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

C1: Robustness and Security
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

**Anonymous Credential Systems**

- **A, B, C**
- **C1: Robustness and Security**
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

User secret usk: 2208A4

\[
\text{Commit(usk)} = E506A2 = \text{usk}
\]
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

1. Blindly signs

User secret usk = 2208A4

2. unblind

How do I sign the user secret (and attributes A,B,C)?
Construction

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

Commit(usk) = B0F36E

usk, A, B, C

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 $(m_1, \ldots, m_n) \in \mathbb{Z}_p^n$

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).

Keys: $pk = (\tilde{g}^x, (\tilde{g}^y)_i^n), \ sk = (x, (y_i)_i^n)$

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

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

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

We add: extensions for Boolean formulas
Extensions for Boolean formulas

C1: Robustness and Security

A, B, C

∧

∨
Extensions for Boolean formulas

Theorem

Let \( \Phi \) denote a Boolean formula over atomic statements in the form “\( m_i = c_i \)”, \( \Pi = (\text{KeyGen}, \text{Sign}, \text{Vrfy}) \) a EUF-CMA secure signature scheme, where \( pk \leftarrow \text{KeyGen}(1^\lambda) \), \( \sigma \) signature on messages/attributes \( m_1, \ldots, m_n \)

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

\[
\{ ((pk, \Phi), (\sigma, m_1, \ldots, m_n)) | \text{Vrfy}_{pk}(\sigma, (m_1, \ldots, m_n)) \land \Phi(m_1, \ldots, m_n) = \text{true} \}
\]

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 \( \land \) and \( \lor \))
- 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