HQC: Hamming Quasi-Cyclic

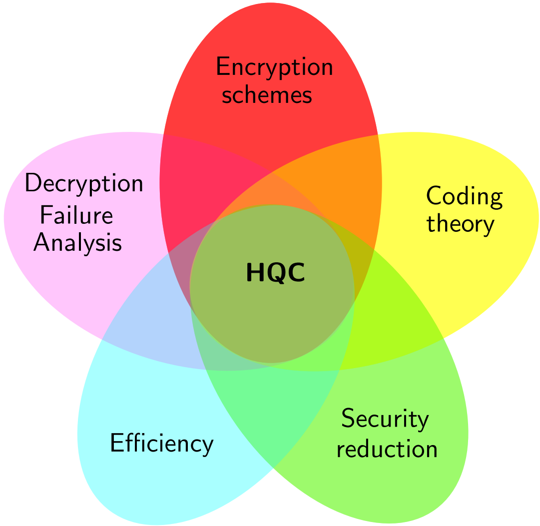
An IND-CCA2 Code-based Public Key Encryption Scheme

August the 24th, 2019
NIST 2ND PQC Standardization Conference
Santa-Barbara
https://pqc-hqc.org

C. Aguilar Melchor	ISAE-Supaéro, University of Toulouse
N. Aragon	University of Limoges
S. Bettaieb	Worldline
L. Bidoux	Worldline
O. Blazy	University of Limoges
J.-C. Deneuville	ENAC, University of Toulouse
P. Gaborit	University of Limoges
E. Persichetti	Florida Atlantic University
G. Zémor	IMB, University of Bordeaux

Outline

HQC Classification / Design Rationale



Important features:

- IND-CPA code-based PKE
- Reduction to a well-known and difficult problem:

  Decoding random quasi-cyclic codes
- No hidden trap in the code
- Efficient decoding (BCH + repetition code)
- Accurate failure rate

HQC Encryption Scheme [ABD+18]

Encryption scheme in **H**amming metric, using **Q**uasi-**C**yclic Codes

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

Alice		Bob
$\mathsf{seed}_{\mathbf{h}} \xleftarrow{\$} \{0,1\}^\lambda$, $\mathbf{h} \xleftarrow{\mathsf{seed}_{\mathbf{h}}} \mathbb{F}_2^n$ $\mathbf{x}, \mathbf{y} \xleftarrow{\$} \mathcal{S}_w^n(\mathbb{F}_2)$, $\mathbf{s} \leftarrow \mathbf{x} + \mathbf{h}\mathbf{y}$	$\xrightarrow{\mathsf{seed}_{\mathbf{h}}, \mathbf{s}}$	$\mathbf{r}_1, \mathbf{r}_2 \xleftarrow{\$} \mathcal{S}_w^n(\mathbb{F}_2)$, $\mathbf{e} \xleftarrow{\$} \mathcal{S}_w^n(\mathbb{F}_2)$ $\mathbf{u} \leftarrow \mathbf{r}_1 + \mathbf{h}\mathbf{r}_2$, $\mathbf{v} \leftarrow \mathbf{m}\mathbf{G} + \mathbf{s}\mathbf{r}_2 + \mathbf{e}$
$\mathbf{m} \leftarrow \mathcal{C}.\mathsf{Decode}(\mathbf{v} - \mathbf{u}\mathbf{y})$	$\xleftarrow{\mathbf{u}, \mathbf{v}}$	

NIST's first round comments

"HQC presents a strong argument that its decryption failure rate is low enough to obtain chosen-ciphertext security. This is the strongest argument, at present, of CCA security among the second-round candidate code-based cryptosystems, where information set decoding is the limiting attack for both private key recovery and message recovery (BIKE, HQC, and LEDAcrypt)".

"However, it pays a significant penalty in key and ciphertext size in comparison to the others (although it still compares very favorably in key size and overall communication bandwidth to the candidate code-based cryptosystems based on Goppa codes)."

Nist's comments (seq)

"Possible areas for further analysis related to HQC include investigating the relation between the search and decisional variants of the QCSD problem, and investigating the effect, if any, of the quasi-cyclic code structure on security."

$\rightarrow$ bandwidth ratio with BIKE is roughly between 3 and 1.5 depending of the version of BIKE

$\rightarrow$ relation between search and decisional problem for QC is an old open question, natural question on the impact of the structure on security (similar case to Euclidean and Rank metrics).

2nd round modifications

- ◇ parameters with DFR below 2^{-128} have been withdrawn
- ◇ minor modification on the proof to counter the easy parity distinguisher
- ◇ precision in the scheme for the bits not covered by the decoding

Parameters

All sizes in **bytes**

NIST Cat.	Instance	pk size sizeof($\mathbf{h}, \mathbf{s}$) (sizeof(seed$_{\mathbf{h}}, \mathbf{s}$))	sk size sizeof($\mathbf{x}, \mathbf{y}$) (sizeof(seed$_{\mathsf{sk}}$))	ct size	DFR
1	HQC-128-1	6,170 (3,125)	252 (40)	6,234	2^{-128}
3	HQC-192-2	11,688 (5,884)	404 (40)	11,752	2^{-192}
5	HQC-256-3	17,714 (8,897)	566 (40)	17,778	2^{-256}

Best known classical attack: [CS16] $\rightarrow$ work factor $2^{-2w \log\left(1-\frac{k}{n}\right)(1+o(1))}$ (Prange [Pra62])
Only minor improvement of a factor $\sqrt{n}$ known from quasi-cyclicity [Sendrier DOOM 2011]
Best known quantum attack: ISD with [Gro96] $\rightarrow$ work factor $\sqrt{\binom{n}{2w} / \binom{n-k}{2w}}$

Reference implementation

- New reference implementation
- Depends on NTL and GF2X libraries

- **New BCH decoding implementation**
- Faster GF arithmetic using hard coded lookup tables
- Syndromes computation uses the faster additive FFT transpose [BCS13, GM10]
- Roots computation uses the faster additive FFT [BCS13, GM10]

Optimized implementation

- AVX2 implementation available
- Significantly improved recently

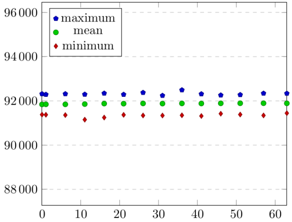
	AVX2 Implementation			Improvement % wrt 2019/07/05		
	Keygen	Encaps	Decaps	Keygen	Encaps	Decaps
HQC 128-1	200,580	383,860	508,954	19	29	25
HQC 192-2	403,358	765,146	983,678	21	25	24
HQC 256-3	651,470	1,257,152	1,618,366	21	22	22

Figure: Performances CPU cycles and comparison to optimized implementation from 2019/07/05 package using an i7-7820 @3.6Ghz CPU

- Other implementation from Robert and Véron with similar timings.

Constant time implementation

- **New constant time BCH decoding algorithm**
  - Constant time variant of Berlekamp's simplified algorithm
  - Constant time implementation of FFT based algorithms for syndrome computation and roots finding



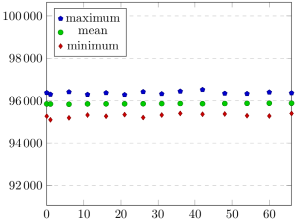


Figure: Performances CPU cycles of constant time decoding algorithm of BCH codes used in HQC

Constant time decoding overhead

◇ Minimal overhead performance

	Decaps		Overhead %
	Non constant time	Constant time	
HQC 128-1	508,954	542,880	7
HQC 192-1	934,222	965,272	4
HQC 192-2	983,678	1,020,738	4
HQC 256-1	1,492,840	1,521,206	2
HQC 256-2	1,564,672	1,605,164	3
HQC 256-3	1,618,366	1,665,788	3

Figure: Performances CPU cycles and overhead when original or constant time BCH decoding is used in the decapsulation step

Timing attack against HQC (eprint 2019/909 [WTBBG19])

- Side-channel chosen ciphertext attack against HQC
- Attack complexity $\mathcal{O}(n^{\frac{5}{2}})$ (runs in less one minute for HQC-128-1)
- Exploits correlation between the error to be decoded and the running time of the BCH decoding algorithm
- Countermeasure based on constant time BCH decoding algorithm

Pros and cons

Advantages:

- **Security reduction to decoding random quasi-cyclic codes**
- Simple and efficient decoding (BCH + repetition code)
- **No more hidden trap**
- Makes use of cyclicity for **efficiency**
- Well-understood, theoretically bounded, and fast decreasing DFR
- Efficient constant time decryption implementation
- Attacks on Hamming metric are well understood (50+ years)

Limitations:

- Non-zero decryption failure rate
- Larger ciphertexts than BIKE-1 and BIKE-3 KEMs ($\approx \times 2$)
- Larger public key than BIKE KEM ($\approx \times 2$), but still reasonable

$\rightarrow$ Overall: balanced scheme with no major weakness and very good features in term of security reduction or constant time implementation

Thank you for your attention.

Carlos Aguilar, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor.
Efficient encryption from random quasi-cyclic codes.
IEEE Transactions on Information Theory, 2018.

Daniel J Bernstein, Tung Chou, and Peter Schwabe.
Mcbits: fast constant-time code-based cryptography.
In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 250–272. Springer, 2013.

Rodolfo Canto Torres and Nicolas Sendrier.
Analysis of information set decoding for a sub-linear error weight.
In Tsuyoshi Takagi, editor, *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*, pages 144–161. Springer, 2016.

Shuhong Gao and Todd Mateer.
Additive fast fourier transforms over finite fields.
IEEE Transactions on Information Theory, 56(12):6265–6272, 2010.

Lov K Grover.
A fast quantum mechanical algorithm for database search.
In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.

Eugene Prange.
The use of information sets in decoding cyclic codes.
IRE Transactions on Information Theory, 8(5):5–9, 1962.

Guillaume Wafo-Tapa, Slim Bettaieb, Loıc Bidoux, and Philippe Gaborit.
A practicable timing attack against HQC and its countermeasure.
IACR Cryptology ePrint Archive, 2019:909, 2019.

HQC official website and updates:

https://pqc-hqc.org/