A Randomized Multi-Modulo RNS Architecture for Double-and-Add in ECC to prevent Power Analysis Side Channel Attacks

Jude Angelo Ambrose, Héctor Pettenghi and Leonel Sousa

18th Asia and South Pacific Design Automation Conference
ASP-DAC 2013
Summary

• Introduction

• Design of Double-and-Add RNS (DARNS).
  – Direct Variable Multi-Moduli Architecture (Direct VMAs).
  – Reverse Variable Multi-Moduli Architecture (Reverse VMAs)

• DARNS in Elliptic Curve Cryptography (ECC).

• Experimental Results.

• Conclusions and Future work.
Introduction: Cryptography Background

Key

Plaintext → Cryptographic algorithm → Message

Cryptographic device (e.g., smart card and reader)

Oscilloscope

Control, Waveform data

Computer

Control, Cyphertexts
Introduction: Types of Side Channel Attacks

- **Simple Power Analysis:** The identification of computations and instructions used by analyzing the power wave using the characteristic signature.

```plaintext
/* Square-and-Multiply Algorithm in RSA
   M: message to encrypt,
   N: public modulus,
   e: a b-bit secret key
   Ciphertext C = M^e mod N => e

   */
   C=M
   for i from 1 to b-1 do
     C = C*C (mod N)
   if d_i = 1 then
     C = C*M (mod N)
   return C
```

b = 1010
Introduction: Types of Side Channel Attacks

- **Differential Power Analysis**: Uses statistical analysis by correlating the predictions with the actual power measurements.

\[
DPA_T[i] = \frac{1}{N_I} \sum_{j=1}^{N_I} P_k[j][i] - \frac{1}{N_I} \sum_{j=1}^{N_I} P_u[j][i]
\]
Introduction: Elliptic Key Cryptography

- **Elliptic Curve Cryptography (ECC)** is a public key cryptographic algorithm where senders will use a private key to encrypt the data and receivers will use the public key for decryption.

- The **benefits** of the ECC is that it uses smaller key size with faster computation to suit small devices in comparison with the contender RSA.
Introduction: Elliptic Key Cryptography vulnerability

- Unprotected Double-and-Add in **ECC** generates distinctive power patterns hence **successfully attacked using SPA and DPA**.
- **State-of-the-art solutions:**
  - Masking the power pattern (Software/algorithms),
  - New algorithms,
  - Software balancing,
  - Hardware implementation.

Introduction: RNS Background

- In Residue Number Systems a binary number is converted in parallel into a set of residue words corresponding to the remains of moduli values:

\[ \{m_1, m_2, m_3\} \]
Introduction: Residue Number System Example

- For a moduli set \( \{15, 16, 17\} \) and an input \( G = 33 \). One Doubling and addition operation is \( Q = 33 \times 2 + 33 = 99 \).

- The binary solution requires large multipliers and adders in comparison with the RNS solution.
Introduction: Our solution for double and add in RNS

- We propose to use randomly controlled Multi-Moduli architectures (MMAs) to obfuscate the secure information from the power profile.
- The MMAs have demonstrated high performance.
Summary

• Introduction

• Design of Double-and-Add RNS (DARNS).
  – Direct Variable Multi-Moduli Architecture (Direct VMAs).
  – Reverse Variable Multi-Moduli Architecture (Reverse VMAs)

• DARNS in Elliptic Curve Cryptography (ECC).

• Experimental Results.

• Conclusions and Future work.
The proposed DARNS architecture has three major components: 1), *DIRECT*; 2), *ARITHMETIC*; and 3), *REVERSE*.
DARNS: Direct Architecture

- **Direct RNS**

- A standard direct Single Modulo Architecture (direct SMA), $f$ odd, transforms an integer $G$ with $m$-bit inputs $\{q_0, q_1, \ldots, q_{m-1}\}$ into a residue word $R$ of $a$-bit outputs $\{r_0, r_1, \ldots, r_{a-1}\}$, with $a = \lceil \log_2(A) \rceil$. $a = n$, $a = n + 1$ for modulo $A = \{2^n - f\}$ and $A = \{2^n + f\}$, respectively.

\[ G = \{g_0, g_1, \ldots, g_{m-1}\} \Rightarrow R = \{r_0, r_1, \ldots, r_{a-1}\} \]
DARNS: Direct Architecture

- **Stage 1:** The pre-computation of the inputs is carried out to obtain the non-common and common bits as well as the required correction factor COR.

\[
T(A_i) = \sum_{j=0}^{m} |2^j|_{A_i} \cdot g_j.
\]

\[
\tau(A_i) = \lceil \log_2(T_{max} + 1) \rceil
\]

- **Stage 2:** The calculation of \( |G|_{A_i} = |T^d(A_i)|_{A_i} \) is carried out by means of a memory-less Final Converter (FC).


18th Asia and South Pacific Design Automation Conference (ASP-DAC 2013), Tokyo, Japan.
DARNS: Adder/Doubling Architecture

- The stage 1 of direct VMA is applied twice to derive $X + Y$, with $X = \{x_0, x_1, ..., x_n\}$ and $Y = \{y_0, y_1, ..., y_n\}$:

$$X + Y = T^{(B_i)} = \sum_{j=0}^{n} 2^j |B_i| \cdot x_j + \sum_{j=0}^{n} 2^j |B_i| \cdot y_j$$

$$|X + Y|_{B_i} = \begin{cases} T^{(B_i)} - (B_i), & \text{if } T^{(B_i)} \geq B_i \\ T^{(B_i)}, & \text{otherwise,} \end{cases}$$

- The last stage consists on a subtraction of the modulo value selected by a MUX. The modulo adder computation is carried out by means of one CPA and a MUX to select the correct arithmetic operation.
DARNS: Reverse Architecture

- The Single Modulo Architecture (SMA) reverse converter with moduli set \( \{m_1, m_2, m_3\} \)

\[
Q = \sum_{i=1}^{3} m_i^{-1} \hat{m}_i R_i = \sum_{i=1}^{3} m_i^{-1} \hat{m}_i R_i - MA(Q) \rightarrow Q = \frac{Q}{m_1} m_1 + R_1
\]

\[
\frac{Q}{m_1} = \frac{Q}{m_1} = \sum_{i=1}^{N} m_i^{-1} \hat{m}_i R_i - \frac{M}{m_1} A(Q) m_1
\]

\[
\frac{Q}{m_1} = \sum_{i=1}^{3} v_i \hat{m}_i
\]

\[
\frac{Q}{m_1} = \frac{Q}{m_1} \hat{m}_1
\]
Summary

• Introduction

• Design of Double-and-Add RNS (DARNS).
  – Direct Variable Multi-Moduli Architecture (Direct VMAs).
  – Reverse Variable Multi-Moduli Architecture (Reverse VMAs)

• DARNS in Elliptic Curve Cryptography (ECC).

• Experimental Results.

• Conclusions and Future work.
DARNS in ECC

Secret key $dk$

Inputs $\{I_1, I_2, \ldots\}$

Random $dr$

DIRECT
ARITHMETIC
REVERSE

DIRECT
ARITHMETIC
REVERSE

DIRECT
ARITHMETIC
REVERSE

DIRECT
ARITHMETIC
REVERSE

PUBLIC KEY

---

18th Asia and South Pacific Design Automation Conference (ASP-DAC 2013), Tokyo, Japan.

03/01/2012
$n = 3 \begin{cases} \{2^{2n} - 3, 2^n + 1\} \\ \{2^{2n}, 2^n + 3\} \end{cases} \quad G = 127$

\[
G = 127 = 000001111111_2  \\
127\text{\_}5 = 2  \\
127\text{\_}11 = 6  \\
127\text{\_}64 = 63 \\
\{2^n - 3, 2^n + 1\} = \{5, 9\}  \\
\{2^n, 2^n + 3\} = \{7, 11\} \\
\]

\[
R_1 = |62 + 62|_{64} = 62 \\
R_2 = |2 + 2|_5 = 4 \\
R_3 = |6 + 6|_{11} = 1 \\
\]

\[
V_1 = 6 \quad v_1 = |6 \times 62|_5 = 42 \\
V_2 = 44 \quad v_2 = |44 \times 4|_5 = 11 \\
V_3 = 5 \quad v_3 = |5 \times 1|_5 = 5 \\
\]

\[
\left| \frac{Q}{m_1} \right| = \sum_{i=1}^{3} v_i \cdot \frac{1}{m_1} \quad \rightarrow \quad \left| \frac{Q}{2^{2n}} \right| = |42 + 11 + 5|_5 = 64 \times 64 = 192 \\
\]

\[
Q = \left| \frac{Q}{m_1} \right| m_1 + R_1 = 192 + 62 = 254 \\
\]

\[
G = \text{input} = 127 \\
Q = \text{output} = 254 \\
\]

---

**18th Asia and South Pacific Design Automation Conference (ASP-DAC 2013), Tokyo, Japan.**
Summary

• Introduction

• Design of Double-and-Add RNS (DARNS).
  – Direct Variable Multi-Moduli Architecture (Direct VMAs).
  – Reverse Variable Multi-Moduli Architecture (Reverse VMAs)

• DARNS in Elliptic Curve Cryptography (ECC).

• Experimental Results.

• Conclusions and Future work.
Experimental Results: Experimental Flow
Experimental Results
Summary

• Introduction

• Design of Double-and-Add RNS (DARNS).
  – Direct Variable Multi-Moduli Architecture (Direct VMAs).
  – Reverse Variable Multi-Moduli Architecture (Reverse VMAs)

• DARNS in Elliptic Curve Cryptography (ECC).

• Experimental Results.

• Conclusions and Future work.
Conclusions

• This paper presents a novel Multi-modulo parallel RNS implementation which chooses different moduli sets randomly.

• Such a randomness and parallelization prevents Differential Power Analysis (DPA), Simple Power Analysis (SPA) during the Double-and-Add operation of the Elliptic Curve Cryptography.

• DPA and Cross Correlation analysis are demonstrated to prove the security of our DARNS architecture.

• Our architecture is not only secure, but performs better for large number of inputs, consume less power, benefiting from the inherent properties of the RNS.
Questions?

Thank you

hector@sips.inesc-id.pt