ROUND5
Update and Future Directions

Hayo Baan¹, Sauvik Bhattacharya¹, Scott Fluhrer², Oscar Garcia-Morchon¹, Thijs Laarhoven³, Rachel Player⁴, Ronald Rietman¹, Markku-Juhani O. Saarinen⁵, Ludo Tolhuizen¹, Jose Luis Torre Arce¹, and Zhenfei Zhang⁶

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
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:


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_0smallICT shows that if the public key can remain static, unstructured proposals are competitive with structured ones.
Round5: Structural Features

- **Unified description** by operating in $\mathcal{R}_{d/n}^{n,q}$, $\mathcal{R}_{n,q} = \mathbb{Z}_q[x]/\Phi_{n+1}(x)$ 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.

- **XE$f$**: Parametrized parity code for $f$-bit forward error correction. Usage of XE$f$ 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 $5-10 \times$ 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 $\text{shake128}_4x$; 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

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

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

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Current</th>
<th>EDA $2^{0.2075b}$</th>
<th>EDA (BKZ + LLL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R5ND_0KEM_2iot</td>
<td>96.1</td>
<td>93.3</td>
<td>135.4</td>
</tr>
<tr>
<td>R5ND_1KEM_5d</td>
<td>128.5</td>
<td>123.3</td>
<td>158.5</td>
</tr>
<tr>
<td>R5ND_3KEM_5d</td>
<td>192.7</td>
<td>185.1</td>
<td>222.5</td>
</tr>
<tr>
<td>R5ND_5KEM_5d</td>
<td>256.4</td>
<td>244.1</td>
<td>321.2</td>
</tr>
</tbody>
</table>

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

- **SIKEp434 [L1]**
- **R5ND_0KEM_2iot [L0]**
- **SIKEp610 [L3]**
- **R5ND_1KEM_5d [L1]**
- **R5ND_1PKE_5d [L1]**
- **SIKEp751 [L5]**
- **LAC-128 [L1]**
- **NTRU-HPS2048509 [L1]**
- **R5ND_3KEM_5d [L3]**
- **R5ND_3PKE_5d [L3]**
- **BabyBear [L2]**
- **NTRU-HPS2048677 [L3]**
- **sntrup653 [L2]**
- **R5ND_5KEM_5d [L5]**
- **NewHope512-CCA [L1]**
- **Saber [L3]**
- **ntrulpr761 [L3]**
- **LAC-192 [L3]**
- **R5ND_5PKE_5d [L5]**
- **Kyber-768 [L3]**
- **NewHope1024-CCA [L5]**

- **Ciphertext Bytes**
- **Public Key Bytes**

- **0 / 17**
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 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

<table>
<thead>
<tr>
<th>Resource</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>LUT</td>
<td>7,168</td>
</tr>
<tr>
<td>FF</td>
<td>3,337</td>
</tr>
<tr>
<td>Slice</td>
<td>2,344</td>
</tr>
<tr>
<td>DSP</td>
<td>0</td>
</tr>
<tr>
<td>MHz</td>
<td>100.0</td>
</tr>
</tbody>
</table>

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):

<table>
<thead>
<tr>
<th>Variant</th>
<th>Latency (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R5ND_1KEM_5d [L1]</td>
<td>0</td>
</tr>
<tr>
<td>R5ND_1PKE_5d [L1]</td>
<td>5</td>
</tr>
<tr>
<td>R5ND_3KEM_5d [L3]</td>
<td>10</td>
</tr>
<tr>
<td>R5ND_3PKE_5d [L3]</td>
<td>15</td>
</tr>
<tr>
<td>R5ND_5KEM_5d [L5]</td>
<td>20</td>
</tr>
<tr>
<td>R5ND_5PKE_5d [L5]</td>
<td>20</td>
</tr>
</tbody>
</table>

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% (\texttt{R5ND\textunderscore 1KEM\textunderscore 0d}) of its time just doing SHAKE \texttt{f1600} computations. With some other lattice algorithms this is even more.
- A fast \texttt{f1600} is huge: The “SHA-3” part of our SoC is as big as the CPU Core!
- SNEIK (NIST LWC) is $\approx 10\%$ of the \texttt{f1600} HW size and much quicker in SW:
As a follow-up of Edoardo Persichetti’s email, **24 challenges** will be published:

- Toy
- Easy
- Medium
- Hard

\[
\begin{array}{c}
\text{R5N1 (non-ring) with } A \text{ using } f^{(0)} \text{ method,} \\
\text{R5N1 (non-ring) with } A \text{ using } f^{(1)} \text{ method,} \\
\text{R5N1 (non-ring) with } A \text{ using } f^{(2)} \text{ method,} \\
\text{R5ND (ring) without error correction,} \\
\text{R5ND (ring) with error correction,} \\
\text{R5ND (ring) with EC, very high failure rate.}
\end{array}
\]
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!