Jan Camenisch

jca@zurich.ibm.com
ibm.biz/jancamenisch
@JanCamenisch

Cryptographic e-Cash

Tuesday, May 31 2016, 9:30-11

In this lecture we will discuss how “traditional” e-cash is built. To this end, we review zero-knowledge proofs for discrete logarithms (often call generalized Schnorr protocols) and signature schemes that work well the such zero-knowledge protocols. We then show how these two building blocks can be combined to construct an e-cash scheme that support privacy.

Reading:

- A signature scheme with efficient protocols, Jan Camenisch and Anna Lysyanskaya, In Security in Communication Networks, 2002.
- On the portability of generalized Schnorr proofs, Jan Camenisch, Aggelos Kiayias, and Moti Yung. In Eurocrypt 2009.