RNS Modular Computations for Cryptographic Applications
Karim Bigou, Arnaud Tisserand

To cite this version:
Karim Bigou, Arnaud Tisserand. RNS Modular Computations for Cryptographic Applications. RAIM: 7ème Rencontre Arithmétique de l’Informatique Mathématique, Apr 2015, Rennes, France. 2015. hal-01141347

HAL Id: hal-01141347
https://inria.hal.science/hal-01141347
Submitted on 11 Apr 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
1. Elliptic Curve Cryptography (ECC)

Elliptic curve over \( \mathbb{F}_p \):
\[
y^2 = x^3 + ax + b \quad \text{with} \quad P \text{ a } \ell \text{-bit prime}
\]

Security levels: \( \ell \in \{160, \ldots, 600\} \) bits

Curve level operations:
- point addition (ADD): \( Q + Q' \)
- point doubling (DBL): \( Q + Q \)
- scalar multiplication: \( [k]Q = Q + \ldots + Q \)

Security (ECDLP): knowing \( Q \) and \( [k]Q, k \) cannot be recovered

ECDLP: Elliptic Curve Discrete Logarithm Problem

2. Residue Number System (RNS)

\( X \) a large \( \ell \)-bit integer is represented by:
\[
\overline{X} = (x_1, \ldots, x_n) = (X \mod m_1, \ldots, X \mod m_n)
\]

RNS base \( B = (m_1, \ldots, m_n) \)

\( n \) pairwise \( w \)-bit co-primes with \( n \times w > \ell \)

The Chinese remainder theorem (CRT) is the base of RNS

Pros:
- carry free between channels
- fast parallel +, −, × and some exact divisions
- non-positional number system, randomization against SCAs
- flexibility for hardware implementations

Cons:
- comparison, modular reduction and division are much harder

3. RNS Computation Flow in ECC Applications

RNS allows to perform some field level operations in parallel

4. State-of-the-Art Algorithms and Architectures

RNS Montgomery Reduction

Input: \( \overline{X}, \overline{X} \)
Output: \( (\overline{X}, \overline{X}) \) with \( \omega = X \cdot M^{-1} \mod P \)

\( P = x \cdot M^{-1} \)
\( Q = x \cdot M^{-1} \)
\( R = x \cdot M^{-1} \)
\( S = x \cdot M^{-1} \)

BE: base extension
\( M = \lceil \log_2 m \rceil \)

5. New RNS Modular Inversion (MI) (CHES 2013)

State-of-the-art RNS MI methods:
- based on Fermat’s Little Theorem (FLT-MI): \( X^{-1} = X^{p - 2} \mod P \)
  - i.e. a large exponentiation with a lot of modular reductions
  - which costs \( O(\log_2 P \times n^2) \) EMUs
- very limited parallelization due to internal data dependencies

Proposed method PM-MI:
- extended binary Euclidean algorithm (binary-ternary version)
- uses the plus-minus trick:
  - if \( X \) and \( Y \) are odd then \( X + Y \equiv 0 \mod 4 \) or \( X - Y \equiv 0 \mod 4 \)
- PM-MI works without BE and costs \( O(\log_2 P \times n) \) EMUs

6. Fast Patterns for RNS Computations (ASAP 2014)

Cost of standard and modular multiplications in RNS:
- standard: \( n \) EMUs
- modular: \( 2n^2 + O(n) \) EMUs

Proposed method:
- splits operands into 2 parts: \( \overline{X} = (K_1) \times (M_2) + (R_3) \)
  - allows to replace \( 2n \) moduli by only \( 2n/2 \)
- reuses split result in various computation patterns
- requires an hypothesis on \( P \): OK for ECC/DH, but not for RSA

Cost for some patterns (256 bits):

<table>
<thead>
<tr>
<th>Operation</th>
<th>our</th>
<th>5-o-t-a</th>
</tr>
</thead>
<tbody>
<tr>
<td>( AB \mod P )</td>
<td>( 2P^2 + 4n )</td>
<td>( 2P^2 + 4n )</td>
</tr>
<tr>
<td>( A^R \mod P )</td>
<td>( 2P^2 + 4n )</td>
<td>( 1.75P^2 + 10.5n )</td>
</tr>
<tr>
<td>( C \cdot A \mod P )</td>
<td>( 2P^2 + 4n )</td>
<td>( 1.75P^2 + 7.0n )</td>
</tr>
<tr>
<td>( C \cdot A^R \mod P )</td>
<td>( 4P^2 + 8n )</td>
<td>( 2.75P^2 + 16.5n )</td>
</tr>
</tbody>
</table>

Usage for Diffie-Hellman or ElGamal:

Funding from DGA-INRIA PhD grant and project PAVOIS ANR 12 BS02 002 01

http://pavois.irisa.fr/