ANWAR HASAN, University of Waterloo

Resisting Fault Analysis Attacks on ECC via Repeated and Parallel Computations

In cryptographic systems, faults can occur naturally and/or due to some malicious acts of an attacker. In the past, researchers showed how an attacker could exploit computational errors to break some popular crypto-systems. This has made the task of verification of the correctness of cryptographic computations quite important. In some applications, further robustness in term of the ability to continue performing correct computations in presence of certain faults is also sought.

In elliptic curve cryptography, a well-known technique to detect errors in its group operation is to verify whether or not the operation output is a point on the curve. This point verification scheme has however been shown to be insufficient against certain types of fault based attacks. In this talk, error-detecting schemes for elliptic curve scalar multiplication, which is fundamental to elliptic curve crypto-systems, are considered. We present structures based on re-computation and parallel computation along with point verification. These structures use encoding techniques that rely on proprieties of elliptic curves and provide a high probability of error detection.

This is joint work with A. Dominguez-Oviedo.