CORR 2001-14

Cryptanalysis of the Sakazaki-Okamoto-Mambo ID-based Key Distribution system over Elliptic Curves (Extended abstract)

Minghua Qu*, Doug Stinson, Scott Vanstone

Abstract In 1997, H. Sakazaki, E. Okamoto and M. Mambo [6] proposed an ID-based key distribution system on an elliptic curve over $\mathbb{Z}_n$. We will cryptanalyze the scheme and demonstrate that when the hashed ID length is about 160 bits, the scheme is insecure. To be specific, after requesting a small number of keys from the Center, our attack allows a new valid key to be constructed without any further interaction with the Center.