Software Implementations

Public-key Cryptography
- Comparison of Public Domain Multi-precision Libraries
- Pairing-based cryptosystems
- Spectral Montgomery Exponentiation

Cryptanalysis
- Comparison and Optimization of Public Domain Implementations for Number Field Sieve
Software Implementations

Public-key Cryptography

- Comparison of Public Domain Multi-precision Libraries
- Pairing-based cryptosystems
- Spectral Montgomery Exponentiation

Cryptanalysis

- Comparison and Optimization of Public Domain Implementations for Number Field Sieve
Comparison of Public Domain Libraries: Operations on Large Integers

Performance

High

GMP, NTL, LiDIA
CLN

OpenSSL
MIRACL

PIOLOGIE

Low

Worst

Primitives

Schemes

Support
Comparison of Public Domain Libraries: Elliptic Curve Operations

<table>
<thead>
<tr>
<th>Performance</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>OpenSSL</td>
</tr>
<tr>
<td></td>
<td>LiDIA</td>
</tr>
<tr>
<td>Low</td>
<td>MIRACL</td>
</tr>
<tr>
<td>Low</td>
<td>CryptoPP</td>
</tr>
</tbody>
</table>

- OpenSSL: High Performance, Primitives
- LiDIA: Low Performance, Schemes
- MIRACL: High Support, Primitives
- CryptoPP: Low Support, Schemes
ECCLIb

- GMU-based software library for Elliptic Curve Cryptography on binary fields
  - Implements multiple algorithms for same operation
    - e.g. 5 different scalar multiplication functions
  - Optimizes the modular reduction time in binary fields

- Includes NIST recommended curves FIPS 186-2

- Operations are optimized for performance
  - 46% faster than OpenSSL for scalar multiplication
Comparison of ECCLib with Other Libraries

- EC-DSA Signature Generation, Ordinary Curves
Software Implementations

Public-key Cryptography
- Comparison of Public Domain Multi-precision Libraries
  - Pairing-based cryptosystems
  - Spectral Montgomery Exponentiation

Cryptanalysis
- Comparison and Optimization of Public Domain Implementations for Number Field Sieve
Adding Pairings to ECClib

- Added pairing-friendly curves to library
- Added operations in extension field GF($2^{4m}$)
- Implemented pairing algorithms over binary fields

![Graph showing the performance comparison between different libraries: ECCLib Full, ECCLib Half, MIRACL Full, MIRACL Half, LiDIA Full, LiDIA Half. The x-axis represents the size in bits, and the y-axis represents the time in seconds.](image)
Software Implementations

Public-key Cryptography

- Comparison of Public Domain Multi-precision Libraries
- Pairing-based cryptosystems
- Spectral Montgomery Exponentiation

Cryptanalysis

- Comparison and Optimization of Public Domain Implementations for Number Field Sieve
Comparison of Public Domain Implementations of Number Field Sieve

Evaluated NFS implementations:

1. Chris Monico: GNU General Number Field Sieve (GGNFS)
2. Per Leslie Jensen: Pleslie’s General Number Field Sieve (pGNFS)
3. Chris Card: factor-by-gnfs
4. Jason Papadopoulos: msieve

**Msieve** is the most efficient—and freely licensed implementation.

**GGNFS** is a close second—and recommended by the Msieve author and users groups.

**GGNFS selected for optimization and further extensions.**