Implementing and Benchmarking Three Lattice-based Post-Quantum Cryptography Algorithms Using Software/Hardware Codesign

Viet B. Dang, Farnoud Farahmand, Michał Andrzejczak, Kris Gaj

George Mason University
Co-Authors

GMU PhD Students

Viet Ba Dang
Farnoud Farahmand

Visiting Scholar

Michał Andrzejczak
Military University of Technology in Warsaw, Poland
Quantum Computers

• Substantial investments by: Google, IBM, Intel, Microsoft, Alcatel-Lucent, NTT

• Quantum computers based on superconducting circuits operating in the temperature close to absolute 0 (~0.01 K)

• November 2017: IBM’s 50-qubit chip
• January 2018: Intel’s 49-qubit chip, “Tangle-Lake”
• March 2018: Google’s 72-qubit chip “Bristlecone”
• October 2019: Quantum supremacy experiment made public by Google

Photos: https://www.technologyreview.com
1994: Shor’s Algorithm, breaks major public key cryptosystems based on

Factoring: RSA

Discrete logarithm problem (DLP): DSA, Diffie-Hellman

Elliptic Curve DLP: Elliptic Curve Cryptosystems

independently of the key size assuming
a sufficiently powerful and reliable quantum computer available
How Real Is the Danger?

“There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031.”

Dr. Michele Mosca
Deputy Director of the Institute for Quantum Computing, University of Waterloo
April 2015

Source: Vandersypen, PQCrypto 2017
Post-Quantum Cryptography (PQC)

- Public-key cryptographic algorithms for which there are no known attacks using quantum computers
- Capable of being implemented using any traditional methods, including software and hardware
- Running efficiently on any modern computing platforms: smartphones, tablets, PCs, servers with FPGA accelerators, etc.
- Based entirely on traditional semiconductor VLSI technology!
Cryptographic Contests 2007-Present

51 hash functions → 1 winner
X.2007  →  X.2012
SHA-3

57 authenticated ciphers → multiple winners
II.2013  →  II.2019
CAESAR

69 Public-Key Post-Quantum Cryptography Schemes
XII.2016  →  TBD
Post-Quantum

Year
07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22
## Round 2 Candidates

26 Candidates announced on January 30, 2019

<table>
<thead>
<tr>
<th>Family</th>
<th>Signature</th>
<th>Encryption/KEM</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice-based</td>
<td>3</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Code-based</td>
<td></td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Multivariate</td>
<td>4</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Symmetric-based</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Isogeny-based</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>9</strong></td>
<td><strong>17</strong></td>
<td><strong>26</strong></td>
</tr>
</tbody>
</table>

Round 2 Evaluation until mid-2020  
To be followed by Round 3, 12-18 months
Evaluation Criteria

Security

Software Efficiency
- µProcessors
- µControllers

Hardware Efficiency
- FPGAs
- ASICs

Flexibility
Simplicity
Licensing
<table>
<thead>
<tr>
<th></th>
<th>#Round 2 candidates</th>
<th>Implemented in hardware</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>5</td>
<td>5</td>
<td>100%</td>
</tr>
<tr>
<td>SHA-3</td>
<td>14</td>
<td>14</td>
<td>100%</td>
</tr>
<tr>
<td>CAESAR</td>
<td>29</td>
<td>28</td>
<td>97%</td>
</tr>
<tr>
<td>PQC</td>
<td>26</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>
Software/Hardware Codesign

Software

Hardware

Most time-critical operation
SW/HW Codesign: Motivational Example 1

### Software

- **Major**: 91%
- **Other**: 9%

### Software/Hardware

- **Major**: ~1%
- **Other**: 9%

**Time saved**: 90%

**Speed-up**: ≥ 100

91% major operation(s)  ➔  ~1% major operation(s) in HW
9% other operations  ➔  9% other operations in SW

**Total Speed-Up**: ≥ 10
Software

- Major: 99%
- Other: 1%

Software/Hardware

- Major: ~1%
- Other: 1%

Time saved 98%

Speed-up ≥ 100

99% major operation(s)
1% other operations

~1% major operation(s) in HW
1% other operations in SW

Total Speed-Up ≥ 50
Platform & Experimental Setup

Xilinx Zynq UltraScale+ MPSoC

PS: Processing System
1.2 GHz ARM Cortex-A53

PL: Programmable Logic
UltraScale+ FPGA logic
SW/HW Codesign: Advantages

- Focus on a few major operations, known to be easily parallelizable
  - much shorter development time (at least by a factor of 10)
  - guaranteed substantial speed-up
  - high-flexibility to changes in other operations (such as candidate tweaks)

- Possibility of implementing multiple candidates by the same research group, eliminating the influence of different assumptions, design skills, tools, etc.
SW/HW Codesign: Potential Pitfalls

- Performance & ranking may strongly depend on
  
  A. features of a particular platform
     - Software/hardware interface
     - Support for cache coherency
     - Differences in max. clock frequency
  
  B. selected hardware/software partitioning
  
  C. optimization of an underlying software implementation

- Limited insight on ranking of purely hardware implementations

First step, not the ultimate solution!
Our Case Study
## Round 2 Candidates

26 Candidates announced on January 30, 2019

<table>
<thead>
<tr>
<th>Family</th>
<th>Signature</th>
<th>Encryption/KEM</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice-based</td>
<td>3</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Code-based</td>
<td></td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Multivariate</td>
<td>4</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Symmetric-based</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Isogeny-based</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>9</strong></td>
<td><strong>17</strong></td>
<td><strong>26</strong></td>
</tr>
</tbody>
</table>

Round 2 Evaluation until mid-2020
To be followed by Round 3, 12-18 months
A way to agree on a common key for secret-key cryptography
SW/HW Codesign: Case Study

7 Lattice-Based Key Encapsulation Mechanisms representing
5 NIST PQC Round 2 Submissions

- LWE (Learning with Error)-based:
  - FrodoKEM
- RLWR (Ring Learning with Rounding)-based:
  - Round5
- Module-LWR-based:
  - Saber

3 schemes with designs described in detail in the FPT paper

NTRU-based:
- NTRU
  - NTRU-HPS
  - NTRU-HRSS
- NTRU Prime
  - Streamlined NTRU Prime
  - NTRU LPRime

4 schemes with results obtained after the paper submission. Presentation only!
## Five Security Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Security Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>At least as hard to break as <strong>AES-128</strong> using exhaustive key search</td>
</tr>
<tr>
<td>II</td>
<td>At least as hard to break as <strong>SHA-256</strong> using collision search</td>
</tr>
<tr>
<td>III</td>
<td>At least as hard to break as <strong>AES-192</strong> using exhaustive key search</td>
</tr>
<tr>
<td>IV</td>
<td>At least as hard to break as <strong>SHA-384</strong> using collision search</td>
</tr>
<tr>
<td>V</td>
<td>At least as hard to break as <strong>AES-256</strong> using exhaustive key search</td>
</tr>
</tbody>
</table>
SW/HW Partitioning

Top candidates for offloading to hardware

From profiling:
- Large percentage of the execution time
- Small number of function calls

From manual analysis of the code:
- Small size of inputs and outputs
- Potential for combining with neighboring functions

From knowledge of operations and concurrent computing:
- High potential for parallelization
Operations Offloaded to Hardware

- Major arithmetic operations
  - Polynomial multiplications
  - Matrix-by-vector multiplications
  - Vector-by-vector multiplications
- All hash-based operations
  - (c)SHAKE128, (c)SHAKE256
  - SHA3-256, SHA3-512
Example: LightSaber Decapsulation

- InnerProduct: 43.52%
- MatrixVectorMul: 43.44%
- GenSecret: 2.30%
- Hash: 3.30%
- GenMatrix: 5.03%
- Other: 2.40%
- Other: 2.40%
LightSaber Decapsulation

Execution time of functions to be moved to hardware
97.60%

Execution time of functions remaining in software
2.40%

Accelerator Speed-Up = 97.60/8.77=11.1

Total Speed-Up = 100/11.17=9.0
Results
Total Execution Time in Software [$\mu$s]  
Decapsulation

<table>
<thead>
<tr>
<th>Round5</th>
<th>Saber</th>
<th>Str NTRU Prime</th>
<th>NTRU LPrime</th>
<th>NTRU-HPS</th>
<th>NTRU-HRSS</th>
<th>FrodoKEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>193</td>
<td>309</td>
<td>2,100</td>
<td>2,304</td>
<td>11,982</td>
<td>8,790</td>
<td>8,790</td>
</tr>
<tr>
<td>416</td>
<td>471</td>
<td>1,376</td>
<td>2,591</td>
<td>8,175</td>
<td>8,175</td>
<td>8,175</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1,651</td>
<td>1,868</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>867</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Levels:  
- Level 1  
- Level 2  
- Level 3  
- Level 4  
- Level 5
### Total Execution Time in Software/Hardware [μs]: Decapsulation

<table>
<thead>
<tr>
<th></th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round5</td>
<td>24</td>
<td>33</td>
<td>43</td>
<td>53</td>
<td>65</td>
</tr>
<tr>
<td>Saber</td>
<td>95</td>
<td>107</td>
<td>116</td>
<td>132</td>
<td>138</td>
</tr>
<tr>
<td>NTRU-HPS</td>
<td>55</td>
<td>77</td>
<td>116</td>
<td>132</td>
<td>150</td>
</tr>
<tr>
<td>Str NTRU Prime</td>
<td>55</td>
<td>77</td>
<td>116</td>
<td>132</td>
<td>150</td>
</tr>
<tr>
<td>NTRU LPrime</td>
<td>55</td>
<td>77</td>
<td>116</td>
<td>132</td>
<td>150</td>
</tr>
<tr>
<td>NTRU-HRSS</td>
<td>55</td>
<td>77</td>
<td>116</td>
<td>132</td>
<td>150</td>
</tr>
<tr>
<td>FrodoKEM</td>
<td>136</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
</tr>
</tbody>
</table>

- **Round5 → Saber**: 24 μs → 33 μs
- **Saber → NTRU-HPS**: 95 μs → 107 μs
- **NTRU-HPS → Str NTRU Prime**: 55 μs → 77 μs
- **Str NTRU Prime → NTRU LPrime**: 55 μs → 77 μs
- **NTRU LPrime → NTRU-HRSS**: 55 μs → 77 μs
- **NTRU-HRSS → FrodoKEM**: 136 μs → 150 μs

- **Level 1**: 24 μs → 33 μs
- **Level 2**: 95 μs → 107 μs
- **Level 3**: 55 μs → 77 μs
- **Level 4**: 132 μs → 138 μs
- **Level 5**: 132 μs → 150 μs

- **Total Time (μs)**: 1,319 → 1,866 → 3,120
Total Speed-ups: Decapsulation
## Accelerator Speed-ups: Decapsulation

<table>
<thead>
<tr>
<th>System</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTRU-HPS</td>
<td>318.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTRU-HRSS</td>
<td>238.0</td>
<td>188.7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FrodoKEM</td>
<td>44.4</td>
<td>46.0</td>
<td>46.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Str NTRU Prime</td>
<td>31.1</td>
<td>37.9</td>
<td>43.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTRU LPrime</td>
<td>28.0</td>
<td>31.2</td>
<td>34.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saber</td>
<td>11.1</td>
<td>17.7</td>
<td>24.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Round5</td>
<td>8.1</td>
<td>9.4</td>
<td>9.8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SW Part Sped up by HW[%]: Decapsulation

<table>
<thead>
<tr>
<th></th>
<th>Round5</th>
<th>NTRU-HPS</th>
<th>NTRU-HRSS</th>
<th>Saber</th>
<th>NTRU LPrime</th>
<th>Str NTRU Prime</th>
<th>FrodoKEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>99.0</td>
<td>97.6</td>
<td>96.4</td>
<td>94.0</td>
</tr>
<tr>
<td>Level 2</td>
<td>100</td>
<td>99.3</td>
<td>98.1</td>
<td>98.4</td>
<td>96.6</td>
<td>96.1</td>
<td>96.8</td>
</tr>
<tr>
<td>Level 3</td>
<td>100</td>
<td>99.4</td>
<td>97.1</td>
<td>97.4</td>
<td>97.4</td>
<td>96.9</td>
<td>97.1</td>
</tr>
<tr>
<td>Level 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>96.3</td>
<td>96.3</td>
<td></td>
</tr>
<tr>
<td>Level 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>96.9</td>
<td>96.9</td>
<td></td>
</tr>
</tbody>
</table>
Conclusions

- For all 7 investigated PQC schemes, major operations offloaded to hardware amounted to at least 94% of the decapsulation time in software.
- Ranking of the investigated candidates affected, but not dramatically changed, by hardware acceleration.
- It might be possible (with participation of several groups) to complete similar designs for all Round 2 candidates within the evaluation period (12-18 months).
- Additional benefit: Comprehensive library of major operations in hardware.
Future Evaluation

- **5 Lattice-based KEMs**
- **4 Remaining Lattice-based KEMs**
- **3 Lattice-based Digital Signatures**
- **7 Code-based KEMs**
- **7 Other Candidates**

**Reported**

**In Progress**

**Remaining/Other groups**

Algorithmic optimizations of software and hardware

Hardware library of basic operations of PQC

Full hardware implementations
Future Research Directions

Current Work

High-Level Synthesis
Vivado, LegUp, etc.

PQC Hardware
Accelerators for RISC-V

Lightweight Implementations
Protected Against Side-Channel Attacks
Q&A

Thank You!

Questions? Comments? Suggestions?

CERG: http://cryptography.gmu.edu
ATHENa: http://cryptography.gmu.edu/athena