SFB 901

ON - THE - FLY COMPUTING

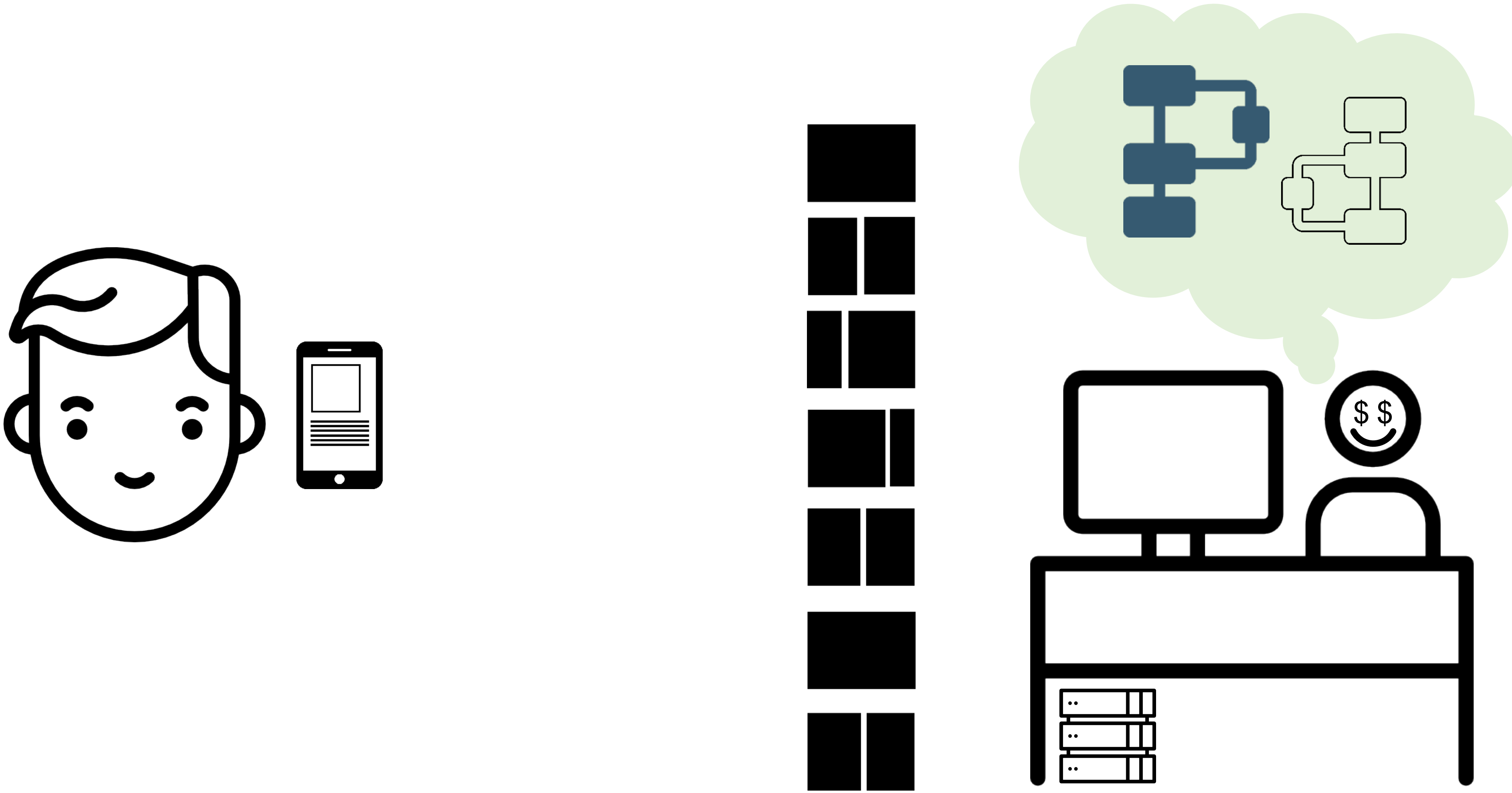
Expressive practical credential systems from standard techniques

CRC 901 - C1

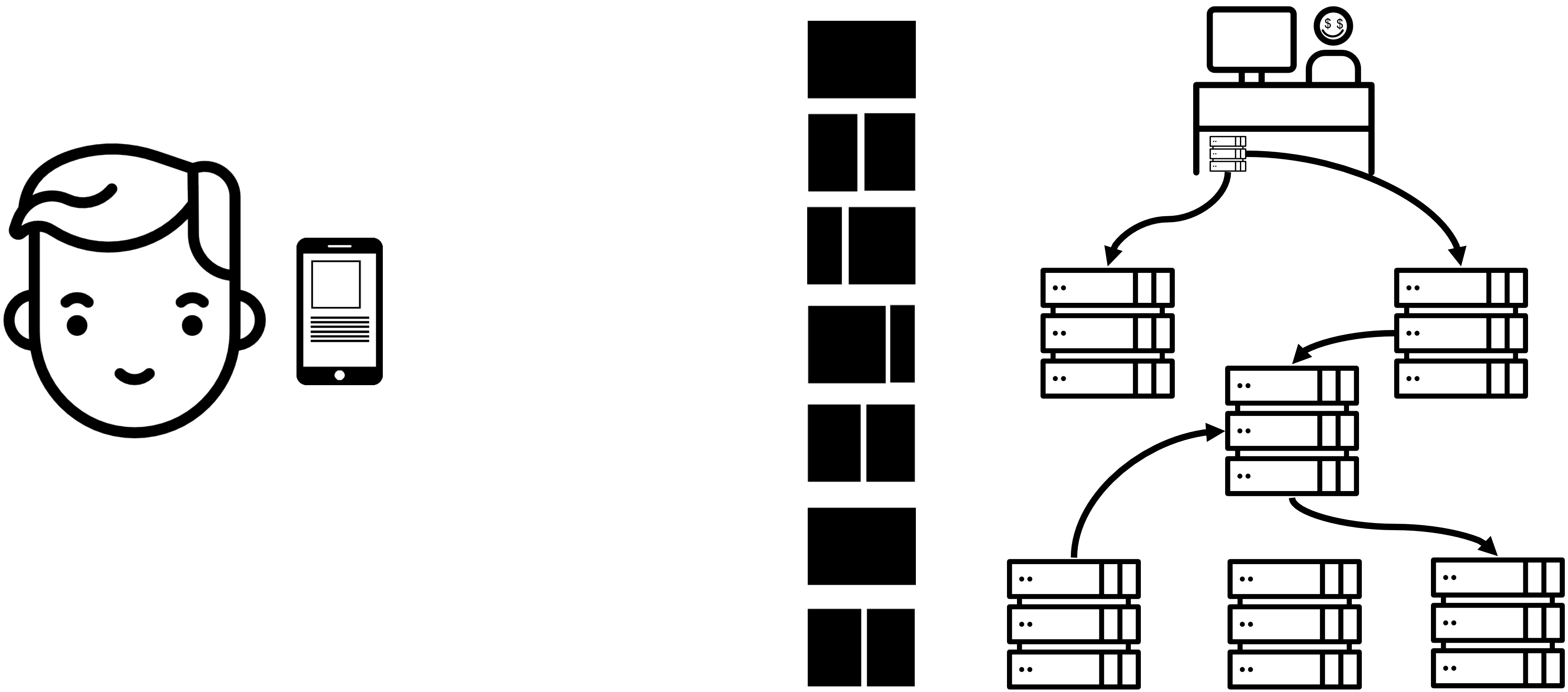
Research Group Codes & Cryptography

Fabian Eidens, Jan Bobolz

Without Credentials



Without Credentials

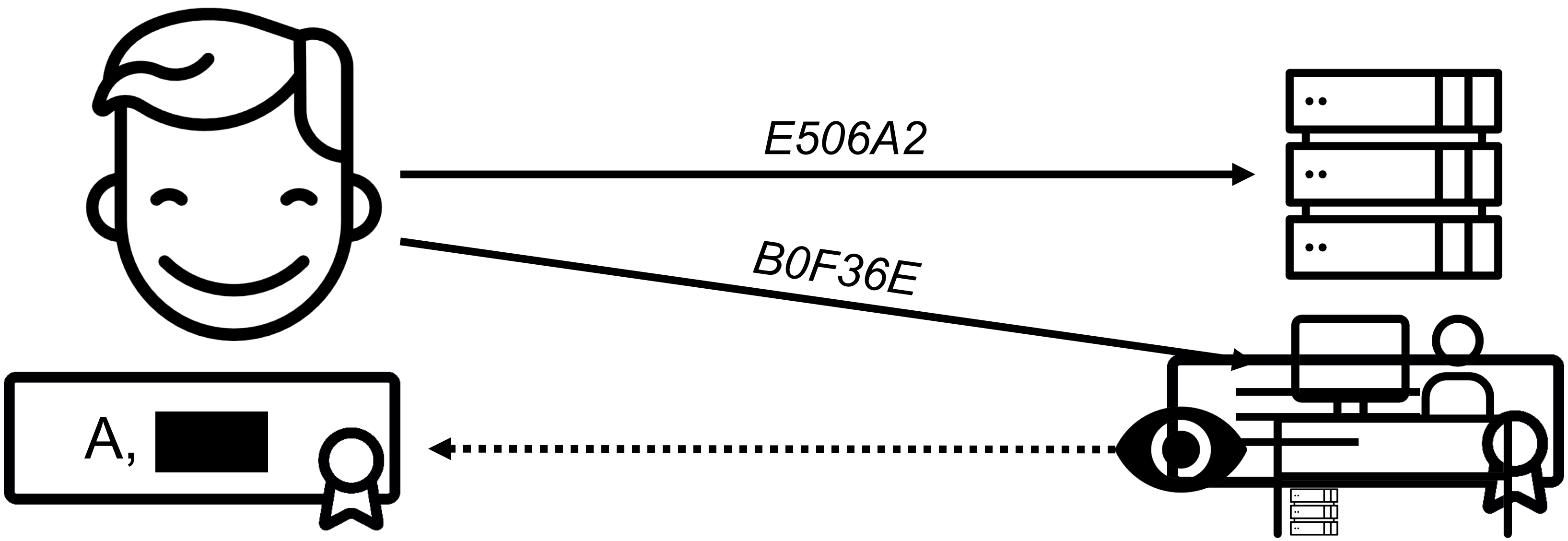


Goals

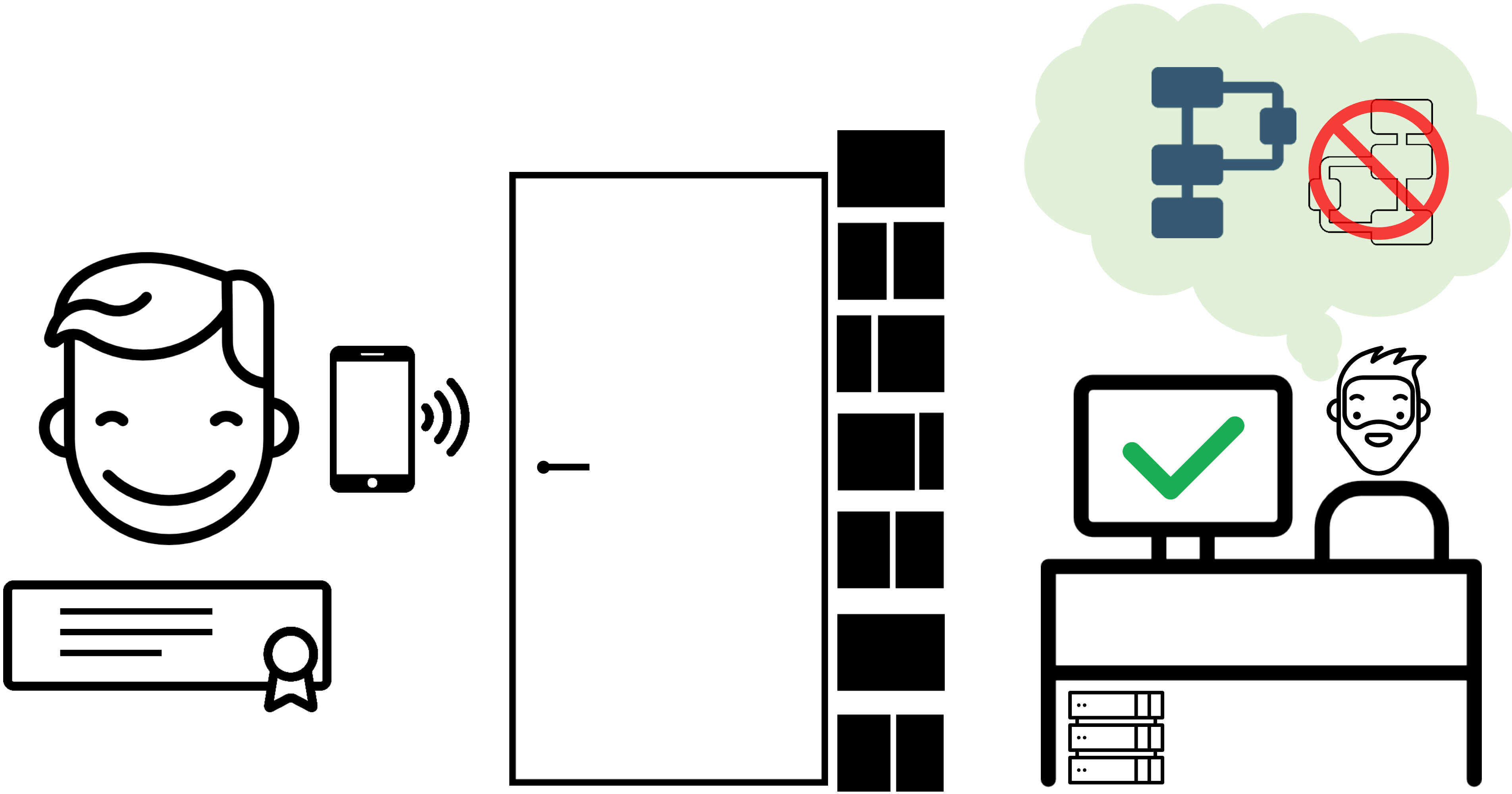
- Anonymity (unlinkability)
- **Some** information flow
  - Anonymity without information flow: trivial
  - Enables business models
- Selective disclosure of information
  - User is in control
  - Only shows what is necessary

Anonymous Credential Systems

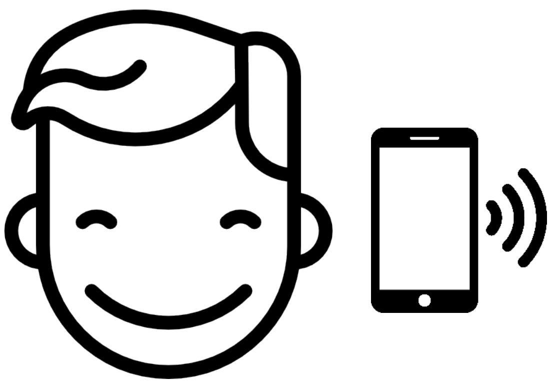
- Users have **pseudonyms**
- Organizations issue users **credentials**
- Credentials certify **attributes**
- Attributes can be selectively **shown** to other organizations
  - User chooses what to share

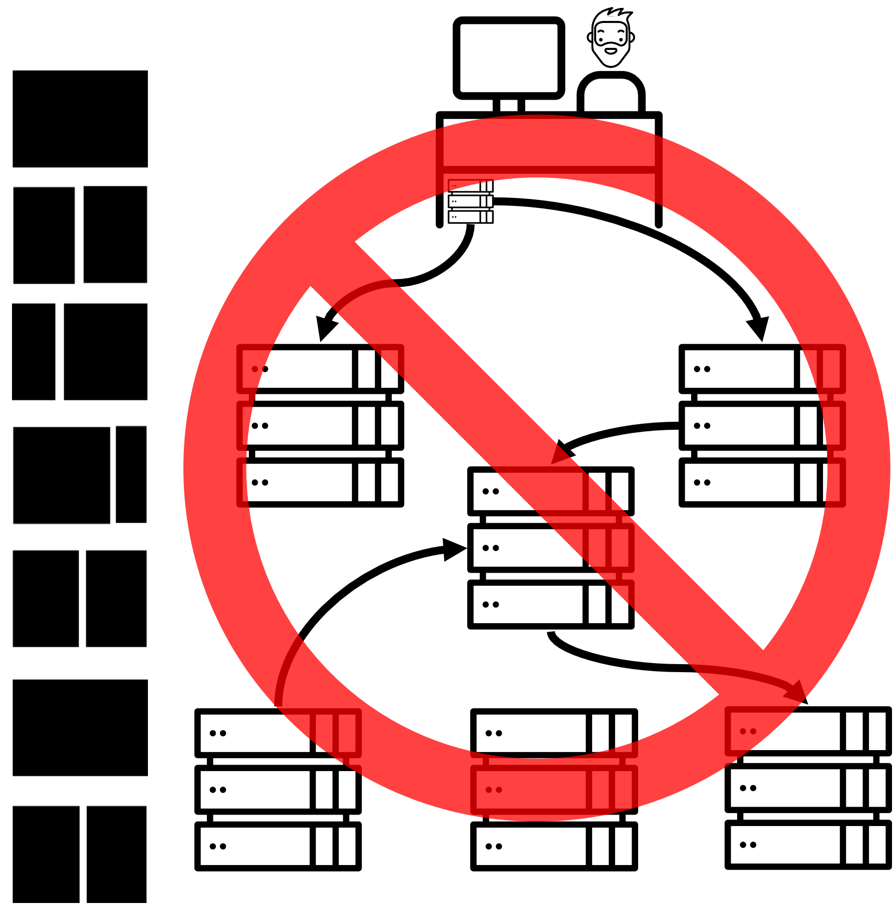


With Credentials



Without Credentials

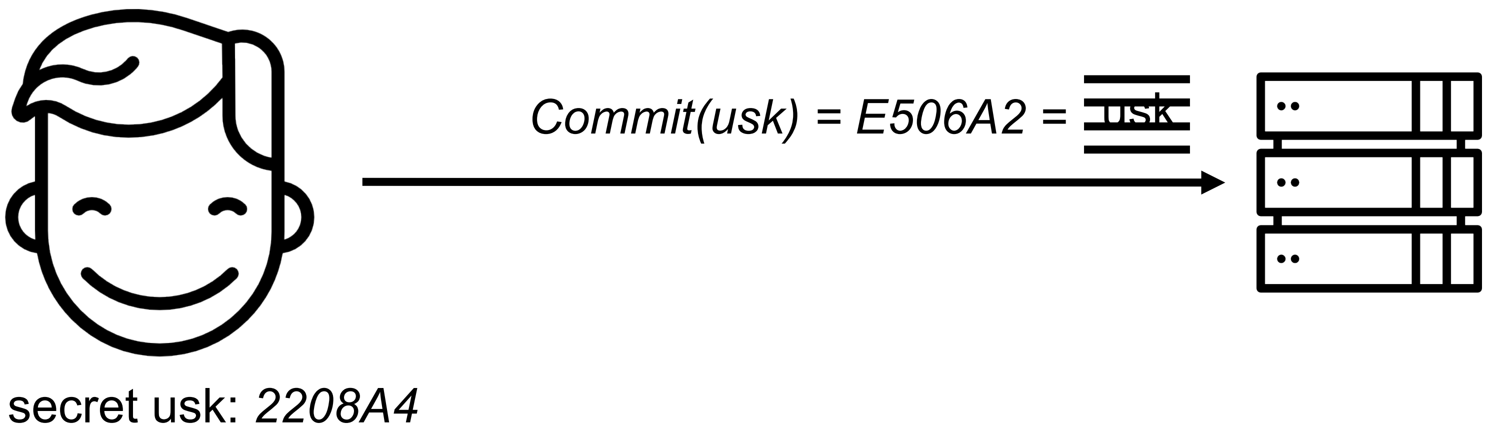




Construction

- Protocol to establish pseudonyms
- Protocol to issue credentials
- Protocol to show credentials

Pseudonym



- **Should** be something to bind credentials to
  - Goal: Issued credentials should only work for one user
- **Should not** reveal information about identity
- Idea: **commitment** to user secret

Construction

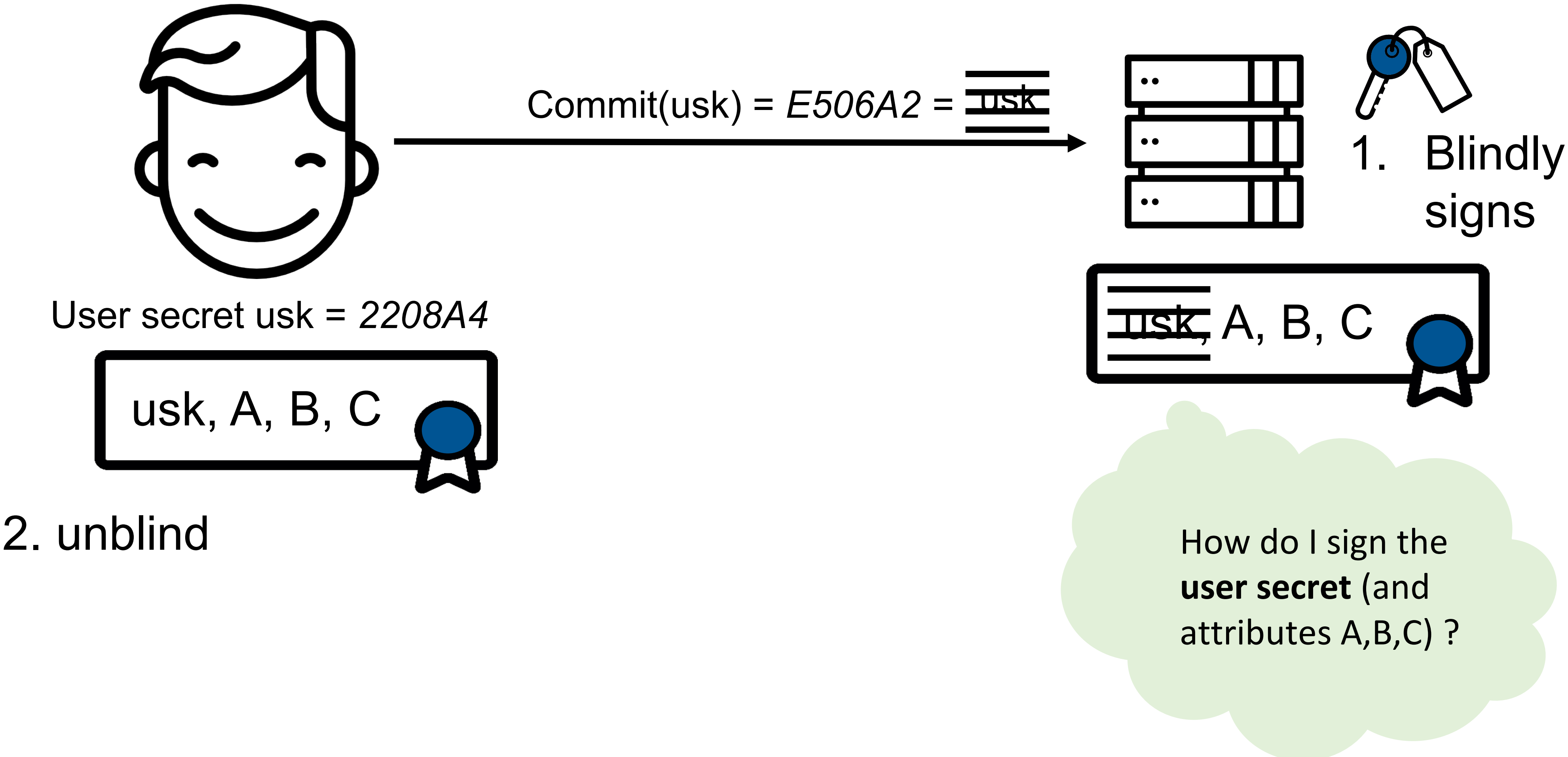
- Protocol to establish pseudonyms
- **Protocol to issue credentials**
- Protocol to show credentials

Credential

- Should be **bound** to a specific **organization**
  - It matters *who* issued an attribute
- Should be **bound** to a specific **user**
- Should **not** be computable by user himself
- Should be **verifiable** by other organizations

- Idea: **signature** on attributes and user secret
  - Private key only known to issuing organization
  - Public key used to verify validity of credential
  - *Including the user secret prohibits handing credentials to other users*

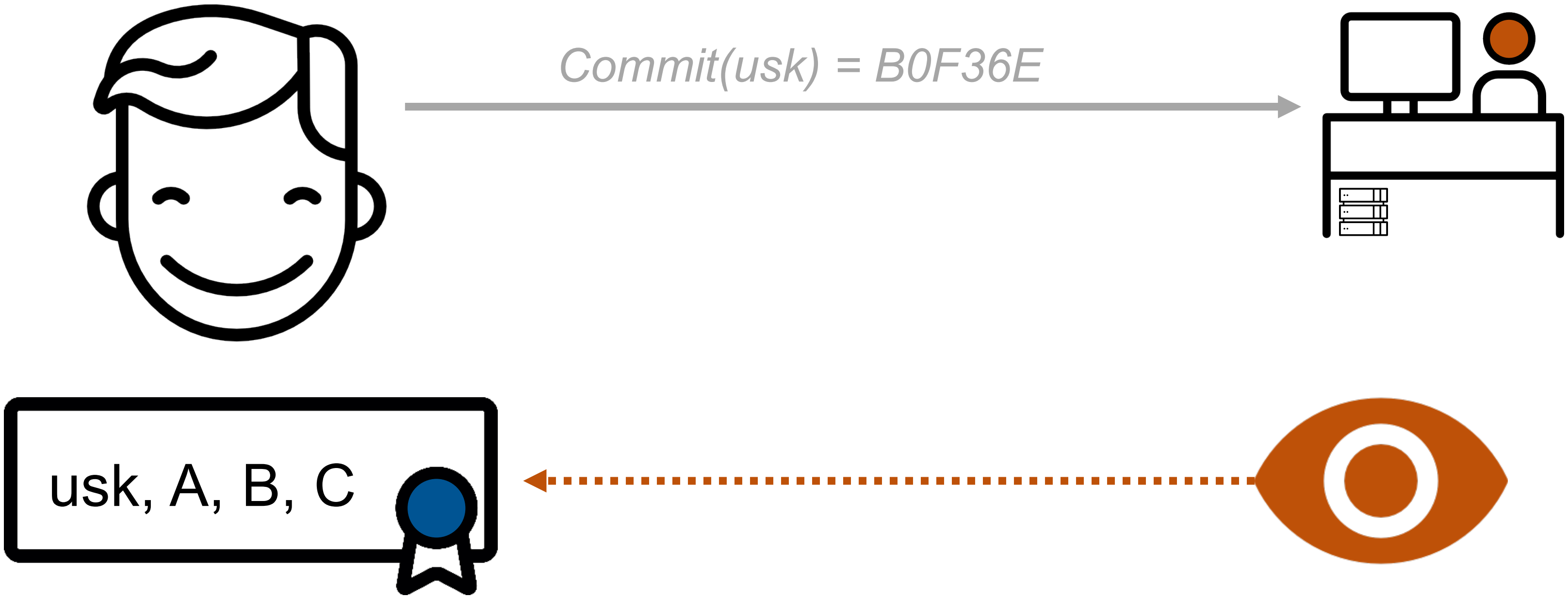
Problem: signing the user secret



Construction

- Protocol to establish pseudonyms
- Protocol to issue credentials
- **Protocol to show credentials**

Showing credentials



We have to **hide** from organization:

- User secret
- Some attributes, e.g. C
- The signature

Showing credentials

Solution:
Zero-knowledge proof of knowledge:

I have a **signature** on a **message „*usk, X,Y,Z*“** such that:

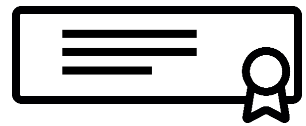
- *usk* is consistent with my pseudonym (commitment)
- *X* = A
- *Y* = B
- *Z* is anything

Construction

- Protocol to establish pseudonyms ➡ Anonymity & bind credentials to user
- Protocol to issue credentials ➡ Unforgeability
- Protocol to show credentials ➡ Unlinkability and selective disclosure

Accomplished Goals:

1. Somebody should certify my information
   - Sign attributes - **Signature Schemes**



2. Certification should work on pseudonyms
   - Blind signature on commitment to user secret - **Two-Party Computation**
3. Want to show credentials anonymously, but also want to get something done
   - Interactive protocol between user and organization
   - Selective disclosure - **Zero-Knowledge Proof of Knowledge Protocols**

Concrete Construction

- Signature scheme: Pointcheval & Sanders (2016)
  - Short, randomizable, efficient protocols
  - Large message (attribute) space, signs $(m_1, \dots, m_n) \in \mathbb{Z}_p^n$

Keys: $pk = (\tilde{g}^x, (\tilde{g}^{y_i})_{i=1}^n),\ sk = (x, (y_i)_{i=1}^n)$

Sign: $\sigma = \left(h, h^{x+\sum m_i y_i}\right)$

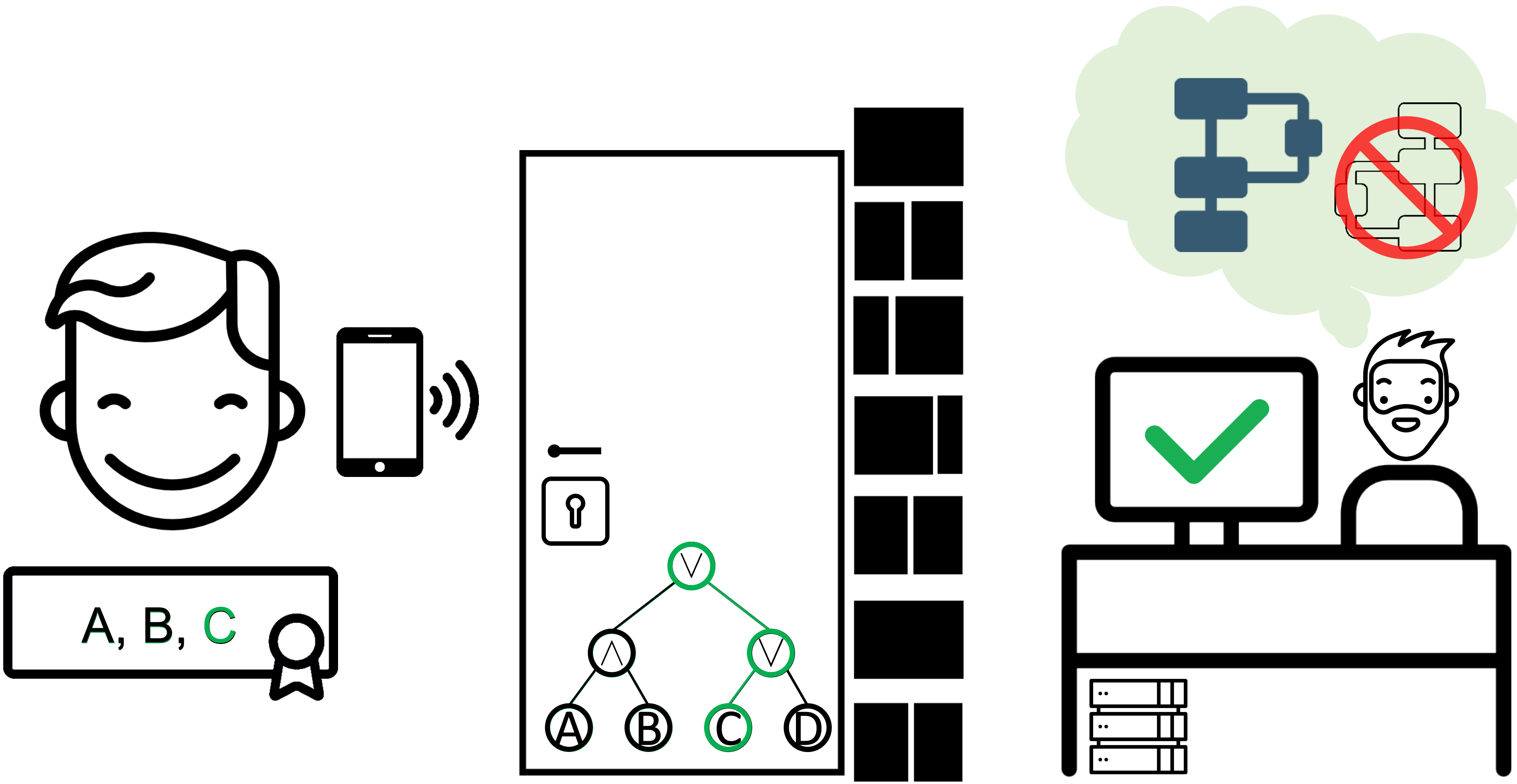
Verify: $e(h, \tilde{g}^x \cdot \prod (\tilde{g}^y)^{m_i}) = e\left(h^{x+\sum m_i y_i}, \tilde{g}\right)$

  - They show:
    - establish pseudonyms: Pedersen commitment on usk.
    - issue credentials: signing committed value (their paper).
    - show credentials: prove knowledge of a signature, revealing a subset of attributes (their paper).

+ secure Credential System (using a generic result by Lysyanskaya (PhD thesis))

We add: extensions for Boolean formulas

Extensions for Boolean formulas



Extensions for Boolean formulas

Theorem

Let Φ denote a Boolean formula over atomic statements in the form "$m_i = c_i$", $\Pi = (\mathrm{KeyGen}, \mathrm{Sign}, \mathrm{Vrfy})$ a EUF-CMA secure signature scheme, where $pk \leftarrow KeyGen(1^\lambda)$, σ signature on messages/attributes $m_1, \dots, m_n$

There exists a four-round concurrent zero-knowledge proof of knowledge protocol for the relation

$$\left\{ \left((pk, \Phi),\ (\sigma, m_1, \dots, m_n) \right) \mid \mathrm{Vrfy}_{pk}\left(\sigma, (m_1, \dots, m_n)\right) \wedge \Phi(m_1, \dots, m_n) = \mathrm{true} \right\}$$

Furthermore, the protocol has $O(n + |\Phi|)$ communication complexity (with reasonable constants)

Theorem goes back to R. Cramer, I. Damgaard, and B. Schoenmakers

Techniques used:

- Equality and inequality proofs over attribute statements (to handle any negation)
- Protocol composition through secret sharing (to handle $\wedge$ and $\vee$)
- Damgård technique (to make protocol concurrent zero-knowledge)

What we are working on

- Extending „bare-bones“ credential systems
  - Publications typically don‘t include desirable features for practice
- Delegatable credentials
- Efficient protocols for showings with predicates
  - Arbitrary Boolean formulas over attribute values
  - Circuits satisfiability of attributes
- Practical design decisions
  - Simple predicates; use **one** signature **per** attribute
  - Complex predicates; use one signature for **all** attributes

Questions

… please visit our poster C1

Thanks to my colleagues

References

- Anna Lysyanskaya. Signature schemes and applications to cryptographic protocol design. PhD thesis, Massachusetts Institute of Technology, 2002
- Pointcheval and Sanders. Short randomizable signatures. In Topics in Cryptology - CT-RSA, Springer, 2016
- R. Cramer, I. Damgaard, and B. Schoenmakers, “Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols.”