Eurocrypt 2012: April 15th - 19th : Cambridge, United Kingdom

U-Prove Revocation with Accumulators

Lan Nguyen

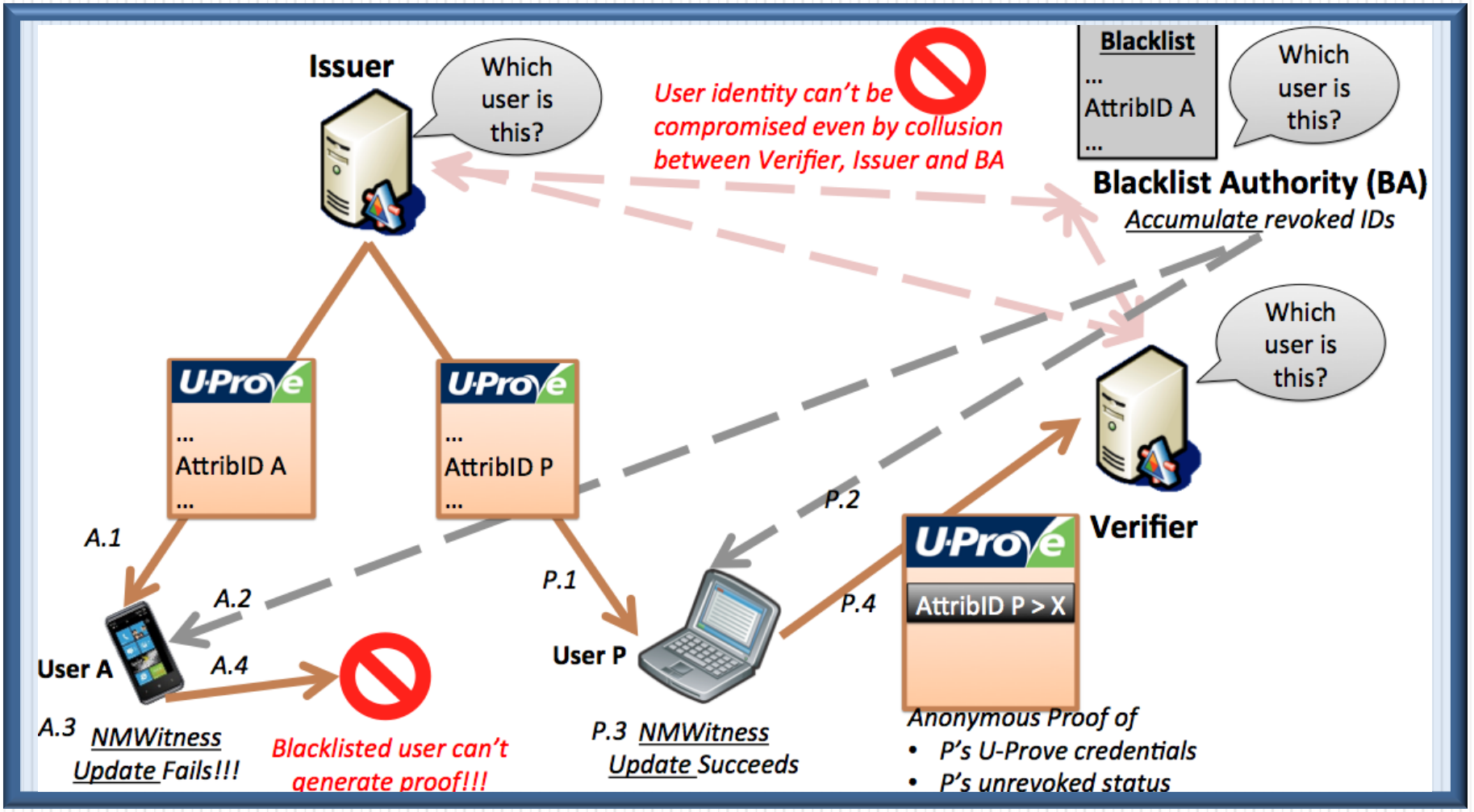
Sherman Chow

Microsoft Research

University of Waterloo

Presentation at Rump Session

Revocation in U-Prove



Accumulator and Blacklisting

- *Aggregate* a set of (blacklisted) elements into a single accumulated value *V*
- *Non-Member (NM) Witness Proof* for proving that *x* is NOT accumulated in *V* (not blacklisted) without revealing *x* (privacy protection)
- *Updates* of *V* and Proofs' Witnesses when the accumulated set changes

(Our) Accumulator's Advantages

- O(1) cost to generate/verify credential proofs
- Only the Verifier needs to compute 2 pairings
- All exponentiations in G_T are moved to G_1
- Crypto agility