Ringers, Sietse; Verheul, Eric; Hoepman, Jaap-Henk

An efficient self-blindable attribute-based credential scheme. (English) [Zbl 1457.94176]


Summary: An attribute-based credential scheme allows a user, given a set of attributes, to prove ownership of these attributes to a verifier, voluntarily disclosing some of them while keeping the others secret. A number of such schemes exist, of which some additionally provide unlinkability: that is, when the same attributes were disclosed in two transactions, it is not possible to tell if one and the same or two different credentials were involved. Recently full-fledged implementations of such schemes on smart cards have emerged; however, these need to compromise the security level to achieve reasonable transaction speeds. In this paper we present a new unlinkable attribute-based credential scheme with a full security proof, using a known hardness assumption in the standard model. Defined on elliptic curves, the scheme involves bilinear pairings but only on the verifier’s side, making it very efficient both in terms of speed and size on the user’s side.

For the entire collection see [Zbl 1422.94003].

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing
14G50 Applications to coding theory and cryptography of arithmetic geometry

Keywords:
attribute-based credentials; unlinkable; self-blindable; elliptic curves; bilinear pairings

Full Text: DOI