SAND2022-10002C

The Center for Cyber Defenders

Expanding computer security knowledge

Elliptical Curve Cryptography Testing

Testing Weaknesses and Strengths

Maria Camila Gaitan-Cardenas

Project Mentor: Jennifer Cordaro

- Problem Statement:
  - Finding vulnerabilities of Elliptical Curve Cryptography.
- Background:
  - Elliptical Curve Cryptography (ECC) is the approach to public key cryptography based on elliptic curve over finite fields. [1]
  - The RSA algorithm is currently the most commonly used algorithm for public key cryptography.
  - ECC is slowly edging out RSA as it provides equivalent, if not higher, level of security with a shorter key length.
  - As a result of this, ECC offers higher speed and security than a RSA certificate.
- Objectives and Approach:
  - The objective of the project is to focus on finding vulnerabilities of ECC, as it becomes more popular in use in cyber security circles.
  - The approach is to run a number of tests within a virtual machine to find the places where ECC lacks and help mitigate the issues.
- Expected Results:
  - Looking for vulnerabilities:
    - Found in Rowhammer Attack.
    - Found due to Access Based attacks.
    - Timing Based attacks or Derating Factor.
    - Side-channel attacks.
    - Power attacks.
    - Brute force attacks.
  - Testing vulnerabilities commonly affecting RSA and seeing if those vulnerabilities affect ECC:
    - Wiener's attack.
    - Recovering private keys through the private exponent (possible with RSA, if d is less than the 4^{th} root of N.)
    - Franklin-Reiter attack.
  - Possible Future vulnerabilities:
    - Vulnerabilities brought forward by Shor's and Grover's algorithms.
- Impact and Benefits: As RSA becomes more obsolete and vulnerable due to the development of faster functioning technology, we need to find an alternative, such as ECC. Finding ECC vulnerabilities will be helpful in mitigating attacks as it becomes more used.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.