NewHope for ARM

Erdem Alkim, Philipp Jakubeit, Peter Schwabe
Digital Security Group, Radboud University, Nijmegen, the Netherlands

Quantum Resistant Cryptography?

- Shor's algorithm published in 1994 solves in polynomial time
  - Factorization problem (e.g. RSA)
  - Discrete logarithm problem (e.g. ECC)
- Quantum computers are expected within 15 years (IBM).
- Threat?
  - Recording encrypted messages today
  - Breaking encryption with quantum computers
- Alternatives?
  - e.g. Lattice based cryptography

NewHope

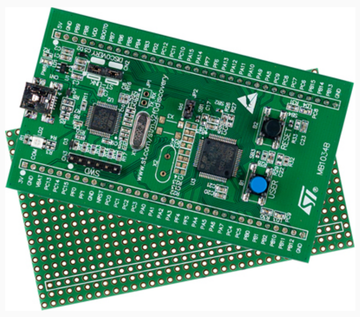
Ring Learning With Errors based ephemeral key exchange

Parameters: $\mathbf{q = 12289 < 2^{14}}$, $\mathbf{n = 1024}$
Error distribution: $\psi_{16}^{\mathbf{n}}$

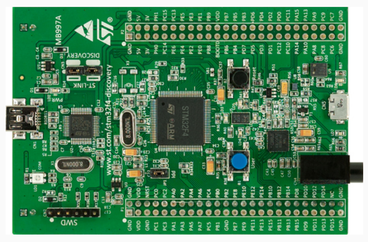
Alice (server)		**Bob (client)**
$\mathbf{seed} \xleftarrow{\$} \{0,\ldots,255\}^{32}$		
$\mathbf{a} \leftarrow$ Parse(SHAKE-128$(\mathbf{seed})$)		
$\mathbf{s}, \mathbf{e} \xleftarrow{\$} \psi_{16}^{\mathbf{n}}$		$\mathbf{s}', \mathbf{e}', \mathbf{e}'' \xleftarrow{\$} \psi_{16}^{\mathbf{n}}$
$\mathbf{b} \leftarrow \mathbf{as} + \mathbf{e}$	$\xrightarrow[\mathbf{1824}\text{ Bytes}]{(\mathbf{seed},\mathbf{b})}$	$\mathbf{a} \leftarrow$ Parse(SHAKE-128$(\mathbf{seed})$)
		$\mathbf{u} \leftarrow \mathbf{as}' + \mathbf{e}'$
		$\mathbf{v} \leftarrow \mathbf{bs}' + \mathbf{e}''$
$\mathbf{v}' \leftarrow \mathbf{us}$	$\xleftarrow[\mathbf{2048}\text{ Bytes}]{(\mathbf{u},\mathbf{r})}$	$\mathbf{r} \xleftarrow{\$}$ HelpRec$(\mathbf{v})$
$\nu \leftarrow$ Rec$(\mathbf{v}', \mathbf{r})$		$\nu \leftarrow$ Rec$(\mathbf{v}, \mathbf{r})$
$\mu \leftarrow$ SHA3-256(ν)		$\mu \leftarrow$ SHA3-256(ν)

- Relevant Building Blocks
  - Error distribution
  - Number theoretic transform (NTT).

ARM Cortex M family, ARMv6M and ARMv7M architecture



- STM32F0 Discovery board
- 8KB RAM
- 32-bit word size
- Thumb + subset Thumb 2
- 8 (+5) General-purpose registers
- 3 Reserved registers (SP,LR,PC)



- STM32F4 Discovery board
- 1MB Flash
- 32-bit word size
- Full Thumb 2
- 13 General-purpose registers
- 3 Reserved registers (SP,LR,PC)

Optimizations

Algorithmic

- Using Montgomery arithmetic
- Using short Barrett reductions
- Performing lazy reduction
- Negative-wrapped convolution
- Precomputing constants

Architectural

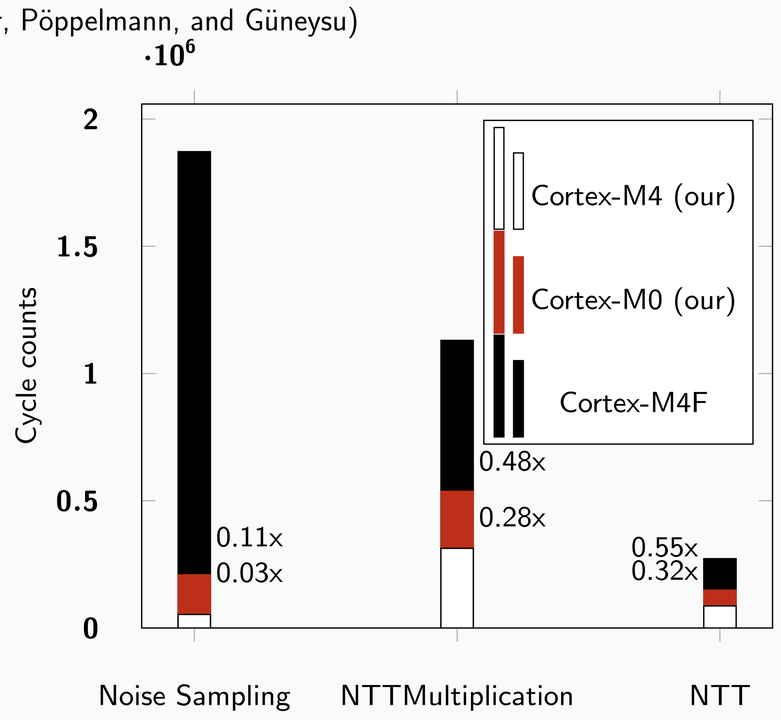
- Unrolling the NTT
- Adapting to word size
- Merging 2 NTT levels for M0
- Merging 3 NTT levels for M4
- Minimizing register reordering

Speed results compared to ECC

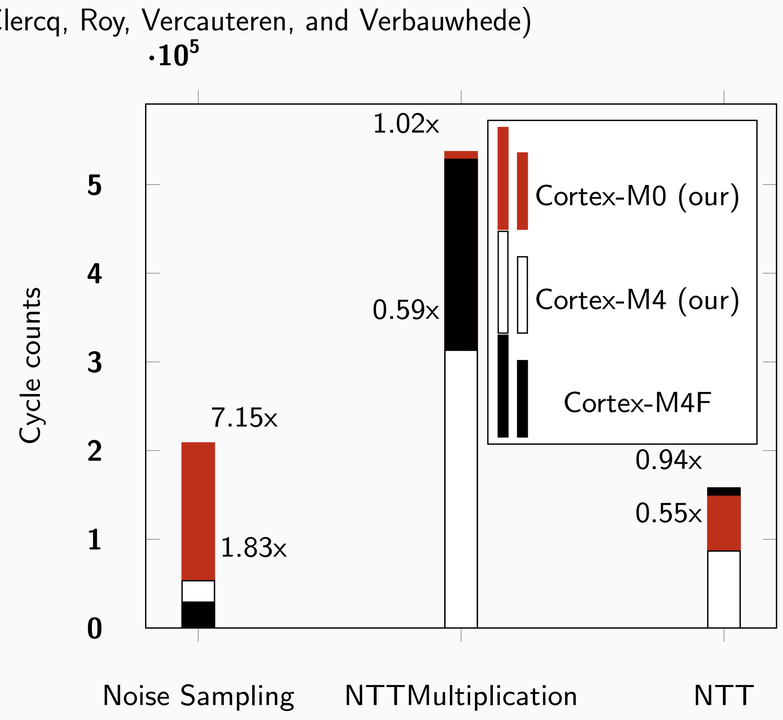
Operation	**Cycle Counts**	**48 MHz**
NewHope on M0	3228606	67.26ms
Curve25519 on M0	3513628	73.02ms
NewHope on M4	1816908	37.85ms
Curve25519 on M4	1607860	≈33.50ms

Comparison to literature

"Lattice-based digital signatures on constrained devices."
(Oder, Pöppelmann, and Güneysu)



"Efficient software implementation of ring-LWE encryption."
(de Clercq, Roy, Vercauteren, and Verbauwhede)



Paper and Code (Published at SPACE 2016)

https://eprint.iacr.org/2016/758.pdf

https://github.com/newhopearm

Radboud University