Published in W. Fischer and J.-M. Schmidt, Eds, *Fault Diagnosis and Tolerance in Cryptography (FDTC 2013)*, p. 73, IEEE Computer Society, 2013.

Elliptic Curve Cryptosystems in the Presence of Faults

(Invited Talk)

Marc Joye
Technicolor
Cesson-Sévigné, France
Email: marc.joye@technicolor.com

Abstract

Elliptic curve cryptography was introduced in the mid 1980s as a promising alternative for cryptographic protocols based on the discrete logarithm problem in the multiplicative group of a finite field (e.g., Diffie-Hellman key exchange or ElGamal encryption/signature). The security of elliptic curve cryptosystems relies on the hardness of solving the elliptic curve discrete logarithm problem (ECDLP).

However, there is no need to make use of strong cryptographic techniques if they are poorly implemented. This talk surveys various fault attacks against elliptic curve cryptosystems. It also presents a number of countermeasures developed so far as well as new ones by exploiting the rich underlying mathematical structure. Finally, several research problems are listed.