Standard Lattice-Based Key Encapsulation on Embedded Devices

James Howe†, Tobias Oder‡, Markus Krausz‡, and Tim Güneysu‡∗.

†University of Bristol, UK; ‡Ruhr-Universität Bochum, Germany; and *DFKI, Germany.
Outline

- Post-quantum cryptography and LWE
- Motivation
- Introduction to Frodo
- Microcontroller design
- Hardware design
- Results and performance analysis
Motivation

NIST have started a post-quantum standardisation “competition”.

The call suggests future rounds will likely involve:
- Evaluations on constrained devices, such as smart cards,
- as well as comparisons of the schemes in hardware.

Why focus on lattice-based / Frodo?
- Extremely versatile and theoretically sound.
- Probably the most secure lattice candidate.
- Less implementations than ideal lattice schemes; has larger keys and no NTT.
- Frodo is ideal for long-term security and constrained (hardware) platforms.
Frodo: Take off the ring!

The design philosophy of FrodoKEM [ABD⁺] combines:

- Conservative yet practical post-quantum constructions.
- Security derived from cautious parameterizations of the well-studied learning with errors problem.
- Thus, close connections to conjectured-hard problems on generic, “algebraically unstructured” lattices.
- Parameter selection is far less constrained than vs ideal lattice schemes.
Frodo: Why should we take off the ring?

These qualities are appealing for practitioners;

- Many IoT use cases require long-term, efficient cryptography.
- Post-quantum cryptography is becoming essential.
- Microcontrollers and FPGAs will play a role in future technologies.
- Suitable for use cases such as satellite communications and V2X.
Frodo: key encapsulation from standard lattices

Algorithm 1 The FrodoKEM encapsulation (shortened)

1: \textbf{procedure} \textsc{Encaps}(pk = \text{seed}_A || b)
2: \hspace{1em} Choose a uniformly random key $\mu \leftarrow U(\{0, 1\}^{\text{len}_\mu})$
3: \hspace{1em} Generate pseudo-random values $\text{seed}_E || k || d \leftarrow G(pk || \mu)$
4: \hspace{1em} Sample error matrix $S', E' \leftarrow \text{Frodo.SampleMatrix}(\text{seed}_E, \bar{m}, n, T_\chi, \cdot)$
5: \hspace{1em} Generate the matrix $A \in \mathbb{Z}_q^{n \times n}$ via $A \leftarrow \text{Frodo.Gen}(\text{seed}_A)$
6: \hspace{1em} Compute $C_1 \leftarrow S' A + E'$
7: \hspace{1em} Sample error matrix $E'' \leftarrow \text{Frodo.SampleMatrix}(\text{seed}_E, \bar{m}, \bar{n}, T_\chi, \cdot)$
8: \hspace{1em} Compute $C_2 \leftarrow S' B + E'' + \text{Frodo.Encode}(\mu)$
9: \hspace{1em} Compute $ss \leftarrow F(c_1 || c_2 || k || d)$
10: \textbf{return} ciphertext $c_1 || c_2 || d$ and shared secret $ss$
11: \textbf{end procedure}
Frodo: key encapsulation from standard lattices

FrodoKEM is comprised of a number of key modules:

- Matrix-matrix multiplication, up to sizes 976.
- Uniform and “Gaussian” error generation.
- Random oracles via cSHAKE for CCA security.

A massive design challenge was to balance memory utilisation, whilst not deteriorating the performance too much to not overexert the limited computing capabilities of the embedded devices.
FrodoKEM has a number of design options we cover:

- Both sets of parameters;
  - FrodoKEM-640 aims to match AES-128 security.
  - FrodoKEM-976 aims to match AES-192 security.

- PRNG from AES and cSHAKE modules.

- We focus on FrodoKEM, rather than the previous key exchange scheme FrodoCCS [BCD+16].
FrodoKEM on ARM

Contribution overview:

- Optimized memory allocation that makes the implementation small enough to fit on embedded microcontrollers.
- An assembly multiplication routine that speeds up our implementation, realizing a performance that fits the requirements of common use-cases.
- Utilises constant runtime to protect against simple side-channel analysis.
- FrodoKEM-640 has a total execution time of 836 ms, running at 168 MHz.
FrodoKEM on ARM

We analysed the memory occupancy during each operation.

Wherever possible, reusing already allocated memory.

This minimised the memory usage for all designs.

Memory usage for AES versions much simpler than for cSHAKE versions.

Figure: FrodoKEM encaps flowchart.
Results and Comparisons

- Clear difference between AES and cSHAKE implementations.
- Due to more efficient AES [SS16], cSHAKE needs load/save from RAM.
- Outperforms other Frodo design, but much slower than Kyber / NewHope.

Table: Cycle counts for our full microcontroller implementations (at 168 MHz).

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Platform</th>
<th>Security Level</th>
<th>Cycle counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>FrodoKEM-640-AES</td>
<td>Cortex-M4</td>
<td>128 bits</td>
<td>140,398,055</td>
</tr>
<tr>
<td>FrodoKEM-976-AES</td>
<td>Cortex-M4</td>
<td>192 bits</td>
<td>315,600,317</td>
</tr>
<tr>
<td>FrodoKEM-640-cSHAKE</td>
<td>Cortex-M4</td>
<td>128 bits</td>
<td>310,131,435</td>
</tr>
<tr>
<td>FrodoKEM-976-cSHAKE</td>
<td>Cortex-M4</td>
<td>192 bits</td>
<td>695,001,098</td>
</tr>
<tr>
<td>KyberNIST-768 [pqm]</td>
<td>Cortex-M4</td>
<td>192 bits</td>
<td>4,224,704</td>
</tr>
<tr>
<td>NewHopeUSENIX-1024 [AJS16]</td>
<td>Cortex-M4</td>
<td>255 bits</td>
<td>2,561,438</td>
</tr>
<tr>
<td>ECDH scalar multiplication [DHH+15]</td>
<td>Cortex-M0</td>
<td>pre-quantum</td>
<td>3,589,850</td>
</tr>
</tbody>
</table>
Results and Comparisons

- Despite being slower, cSHAKE requires less memory than AES.
- Our memory optimisations save between 30-40% compared to PQM4.
- Versus the referenced designs we also save 66% in peak stack usage.

**Table:** Stack usage in bytes for our microcontroller implementations.

<table>
<thead>
<tr>
<th>Operation</th>
<th>FrodoKEM-AES $n = 640$</th>
<th>FrodoKEM-AES $n = 976$</th>
<th>FrodoKEM-cSHAKE $n = 640$</th>
<th>FrodoKEM-cSHAKE $n = 976$</th>
<th>FrodoKEM-cSHAKE [pqm] $n = 640$</th>
<th>% Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keypair</td>
<td>23,396</td>
<td>35,484</td>
<td>22,376</td>
<td>33,800</td>
<td>36,536</td>
<td>39%</td>
</tr>
<tr>
<td>Encaps</td>
<td>41,292</td>
<td>63,484</td>
<td>37,792</td>
<td>57,968</td>
<td>58,328</td>
<td>35%</td>
</tr>
<tr>
<td>Decaps</td>
<td>51,684</td>
<td>63,628</td>
<td>48,184</td>
<td>58,112</td>
<td>68,680</td>
<td>30%</td>
</tr>
</tbody>
</table>
Contribution overview:

- Proposes a generic LWE multiplication core which computes vector-matrix multiplication and error addition.
- Generates future random values in parallel, minimising delays between vector-matrix multiplications.
- Hybrid pre-calculated / on-the-fly memory management is used, which continuously updates previous values.
- Ensures constant runtime by parallelising other modules with multiplication.
- FrodoKEM-640 has a total execution time of 60 ms, running at 167MHz.
FrodoKEM on FPGA

Figure: An overview of our FPGA design of FrodoKEM Encapsulation.
Results and Comparisons

- Competes with NewHope area consumption, but much slower performance.
- Huge savings in BRAM compared to LWE Encryption [HMO$^+$ 16].

Table: FPGA consumption and performance of our proposed designs, benchmarked on Artix-7.

<table>
<thead>
<tr>
<th>Cryptographic Operation</th>
<th>LUT/FF</th>
<th>Slice</th>
<th>DSP</th>
<th>BRAM</th>
<th>MHz</th>
<th>Ops/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>FrodoKEM-640 Keypair</td>
<td>6621/3511</td>
<td>1845</td>
<td>1</td>
<td>6</td>
<td>167</td>
<td>51</td>
</tr>
<tr>
<td>FrodoKEM-640 Encaps</td>
<td>6745/3528</td>
<td>1855</td>
<td>1</td>
<td>11</td>
<td>167</td>
<td>51</td>
</tr>
<tr>
<td>FrodoKEM-640 Decaps</td>
<td>7220/3549</td>
<td>1992</td>
<td>1</td>
<td>16</td>
<td>162</td>
<td>49</td>
</tr>
<tr>
<td>FrodoKEM-976 Keypair</td>
<td>7155/3528</td>
<td>1981</td>
<td>1</td>
<td>8</td>
<td>167</td>
<td>22</td>
</tr>
<tr>
<td>FrodoKEM-976 Encaps</td>
<td>7209/3537</td>
<td>1985</td>
<td>1</td>
<td>16</td>
<td>167</td>
<td>22</td>
</tr>
<tr>
<td>FrodoKEM-976 Decaps</td>
<td>7773/3559</td>
<td>2158</td>
<td>1</td>
<td>24</td>
<td>162</td>
<td>21</td>
</tr>
<tr>
<td>cSHAKE*</td>
<td>2744/1685</td>
<td>766</td>
<td>0</td>
<td>0</td>
<td>172</td>
<td>1.2m</td>
</tr>
<tr>
<td>Error+AES Sampler*</td>
<td>1901/1140</td>
<td>756</td>
<td>0</td>
<td>0</td>
<td>184</td>
<td>184m</td>
</tr>
<tr>
<td>NewHopeUSENIX Server [OG17]</td>
<td>5142/4452</td>
<td>1708</td>
<td>2</td>
<td>4</td>
<td>125</td>
<td>731</td>
</tr>
<tr>
<td>NewHopeUSENIX Client [OG17]</td>
<td>4498/4635</td>
<td>1483</td>
<td>2</td>
<td>4</td>
<td>117</td>
<td>653</td>
</tr>
<tr>
<td>LWE Encryption [HMO$^+$ 16]</td>
<td>6078/4676</td>
<td>1811</td>
<td>1</td>
<td>73</td>
<td>125</td>
<td>1272</td>
</tr>
</tbody>
</table>
Conclusions

- We show that hardware significantly minimises the performance distance between standard and ideal lattice-based KEM, able to utilise less than 2000 slices and remain practical.

- Memory optimisations for microcontrollers show 66% savings vs reference design and 40% vs optimised PQM4 design.

- It would be interesting to see results for Frodo on FPGA with increased multipliers. As well as how it performs vs. other NIST PQC candidates.
Conclusions

Our results show the efficiency of FrodoKEM and help to assess the practical performance of a possible future post-quantum standard.
Although rings are still good to use, unless you’re Gollum...

Thank you for listening. Any questions?
References

FrodoKEM Learning With Errors key encapsulation.

Erdem Alkim, Philipp Jakubeit, and Peter Schwabe.
NewHope on ARM cortex-M.

Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila.
Frodo: Take off the ring! practical, quantum-secure key exchange from LWE.
Michael Düll, Björn Haase, Gesine Hinterwälder, Michael Hutter, Christof Paar, Ana Helena Sánchez, and Peter Schwabe.
High-speed curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers.

Lattice-based encryption over standard lattices in hardware.

Tobias Oder and Tim Güneysu.
Implementing the NewHope-simple key exchange on low-cost FPGAs.

pqm4 - post-quantum crypto library for the ARM Cortex-M4.
References III

Peter Schwabe and Ko Stoffelen.
All the AES you need on Cortex-M3 and M4.