Thwarting Active Side-Channel Attacks of Ring Polynomial Multiplication in $\frac{\mathbb{Z}/p\mathbb{Z}[x]}{x^n+1}$ for Post-Quantum Cryptography Benchmarked on ASIC

Ausmita Sarker, Mehran Mozaffari Kermani, and Reza Azarderakhsh
University of South Florida
(contact mehran2@usf.edu for any questions)

Motivation: Why Post-Quantum Cryptography?

- With the potential advent of **quantum computers**, public-key cryptographic algorithms will be broken.
- We cannot wait till such compromising attacks break our security, especially in **deeply-embedded hardware systems**.
- **Post-quantum cryptography** ensures security and feasible implementation in post-quantum era.
- The steady progress in quantum computing has motivated standardization by the NIST (**initiated in April 2018).**

Motivation: Active Side-Channel Attacks

- **A rush to move to post-quantum cryptographic algorithms**, resistant against quantum computers, may have some unforeseen and possibly dangerous consequences.
- **Side channel attacks** are indisputably much easier to mount and much more difficult to protect against compared to any algorithmic attacks based on special-purpose hardware.
- **Active fault attacks** are based on injecting malicious transient faults to retrieve sensitive information on hardware platforms such as ASIC and FPGA.

Motivation: Ring Polynomial Multiplication

- **Ring polynomial multiplication (RPM)**, an exhaustive arithmetic process, is an integral part of a number of post-quantum cryptographic algorithms.
- RPM is used in ring learning with error (Ring-LWE) on **lattice-based cryptosystems**, fully homomorphic encryption (FHE) and somewhat homomorphic encryption (SHE).
- Implementation of cryptographic primitives can fall victim to active hardware side-channel attacks, **whose secure countermeasures are proposed in this work** for RPM in $\frac{\mathbb{Z}/p\mathbb{Z}[x]}{x^n+1}$.

RPM in Post-Quantum Cryptography

- In this research, we have considered polynomial in the ring $\mathbb{R} = \frac{\mathbb{Z}/p\mathbb{Z}[x]}{x^n+1}$. Efficient error detection schemes are derived to thwart natural and malicious faults.
- Let two polynomials in this ring be $a(x)$ and $b(x)$. The multiplication of $a(x)$ and $b(x)$, used in **Ring-LWE lattice-based post-quantum cryptography**, is derived as:

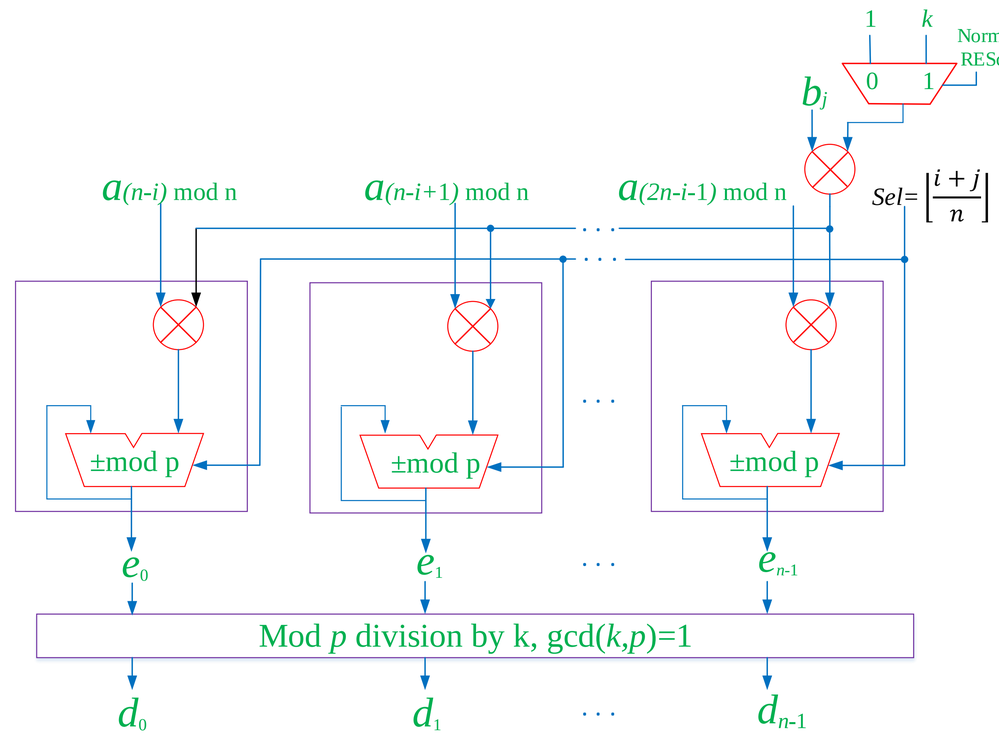
$$c(x) = a(x).b(x) = \sum_{i=0}^{n-1}\sum_{i=0}^{n-1}(-1)^{\lfloor \frac{i+j}{n} \rfloor} a_i b_j x^{i+j \bmod n} \bmod f(x). \quad (1)$$

- The multiplication within $\mathbb{R} = \frac{\mathbb{Z}/p\mathbb{Z}[x]}{x^n+1}$ can be expressed as:

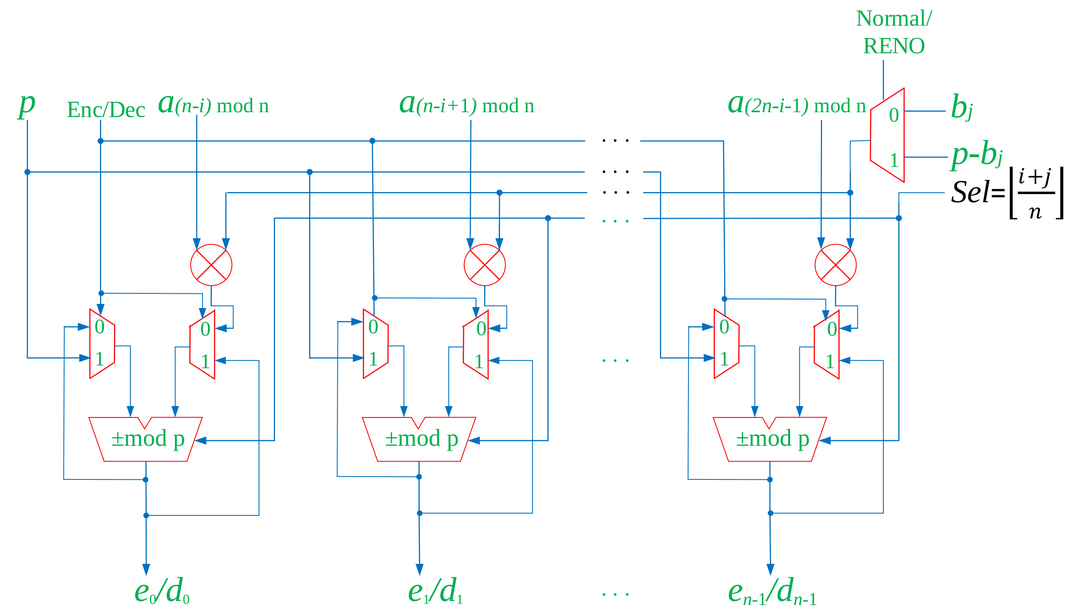
$$\begin{pmatrix} a_0 & -a_{n-1} & . & . & . & -a_1 \\ a_1 & a_0 & . & . & . & -a_2 \\ a_2 & a_1 & . & . & . & -a_3 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{n-1} & a_{n-2} & . & . & . & a_0 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ . \\ . \\ . \\ b_{n-1} \end{pmatrix} \quad (2)$$

Proposed Schemes

We have presented two schemes in this research as follows.
REScO: REcomputing with Scaled Operands for RPM



RENO: REcomputing with Negated Operands for RPM



ASIC Assessments and Comparisons

High error coverage is achieved for the proposed constructions. ASIC assessments using Synopsys Design Compiler and VHDL with TSMC 65-nm for two security levels and two of our architectures is presented below:

Table I
IMPLEMENTATION RESULTS FOR ASIC TSMC 65-NM (PROP. 1: NEGATING BOTH OPERANDS, PROP. 2: NEGATING ONE OPERAND)

Architecture	Area (μm^2)	Delay (ns)	Power (mW) at 50MHz
Original (m-sec.)	162,112	7.30	8.4
Original (h-sec.)	263,382	7.36	13.5
Prop. 1 (m-sec.)	193,412 (19.3%)	10.42 (42.7%)	9.9 (17.8%)
Prop. 1 (h-sec.)	311,330 (18.2%)	10.85 (47.4%)	15.6 (15.5%)
Prop. 2 (m-sec.)	187,607 (15.7%)	9.12 (24.9%)	9.7 (15.4%)
Prop. 2 (h-sec.)	292,307 (11.0%)	9.31 (26.4%)	15.1 (11.8%)

m-sec.: moderate security, h-sec.: high security

Final Remarks

To the best of our knowledge, this is the first work in open literature to provide a generalized error detection scheme applicable to different RPMs for thwarting fault attacks in post-quantum cryptography. *This work is a step-forward towards scrutinizing the engineering aspects of post-quantum cryptography.*

"This work is under review in an *IEEE Transactions* journal.
The authors acknowledge the support of National Science Foundation (NSF) of the US."