The discrete logarithm problem on elliptic curves in binary fields: analysis and experiments

Presenter: Shivankar Ojha (sxo4955@rit.edu) Advisor: Stanislaw Radziszowski
Department of Computer Science, Rochester Institute of Technology, Rochester, NY

Introduction and Motivation
- The discrete logarithm problem, in mathematics: find an integer \( x \), in a prime field \( \mathbb{Z}_p \), such that \( a^x = \beta \mod p \).
- This problem also has a different form, which is in terms of points on an elliptic curve in a binary field.
- This problem is considered intractable and forms the backbone of many secure encryption algorithms.
- The purpose of this study is to explore algorithms which target the discrete logarithm problem and measure their performance and effectiveness.

Objectives
- Implementation of binary Galois field arithmetic library.
- Implementation and exploration of an elliptic curve framework defined in binary Galois fields.
- Implementation of algorithms for finding the discrete logarithm in elliptic curves and binary fields.
- Evaluation of the performance and effectiveness of these algorithms and make conclusions based on these performance measures.

Background
- Binary Galois fields of the form \( \mathbb{GF}(2^p) \) and computations in them.
- Some elements of \( \mathbb{GF}(2^p) \) with irreducible: \( a^2 + a + 1 \)

<table>
<thead>
<tr>
<th>Bit representation</th>
<th>Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>00001</td>
<td>1</td>
</tr>
<tr>
<td>00010</td>
<td>( a^2 + a )</td>
</tr>
<tr>
<td>00110</td>
<td>( a^2 + 1 )</td>
</tr>
<tr>
<td>01111</td>
<td>( a^2 + a + 1 )</td>
</tr>
<tr>
<td>11111</td>
<td>( a^2 + a^2 + 1 )</td>
</tr>
</tbody>
</table>

Table 1: Some elements of Galois field \( \mathbb{GF}(2^p) \)

- Types of elliptic curves as defined by NIST:
  - Pseudorandom: Coefficients generated by hash function.
  - Special: Coefficients generated to maximize efficiency of operations.

- Koblitz curves: A special curve defined over \( \mathbb{GF}(2) \) of the form \( y^2 + x y = x^3 + b \).
- An example of an elliptic curve defined in \( \mathbb{GF}(2^2) \): \((00,11), (11,00), (11,11), (01,10), (01,11)\) and \( O \).

- Point at infinity: \( O + P = P \).
- Point multiple: \( x \cdot a = a + a + a + \ldots + x \) times.
  Computed using double and add algorithm.
- Point addition: \( P + Q = R \) also on elliptic curve.
- The order of point: For order \( n \), \( n \cdot P = O \).
- Inverse or negative of a point: \( P + (-P) = O \).
- The discrete logarithm problem: Find \( x \) such that \( \beta = x \cdot a \).
- Order of curve: The number of points on the curve.
- Point counting: School’s algorithm or software like sagemath.

Implementation
- Implementation of a Galois field arithmetic library in JAVA.
- Implementing an elliptic curve in binary fields framework and incorporate it with the Galois field library designed earlier.
- Implementing point counting mechanism using brute force for smaller curves for verification.
- Implementation of these three algorithms, based on discrete logarithm problem:
  1. Shanks
  2. Pollard Rho
  3. Pohlig-Hellman
- Implementing a framework for recording performance measures for all these algorithms and later comparing them.

Results and analysis
There were two ways for measuring performance of the three algorithms:
- Testing them with points defined over different curves.
- Testing them with points defined over the same curve.

Current status
- The NSA has called for a move to post quantum cryptography techniques and has discouraged ECC[1]. Although ECC remains secure at the moment, it has been in use for over 15 years and change is imminent.

Implementation
- Implementation of binary Galois field arithmetic library.
- Implementing a framework for recording performance measures.
- Testing them with points defined over the same curve.
- Testing them with points defined over different curves.
- There were two ways for measuring performance of the three algorithms:
  - Implementing point counting mechanism using brute force for smaller curves for verification.
  - Implementing a framework for recording performance measures for all these algorithms and later comparing them.

Conclusion
This implementation was tested for the instances of the discrete logarithm problem in curves defined in fields up to \( 2^{163} \). The curves used in industry begin from \( 2^{163} \). Hence, the discrete logarithm problem is still reasonably safe, although certain curves including Koblitz are not. It was also found that the Pollard Rho algorithm was fastest but it was not complete like Pohlig-Hellman and Shanks.

References