

CAREER: Efficient Cryptographic Protocols for Secure and Private Electronic Transactions



Anna Lysyanskaya (<http://www.cs.brown.edu/~anna>)

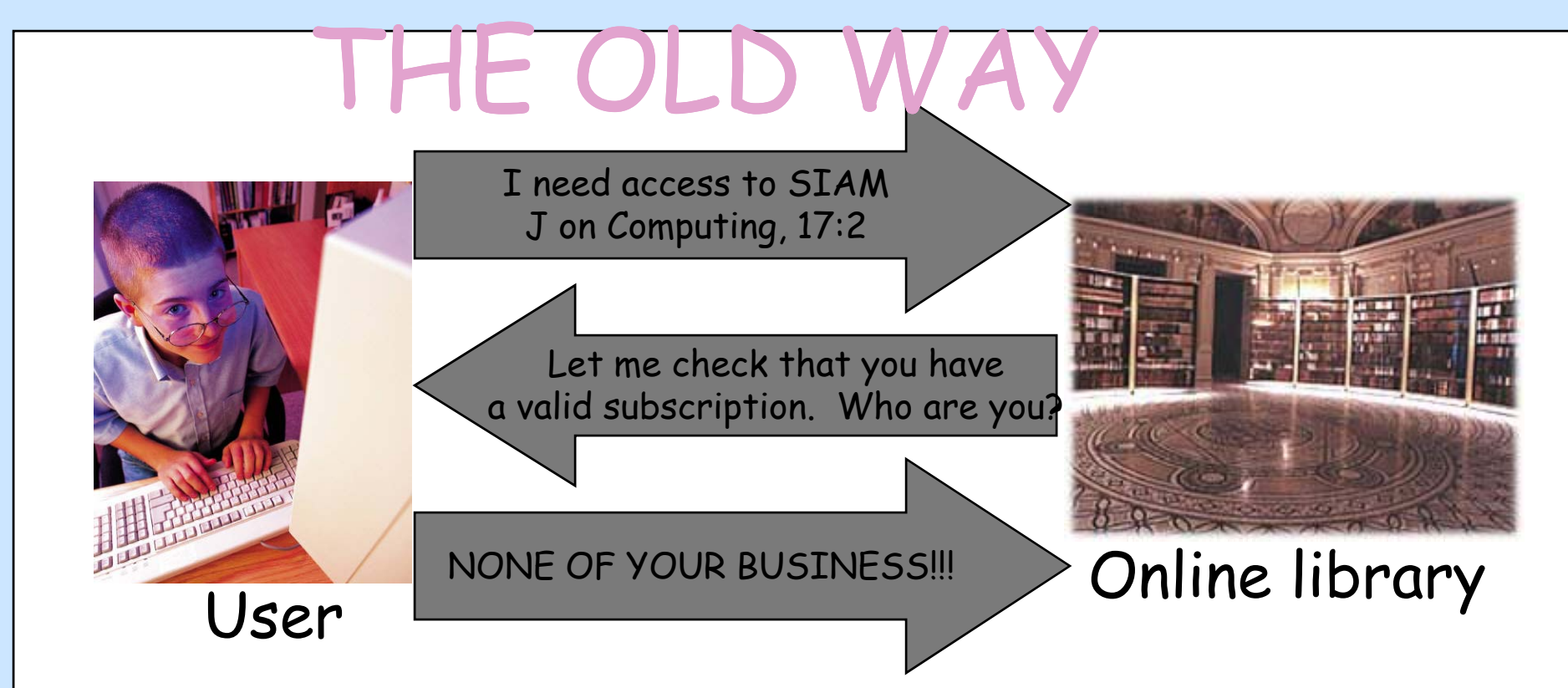
AUTHENTICATION WITHOUT IDENTIFICATION

A typical computer user performs a multitude of electronic transactions each day. Each of them must be

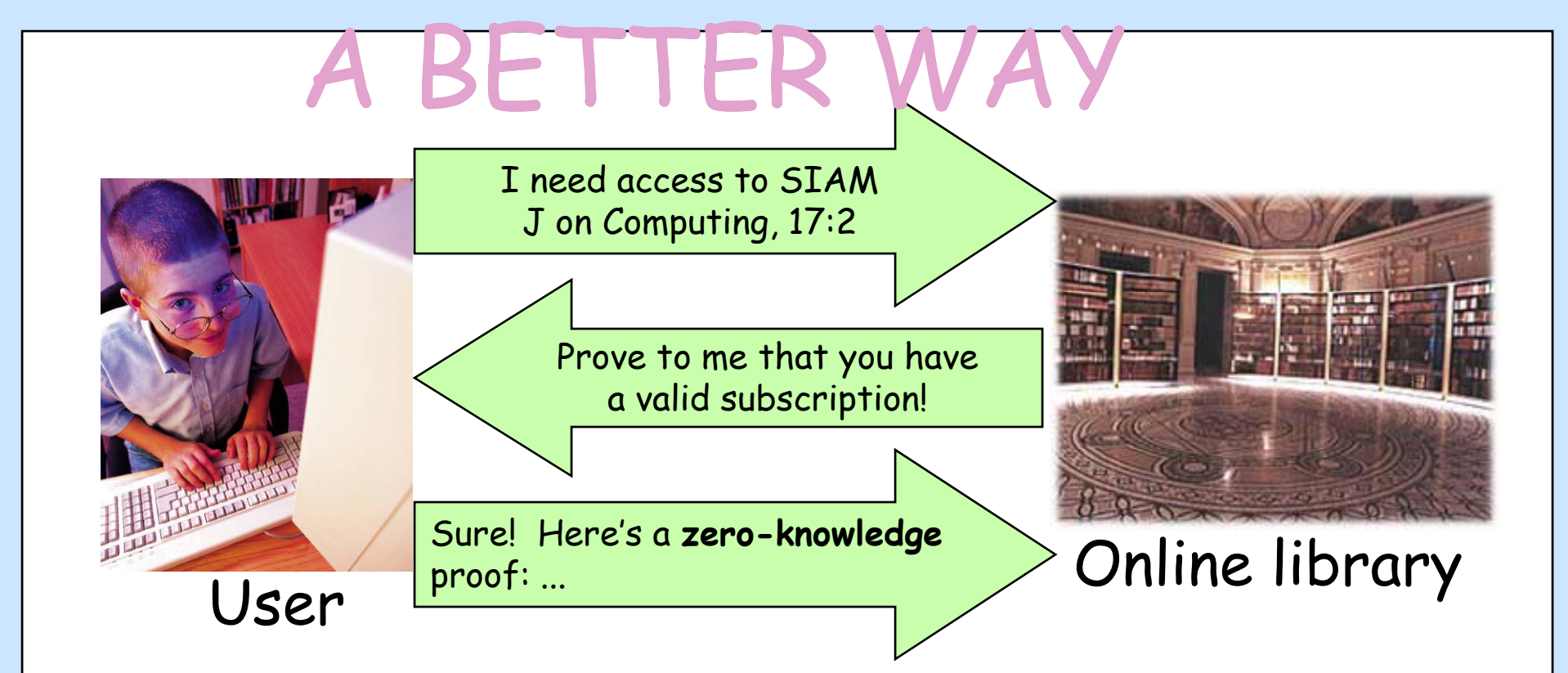
secure: it should be carried out by authorized users only, and the information entered must be authentic

private: personal information or account balances should not become available without a user's explicit consent

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



VS.



Prior Work

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

Zero-knowledge proofs [GMR88,BCC88,GMW86,...]
Multi-party computation [Yao84,GMW87,CCD88,BGW88,...]

More efficient schemes for concrete applications:

anonymous credentials [Chaum85,...,Brands99,LRSW99, CLO1a,CLO1b]: PI's prior work
group signatures [CvH91,...,CS97,...,ACJT00,BMW03], blind signatures [Cha81,...,Brands99]

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.

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 $C = \text{Commit}(x,r)$ (e.g. Pedersen commitment $g^x h^r$)
client's private input: (x,r) ; signer's private input: sk
client's private output: $\sigma = \text{spk}(x)$; signer's private output: \perp
 - (2) proving that a committed value is signed, i.e. protocol between Client and Verifier
common input: Signer's PK and $C = \text{Commit}(x,r)$
client's private input: (x,r,σ)
verifier's output: $\text{Verify}(PK,x,\sigma)$ (just that one bit of information)
- defined and first realized in [L02,CLO2]
- realized under the Strong RSA assumption [L02,CLO2]
- alternative, more efficient constructions based on the LRSW or on the SDH assumptions in groups with bilinear maps [CLO4, cited as (8) below]
- non-interactive provably secure construction [BCKLO8, cited as (2) below]
- applied to obtain compact e-cash (was a long-standing open problem) [CHLO5, cited as (7) below] and uncloneable group identification [CHKLM06, cited as (4) below]
- implemented (IBM); adopted by TCG (part of direct anonymous attestation)
- 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 sets [CHLMR05]
 - hierarchical identity-based encryption for multi-dimensional hierarchies [YFDL04]: hierarchical identity-based encryption where the sender need not know the details of the hierarchy.

Selected Publications

1. Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, Hovav Shacham. "Delegatable Anonymous Credentials."
2. Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya. "Non-interactive Anonymous Credentials." TCC 2008.
3. Melissa Chase, Anna Lysyanskaya. "Simulatable VRFs and Applications to NIZK." Crypto 2007.
4. Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, Maria Meyerovich. "How to Win the Clone Wars." ACM CCS 2006.
5. Melissa Chase, Anna Lysyanskaya. "On Signatures of Knowledge." Crypto 2006.
6. Jan Camenisch, Anna Lysyanskaya. "A Formal Treatment of Onion Routing." Crypto 2005.
7. Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya. "Compact E-Cash." Eurocrypt 2005.
8. Jan Camenisch, Anna Lysyanskaya. "Signature Schemes and Anonymous Credentials from Bilinear Maps." Crypto 2004