

Sujoy Sinha Roy



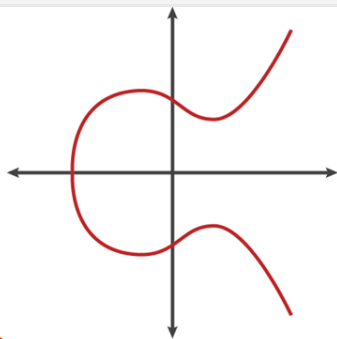
PhD, 2012-2017
KU Leuven



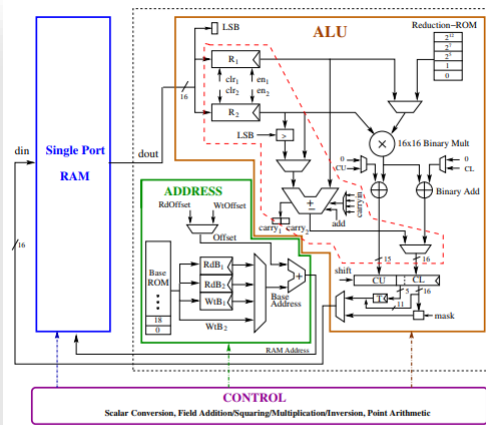
Post Doc., 2017-2018
KU Leuven



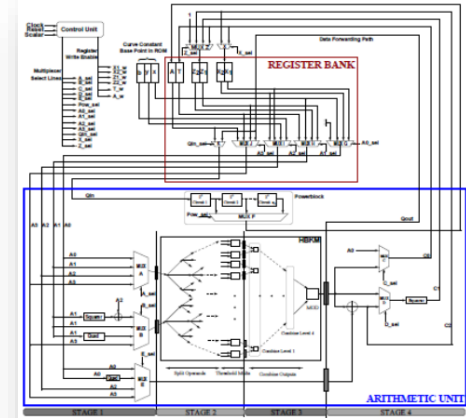
Lecturer, 2018 Sept -
University of Birmingham



Elliptic Curve Crypto



Lightweight ECC

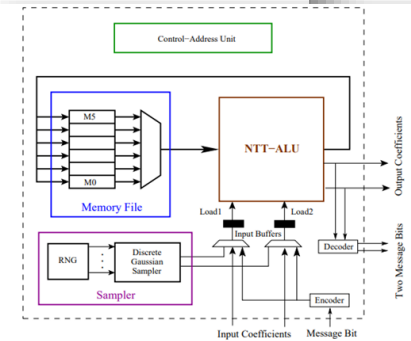


High-Speed ECC

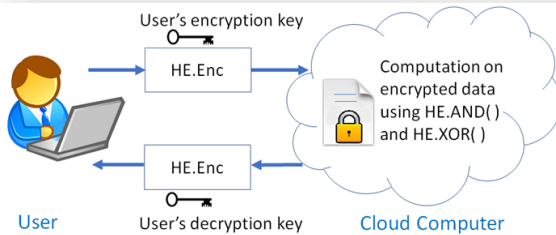
$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \cdot \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \\ \vdots \\ e_m \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \\ \vdots \\ b_m \end{pmatrix}$$

Lattice-based Cryptography

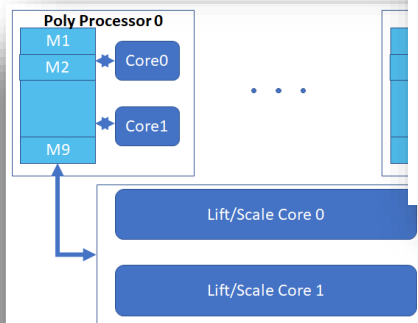
Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM (NIST Submissi



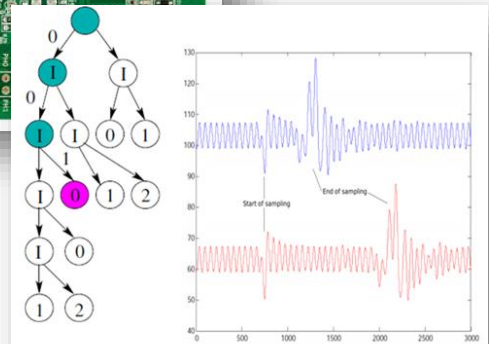
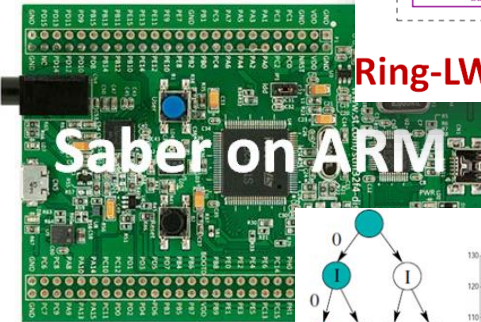
Ring-LWE Cryptoprocessor



Homomorphic Encryption



Ring-LWE Homomorphic Processor



Gaussian Sampling

Ideal Lattice-based Diffie-Hellman key-exchange



Public: polynomial a



$$s \leftarrow \text{error}()$$

$$e \leftarrow \text{error}()$$

$$b = a \cdot s + e$$

$$s' \leftarrow \text{error}()$$

$$e' \leftarrow \text{error}()$$

$$b' = a \cdot s' + e'$$

$$c = b' \cdot s = a \cdot s \cdot s' + e' \cdot s$$

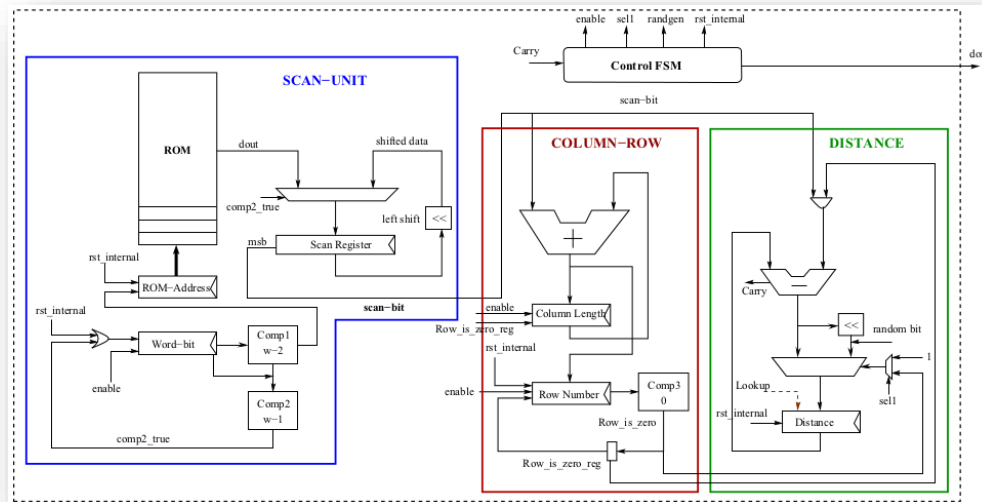
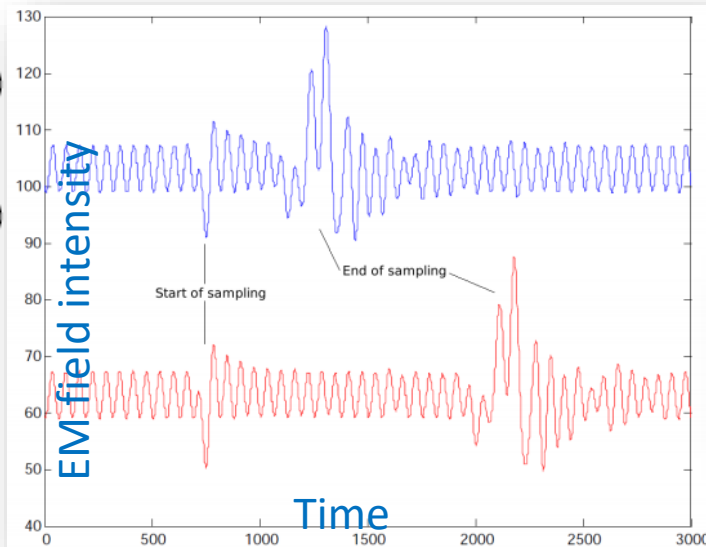
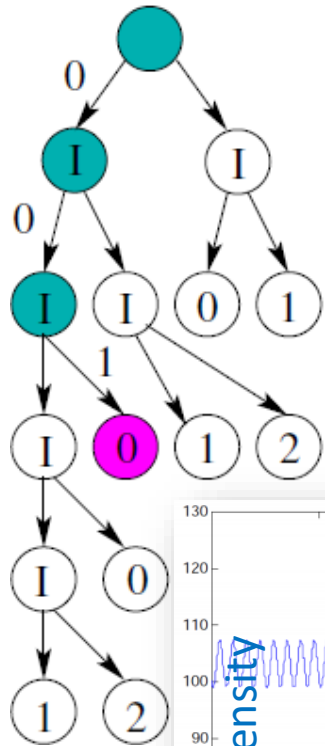
$$c' = b \cdot s' = a \cdot s \cdot s' + e \cdot s'$$

Shared poly with noise

$$\text{Difference} = |e' \cdot s - e \cdot s'|$$

Knuth-Yao

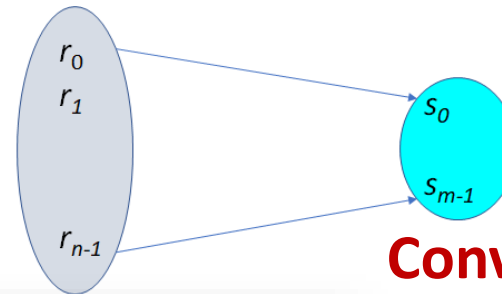
Random walk



Tiny HW architecture



Area: 44 slices
Cycles (avg.) 1.5



Convolution + Boolean Decomp + Bitslicing

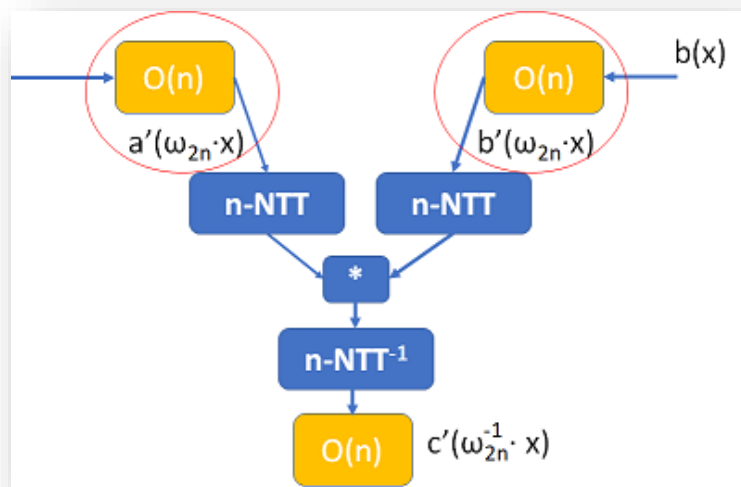
$$\begin{aligned} s_0 &= f^0(r_0, r_1, \dots, r_{n-1}) \\ &\dots \\ s_{m-1} &= f^{m-1}(r_0, r_1, \dots, r_{n-1}) \end{aligned}$$

Constant-time SW₄

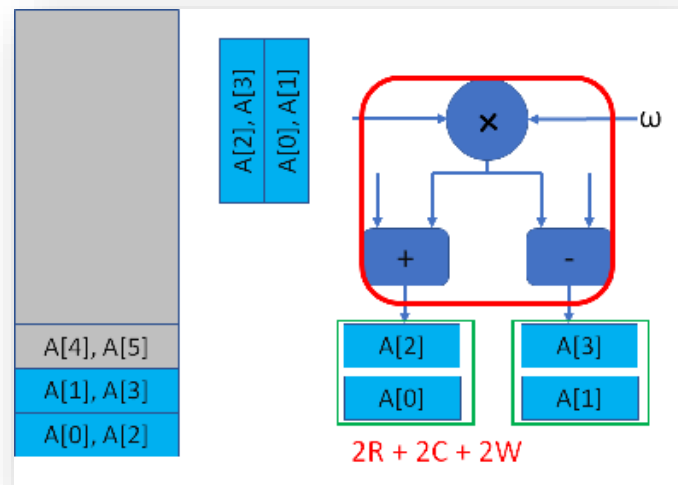
Polynomial Multiplication using NTT

Before $O(n) + O(n) + O(n \log n) + O(n)$

Eliminated
precomputation



Reduced memory
access overhead



Now ~~$O(n)$~~ + ~~$O(n)$~~ + $\frac{1}{2}O(n \log n)$ + $O(n)$

High-Speed lattice-based Cryptoprocessor, CHES 2014

First masking scheme for lattice-based crypto, CHES 2015

NIST National Institute of Standards and Technology
Information Technology Laboratory

Computer Security Division
Computer Security Resource Center

CSRC Home About Projects / Research Publications News & Events

Post-Quantum Cryptography Project

- Documents
- Workshops / Timeline
- Federal Register Notices
- Email Listserve
- PQC Project Contact
- Archive Information

Post-Quantum Cryptography Standardization

- Call for Proposals Announcement
- Call for Proposals
- Submission Requirements
- Minimum Acceptability Requirements

CSRC HOME > GROUPS > CT > POST-QUANTUM CRYPTOGRAPHY PROJECT

POST-QUANTUM CRYPTO PROJECT

NEWS -- December 15, 2016: The National Institute of Standards and Technology (NIST) is now accepting submissions for quantum-resistant public-key cryptographic algorithms. The deadline for submission is **November 30, 2017**. Please see the Post-Quantum Cryptography Standardization menu at left for the complete submission requirements and evaluation criteria.

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can

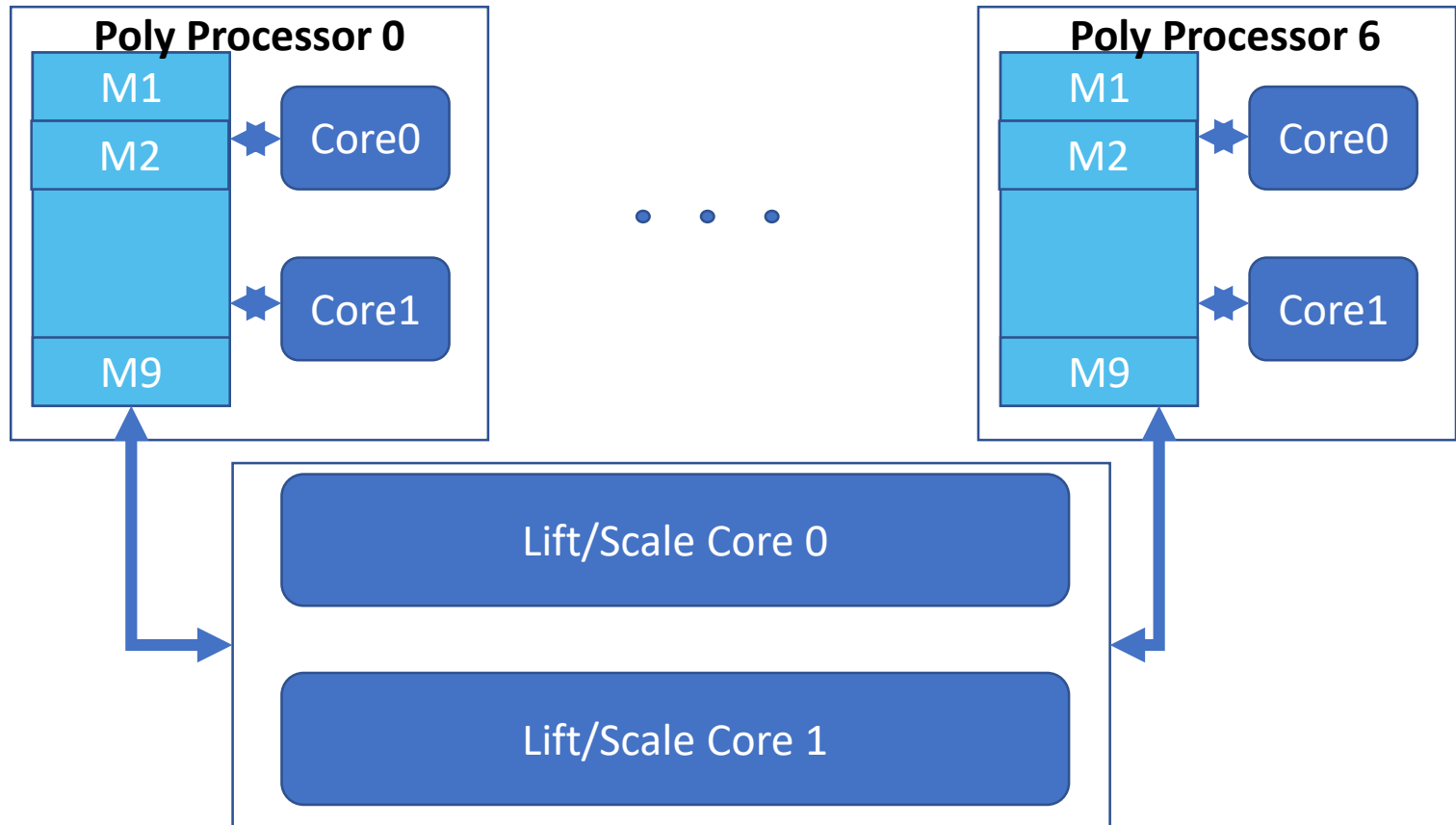
Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM

LWR problem

$$b = \left[\frac{p}{q} A s \right] \text{ where } p < q$$

Efficient, Flexible and Secure

Accelerator for homomorphic evaluation: privacy-preserving cloud computing



400 homomorphic multiplications / s
Faster than Tesla K80 GPU

To appear in High Performance Computing Architecture (HPCA) 2018

Thank you