Differential Analysis Attacks and Countermeasures in Elliptic Curve Cryptography

Tiawna Cayton
tlcayton2@cs.ucsb.edu
University of California, Santa Barbara

Abstract

Differential power analysis can be a powerful tool against the security of cryptographic implementations. Since the introduction of such attacks, much research has been done to examine these attacks as well as ways to thwart them. In this paper we will specifically look at attacks on implementations of elliptic curve cryptography. We will explore what DPA attacks look like on EC Diffie-Hellman key exchange as well as other EC implementations. We will then examine countermeasures that can be implemented to protect against such attacks and explore several of these countermeasures including algebraic approaches as well as varying methods of implementation.

References

[1] Marc Joye and Cristophe Tymen. *Protections Against Differential Analysis for Elliptic Curve Cryptography - An Algebraic Approach.*, CHES (2001). DOI:10.1007/3-540-44709-1_31.

[2] Jean-SÃľbastien Coron. *Resistance Against Differential Power Analysis For Elliptic Curve Cryptosystems.* CHES (1999) DOI: 10.1007/3-540-48059-5_25.