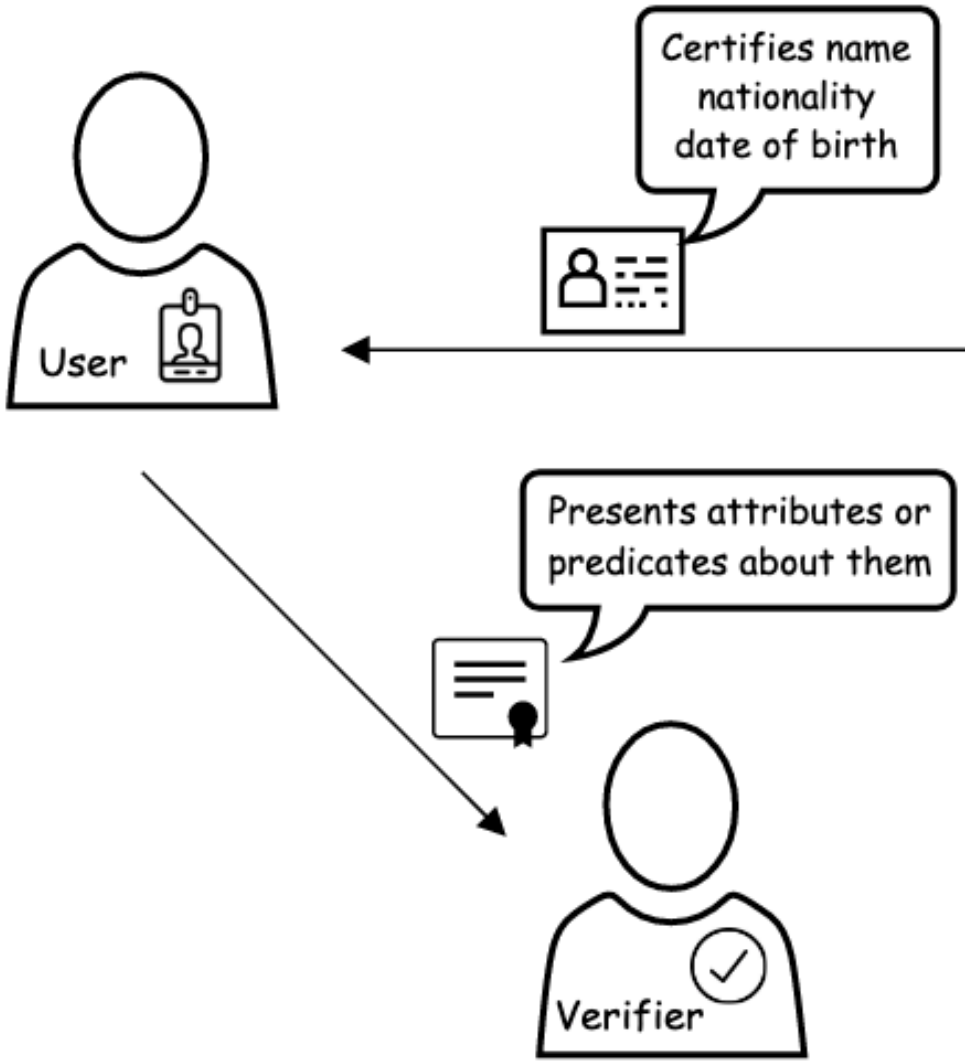


Attribute-based credentials



Multi-show ABC's: arbitrary number of unlinkable showings

Attribute-based credentials



Multi-show ABC's: arbitrary number of unlinkable showings

Multi-authority ABC's: single credential for attributes issued by multiple authorities

Attribute-based credentials: differences

Attribute-based credentials: differences

Expressiveness

Attribute-based credentials: differences

Expressiveness

Efficiency

Attribute-based credentials: differences

Expressiveness

Efficiency

Communication

Attribute-based credentials: differences

Expressiveness

Efficiency

Communication

Security model

Attribute-based credentials: differences

Expressiveness

Efficiency

Communication

Security model

Revocation

Attribute-based credentials: lines of work

Attribute-based credentials: lines of work

- CL signatures [CL04]: Idemix [Zur13] and [TG20]

Attribute-based credentials: lines of work

- CL signatures [CL04]: Idemix [Zur13] and [TG20]
- Aggregatable signatures: [CL11] and [HP20]

Attribute-based credentials: lines of work

- CL signatures [CL04]: Idemix [Zur13] and [TG20]
- Aggregatable signatures: [CL11] and [HP20]
- Sanitizable signatures: [CL13]

Attribute-based credentials: lines of work

- CL signatures [CL04]: Idemix [Zur13] and [TG20]
- Aggregatable signatures: [CL11] and [HP20]
- Sanitizable signatures: [CL13]
- Redactable signatures: [CDHK15] and [San20]

Attribute-based credentials: lines of work

- CL signatures [CL04]: Idemix [Zur13] and [TG20]
- Aggregatable signatures: [CL11] and [HP20]
- Sanitizable signatures: [CL13]
- Redactable signatures: [CDHK15] and [San20]
- Structure-Preserving Signatures on Equivalence Classes (SPS-EQ): [HS14], [DHS15] and [FHS19]

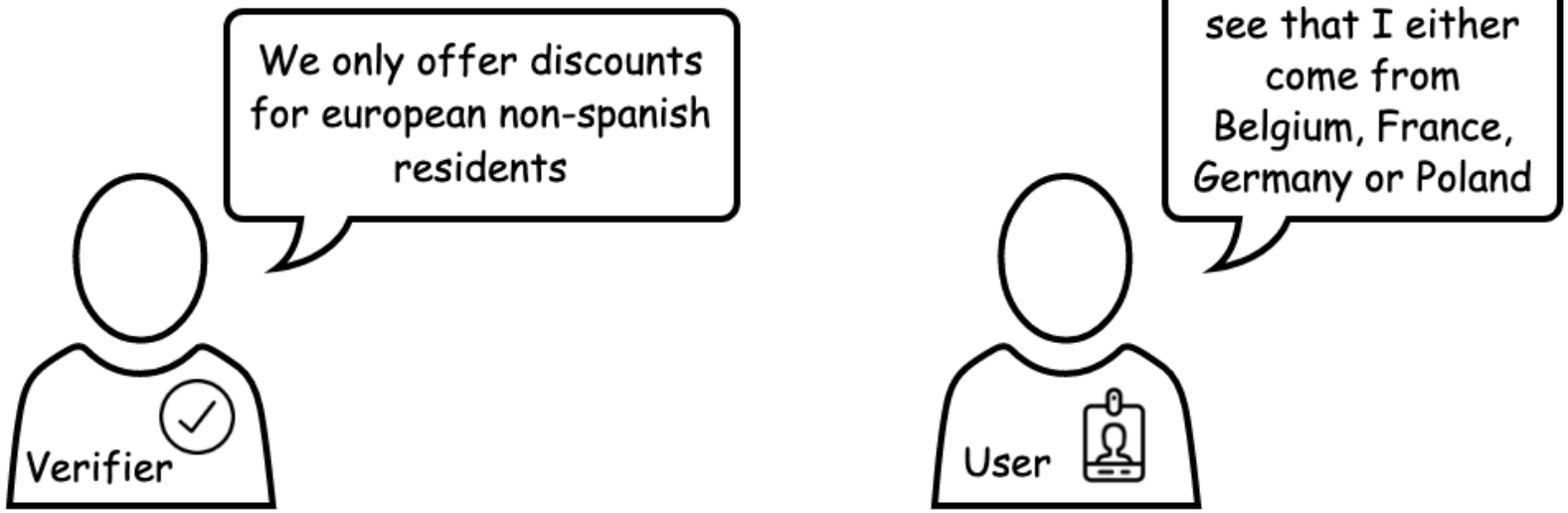
Attribute-based credentials: lines of work

- CL signatures [CL04]: Idemix [Zur13] and [TG20]
- Aggregatable signatures: [CL11] and [HP20]
- Sanitizable signatures: [CL13]
- Redactable signatures: [CDHK15] and [San20]
- Structure-Preserving Signatures on Equivalence Classes (SPS-EQ): [HS14], [DHS15] and [FHS19]
- All previous constructions leak the issuer's identity

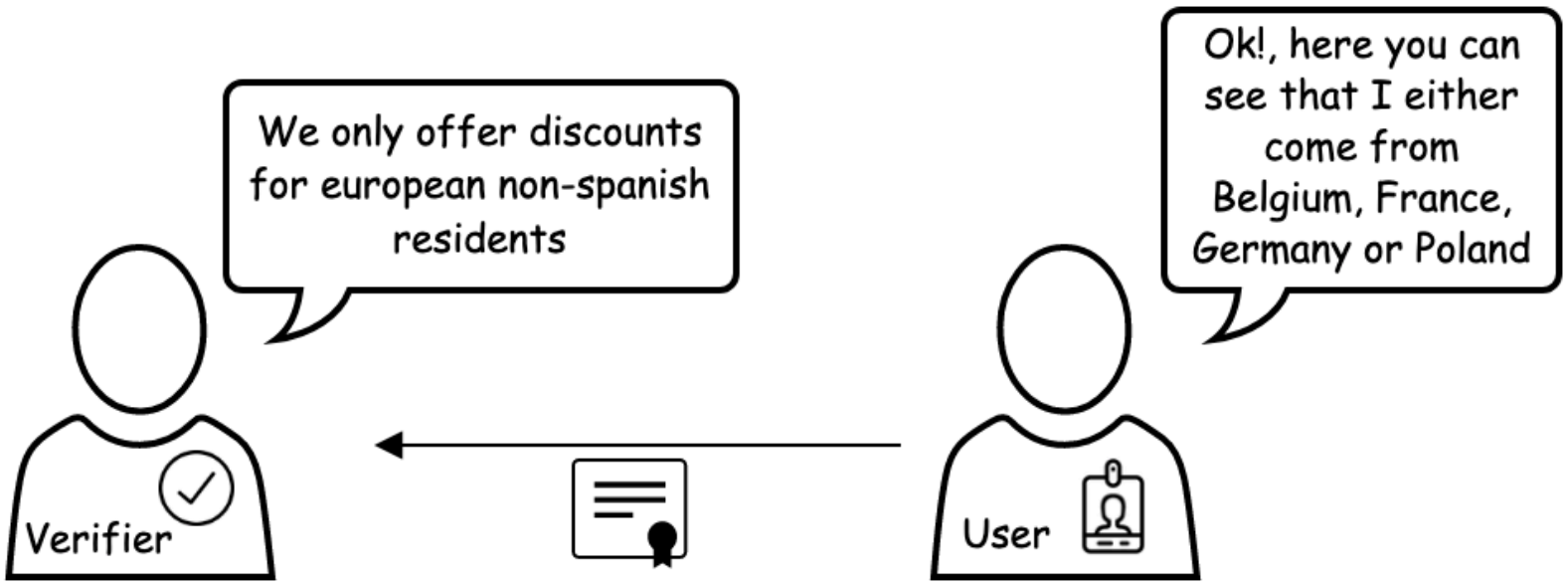
Motivation: self-sovereign identity across Europe

Motivation: self-sovereign identity across Europe

Motivation: self-sovereign identity across Europe



Motivation: self-sovereign identity across Europe



Agenda

Structure-Preserving Signatures on Equivalence Classes

Structure-Preserving Signatures on Equivalence Classes

- Controlled form of malleability: $(\sigma, m) \rightarrow (\sigma', m')$

Structure-Preserving Signatures on Equivalence Classes

- Controlled form of malleability: $(\sigma, m) \rightarrow (\sigma', m')$
- Message space can be partitioned into equivalence classes

Structure-Preserving Signatures on Equivalence Classes

- Controlled form of malleability: $(\sigma, m) \rightarrow (\sigma', m')$
- Message space can be partitioned into equivalence classes
  - *e.g.*, $m \in \mathbb{G}^\ell \sim_{\mathcal{R}} m' \in \mathbb{G}^\ell \iff \mu \in \mathbb{Z}_p^*$ s.t. $m' = \mu m$

Structure-Preserving Signatures on Equivalence Classes

- Controlled form of malleability: $(\sigma, m) \rightarrow (\sigma', m')$
- Message space can be partitioned into equivalence classes
  - *e.g.*, $m \in \mathbb{G}^\ell \sim_{\mathcal{R}} m' \in \mathbb{G}^\ell \iff \mu \in \mathbb{Z}_p^*$ s.t. $m' = \mu m$
- Unforgeability holds with respect to classes

Structure-Preserving Signatures on Equivalence Classes

- Controlled form of malleability: $(\sigma, m) \rightarrow (\sigma', m')$
- Message space can be partitioned into equivalence classes
  - *e.g.*, $m \in \mathbb{G}^\ell \sim_{\mathcal{R}} m' \in \mathbb{G}^\ell \iff \mu \in \mathbb{Z}_p^*$ s.t. $m' = \mu m$
- Unforgeability holds with respect to classes
- Message-signature pairs in the same class are unlinkable

Structure-Preserving Signatures on Equivalence Classes

- Controlled form of malleability: $(\sigma, m) \rightarrow (\sigma', m')$
- Message space can be partitioned into equivalence classes
  - *e.g.*, $m \in \mathbb{G}^\ell \sim_{\mathcal{R}} m' \in \mathbb{G}^\ell \iff \mu \in \mathbb{Z}_p^*$ s.t. $m' = \mu m$
- Unforgeability holds with respect to classes
- Message-signature pairs in the same class are unlinkable
- Recently extended to consider equivalence classes on the key space (*e.g.*, [BHKS18, CL19, CL21])

Agenda

The ABC framework from [FHS19]

The ABC framework from [FHS19]

- A credential is a **signature** on a (randomizable) accumulator representing a **set of attributes**

The ABC framework from [FHS19]

- A credential is a **signature** on a (randomizable) accumulator representing a **set of attributes**
- A credential showing involves the joint randomization of a message-signature pair

The ABC framework from [FHS19]

- A credential is a **signature** on a (randomizable) accumulator representing a **set of attributes**
- A credential showing involves the joint randomization of a message-signature pair
- The accumulator ([Ngu05]) uses batch membership proofs to allow **constant-size** showings

The ABC framework from [FHS19]

- A credential is a **signature** on a (randomizable) accumulator representing a **set of attributes**
- A credential showing involves the joint randomization of a message-signature pair
- The accumulator ([Ngu05]) uses batch membership proofs to allow **constant-size** showings
- Main drawback: **expressiveness is limited**

Towards improved constructions

Towards improved constructions

- We focused on improving the following aspects:

Towards improved constructions

- We focused on improving the following aspects:
  - expressiveness (extending the accumulator)

Towards improved constructions

- We focused on improving the following aspects:
  - expressiveness (extending the accumulator)
  - efficiency (leveraging user/verifier costs)

Towards improved constructions

- We focused on improving the following aspects:
  - expressiveness (extending the accumulator)
  - efficiency (leveraging user/verifier costs)
  - security model (~~GGM~~ Standard model + CRS)

Agenda

Overview of results

Overview of results

- Based on previous works [KSD19, CH20], we **obtained a new SPS-EQ** working on the message and key spaces

Overview of results

- Based on previous works [KSD19, CH20], we **obtained a new SPS-EQ** working on the message and key spaces
- Extended the accumulator from [FHS19] with [GOP+16] to **support batch non-membership proofs**

Overview of results

- Based on previous works [KSD19, CH20], we **obtained a new SPS-EQ** working on the message and key spaces
- Extended the accumulator from [FHS19] with [GOP+16] to **support batch non-membership proofs**
- Incorporated a proof of exponentiation ([Tha19]) to **outsource computational cost** from the verifier to the user

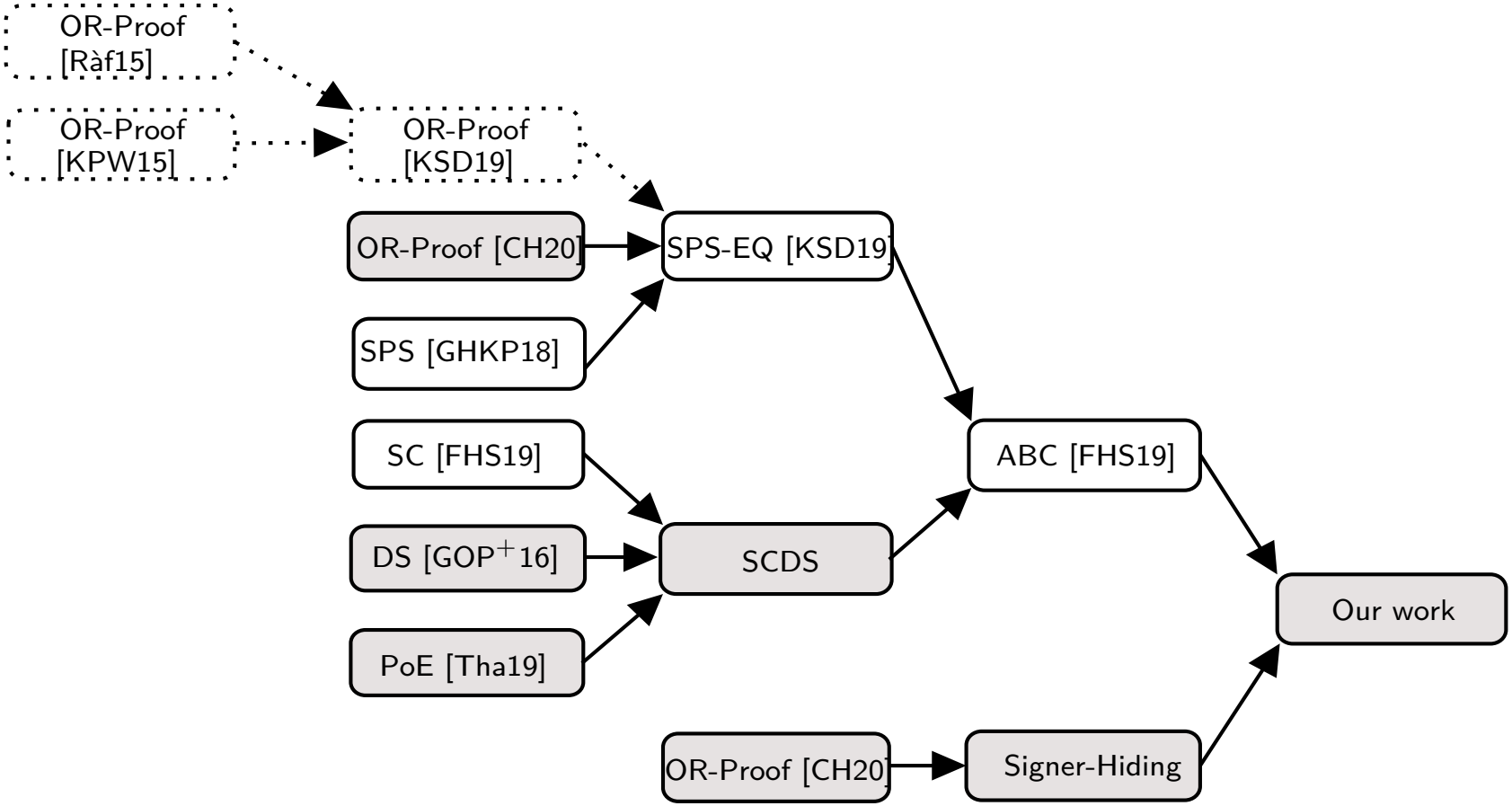
Overview of results

- Based on previous works [KSD19, CH20], we **obtained a new SPS-EQ** working on the message and key spaces
- Extended the accumulator from [FHS19] with [GOP+16] to **support batch non-membership proofs**
- Incorporated a proof of exponentiation ([Tha19]) to **outsource computational cost** from the verifier to the user
- Proposed a 1-out-of-n NIZK OR-proof so that **users can hide the issuer identity** during a showing

Overview of results

- Based on previous works [KSD19, CH20], we **obtained a new SPS-EQ** working on the message and key spaces
- Extended the accumulator from [FHS19] with [GOP+16] to **support batch non-membership proofs**
- Incorporated a proof of exponentiation ([Tha19]) to **outsource computational cost** from the verifier to the user
- Proposed a 1-out-of-n NIZK OR-proof so that **users can hide the issuer identity** during a showing
- Extended the security model from [FHS19]

Overview of results



Agenda

Signer-hiding: Construction

Signer-hiding: Construction

- Main idea:

Signer-hiding: Construction

- Main idea:
  - Randomize the credential and issuer's public-key consistently

Signer-hiding: Construction

- Main idea:
  - Randomize the credential and issuer's public-key consistently
  - Present them to the verifier alongside a proof of correct randomization of issuer's public-key

Signer-hiding: Construction

- Main idea:
  - Randomize the credential and issuer's public-key consistently
  - Present them to the verifier alongside a proof of correct randomization of issuer's public-key
- The 1-out-of-n OR-proof is a fully adaptive NIZK argument

Signer-hiding: Construction

- Main idea:
  - Randomize the credential and issuer's public-key consistently
  - Present them to the verifier alongside a proof of correct randomization of issuer's public-key
- The 1-out-of-n OR-proof is a fully adaptive NIZK argument
- Users can select arbitrary long sets of public keys to compute a proof with linear cost

Signer-hiding: Formalization

Signer-hiding: Formalization

An ABC system supports signer-hiding if for all $\lambda > 0$, all $q > 0$, all $n > 0$, all $t > 0$, all $\mathcal{X}$ with $0 < |\mathcal{X}| \leq t$, all $\emptyset \neq \mathcal{S} \subset \mathcal{X}$ and $\emptyset \neq \mathcal{D} \not\subseteq \mathcal{X}$ with $0 < |\mathcal{D}| \leq t$, and p.p.t adversaries $\mathcal{A}$, the following holds

$$\Pr\left[\begin{array}{l} \mathsf{pp} \xleftarrow{\$} \mathsf{Setup}(1^\lambda, 1^q); \\ \forall\ i \in [n] : (\mathsf{osk}_i, \mathsf{opk}_i) \xleftarrow{\$} \mathsf{OrgKGen}(\mathsf{pp}); \\ (\mathsf{usk}, \mathsf{upk}) \xleftarrow{\$} \mathsf{UsrKGen}(\mathsf{pp}); j \xleftarrow{\$} [n]; \\ (\mathsf{cred}, \top) \xleftarrow{\$} (\mathsf{Obtain}(\mathsf{usk}, \mathsf{opk}_j, \mathcal{X}), \\ \qquad\qquad\qquad \mathsf{Issue}(\mathsf{upk}, \mathsf{osk}_j, \mathcal{X})); \\ j^* \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\mathsf{Show}}}(\mathsf{pp}, \mathcal{S}, \mathcal{D}, \mathsf{opk}_i)_{i \in [n]}) \end{array} : \ j^* = j \right] \leq \frac{1}{n}$$

Agenda

Conclusions and Future Work

Conclusions and Future Work

- Our results explore multiple paths to extend the ABC framework from [FHS19]

Conclusions and Future Work

- Our results explore multiple paths to extend the ABC framework from [FHS19]
- We obtained a more flexible framework leveraging different trade-offs

Conclusions and Future Work

- Our results explore multiple paths to extend the ABC framework from [FHS19]
- We obtained a more flexible framework leveraging different trade-offs
- The proposed signer-hiding notion enables more use cases

Conclusions and Future Work

- Our results explore multiple paths to extend the ABC framework from [FHS19]
- We obtained a more flexible framework leveraging different trade-offs
- The proposed signer-hiding notion enables more use cases
- Exploring the use of aggregatable signatures with SPS-EQ in the multi-authority setting could enable even more use cases

Conclusions and Future Work

- Our results explore multiple paths to extend the ABC framework from [FHS19]
- We obtained a more flexible framework leveraging different trade-offs
- The proposed signer-hiding notion enables more use cases
- Exploring the use of aggregatable signatures with SPS-EQ in the multi-authority setting could enable even more use cases
- Devising other ways to define equivalence classes could lead to new and more efficient constructions

Thank you for your time!

References I

Michael Backes, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider.
Signatures with Flexible Public Key: Introducing Equivalence Classes for Public Keys.
In Thomas Peyrin and Steven Galbraith, editors, Advances in Cryptology – ASIACRYPT 2018, pages 405–434, Cham, 2018. Springer International Publishing.

Jan Camenisch, Maria Dubovitskaya, Kristiyan Haralambiev, and Markulf Kohlweiss.
Composable and Modular Anonymous Credentials: Definitions and Practical Constructions.
In Tetsu Iwata and Jung Hee Cheon, editors, Advances in Cryptology – ASIACRYPT 2015, pages 262–288, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

References II

Geoffroy Couteau and Dominik Hartmann.
Shorter Non-interactive Zero-Knowledge Arguments and ZAPs for Algebraic Languages.
In Daniele Micciancio and Thomas Ristenpart, editors, Advances in Cryptology – CRYPTO 2020, pages 768–798, Cham, 2020. Springer International Publishing.

Jan Camenisch and Anna Lysyanskaya.
Signature Schemes and Anonymous Credentials from Bilinear Maps.
In Matt Franklin, editor, Advances in Cryptology – CRYPTO 2004, pages 56–72, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

References III


Sébastien Canard and Roch Lescuyer.
Anonymous Credentials from (Indexed) Aggregate Signatures.
In Proceedings of the 7th ACM Workshop on Digital Identity Management, DIM '11, page 53–62, New York, NY, USA, 2011. Association for Computing Machinery.


Sébastien Canard and Roch Lescuyer.
Protecting Privacy by Sanitizing Personal Data: A New Approach to Anonymous Credentials.
In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ASIA CCS '13, page 381–392, New York, NY, USA, 2013. Association for Computing Machinery.

References IV


Elizabeth C. Crites and Anna Lysyanskaya.
Delegatable Anonymous Credentials from Mercurial Signatures.
In Mitsuru Matsui, editor, Topics in Cryptology – CT-RSA 2019, pages 535–555, Cham, 2019. Springer International Publishing.


Elizabeth C. Crites and Anna Lysyanskaya.
Mercurial signatures for variable-length messages.
Proceedings on Privacy Enhancing Technologies, 2021(4):441–463, 2021.


David Derler, Christian Hanser, and Daniel Slamanig.
A New Approach to Efficient Revocable Attribute-Based Anonymous Credentials.
In Jens Groth, editor, Cryptography and Coding, pages 57–74, Cham, 2015. Springer International Publishing.

References V

Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig.
Structure-Preserving Signatures on Equivalence Classes and Constant-Size Anonymous Credentials.
Journal of Cryptology, 32:498–546, 2019.

Romain Gay, Dennis Hofheinz, Lisa Kohl, and Jiaxin Pan.
More Efficient (Almost) Tightly Secure Structure-Preserving Signatures.
In Jesper Buus Nielsen and Vincent Rijmen, editors, Advances in Cryptology – EUROCRYPT 2018, pages 230–258, Cham, 2018. Springer International Publishing.

References VI

Esha Ghosh, Olga Ohrimenko, Dimitrios Papadopoulos, Roberto Tamassia, and Nikos Triandopoulos.
Zero-Knowledge Accumulators and Set Algebra.
In Proceedings, Part II, of the 22nd International Conference on Advances in Cryptology — ASIACRYPT 2016 - Volume 10032, page 67–100, Berlin, Heidelberg, 2016. Springer-Verlag.

Chloé Hébant and David Pointcheval.
Traceable Constant-Size Multi-Authority Credentials.
Cryptology ePrint Archive, Report 2020/657, 2020.

Christian Hanser and Daniel Slamanig.
Structure-Preserving Signatures on Equivalence Classes and Their Application to Anonymous Credentials.
In Palash Sarkar and Tetsu Iwata, editors, Advances in Cryptology – ASIACRYPT 2014, pages 491–511, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

References VII

Eike Kiltz, Jiaxin Pan, and Hoeteck Wee.
Structure-Preserving Signatures from Standard Assumptions, Revisited.
In Rosario Gennaro and Matthew Robshaw, editors, Advances in Cryptology – CRYPTO 2015, pages 275–295, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

Mojtaba Khalili, Daniel Slamanig, and Mohammad Dakhilalian.
Structure-Preserving Signatures on Equivalence Classes from Standard Assumptions.
In Steven D. Galbraith and Shiho Moriai, editors, Advances in Cryptology – ASIACRYPT 2019, pages 63–93, Cham, 2019. Springer International Publishing.

References VIII

Lan Nguyen.
Accumulators from Bilinear Pairings and Applications.
In Alfred Menezes, editor, Topics in Cryptology – CT-RSA 2005, pages 275–292, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

Carla Ràfols.
Stretching groth-sahai: Nizk proofs of partial satisfiability.
In Yevgeniy Dodis and Jesper Buus Nielsen, editors, Theory of Cryptography, pages 247–276, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

References IX

Olivier Sanders.
Efficient Redactable Signature and Application to Anonymous Credentials.
In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, Public-Key Cryptography – PKC 2020, pages 628–656, Cham, 2020. Springer International Publishing.

Syh-Yuan Tan and Thomas Groß.
MoniPoly - An Expressive q-SDH-Based Anonymous Attribute-Based Credential System.
In Shiho Moriai and Huaxiong Wang, editors, Advances in Cryptology - ASIACRYPT 2020, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part III, volume 12493, pages 498–526. Springer, 2020.

References X

S. Thakur.
Batching non-membership proofs with bilinear accumulators.
IACR Cryptol. ePrint Arch., 2019:1147, 2019.

IBM Research Zurich.
Specification of the identity mixer cryptographic library v2.3.0., 2013.