Ferradi, Houda; **Géraud, Rémi**; **Naccache, David**

Slow motion zero knowledge identifying with colliding commitments. (English) Zbl 1409.94872

Lin, Dongdai (ed.) et al., Information security and cryptology. 11th international conference, Inscrypt 2015, Beijing, China, November 1–3, 2015. Revised selected papers. Cham: Springer. Lect. Notes Comput. Sci. 9589, 381-396 (2016).

Summary: Discrete-logarithm authentication protocols are known to present two interesting features: the first is that the prover's commitment, $x = g^r$, claims most of the prover's computational effort. The second is that x does not depend on the challenge and can hence be computed in advance. Provers exploit this feature by pre-loading (or pre-computing) ready to use commitment pairs r_i, x_i. The r_i can be derived from a common seed but storing each x_i still requires 160 to 256 bits when implementing DSA or Schnorr.

This paper proposes a new concept called slow motion zero-knowledge (SM-ZK). SM-ZK allows the prover to slash commitment size (by a factor of 4 to 6) by combining classical zero-knowledge and a timing channel. We pay the conceptual price of requiring the ability to measure time but, in exchange, obtain communication-efficient protocols.

For the entire collection see [Zbl 1337.94003].

MSC:

94A60 Cryptography

Full Text: DOI