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

THE UNIVERSITY OF NEW SOUTH WALES

inesc id lisboa

INSTITUTO SUPERIOR TÉCNICO

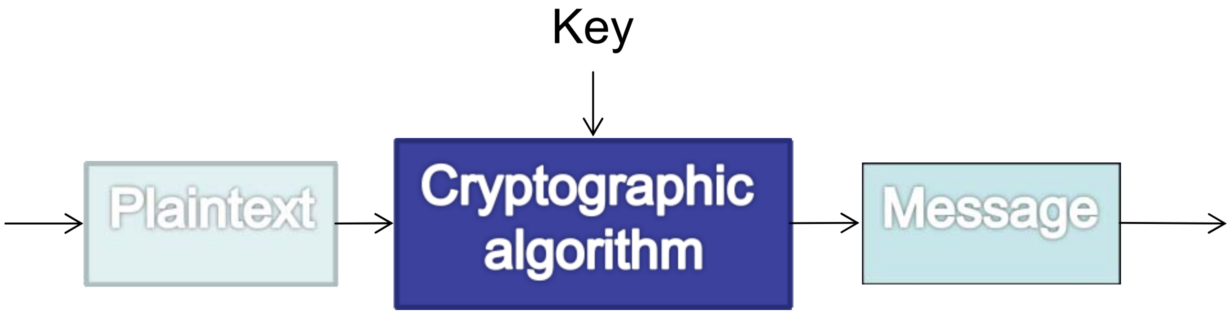
technology
from seed

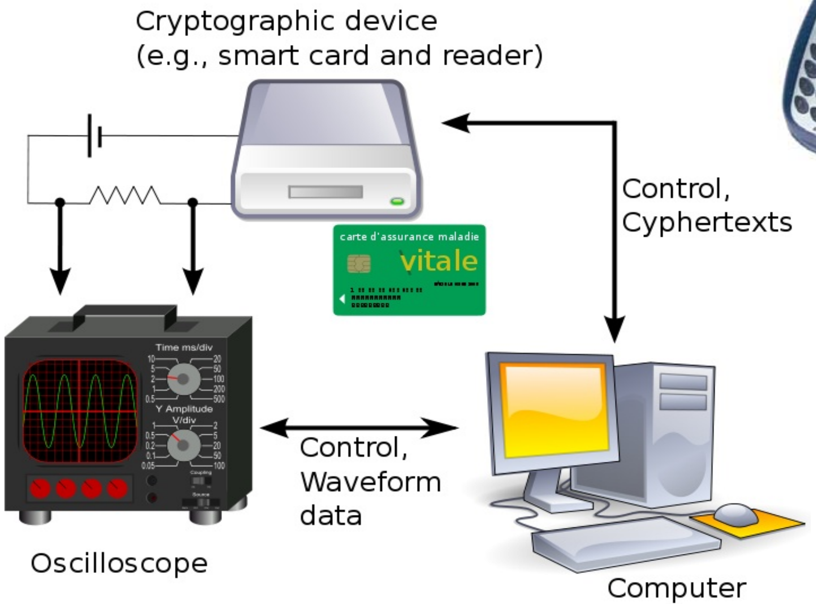
Summary

- Introduction
- Design of Double-and-Add RNS (DARNS).
  - Direct Variable Multi-Moduli Architecture (Direct VMAs).
  - Double-and-Add Multi-Moduli Architectures (Arithmetic VMAs).
  - Reverse Variable Multi-Moduli Architecture (Reverse VMAs)
- DARNS in Elliptic Curve Cryptography (ECC).
- Experimental Results.
- Conclusions and Future work.

Introduction: Cryptography Background

technology from seed





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

- /* Square-and-Multiply Algorithm in **RSA**

  M: message to encrypt,

  N: public modulus,

  e: a ***b***-bit *secret* key

  Ciphertext **C** = $\mathbf{M^e}$ **mod N** => e

  */

  C=M

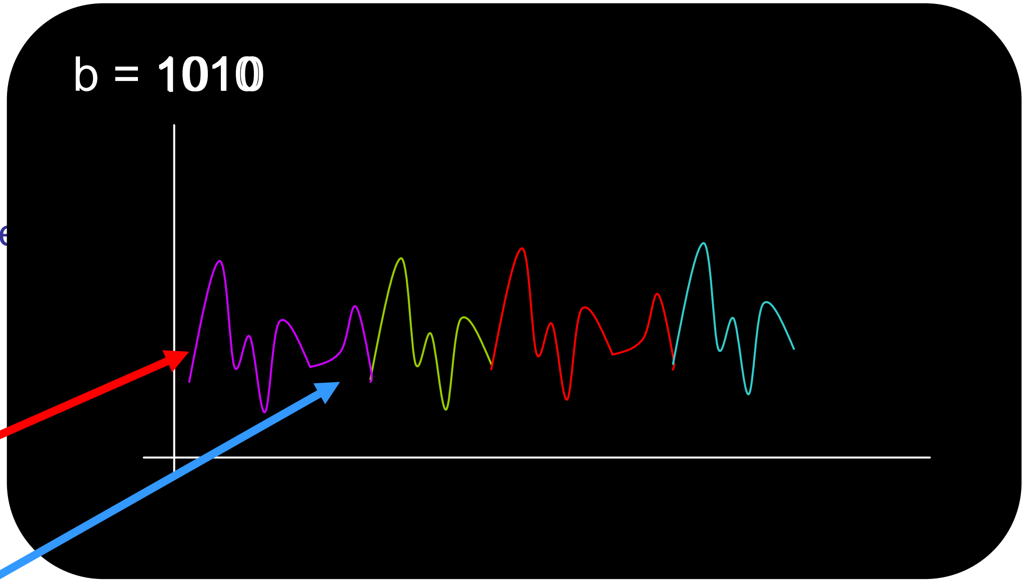
  for i from 1 to *b*-1 do

  C= C*C (mod N)

  if d_i = 1 then

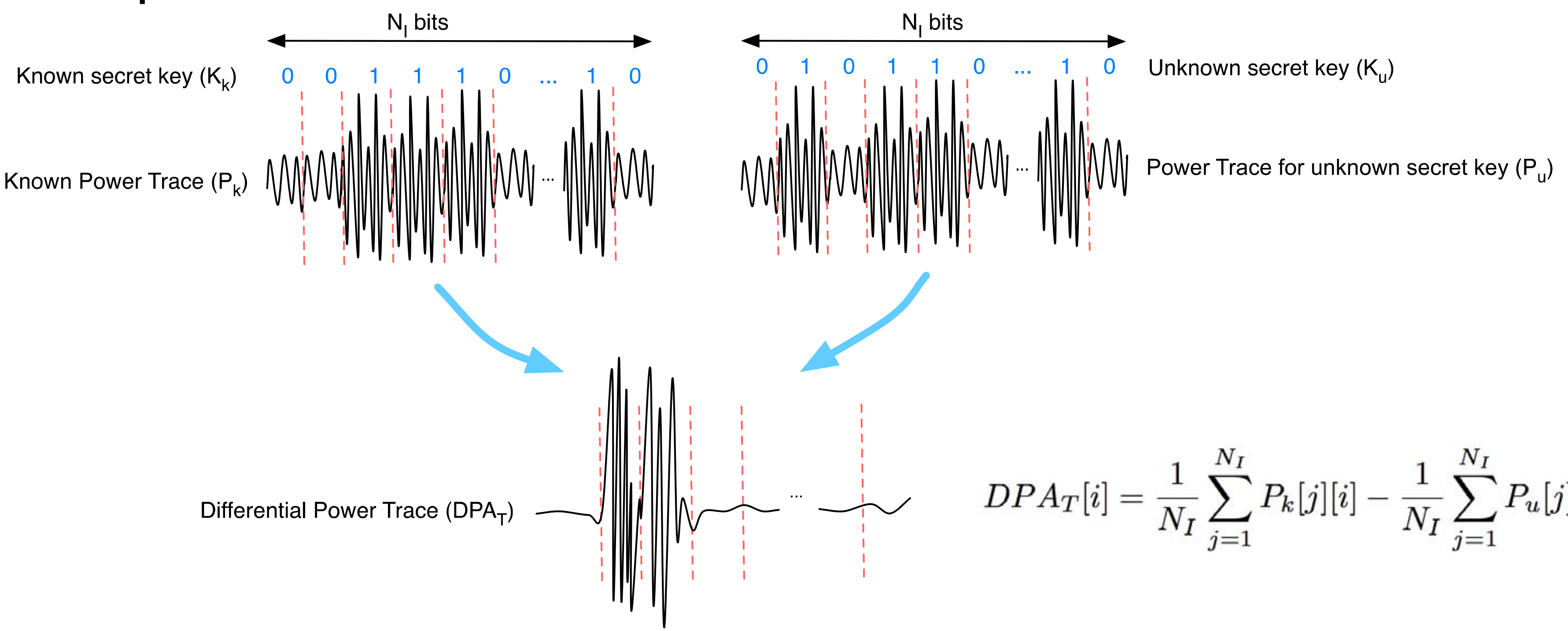
  C = C*M (mod N)

  return C



Introduction: Types of Side Channel Attacks

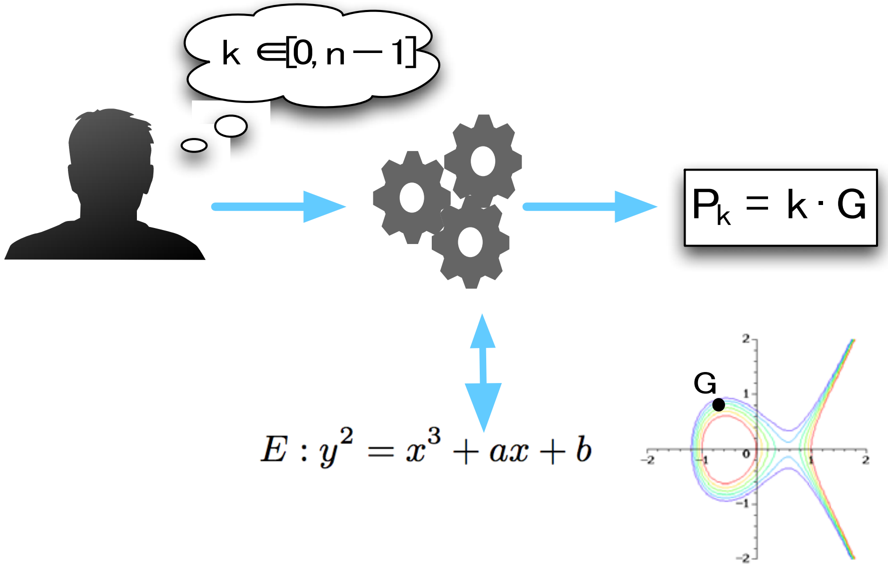
- **Differential Power Analysis:** Uses statistical analysis by correlating the predictions with the actual power measurements.



$$DPA_T[i] = \frac{1}{N_I}\sum_{j=1}^{N_I} P_k[j][i] - \frac{1}{N_I}\sum_{j=1}^{N_I} P_u[j][i]$$

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

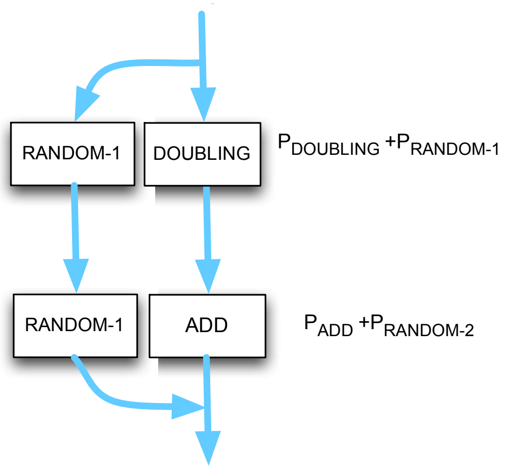


Algorithm 1: Double-and-Add

```
Input: G, k
Output: P_k = k.G
Q <- G
for i from l-2 to 0 do
    /* Double portion */
    Q <- 2.Q
    if d_i == 1 then
        /* Add portion */
        Q <- Q + G
P_k <- Q
return Q
```

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**:

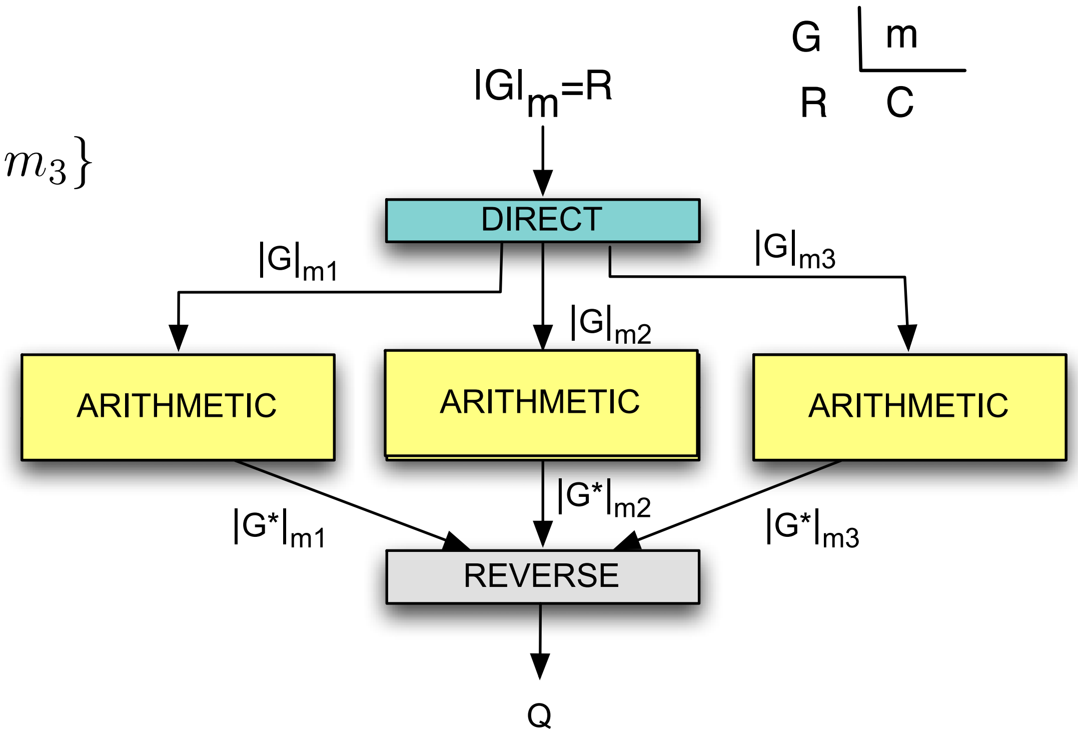


*K. Itoh, T. Izu, and M. Takenaka, "Address-Bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA," in *CHES*, 2003.

Introduction: RNS Background

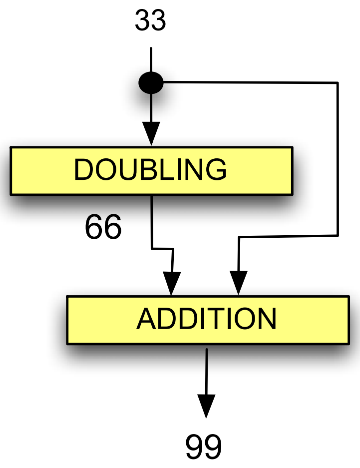
•In Residue Number Systems a binary number is converted in parallel into a set of residue words corresponding to the remains of moduli values:

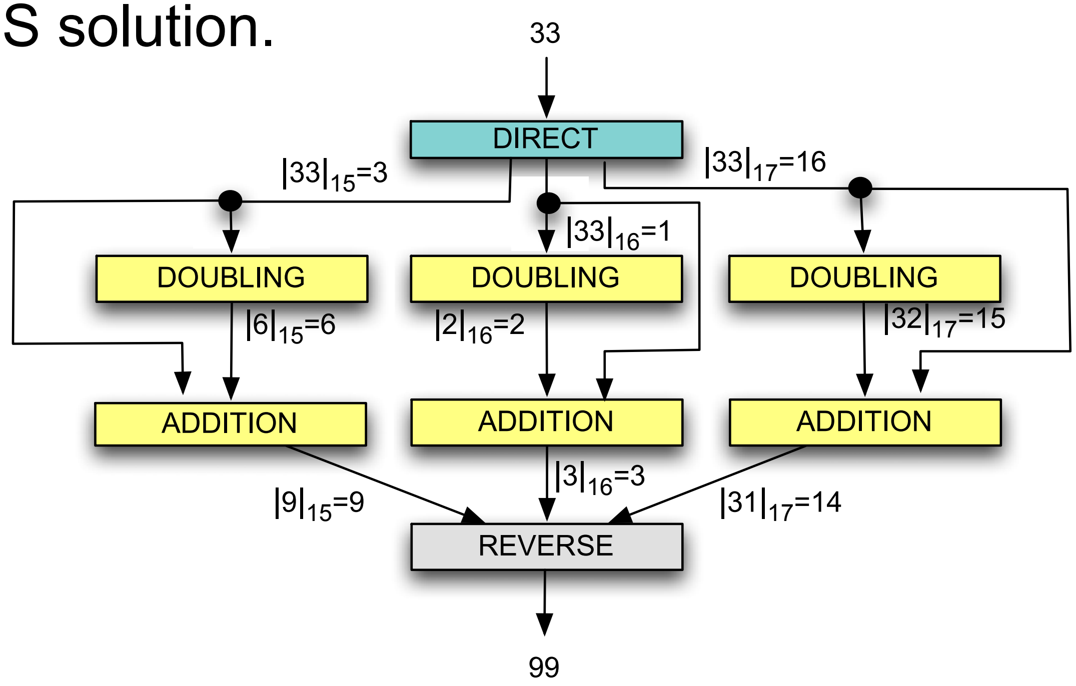
$$\{m_1, m_2, m_3\}$$



Introduction: Residue Number System Example

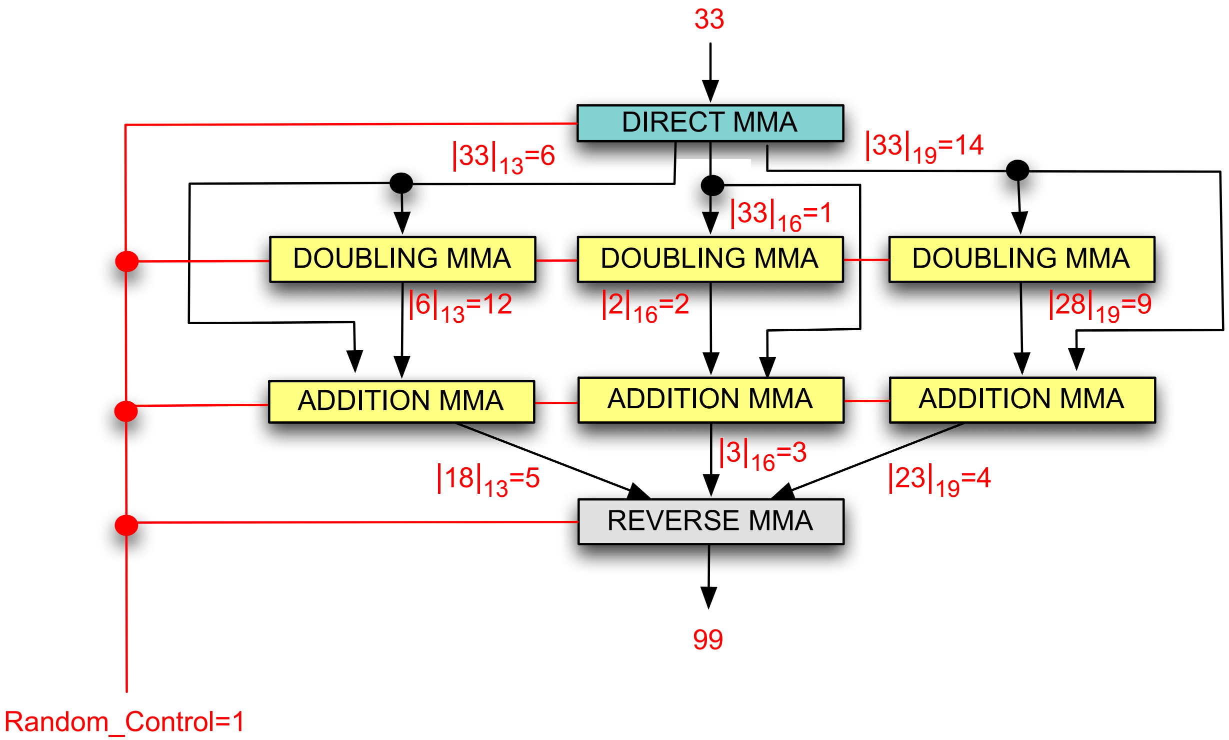
- For a moduli set $\{15, 16, 17\}$ and an input $G = 33$. One Doubling and addition operation is $Q = 33 \times 2 + 33 = 99$.
- The binary solution requires large multipliers and adders in comparison with the RNS solution.





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.



technology
from seed

THE UNIVERSITY OF NEW SOUTH WALES

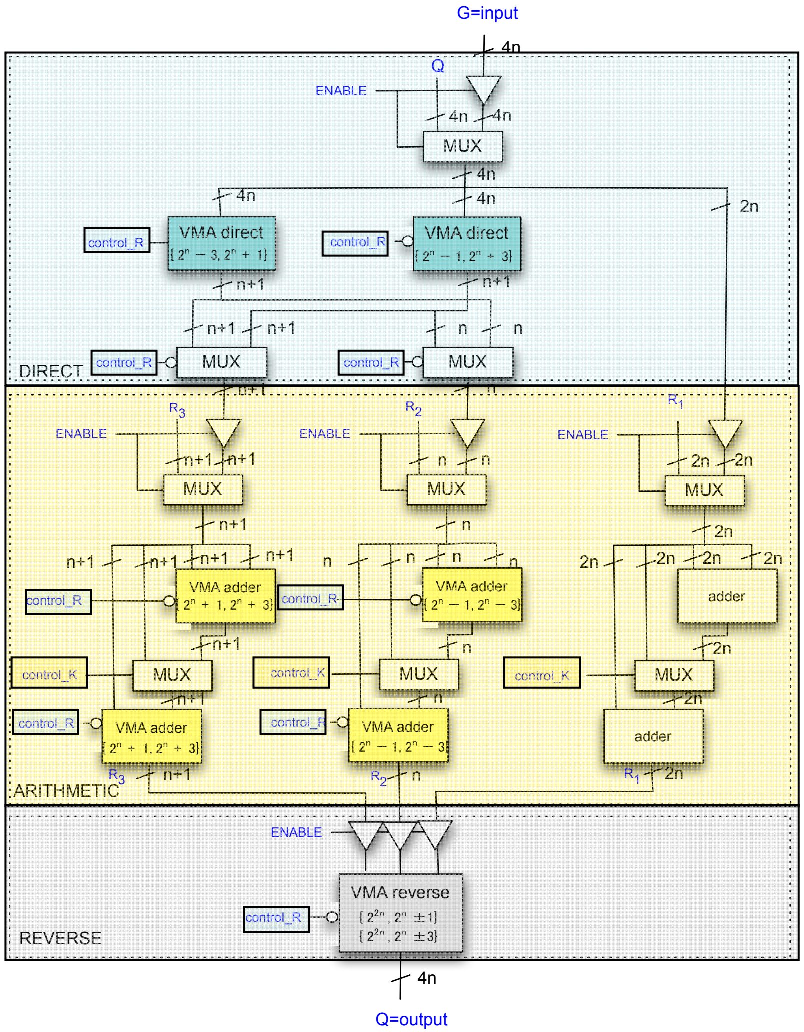
INSTITUTO SUPERIOR TÉCNICO

Summary

- Introduction
- Design of Double-and-Add RNS (DARNS).
  - Direct Variable Multi-Moduli Architecture (Direct VMAs).
  - Double-and-Add Multi-Moduli Architectures (Arithmetic VMAs).
  - Reverse Variable Multi-Moduli Architecture (Reverse VMAs)
- DARNS in Elliptic Curve Cryptography (ECC).
- Experimental Results.
- Conclusions and Future work.

DARNS Architecture

- The proposed DARNS architecture has three major components: 1), *DIRECT;* 2), *ARITHMETIC*; and 3), *REVERSE*.



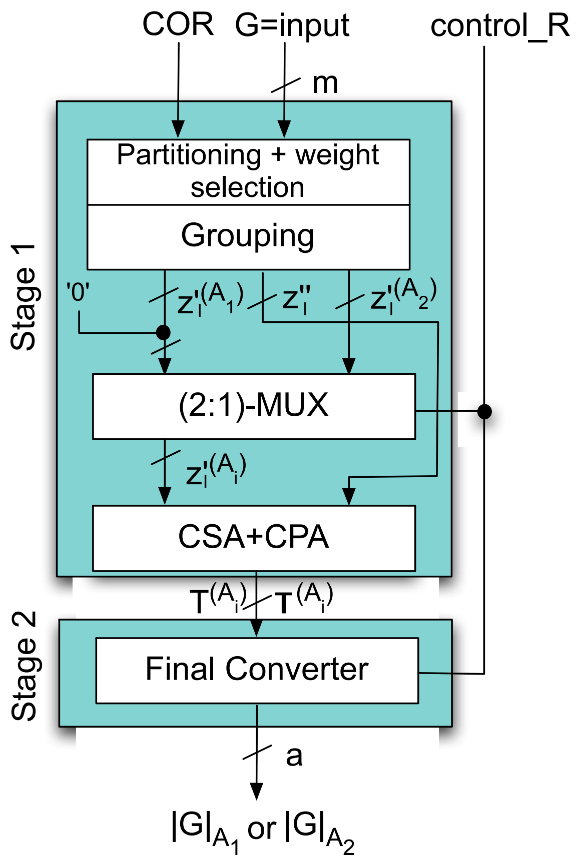
DARNS: Direct Architecture

Direct RNS

- A standard direct Single Modulo $A=\{2^n \pm f\}$ Architecture **(direct SMA)**, f odd, transforms an integer G with m-bit inputs $(\{g_0, g_1 ..., g_{m-1}\})$ into a residue word R of a-bit outputs $(\{r_0, r_1, ..., r_{a-1}\})$ with $a=\lceil log_2(A) \rceil$, $a=n$, $a=n+1$ for modulo $A=\{2^n - f\}$ and $A=\{2^n + f\}$, respectively.

$$G=\{g_0, g_1, \cdots, g_{m-1}\} \Rightarrow R=\{r_0, r_1, \cdots, r_{a-1}\}$$

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.

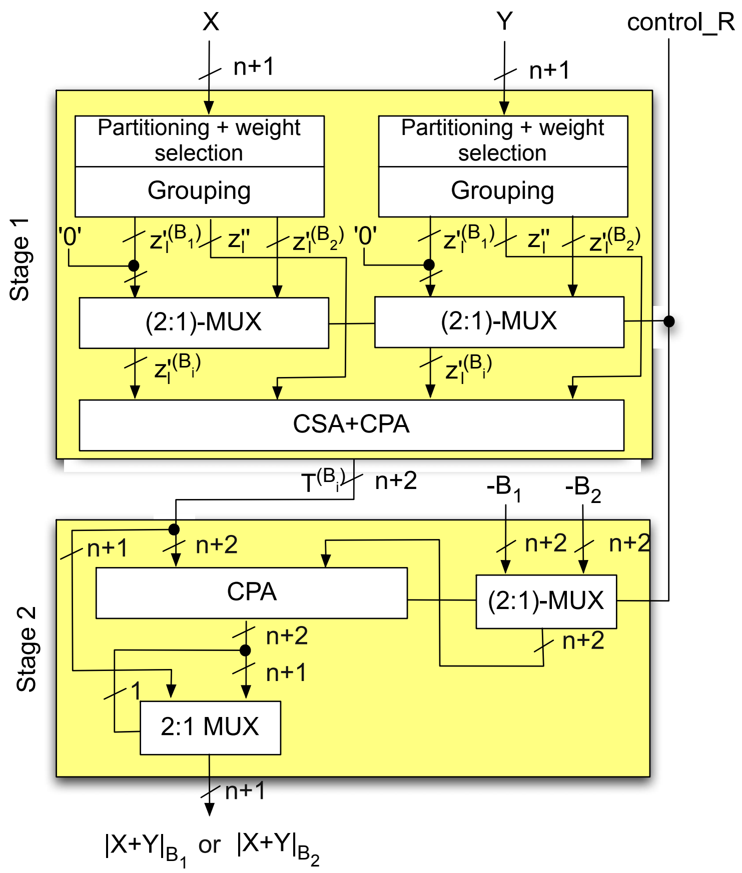
$$T^{(A_i)} = \sum_{j=0}^{m} \left| \left| 2^j \right|_{A_i} \right| g_j.$$

$$\tau^{(A_i)} = \lceil log_2(T_{max} + 1) \rceil$$

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

H. Pettenghi, L. Sousa, and J. Ambrose, "Efficient implementation of multi-moduli architectures for binary-to-rns conversion," in *Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific*, 2012, pp. 819 –824.

DARNS: Adder/Doubling Architecture



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

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

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

$$T_{max}^{(B_i)} < 2 \times (B_i)$$

- 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

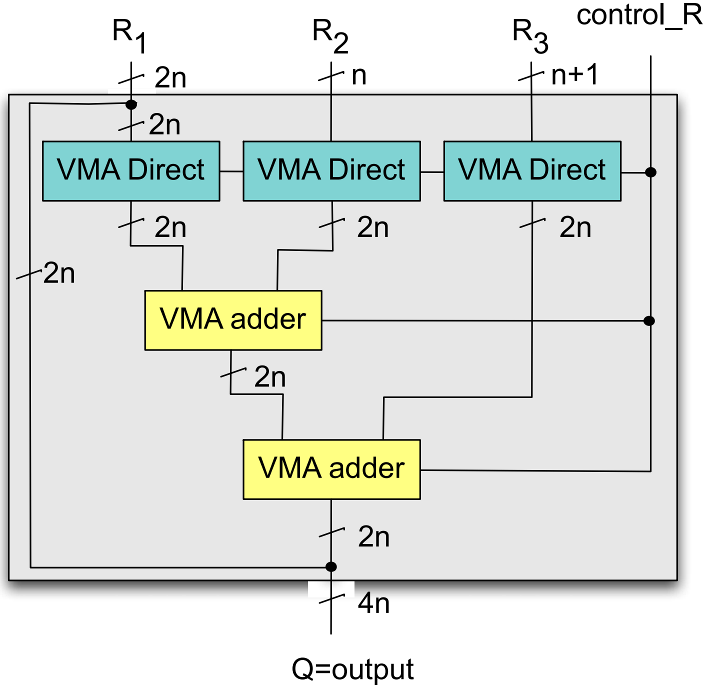
- The Single Modulo Architecture (SMA) reverse converter with moduli set $\{m_1, m_2, m_3\}$:

$$Q = \left|\sum_{i=1}^{3} \hat{m}_i \left|\hat{m}_i^{-1}\right|_{m_i} R_i\right|_M = \sum_{i=1}^{3} \hat{m}_i \left|\hat{m}_i^{-1}\right|_{m_i} R_i - MA(Q) \longrightarrow Q = \left\lfloor \frac{Q}{m_1} \right\rfloor m_1 + R_1$$

$$\left\lfloor \frac{Q}{m_1} \right\rfloor = \left|\left\lfloor \frac{Q}{m_1} \right\rfloor\right|_{\hat{m}_1} = \left| \left|\left\lfloor \sum_{i=1}^{N} \left|\hat{m}_i^{-1}\right|_{m_i} \frac{\hat{m}_i}{m_1} R_i \right\rfloor\right|_{\hat{m}_1} - \overbrace{\left|\frac{M}{m_1} A(Q)\right|_{\hat{m}_1}}^{=0} \right|_{\hat{m}_1}$$

$$= \left| \overset{v_1}{\left|\left\lfloor \left|\hat{m}_1^{-1}\right|_{m_1} \frac{\hat{m}_1}{m_1} R_1 \right\rfloor\right|_{\hat{m}_1}} + \overset{v_2}{\left| \overbrace{\left|\hat{m}_2^{-1}\right|_{m_2} \frac{\hat{m}_2}{m_1}}^{V_2} R_2 \right|_{\hat{m}_1}} + \overset{v_3}{\left| \overbrace{\left|\hat{m}_3^{-1}\right|_{m_3} \frac{\hat{m}_3}{m_1}}^{V_3} R_3 \right|_{\hat{m}_1}} \right|_{\hat{m}_1}$$

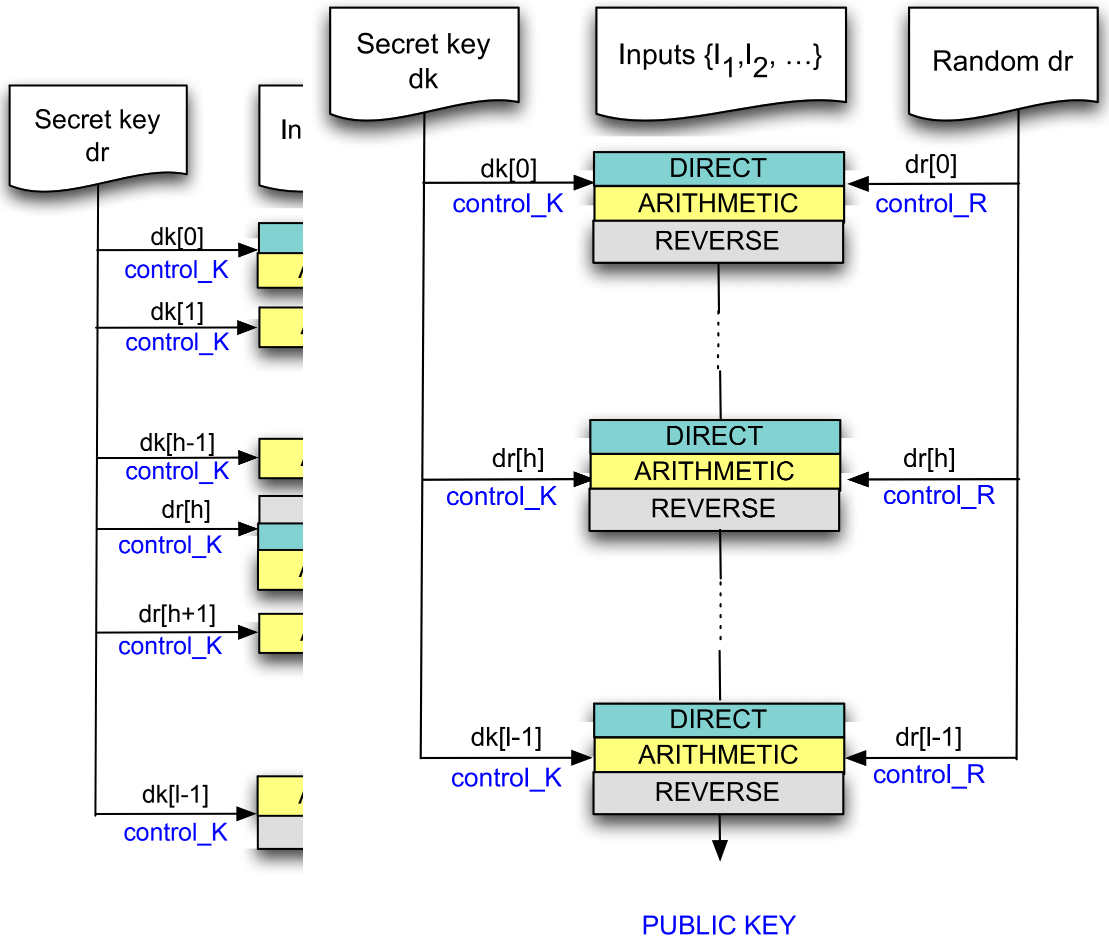
$$\left\lfloor \frac{Q}{m_1} \right\rfloor = \left|\sum_{i=1}^{3} v_i\right|_{\hat{m}_1}$$



Summary

- Introduction
- Design of Double-and-Add RNS (DARNS).
  - Direct Variable Multi-Moduli Architecture (Direct VMAs).
  - Double-and-Add Multi-Moduli Architectures (Arithmetic VMAs).
  - Reverse Variable Multi-Moduli Architecture (Reverse VMAs)
- DARNS in Elliptic Curve Cryptography (ECC).
- Experimental Results.
- Conclusions and Future work.

DARNS in ECC



l-bits

bits	allowed RANDOM(pattern)
3	4
4	6
5	8
...	...
l	2l-2

DARNS in ECC: Example

$$n = 3 \quad \{2^{2n}, 2^n \pm 1\} \quad \{2^{2n}, 2^n \pm 3\} \qquad G = 127$$

$$\{2^n - 3, 2^n + 1\} = \{5, 9\} \qquad |127|_5 = 2$$

$$\{2^n - 1, 2^n + 3\} = \{7, 11\} \qquad |127|_{11} = 6$$

$$|127|_{64} = 63$$

$$R_1 = |62 + 62|_{64} = 62$$

$$R_2 = |2 + 2|_5 = 4$$

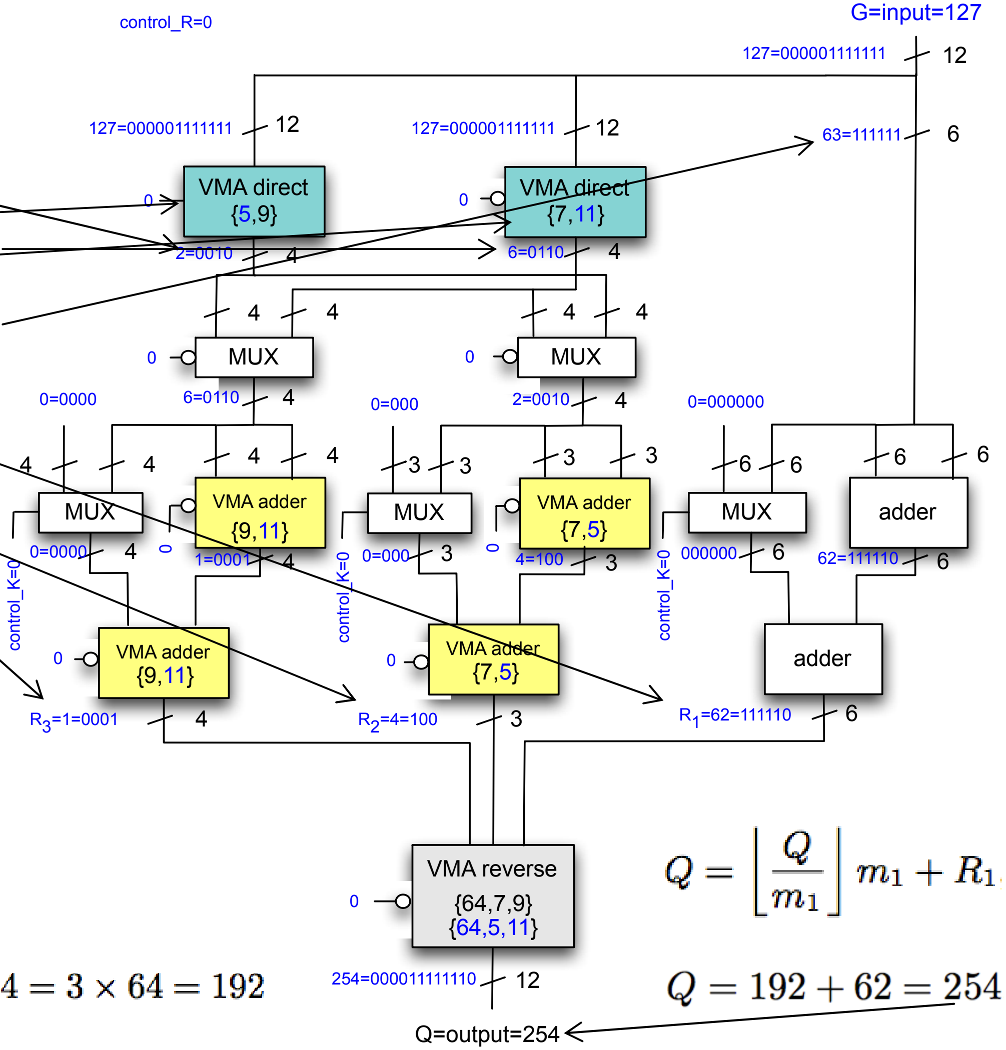
$$R_3 = |6 + 6|_{11} = 1$$

$$V_1 = 6 \qquad v_1 = |6 \times 62|_{55} = 42$$

$$V_2 = 44 \qquad v_2 = |44 \times 4|_{55} = 11$$

$$V_3 = 5 \qquad v_3 = |5 \times 1|_{55} = 5$$

$$\left\lfloor \frac{Q}{m_1} \right\rfloor = \left| \sum_{i=1}^{3} v_i \right|_{\hat{m}_1} \longrightarrow \left\lfloor \frac{Q}{2^{2n}} \right\rfloor 2^{2n} = |42 + 11 + 5|_{55}\, 64 = 3 \times 64 = 192$$



$$Q = \left\lfloor \frac{Q}{m_1} \right\rfloor m_1 + R_1$$

$$Q = 192 + 62 = 254$$

technology
from seed

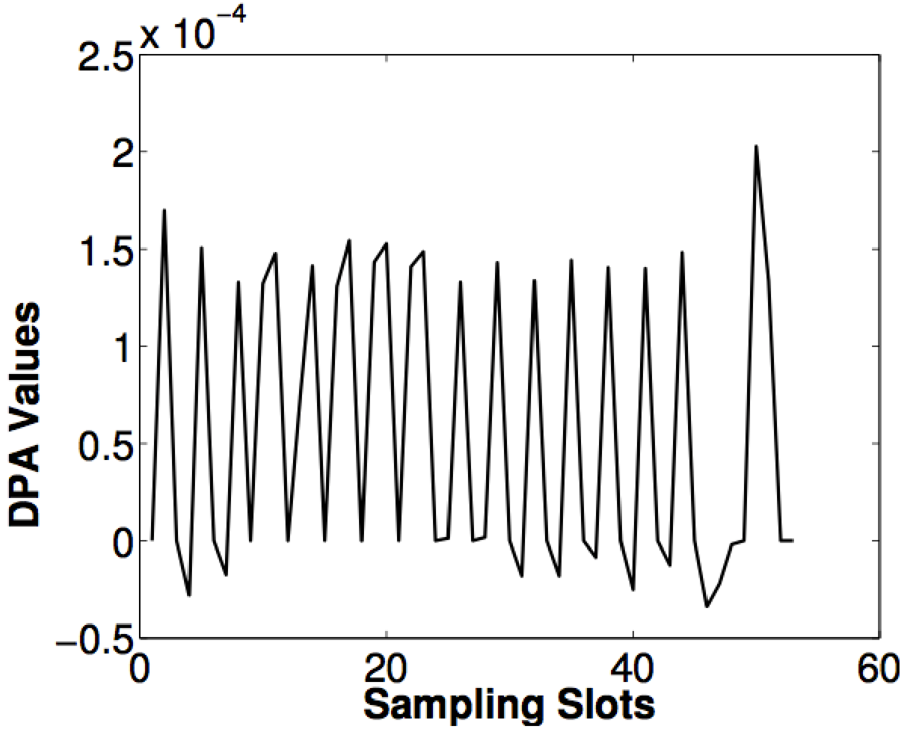
Summary

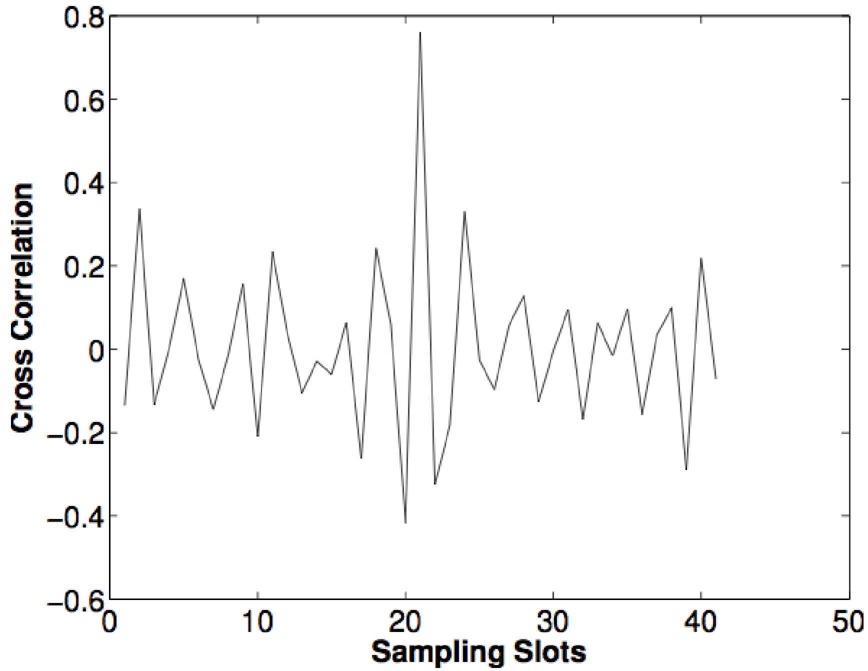
- Introduction
- Design of Double-and-Add RNS (DARNS).
  - Direct Variable Multi-Moduli Architecture (Direct VMAs).
  - Double-and-Add Multi-Moduli Architectures (Arithmetic VMAs).
  - Reverse Variable Multi-Moduli Architecture (Reverse VMAs)
- DARNS in Elliptic Curve Cryptography (ECC).
- **Experimental Results.**
- Conclusions and Future work.

technology
from seed

Experimental Results: Experimental Flow

Experimental Results





technology
from seed

Summary

- Introduction
- Design of Double-and-Add RNS (DARNS).
  - Direct Variable Multi-Moduli Architecture (Direct VMAs).
  - Double-and-Add Multi-Moduli Architectures (Arithmetic 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

THE UNIVERSITY OF NEW SOUTH WALES

INSTITUTO SUPERIOR TÉCNICO

hector@sips.inesc-id.pt