HQC: Hamming Quasi-Cyclic
An IND-CCA2 Code-based Public Key Encryption Scheme

November 30, 2022
NIST 4TH PQC STANDARDIZATION CONFERENCE
https://pqc-hqc.org

C. Aguilar Melchor
N. Aragon
S. Bettaieb
L. Bidoux
O. Blazy
J. Bos
J.-C. Deneuville
Sandbox
Naquidis, France
Worldline
TII, UAE
Ecole Polytechnique, France
Worldline
ENAC, University of Toulouse

A. Dion
P. Gaborit
J. Lacan
E. Persichetti
J.-M. Robert
P. Véron
G. Zémor
ISAE-Supaéro, Univ. Toulouse
University of Limoges
ISAE-Supaéro, Univ. Toulouse
Florida Atlantic University
University of Toulon
University of Toulon
IMB, University of Bordeaux
Outline

1. HQC design rationale and recap
2. Fourth round tweaks
3. Optimized implementations
HQC Classification / Design Rationale

Important features:
- IND-CCA2 code-based PKE
- Reduction to a well-known and difficult problem:
  Decoding random quasi-cyclic codes
- No hidden trap in the code
- Efficient decoding
- Precise DFR analysis
HQC Encryption Scheme

Encryption scheme in Hamming metric, using Quasi-Cyclic Codes

- **Notation:** Secret data - Public data - One-time Randomness
- **** is the generator matrix of some public code **
- \( S^n_w(\mathbb{F}_2) = \{ x \in \mathbb{F}_2^n \text{ such that } \omega(x) = w \} \)

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>( seed_h \xleftarrow{$} {0, 1}^\lambda, \quad h \xleftarrow{$} \mathbb{F}_2^n )</td>
<td></td>
</tr>
<tr>
<td>( x, y \xleftarrow{$} S^n_w(\mathbb{F}_2), s \leftarrow x + hy )</td>
<td></td>
</tr>
<tr>
<td>( m \leftarrow C.\text{Decode}(v - uy) )</td>
<td></td>
</tr>
<tr>
<td>( seed_h, s \xrightarrow{\text{se}} )</td>
<td></td>
</tr>
<tr>
<td>( r_1, r_2 \xleftarrow{$} S^n_w(\mathbb{F}_2), e \xleftarrow{$} S^n_w(\mathbb{F}_2) )</td>
<td></td>
</tr>
<tr>
<td>( u \leftarrow r_1 + hr_2, \quad v \leftarrow mG + sr_2 + e )</td>
<td></td>
</tr>
</tbody>
</table>

P. Gaborit

Hamming Quasi-Cyclic

November 30, 2022
Fourth round tweaks

- **Multi-ciphertext attack**: Addition of a public salt value into the ciphertext, in order to counter a simple multi-ciphertext attack discussed in NIST’s PQC mailing list in July 2021. Although the attack is not in the security model considered, we chose to make a modification. The randomness $\theta$ is now computed from a salt together with the public key.

$$\theta = \text{shake256}_512(m||public\ key||salt)$$

- **Countermeasure to a timing attack**: In the recent paper [GHJLNS22]: the authors propose an attack on BIKE and HQC on the sampling of small weight vectors. We modified the generation of the small vectors according a paper by N. Sendrier [Sen21] which avoids the attack at a cost of a small bias which does not impact the security. In practice this countermeasure implies a loss of a few percentages points in our performance.

- **Constant time reference implementation**: we included a constant time (not optimized) reference version.
## Parameters and performances

Sizes in kilo bytes, performances in kilo cycles:

<table>
<thead>
<tr>
<th></th>
<th>Public key size</th>
<th>Ciphertext size</th>
<th>Keygen</th>
<th>Encaps</th>
<th>Decaps</th>
<th>DFR</th>
</tr>
</thead>
<tbody>
<tr>
<td>hqc-128</td>
<td>2,249</td>
<td>4,497</td>
<td>87</td>
<td>204</td>
<td>362</td>
<td>$&lt; 2^{-128}$</td>
</tr>
<tr>
<td>hqc-192</td>
<td>4,522</td>
<td>9,042</td>
<td>204</td>
<td>465</td>
<td>755</td>
<td>$&lt; 2^{-192}$</td>
</tr>
<tr>
<td>hqc-256</td>
<td>7,245</td>
<td>14,485</td>
<td>409</td>
<td>904</td>
<td>1505</td>
<td>$&lt; 2^{-256}$</td>
</tr>
</tbody>
</table>
Optimized implementations

We thank the community for their support in trying to improve the security of HQC for side channel attacks and for improvements on hardware implementations of HQC.

- [DXNNS22] VHDL hardware implementation which largely outperforms our HLS implementation and obtains very good performance using a small surface.

- [Loi22] Efficient implementation of HQC for embedded systems (ARMv7)

- **Versatility of the scheme**: possibility to consider customized versions of HQC for hardware with very light decoder (replace RS+RM with only Repetition code or Repetition code + Hamming codes for instance).
References


Questions?

HQC official website and updates:

https://pqc-hqc.org/