Empowering Anonymity:
Delegatable Anonymous Credentials

PI: Anna Lysyanskaya, www.cs.brown.edu/~anna

Anonymous credentials still reveal the identity of the issuer.

Example: Anonymous user Alice proves that she is an undergraduate student at Brown. We learn that she goes to Brown, but not who she is.

That info alone may be sufficient to discover the identity of a user!

Example: Alice has a student cred from Brown, and an over-21 cred from her home town. But she is the only one at Brown from her town!

In a delegatable anonymous credential (DelCred) system, we don't learn Alice's university or home town. Moreover, Alice can anonymously delegate her credentials.

Participants in a DelCred system: root authorities (e.g., college accreditation agencies and state governments), and users (Brown University, Alice's home town, Alice herself).
What participants do: anonymously obtain credentials from root authorities, anonymously delegate credentials to other users, anonymously prove possession of credentials.
Security guarantees: unforgeability – underlying (hidden) identity still well-defined, can't use a cred you don't have; anonymity – don't reveal any info when delegating/proving possession of credentials.

What was known:

- DelCreds for long delegation chains from Groth-Sahai NIZK proofs and structure-preserving sigs [BCCKLS09,CKLM14]
- DelCreds for short chains from general assumptions [CL06]

What is needed:

- Direct constructions that don't rely on NIZK
- Incorporating credential attributes, conditional anonymity, revocation
- Modular constructions from signature schemes with the "right" properties

Our results so far:

- New building block: a mercurial signature [CL17]
  - given σ on m under pk, can transform it into σ' on m' under pk'
  - where $(m,m') \in R_m$, and $(pk,pk') \in R_{pk}$ for equiv relations R_m, R_{pk}
- Merc sig construction in Type III generic group model [CL17]
- Merc sig => DelCred [CL17]
  - if cannot efficiently test membership in R_m, R_{pk}, and signature has structure-preserving properties, allows to "blind" an authorization chain, lending itself to DelCred
- Lends itself to attributes [CL17a]
- New results on revocation of anonymous credentials [BCDLRSY17]

Bibliography

[BCCKLS09] Belenkiy, Camenisch, Chase, Kohlweiss, Lysyanskaya, Shacham. "Randomizable proofs and delegatable anonymous credentials." CRYPTO 2009.
[BCDLRSY17] Baldimtsi, Camenisch, Dubovitskaya, Lysyanskaya, Reyzin, Samelin, Yakubov. "Accumulators with applications to anonymity-preserving revocation." Euro S&P 2017, to appear.
[CKLM14] Chase, Kohlweiss, Lysyanskaya, Meiklejohn. "Malleable signatures: new definitions and delegatable anonymous credentials." CSF 2014.
[CL06] Chase, Lysyanskaya. "On signatures of knowledge." CRYPTO 2006.
[CL17] Crites, Lysyanskaya. "Delegatable anonymous credentials from mercurial signatures." Manuscript in submission.
[CL17a] Crites, Lysyanskaya. "A direct construction of delegatable anonymous credentials with attributes." Manuscript in progress.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

Brown University