SUMIN LEEM, University of Calgary

Cryptographic pairings and applications

Cryptographic pairings are bilinear, non-degenerate and computable maps, defined on elliptic or hyperelliptic curves. The primary application of a pairing is to enable tri-partite key exchange, but there are other useful and unique applications. Pairings can also be used for the remote secure authentication of authorized users using short space-efficient digital signatures. Pairings also have an important role in realizing ID-based cryptography, which uses a user's ID as a compact and user-friendly public encryption key. In this talk, we first introduce properties and some examples of pairings. We then discuss applications of pairings mentioned above.