Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

der Bundeswehr
Universität München

Anonymous Credentials: Past, Present, and Future

Daniel Slamanig

Universität der Bundeswehr München

Workshop on Cryptographic Tools for Blockchains

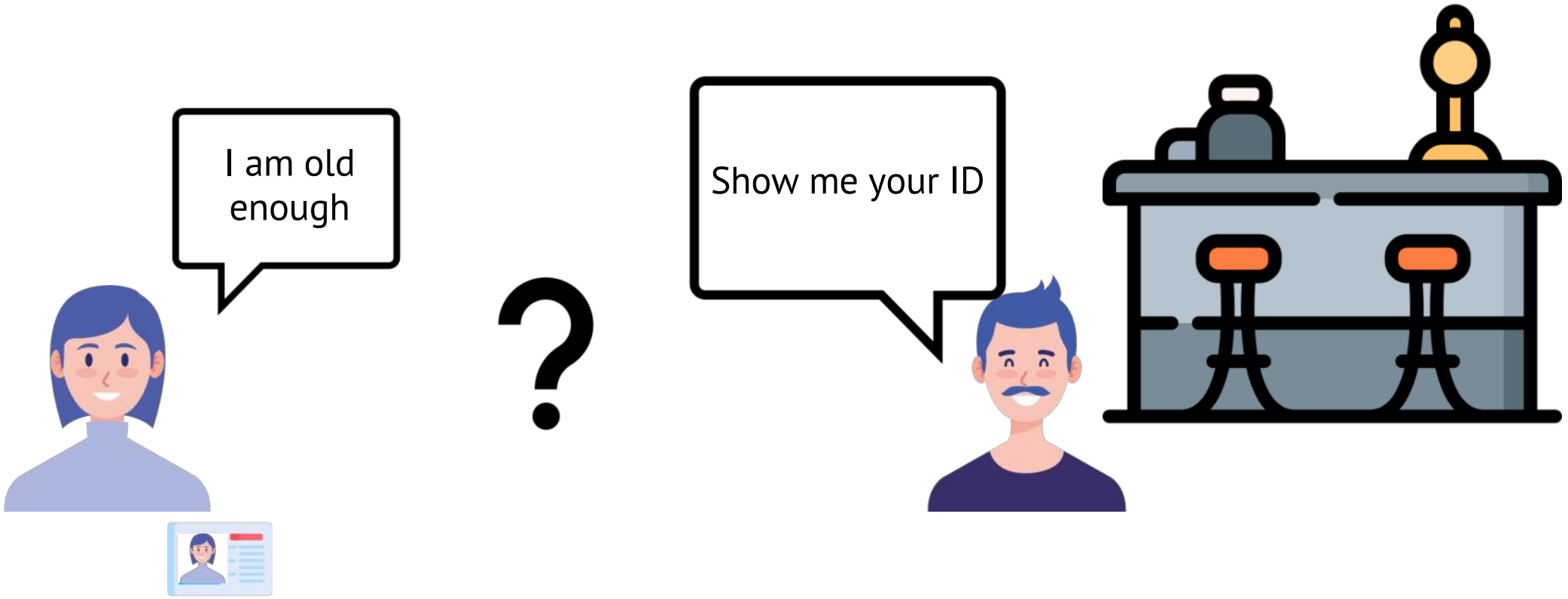
— affiliated with Eurocrypt 2025 —

Madrid, Spain, 3rd of May

OUTLINE

- Motivation for Privacy-Preserving Authentication
- Anonymous Credentials (conceptually)
- Properties and types of Anonymous Credentials
- Decentralizing Anonymous Credentials
- Construction paradigms
- The post-quantum picture and future directions

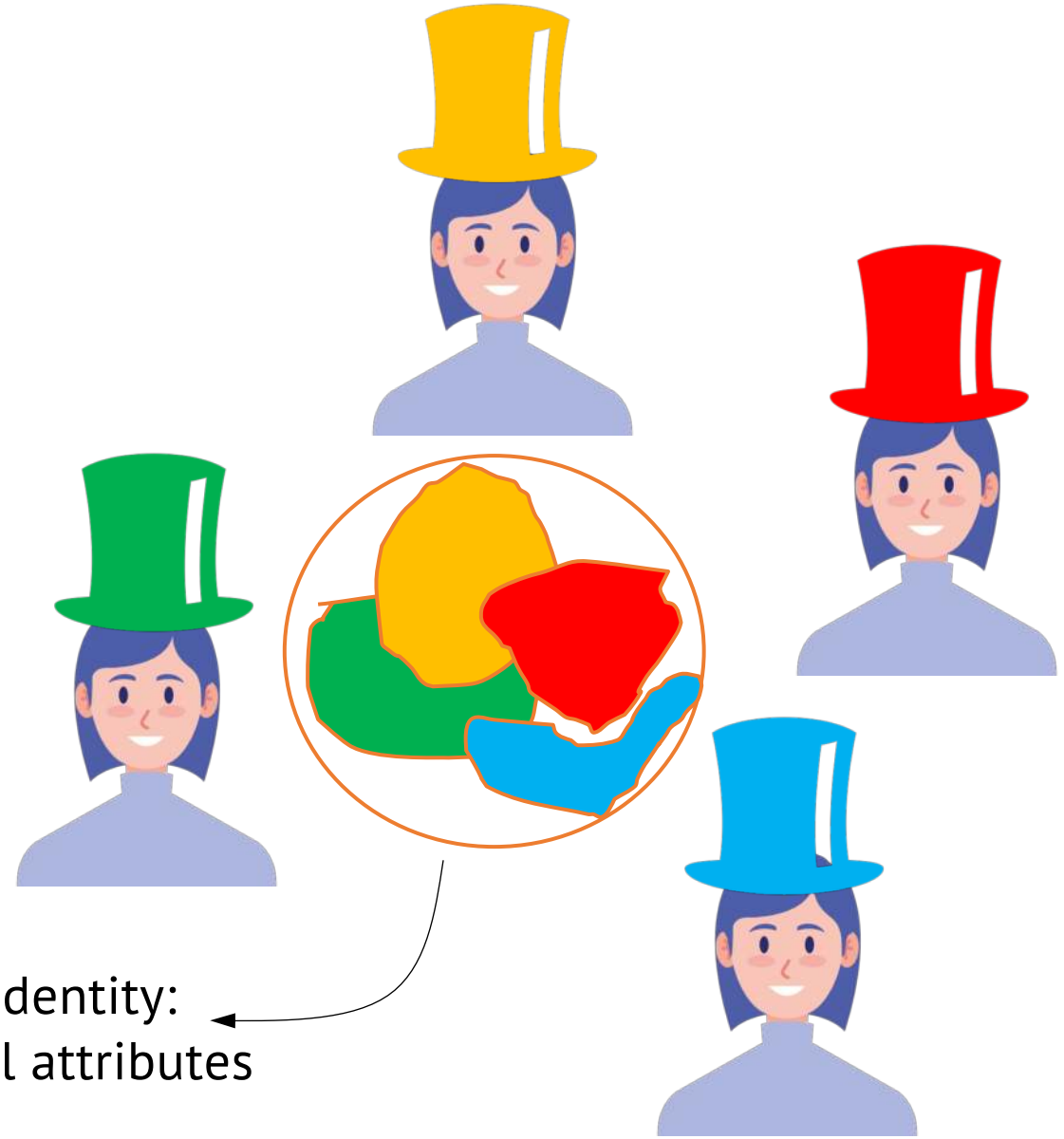
MOTIVATION FOR PRIVACY-PRESERVING AUTHENTICATION



- Showing the ID reveals much more information than required (age)
- Data minimization – significant problem in the digital world

BEFORE WE BEGIN: WHAT IS AN IDENTITY?

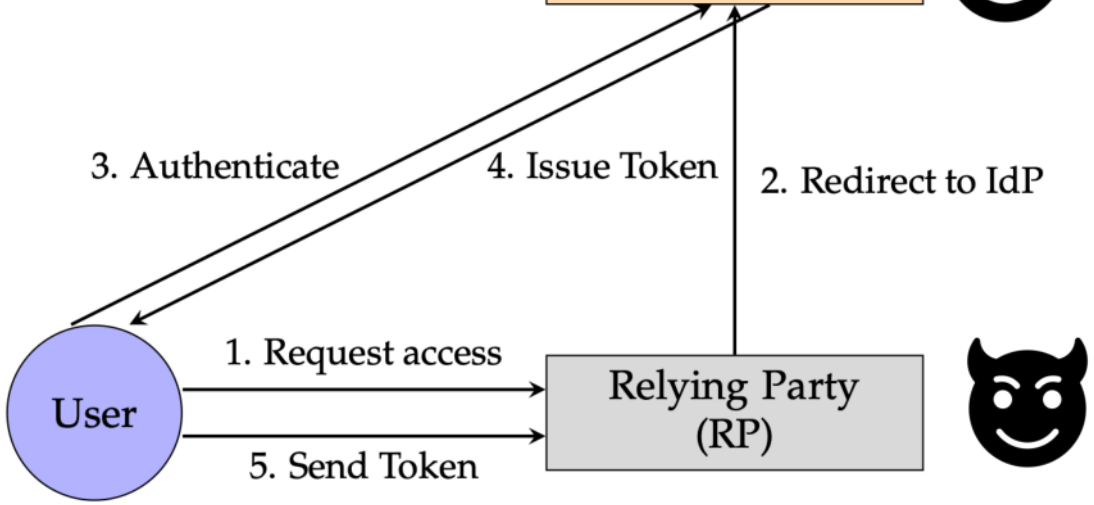
- Everyone has a set of **partial identities** (work, leisure, health, etc.)
- The union of all those defines the **complete identity**
- Often people want to (strictly) **separate** partial identities!



TRADITIONAL AUTHENTICATION ON THE WEB

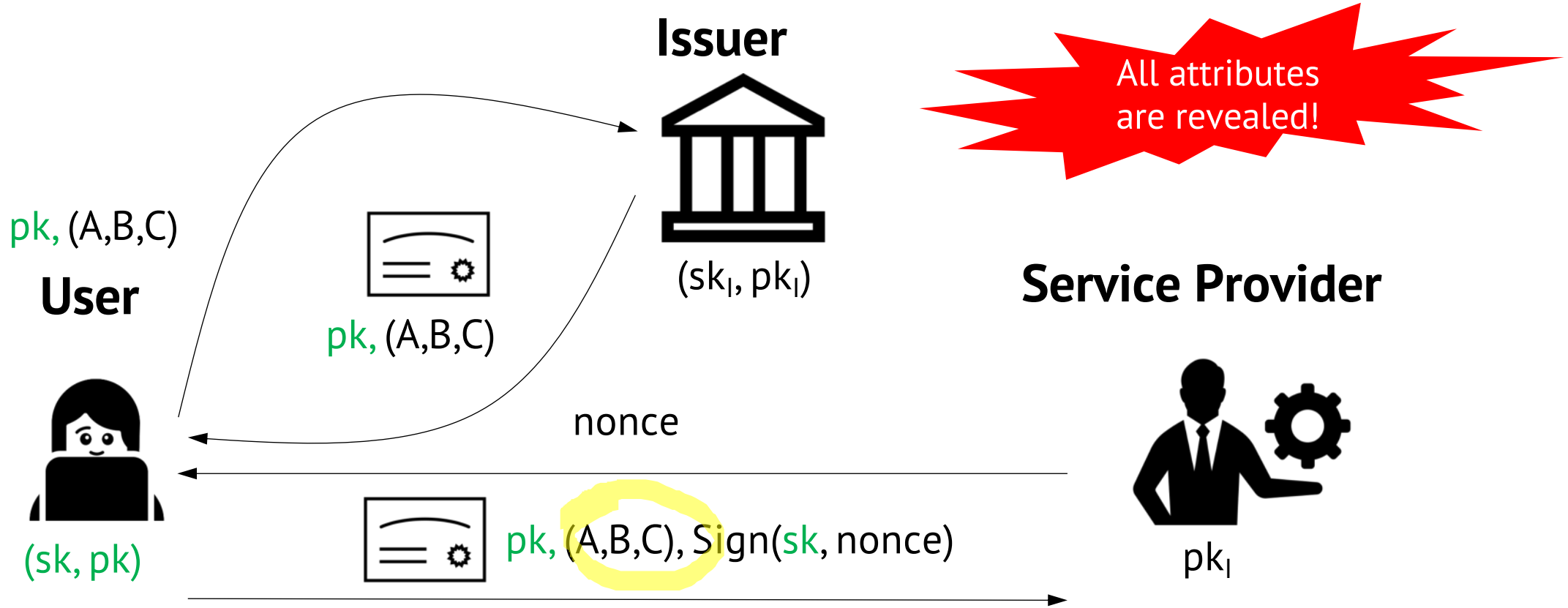
- Single Sign On (SSO): Password- or signature-based user authentication at a single centralized entity (Identity provider)
- Identity Provider (IdP) model:
  - Profile (your attributes) resides at the IdP
  - Service provider (RP) does not need to know everything
  - IdP knows everything
  - **IdP and RP together know everything!**

- **OpenID Connect** (OIDC) emerged as the open standard for online authentication and authorization



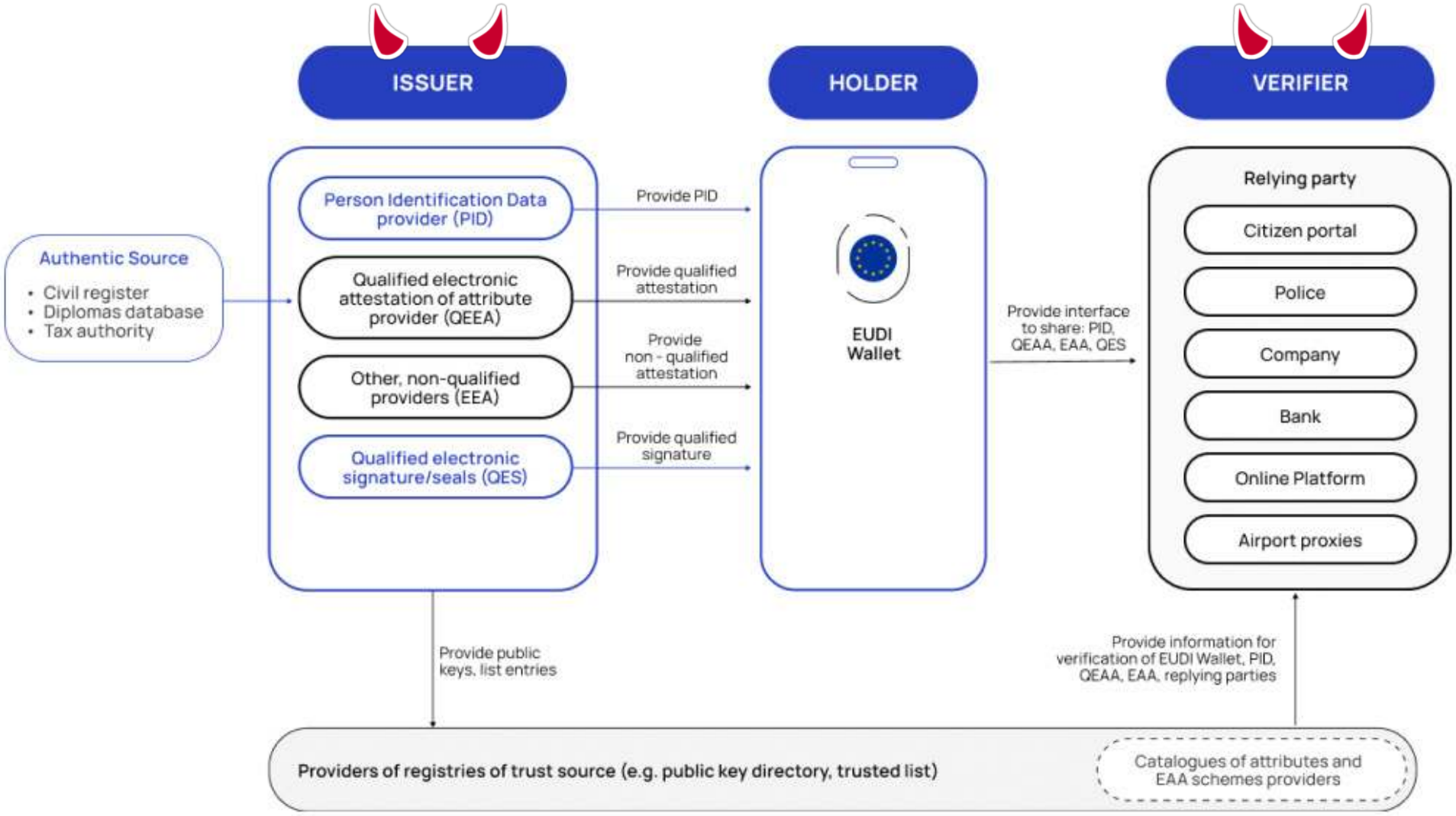
TRADITIONAL AUTHENTICATION: GOVERNMENTAL IDENTITY

- Digital credentials (e.g., eIDs)
  - Signature over pk and all the attributes (certificate) from some authority
  - Always reveal everything - **no selective disclosure**



EUROPEAN DIGITAL IDENTITY (EUDI)

Privacy broken?



EUDI: CURRENT APPROACH (ISO/IEC 18013-5:2021)

Same concept as used in the **mobile driving licence (mDL)** application

- More technically:
  - Issuers sign as message being **a representation of attributes**
  - Think of the **message** $\boldsymbol{m = (h_1, \ldots, h_n)}$ as a **list of "salted hashes"** $\boldsymbol{h_i = H(a_i || r_i)}$ which hide the attribute a_i as long as the randomness r_i is not revealed
  - **Selectively revealing attributes** means publishing (a_i, r_i) and hiding attributes means only publishing h_i
- Such credentials can **only be shown once in an unlinkable way**
  - Frequent issuing (batch issuing) and only use them once!
- When Issuers and Verifiers collaborate, then they can **fully break privacy**!
  - Compatible with rolled-out cryptography. But we can do much better!

ANONYMOUS CREDENTIALS

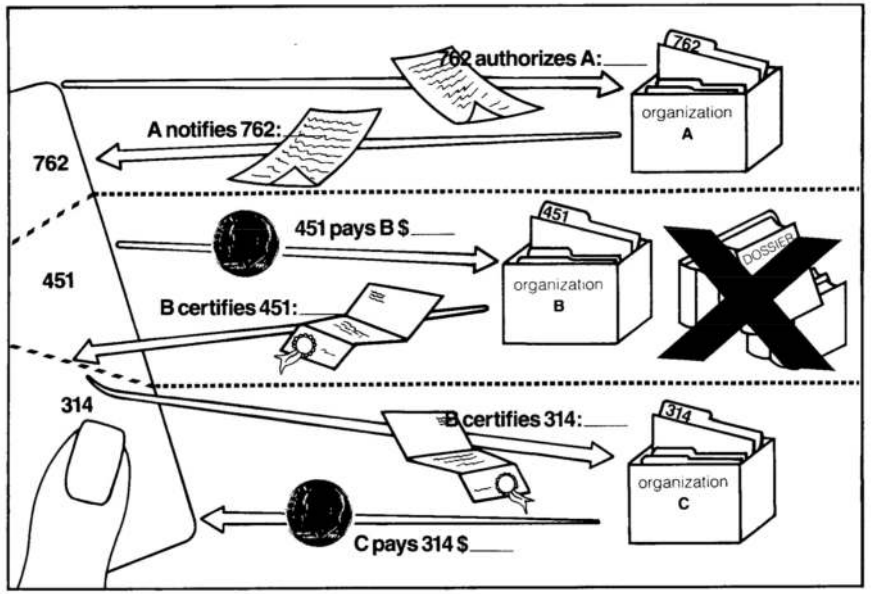
Communications of the ACM, 1985

SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE

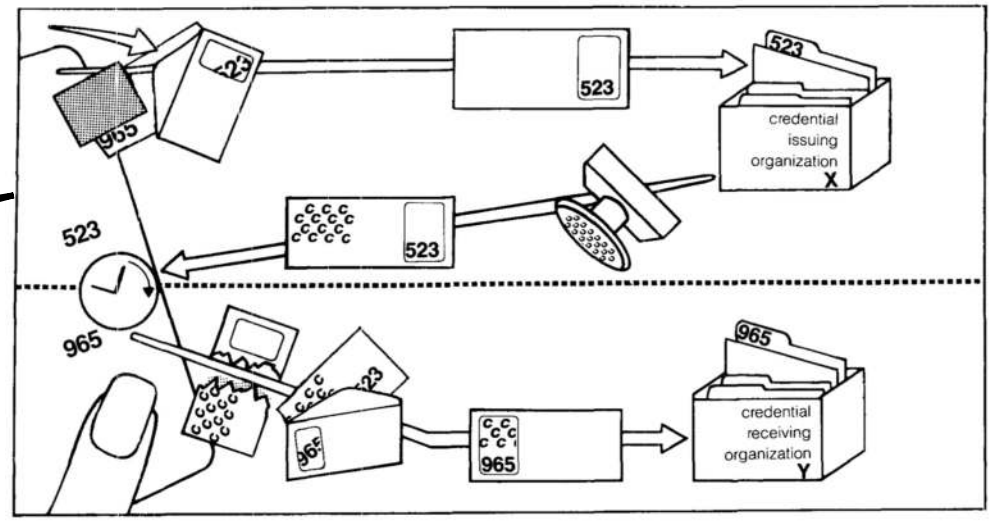
The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the security of both individuals and organizations.

DAVID CHAUM

Use of different “pseudonyms” with different organizations



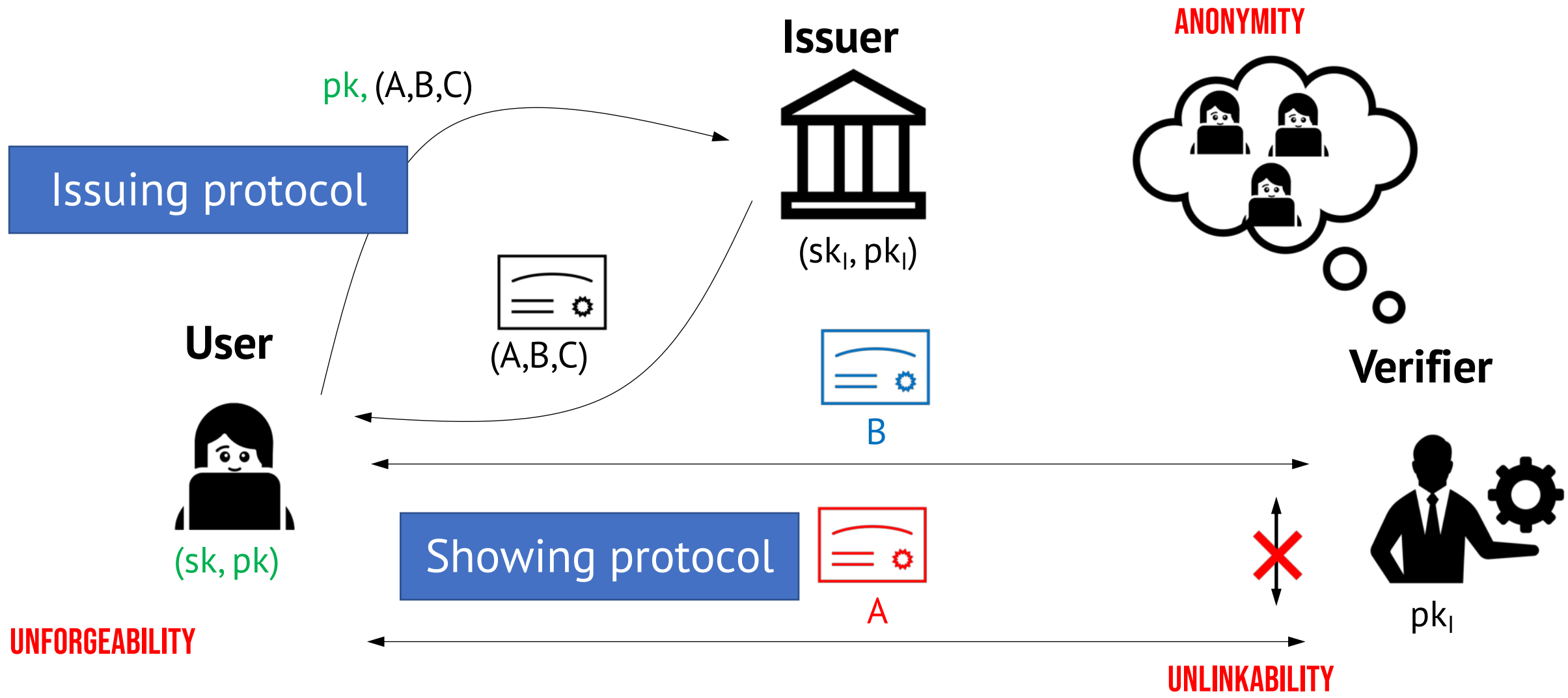
Untraceable credential/attribute transfers between “pseudonyms”



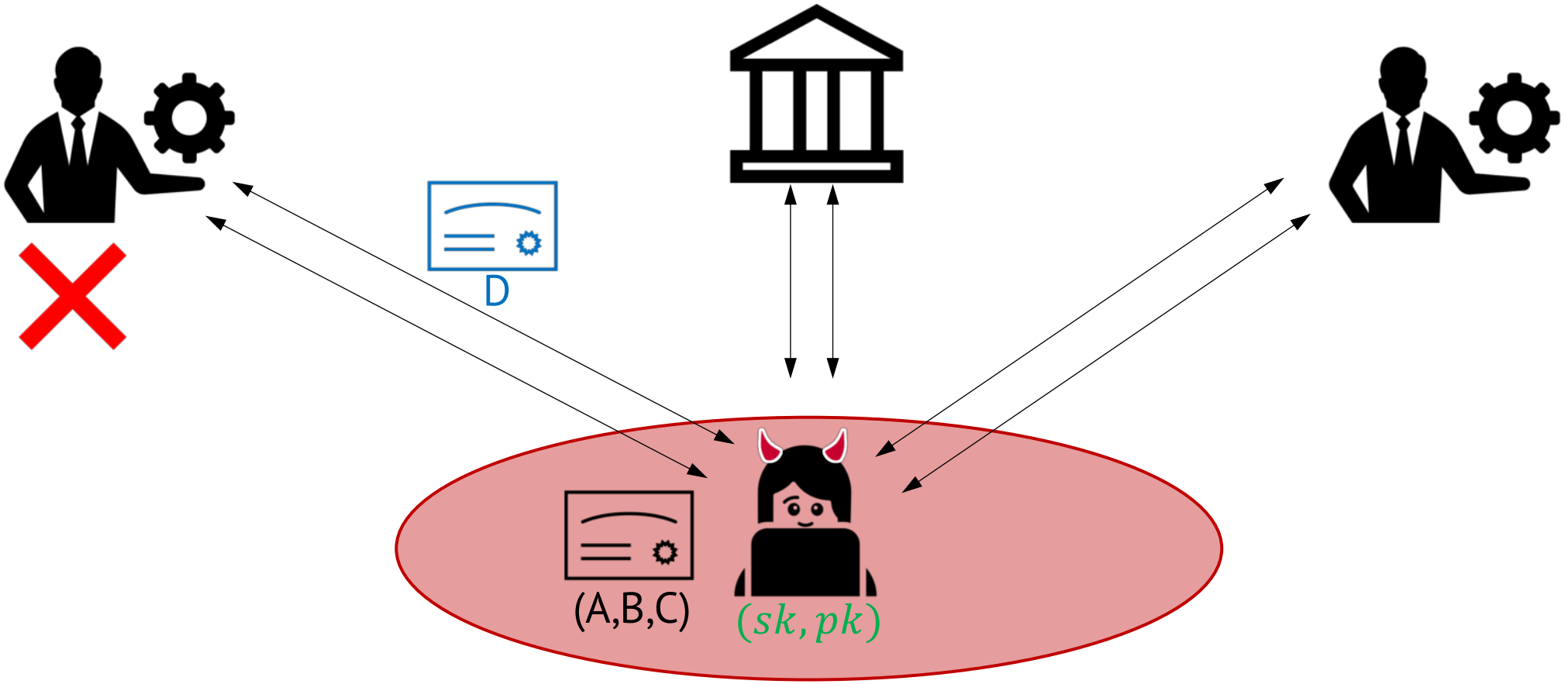
A BIT OF HISTORY OF ANONYMOUS CREDENTIALS

- Envisioned by David Chaum in the 80ies
- First constructions by Jan Camenisch and Anna Lysyanskaya (~20 years ago)
- For a long time, mostly research projects and no significant deployments in industry
- In the last few years more and more real-world applications
- Recently also discussion around major deployment by public bodies
  - European Union Digital Identity Wallets (EUDIW)
  - Mobile driver's license (mDL) in the United States
  - …
- Many different constructions of ACs with different properties/trade-offs available today
- Two main design paradigms
  - Zero-knowledge credentials
  - Self-blindable credentials

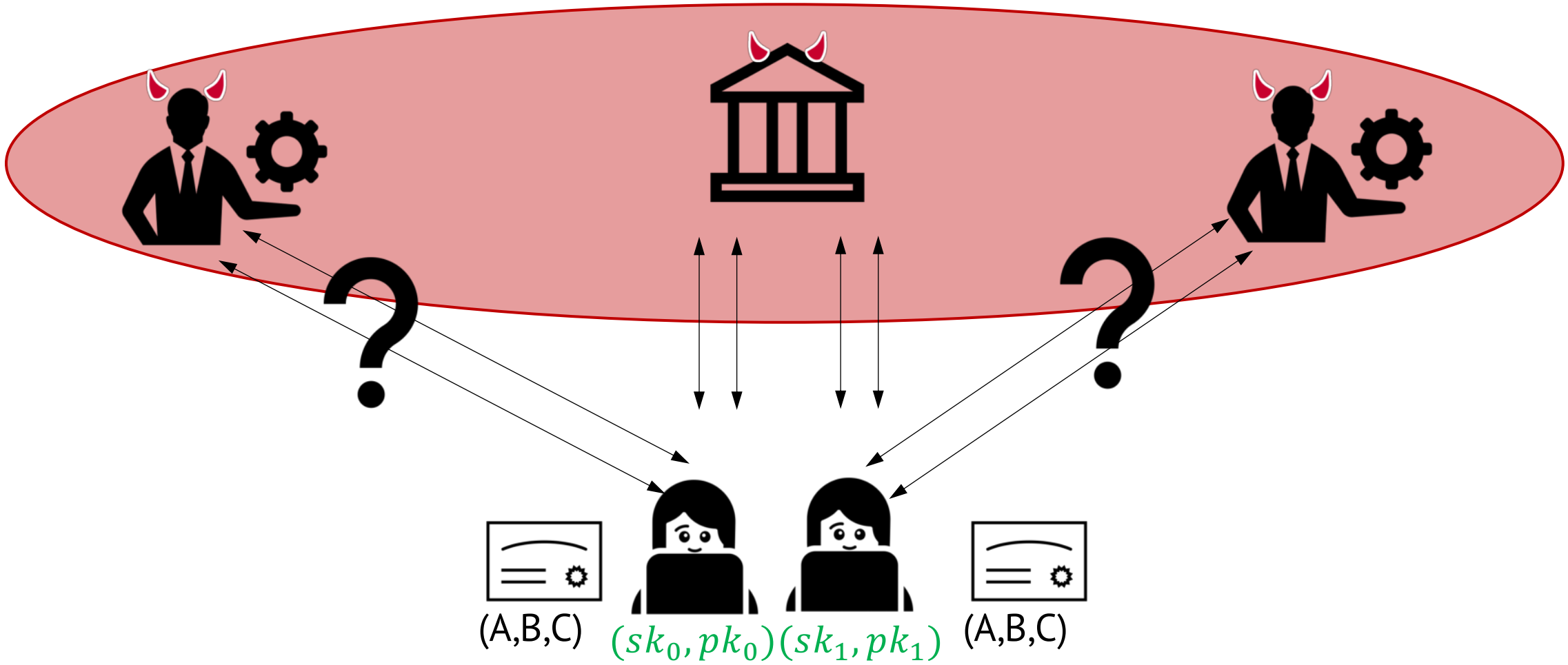
ANONYMOUS CREDENTIALS (CONCEPTUALLY)



VERY INFORMAL SECURITY: UNFORGEABILITY



VERY INFORMAL SECURITY: ANONYMITY



BASIC FEATURES OF ACS

- **Single-use vs. multi-use credentials**
  - In single-use showings of the same credential are linkable (traceable). In multi-use they can be shown an unlimited number of time in an unlinkable way
- **Support of attributes**
  - Credentials might encode attributes or just represent *anonymous tokens*
- **Expressiveness of attribute presentations**
  - Either only allow to reveal or withhold (selective disclosure) or be able to prove arbitrary statements about attributes encoded in the credential
- **Everyone or only designated parties can be verifier (“public key vs. secret key”)**
  - Standard vs. keyed-verification anonymous credentials
- **Non-transferability**
  - Discourage/prevent sharing of credentials

EXTENDED FEATURES OF ACS I/II

- **Revocation**
  - Invalidate already issued credentials (put credentials on a revocation list)
- **Blind issuing of attributes**
  - Issuer does not learn the attributes, e.g., just that user knows them; they are the same as in another credential
- **Issuer-hiding**
  - Do not reveal the issuer of a credential to the verifier
  - Just show that a “issuer-policy” (acceptable issuers) defined by the verifier is satisfied

EXTENDED FEATURES ACS II/II

- **Pseudonyms**
  - From a credential and a given context (string) always derive the same pseudorandom identifier
  - E.g., all actions in the health domain are linkable, but unlinkable to other domains
- **Inspection**
  - Escrow identifying information with a showing; this can be opened by a third party when required
- **Delegation**
  - Credentials issuing in a hierarchical manner (like in PKI) with privacy

A more exhaustive list can be found in: D. Slamanig: Privacy-Preserving Authentication: Theory vs. Practice
https://arxiv.org/pdf/2501.07209

DECENTRALIZATION

- Reduction of trust in centralized entities
- Distribute power and increase availability
  - Blockchain technologies and cryptocurrencies are prime examples
- Self-sovereign identity (SSI)
  - Leveraging distributed ledger technologies (DLTs) and concepts such as decentralized identifiers (DIDs)
  - Combine with anonymous credentials: e.g., verifiable credentials with ZK showing

DECENTRALIZATION AND ANONYMOUS CREDENTIALS

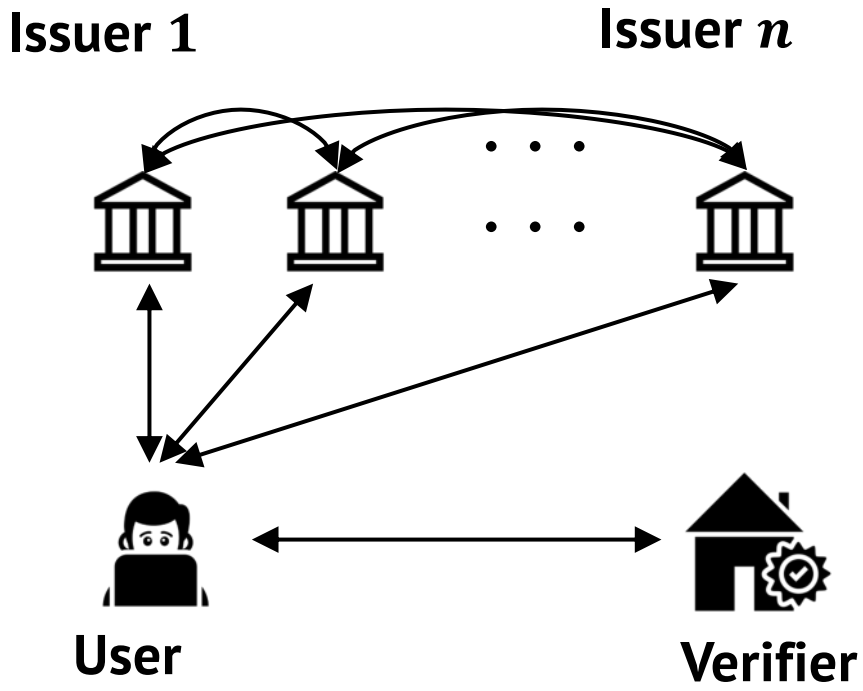
- Remove the issuer [GGM14]
  - Everyone can register credentials on the blockchain
  - Accepted if included in the blockchain (can be various criteria)

- Map existing credential [RWGM23]
  - Collect credentials or identity documents (not necessarily ACs) from various issuers
  - Convert them into anonymous credentials registered in some ledger (blockchain) and start from there

- Distribute/decentralize the issuer
  - Use a traditional AC approach but distribute the issuer/have multiple issuers
  - Use of DLT technologies for registration, revocation, etc.

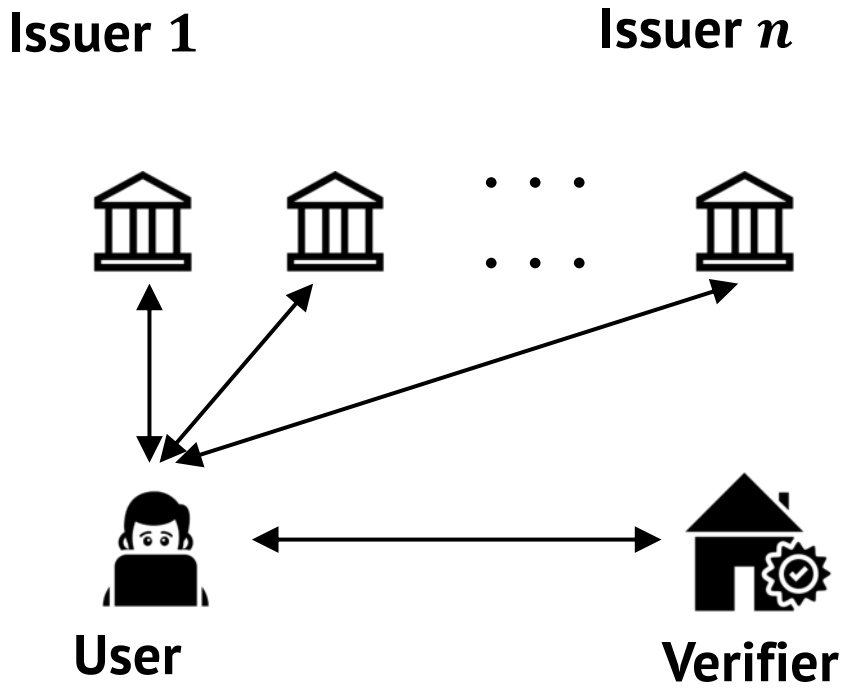
THRESHOLD-ISSUANCE ANONYMOUS CREDENTIALS

- Distribute the power to issue credentials among multiple parties: k out of n required
- Issuers together generate one key for issuing
- There is one public key in the system
- Ideally the issuers only need to interact during a setup (to generate the key) but not during issuing
- Users obtain a credential that is valid under the issuer key



DECENTRALIZED / MULTI-AUTHORITY ANONYMOUS CREDENTIALS

- System consists of n independent issuers
- Users can collect credentials from different issuers
- Ideally the credential showing is compact
- **Issuer hiding-feature** might be required as the combination of issuers used during showing might reveal too much information
  - Think of collecting credentials from different issuers within the EU
  - The combination of issuers might reduce anonymity significantly!



MULTI-USE ANONYMOUS CREDENTIALS (ZK CREDENTIALS)

Issuer

Issue Credential

$\mathsf{Sign}(\mathsf{sk}_{CA}, \mathsf{pk}_A)$

User

pk_A

Show Credential

Ω

Service Provider

NIZK Ω :

$\exists(\sigma, \mathsf{pk}_A) : \mathsf{Verify}(\mathsf{pk}_{CA}, \mathsf{pk}_A, \sigma) = 1$

MULTI-USE ANONYMOUS CREDENTIALS

- Use of specific signature schemes, e.g., CL, BBS(+), PS, to encode attributes and support efficient zero-knowledge proofs
- Encoding of attributes
  - Using CL/BBS/PS to sign a Pedersen commitment to attributes
  - Use efficient zero-knowledge proofs to prove statements over attributes
- First such scheme: IBM's Identity Mixer (idemix)
- Currently, a popular choice in industry is to build upon BBS(+)
- Due to the significant progress in zk-SNARKs, there is now also another option
  - Instantiate the generic template "signature + NIZK" with a zk-SNARKs and "any" signature scheme (e.g., ECDSA)

THE GENERIC APPROACH

- User obtains a signature on her ECDSA public key and a message (representation of the attributes) from an issuer
- Signature-based authentication: the user signs some challenge string
- User takes a zk-SNARK to prove that they know a valid ECDSA signature from an issuer on a user ECDSA public key AND a message (representation of the attributes) where some attributes are opened (one reveals a_i and r_i) and some are not revealed AND a second signature under the user's ECDSA key on the challenge string

THE GENERIC APPROACH

Session 1: Credentials and Signatures

Chair: Cathie Yun

EU Digital Identity and Anonymous Credentials - A Happy End?

Show abstract ›

Anja Lehmann

Media:

What Happened to the ZK Dream?

Show abstract ›

Carmit Hazay, Tarik Riviere, Muthuramakrishnan Venkitasubramaniam, Ruihan Wang

Media:

Anonymous credentials from ECDSA

Show abstract ›

Matteo Frigo, abhi shelat

Media:

Stronger Privacy for Existing Credentials

Show abstract ›

Christian Paquin, Guru Vamsi Policharla, Greg Zaverucha

Media:

Zero-knowledge Proofs for Legacy Signatures

Show abstract ›

Pui Yung Anna Woo, Chad Sharp, Paul Grubbs, Chris Peikert

Media:

https://eprint.iacr.org/2024/2010

https://eprint.iacr.org/2024/2013

https://eprint.iacr.org/2025/538

SELF-BLINDABLE ANONYMOUS CREDENTIALS

Replace explicit NIZK proofs with randomization and adaption!

Issuer

Issue Credential

$\mathsf{Sign}(\mathsf{sk}_{CA}, \mathsf{pk}_A)$

User

Show Credential

Service Provider

$\mathsf{pk}_A = (g, g^x)$

$(g, g^x),\ \mathsf{Sign}(\mathsf{sk}_{CA}, (g, g^x))$

Knowledge of μx e.g., via a signature

Switch representative using μ

$(g^\mu, g^{\mu x}),\ \mathsf{Sign}(\mathsf{sk}_{CA}, (g^\mu, g^{\mu x}))$

STATUS QUO

Lack of standardization and hardware support

- Highly-efficient ZK-credentials and self-blindable credentials
  - Require rich algebraic structure: pairings!
- **Removing pairings?**
  - Use of **keyed-verification anonymous credentials (KVACs)** (verification needs the issuer secret key), i.e., BBS-MAC or PS-MAC: use of any EC group!
  - Make KVACs publicly verifiable: BBS# (https://ia.cr/2025/619) and Server-Aided Anonymous Credentials (https://ia.cr/2025/513)
- **Generic ”zkSNARK” approach?**
  - Practical efficiency but far less efficient
  - Proving hash functions (ROs) in zk: assuming provable security of scheme (e.g., ECDSA) with concrete hash function

Provable security?

POST-QUANTUM ANONYMOUS CREDENTIALS

- Strong push towards post-quantum cryptography in industry and governments (and everywhere)
  - Strong focus on countering "**store now, decrypt later**" attacks
- Authentication primitives (like ACs) less critical than encryption
  - Also: many classical AC schemes provide **unconditional privacy**!
- But… if one considers deploying ACs now, post-quantum should be considered (”crypto-agility”)
- Do we have post-quantum ACs available?

POST-QUANTUM ANONYMOUS CREDENTIALS

A Framework for Practical Anonymous Credentials from Lattices

Jonathan Bootle
jbt@zurich.ibm.com
IBM Research Europe - Zurich, Switzerland

Vadim Lyubashevsky
vad@zurich.ibm.com
IBM Research Europe - Zurich, Switzerland

Ngoc Khanh Nguyen
khanh.nguyen@epfl.ch
EPFL, Switzerland

Alessandro Sorniotti
aso@zurich.ibm.com
IBM Research Europe - Zurich, Switzerland

Implementation of a Post-Quantum Anonymous Verifiable Credential Framework

Davide Margaria, Alessandro Pino, Andrea Vesco
Cybersecurity Research Group
LINKS Foundation
Torino, Italy
{name.surname}@linksfoundation.com

Giuseppe D'Alconzo, Antonio J. Di Scala,
Enrico Guglielmino, Carlo Sanna
Cryptography and Number Theory Group
Department of Mathematical Sciences – Politecnico di Torino
Torino, Italy
{name.surname}@polito.it

- Recent constructions of lattice-based anonymous credentials
  - Trade-offs in efficiency and recent (interactive) assumptions
  - First proof of concept implementations (e.g., LaZer Library, EU QUBIP project)
- Alternative hardness assumptions?
  - Lack of rich algebraic structure
  - From some assumption families we have blind signatures
    - Going to ACs (even single-use) requires adding attributes (suitable commitments and ZK proofs) – non-trivial!
- Use of generic "signature + zk-SNARK" template?
  - Proving hash functions inside zk-SNARK circuit, recursive zk-SNARKs (for SNARK-based signatures)
  - Use of SNARK-friendly hashing (e.g., zkDilithium: https://eprint.iacr.org/2023/414)

CONCLUSIONS

- Currently enrolled identity solutions typically provide very weak privacy protection
- Anonymous credentials are the right tool, well understood and still very active in the research community
- Unfortunately, they have not seem widespread deployment for many years
- In recent years we see a growing interest from the industry (and governments)
- Current trend is to engineer them to be compatible with “legacy cryptography” (mostly ECDSA and deployed EC groups)
- To complete the post-quantum picture, a lot of research is still required!

der Bundeswehr
Universität München

@drl3c7er.bsky.social

https://www.unibw.de/crypto-en | https://danielslamanig.info

FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München