A BETTER WAY

Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya. Compact Eypobtaining a signature on a committed value i.e. protocol between Client and Signer

Signature schemes with efficient protocols for realized under the Strong RSA assumption [L02,CL02]

Prove to me that you have


GoAL: limit the information transmitted in each transaction to a bare minimum without compromising its authenticity.

THE OLD WAY

I need access to SLAM

Jan Camenisch, Anna Lysyanskaya (http://www.cs.brown.edu/~anna)

A BETTER WAY

I need access to SLAM

Let me check that you have a valid subscription. Who are you?

Our Progress

- Signature schemes with efficient protocols for (1) obtaining a signature on a committed value, i.e. protocol between Client and Signer common input: Signer’s PK and C = Commit(x,r) (e.g. Pedersen commitment g^x mod p)
  - defined and first realized in [L02,CL02]
  - realized under the Strong RSA assumption [L02,CL02]
  - alternative, more efficient constructions based on the LDSW or on the SDH assumptions in groups with bilinear maps [CLO4, cited as (8) below]
- non-interactive provably secure construction [BCKL08, cited as (2) below]
- applied to obtain compact e-cash (wast a long-standing open problem) [CHLO05, cited as (7) below] and uncloneable group identification [CHLMO06, cited as (4) below]
- implemented (IBM); adopted by TCG (part of direct anonymous attestation)

Prior Work

The theory: a lot (not everything) can be done in principle, but not very efficiently

Zero-knowledge proofs [GM88, BCC88, GMW86, ...]

Multi-party computation [Yao84, GMW87, CDD88, BGGW88, ...]

More efficient schemes for concrete applications:

- anonymous credentials [Chaum85, ..., Brands99, LRSW99, CL01a, CL01b]: PI’s prior work
group signatures [GNS98, CS97, ..., ACTJT00, BMW03], blind signatures [Cha81, ..., Brands99]

- General framework: possession of a signature/credential implies possession of a secret key allowing one to issue further credentials [CLO6, cited as (5) below]
  - we actually solved a more general problem: we defined and realized, for the first time, the general signature of knowledge primitive
  - this yields the first delegatable anonymous credential system
  - also gave an efficient delegatable anonymous credential system [1]

- Other privacy-preserving tools:
  - a formal treatment of onion routing: the first definition of security and a provably secure public-key scheme satisfying the definition [CLO5, cited as (6) below]; onion routing is the best known way of achieving anonymous channels in practice
  - mercurial commitments and zero-knowledge proofs [CHLMR05]
  - hierarchical identity-based encryption for multi-dimensional hierarchies (VFDD04); hierarchical identity-based encryption where the sender need not know the details of the hierarchy.

This Work

Making this a reality: practical and provably secure tools to build systems that allow authentication without identification.

More concretely: Developing the security requirements of the primitives for such systems and realizing these primitives efficiently.

Selected Publications