ROUND5

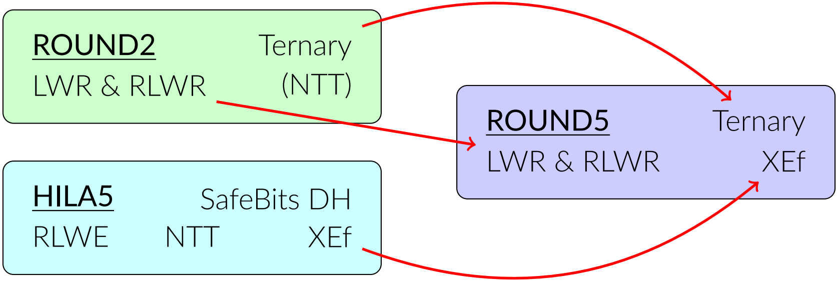
Update and Future Directions

Hayo Baan[1], Sauvik Bhattacharya[1], Scott Fluhrer[2], Oscar Garcia-Morchon[1], Thijs Laarhoven[3], Rachel Player[4], Ronald Rietman[1], Markku-Juhani O. Saarinen[5], Ludo Tolhuizen[1], Jose Luis Torre Arce[1], and Zhenfei Zhang[6]

1) Philips, NL
2) Cisco, US
3) TU/e, NL
4) RHUL, UK
5) PQShield, UK
6) Algorand, US

Second NIST PQC Standardization Conference
24 August 2019 – University of California, Santa Barbara

Round2 + Hila5 = Round5



- Round5 is a result of a merger between two first-stage NIST PQC candidates, Round2 and Hila5, and further design and analysis.
- Round5 is one of 9 lattice-based candidates in the second stage. It is based on Learning With Rounding (LWR) and Ring Learning With Rounding (RLWR).
- XEf error correction codes were the main feature inherited from Hila5.

Round5 Status

Round5 was announced in August 2018, and manuscripts were circulated early to gather feedback before submission to NIST in March 2019. Currently:

- **Bandwidth:** Has smallest key and message sizes among lattice candidates.
- **Performance:** Matching other candidates, very fast on embedded targets.
- **Flexibility:** Only lattice scheme with both ring and non-ring configurations with a unified description. Three security levels (NIST 1-3-5), CPA and CCA, optional error correction.

Publications:

[BBF+19] **"Round5: Compact and Fast Post-quantum Public-Key Encryption."** PQCrypto 2019, LNCS 11505, pp. 83–102, Springer 2019.

[SBG+18] **"Shorter Messages and Faster Post-Quantum Encryption with Round5 on Cortex M."** CARDIS 2018, LNCS 11389, pp. 95–110, Springer 2018.

Parameter Sets

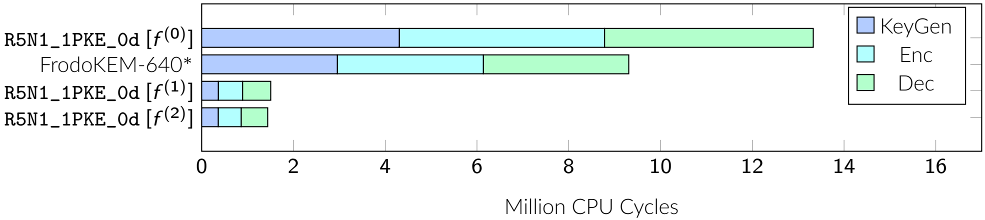
- Wide and dense design space supports applications with different trust assumptions, security levels, and performance requirements.
- The proposed parameter sets illustrate how NIST can pick up final parameters for standardization (depending on priorities that it sets):
  - Non-ring (**R5N1**) versions are more conservative than ring (**R5ND**) versions.
  - CPA-KEM is $\approx 10\,\%$ smaller (and faster) than CCA-PKE (CCA-KEM).
  - **R5ND** with error correction can be up to 25% smaller than without.
- Special variants demonstrate corner cases:
  - **R5ND_0KEM_2iot** shows how small Round5 can be.
  - **R5N1_3PKE_0smallCT** shows that if the public key can remain static, unstructured proposals are competitive with structured ones.

Round5: Structural Features

- **Unified description** by operating in $\mathcal{R}_{n,q}^{d/n}$, $\mathcal{R}_{n,q} = \mathbb{Z}_q[x]/\Phi_{n+1}(x)$ with $n+1$ prime. Non-ring and ring correspond to $n = 1$ and $n = d$, respectively.
- **LWR** / **RLWR** leads to lower bandwidth. No (Gaussian) noise sampling needed – fast, reduces need for random bits.
- **Power-of-2** moduli p, q, t; trivial reduction.
- **XEf**: Parametrized parity code for f-bit forward error correction. Usage of XEf requires ciphertext operations in $\mathcal{R}_{n,q} = x^{n+1} - 1$ and balanced secrets. Constant time (no branches or table lookups). Easy to mask.
- **Timing countermeasure** options with less than **50%** performance penalty. Can be masked to protect against EM and other more advanced side-channels.

Public Parameter A Generation

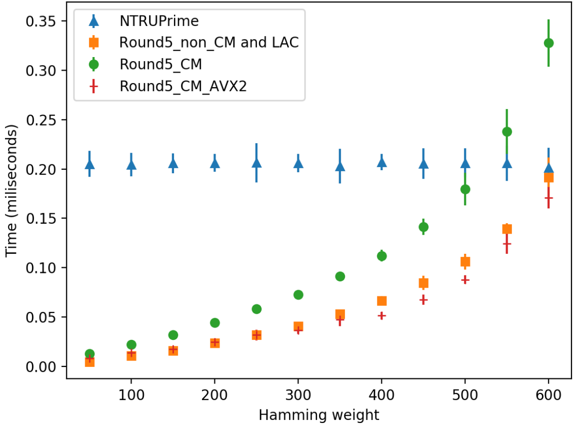
- Round5 defines three methods $f^{(0)}$, $f^{(1)}$, $f^{(2)}$ to generate public parameter **A**.
- $f^{(0)}$ derives **A** from a random seed with a "DRBG". It is always used in ring setting, and can be used for non-ring as well – but can be slow (large matrices).
- Non-ring variants benefit from 5-10 × faster performance with $f^{(1)}$ and $f^{(2)}$, which provide protection against pre-computation and backdoor attacks at the price of keeping some structure. $f^{(2)}$ is currently the "default" for non-ring.



Note (*): *Frodo640 AVX2 code relies on* ***shake*****128_4*****x****; R5N1_1PKE_0d [$f^{(0)}$] does not.*

Fixed-Weight Ternary Secrets

Secret coefficients $\in \{-1, 0, +1\}$, with fixed number of $0, \pm 1$. This means that "row" operations can be implemented with additions and subtractions (same number each).



- Excellent performance.
- Leads to lower failure probability.
- Harden against active attacks.
- Used in LAC, NTRUPrime, Round5 with three different types of implementations.

New AVX2 code (available at **`https://github.com/round5/code`**) improves performance, for example **`R5N1_3PKE_0smallCT`**: 33%, **`R5ND_5KEM_0d`**: 11%.

Validation of the Failure Model

		R5ND_1KEM_5d	R5ND_3KEM_5d	R5ND_5KEM_5d
Total Runs	S	8.5×10^9	2.2×10^9	2.8×10^9
One Error	n_1	$226,639$	$4,120$	$2,685,625$
Two Errors	n_2	6	0	$1,314$
Experimental	$\hat{p}_b$	$2^{-22.19}$	$2^{-26.61}$	$2^{-18.02}$
	n_2/S	$2^{-30.40}$	N/A	$2^{-21.02}$
Model	$\hat{p}_b$	$2^{-21.35}$	$2^{-26.61}$	$2^{-17.99}$
	n_2/S	$2^{-31.40}$	$2^{-39.06}$	$2^{-21.06}$

Experimental validation of the failure model can be done with standard `R5ND_xKEM_5d` parameter sets that have **high** failure probability.

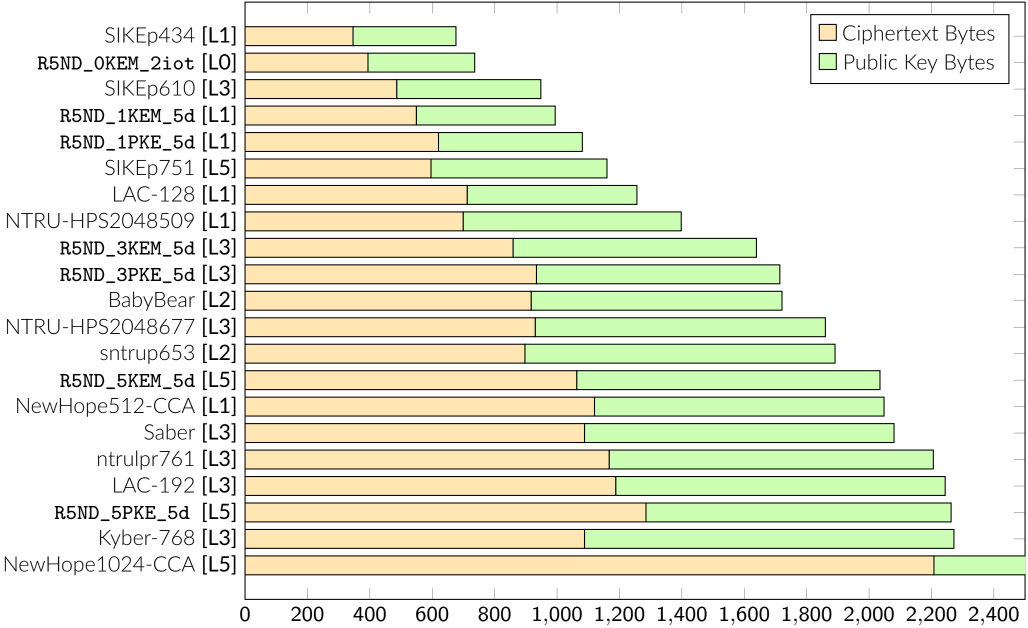
Tighter Security Analysis

- We're working on a tighter security analysis for Round5's small secrets, namely hybrid and extended dual (EDA) attacks.
- Preliminary results indicate that some parameter sets might lose up to 12 bits.
- Limited impact on security due to the underlying assumptions – e.g. the generation of $2^{0.2075b}$ short vectors in a single sieving call.

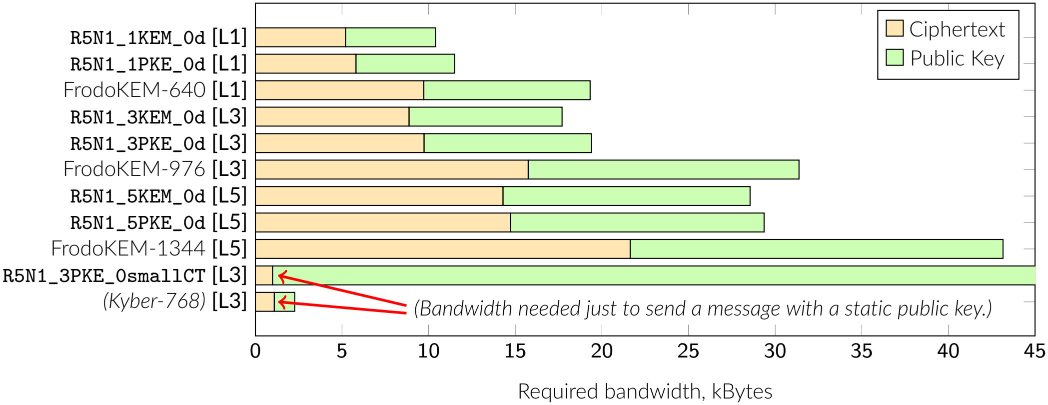
	Cost with Classical Sieving		
Configuration	**Current**	**EDA $2^{0.2075b}$**	**EDA (BKZ + LLL)**
R5ND_0KEM_2iot	96.1	93.3	135.4
R5ND_1KEM_5d	128.5	123.3	158.5
R5ND_3KEM_5d	192.7	185.1	222.5
R5ND_5KEM_5d	256.4	244.1	321.2

- A slight increase of parameters might apply for third round or standardization.
- Limited impact on bandwidth due to Round5's dense design space.

Bandwidth: R5ND Ring Variants

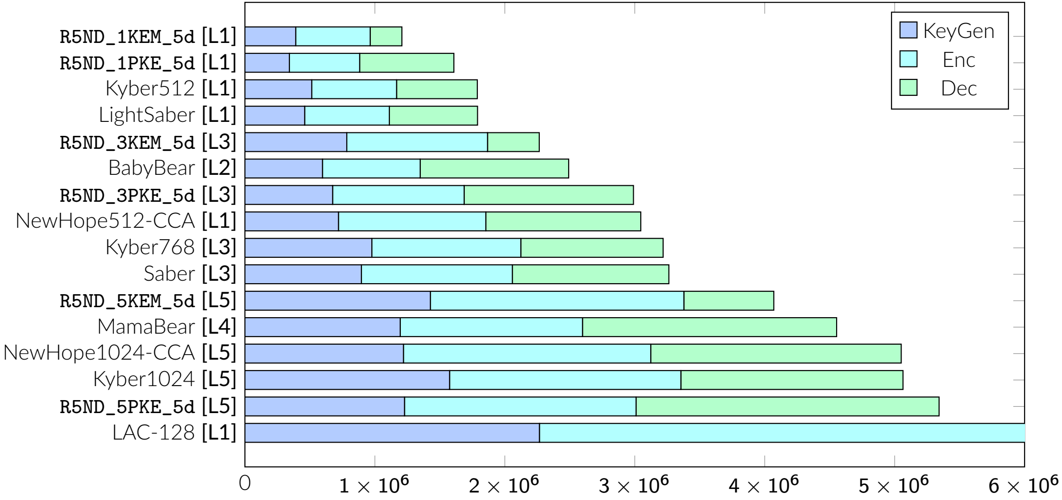


Bandwidth: R5N1 Non-Ring Variants



- Frodo's bandwidth requirements for L1 (L3) security are higher or roughly equivalent to Round5's needs for higher L3 (L5) security, respectively.
- `R5N1_3PKE_0smallCT` has a smaller (< 1kB) ciphertext size than most structured lattice proposals. It is a viable solution for applications with a static public key.

Embedded Performance: Cortex M4



Notes: These STM32F407 (@ 24Mhz) cycle measurements are from "pqm4" (**https://github.com/mupq/pqm4**) and "r5embed" (**https://github.com/r5embed/r5embed**) projects. Note that some some candidates are simply not suitable for lightweight applications; tens or hundreds of times slower and power consuming.

Real-World Round5 Hardware-Software Codesign

(PQShield's) RISC-V - based Security Microcontrollers can run **all variants of Round5** on the **same hardware**. The design is intended for ASIC (numbers announced later), but here are some current real-world Round5 Artix-7 FPGA results for comparison:

Resource Utilization

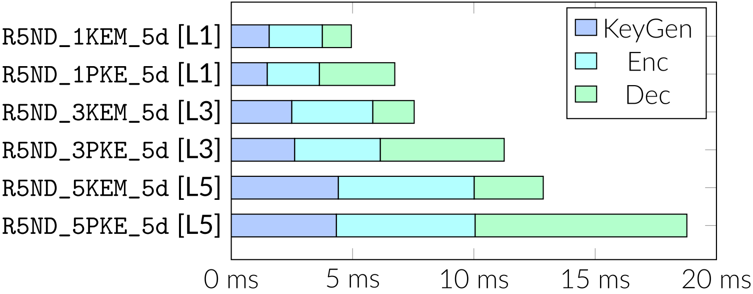
Artix-7 (XC7A35T) SoC

LUT	7,168
FF	3,337
Slice	2,344
DSP	0
MHz	100.0

Contained in this SoC:

- Single-cycle RV32I
- Lattice Coprocessor
- SHA-3 Accellerator
- UART RX/TX, GPIO

Latency for Ring Variants (Measured with NIST Software API):

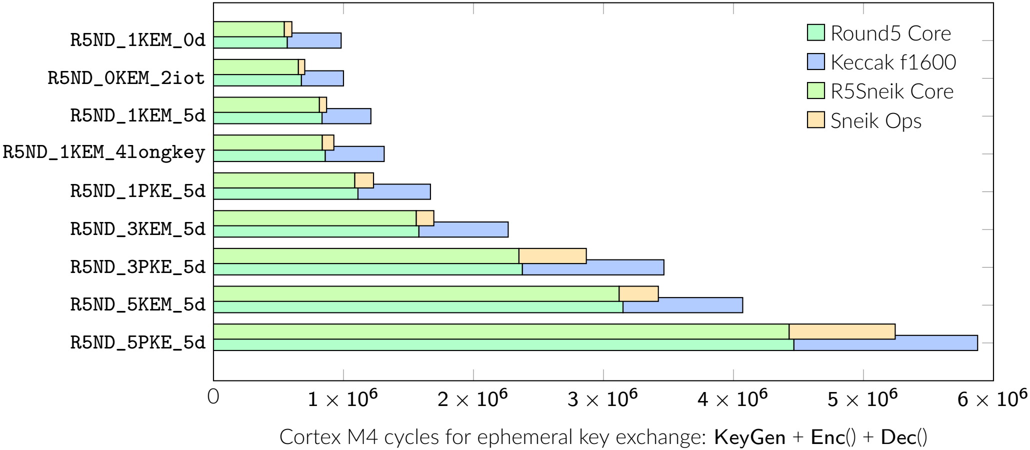


The coprocessors save > 80% of RISC-V cycles in this version.

Note: *This full, low-power SoC MCU uses under 10% of the resources of the FPGA part of the "GMU" (Zynq UltraScale+) Round5 codesign.*

A Note about SHAKE and R5Sneik

- Round5 can spend up to 40% (`R5ND_1KEM_0d`) of its time just doing SHAKE *f*1600 computations. With some other lattice algorithms this is even more.
- A fast *f*1600 is huge: The "SHA-3" part of our SoC is as big as the CPU Core!
- SNEIK (NIST LWC) is ≈ 10% of the *f*1600 HW size and much quicker in SW:



Round5 Challenges

As a follow-up of Edoardo Persichetti's email, **24 challenges** will be published:

$$
\left.\begin{array}{r}\text{Toy}\\ \text{Easy}\\ \text{Medium}\\ \text{Hard}\end{array}\right\} 4 \times 6 \left\{\begin{array}{l}
\text{R5N1 (non-ring) with } \mathbf{A} \text{ using } f^{(0)} \text{ method,}\\
\text{R5N1 (non-ring) with } \mathbf{A} \text{ using } f^{(1)} \text{ method,}\\
\text{R5N1 (non-ring) with } \mathbf{A} \text{ using } f^{(2)} \text{ method,}\\
\text{R5ND (ring) without error correction,}\\
\text{R5ND (ring) with error correction,}\\
\text{R5ND (ring) with EC, very high failure rate.}
\end{array}\right.
$$

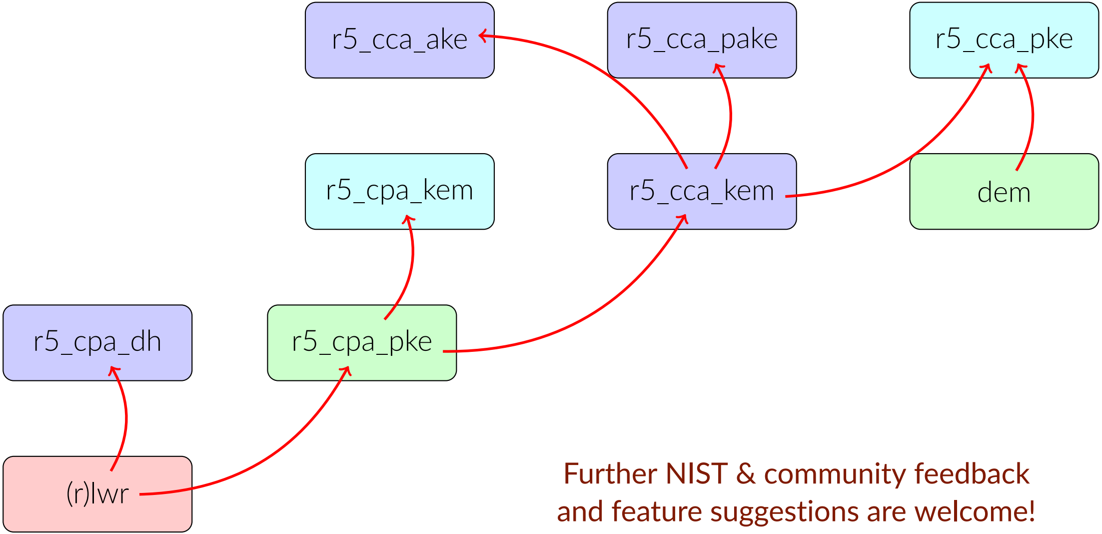
Conclusions and Way Forward

Round5 suits a wide range of applications with its unified design, dense parameter space, great bandwidth, and excellent performance on a variety of platforms.

Coming soon:

- New implementations: Single code base for multiple platforms.
- Further work to scrutinize Round5 security.
- Round5 challenges online.
- Expose internal Round5 CCAKEM to implementers and offer new building blocks on top of it: AKE, PAKE next to the submitted Round5 PKE.

Questions and Suggestions



Further NIST & community feedback and feature suggestions are welcome!