HQC: Hamming Quasi-Cyclic

An IND-CCA2 Code-based Public Key Encryption Scheme

April the 13th, 2018
NIST 1st PQC Standardization Conference
Fort Lauderdale
https://pqc-hqc.org

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

Outline

Outline

HQC Classification / Design Rationale

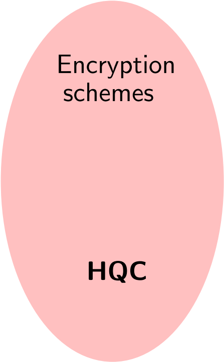
HQC

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 Classification / Design Rationale



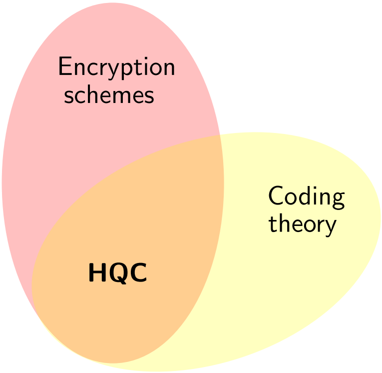
Important features:

- 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 Classification / Design Rationale

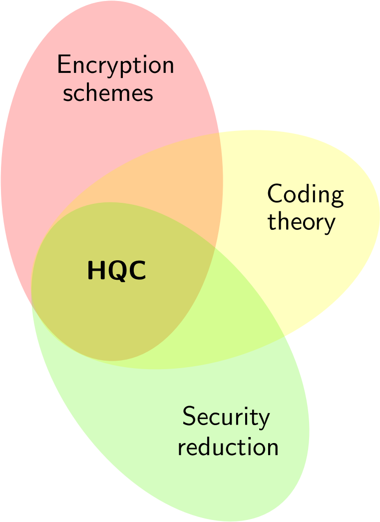


Important features:

- 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 Classification / Design Rationale



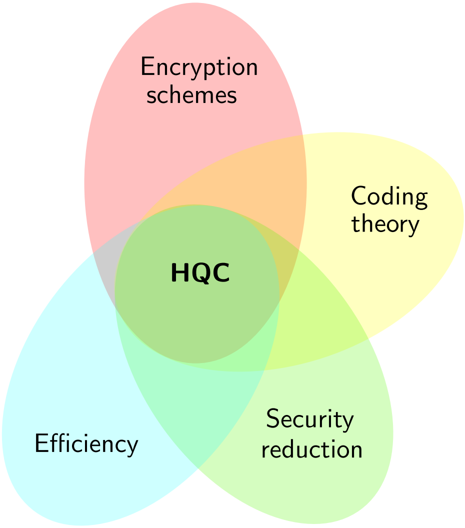
Important features:

- 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 Classification / Design Rationale



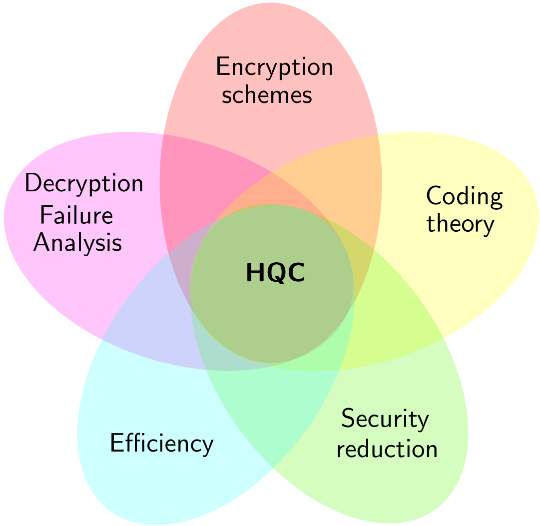
Important features:

- 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 Classification / Design Rationale



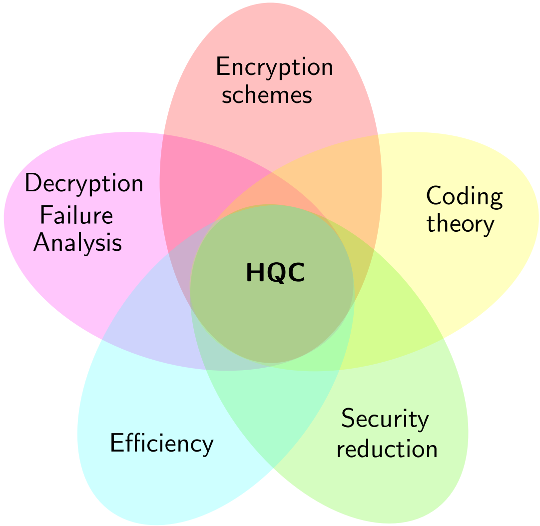
Important features:

- 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 Classification / Design Rationale

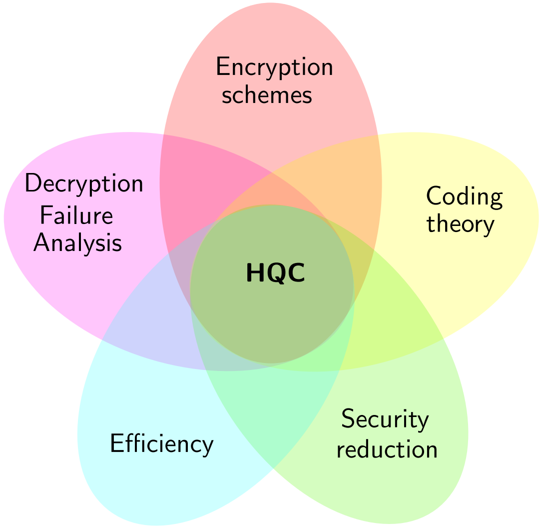


Important features:

- 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 Classification / Design Rationale

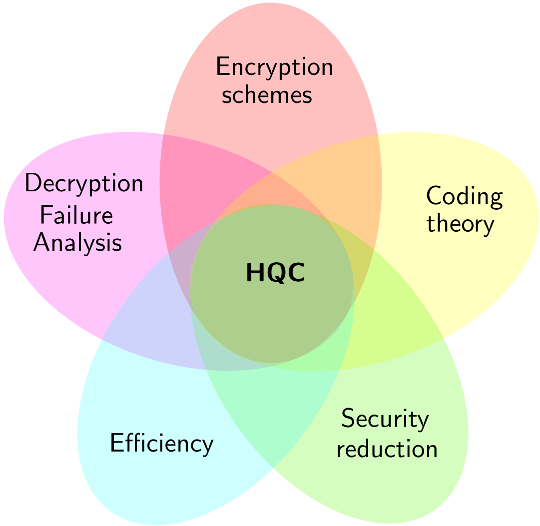


Important features:

- 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 Classification / Design Rationale

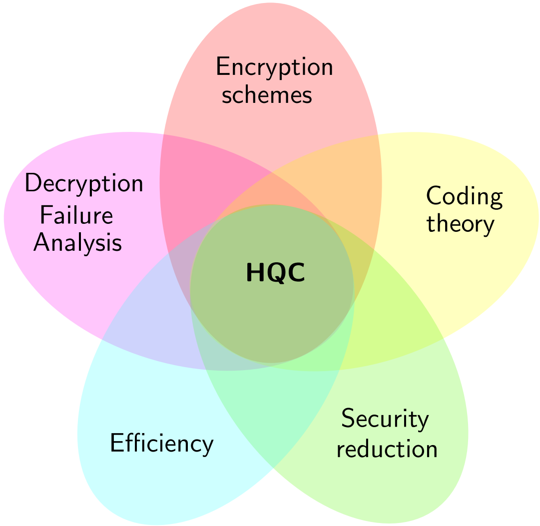


Important features:

- 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 Classification / Design Rationale

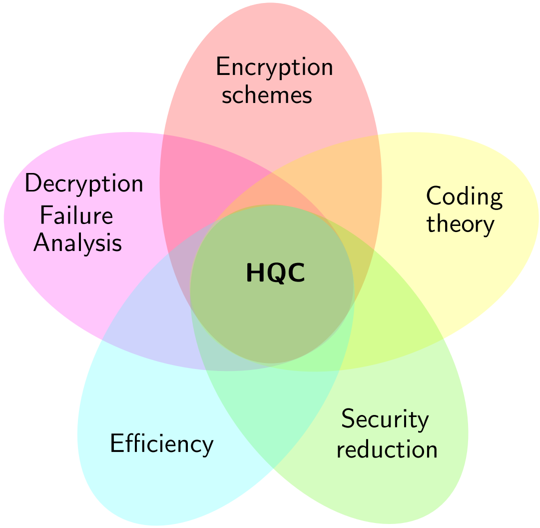


Important features:

- 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 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

Outline

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 $\mathcal{C}$
- $\mathcal{S}_w^n(\mathbb{F}_2) = \{\mathbf{x} \in \mathbb{F}_2^n$ such that $\omega(\mathbf{x}) = w\}$

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

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

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

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

HQC Instantiation

HQC is a generic framework to build efficient and secure code-based cryptosystems

Proposed instantiation:

- BCH codes tensored with repetition codes
  - Efficient decoding
  - Accurate DFR estimates

Time in ms
Intel® Core™ i7-4770 CPU @ 3.4GHz

Instance	KeyGen	Encaps	Decaps
Strength 1	0.17-0.19	0.36-0.40	0.57-0.63
Strength 3	0.37-0.43	0.77-0.89	1.13-1.28
Strength 5	0.65-0.82	1.38-1.76	1.96-2.50

(Number of cycles available in supporting documentation)

Theorem

HQC is IND-CPA under 2-DQCSD and 3-DQCSD.

2-Decisional Quasi-Cyclic Syndrome Decoding and 3-DQCSD Problems

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{x}, \mathbf{y}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\mathbf{s} = \begin{pmatrix} \mathbf{I}_n & \mathbf{h} \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{h} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{s} \end{pmatrix} \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{e} \\ \mathbf{r}_2 \end{pmatrix}$

HQC Instantiation

HQC is a generic framework to build efficient and secure code-based cryptosystems

Proposed instantiation:

- BCH codes tensored with repetition codes
  - Efficient decoding
  - Accurate DFR estimates

Time in ms
Intel® Core™ i7-4770 CPU @ 3.4GHz

Instance	KeyGen	Encaps	Decaps
Strength 1	0.17-0.19	0.36-0.40	0.57-0.63
Strength 3	0.37-0.43	0.77-0.89	1.13-1.28
Strength 5	0.65-0.82	1.38-1.76	1.96-2.50

(Number of cycles available in supporting documentation)

Theorem

HQC is IND-CPA under 2-DQCSD and 3-DQCSD.

2-Decisional Quasi-Cyclic Syndrome Decoding and 3-DQCSD Problems

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{x}, \mathbf{y}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\mathbf{s} = \begin{pmatrix} \mathbf{I}_n & \mathbf{h} \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{h} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{s} \end{pmatrix} \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{e} \\ \mathbf{r}_2 \end{pmatrix}$

HQC Instantiation

HQC is a generic framework to build efficient and secure code-based cryptosystems

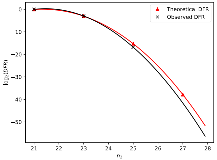
Proposed instantiation:

- BCH codes tensored with repetition codes
  - Efficient decoding
  - Accurate DFR estimates

Time in ms
Intel® Core™ i7-4770 CPU @ 3.4GHz

Instance	KeyGen	Encaps	Decaps
Strength 1	0.17-0.19	0.36-0.40	0.57-0.63
Strength 3	0.37-0.43	0.77-0.89	1.13-1.28
Strength 5	0.65-0.82	1.38-1.76	1.96-2.50

(Number of cycles available in supporting documentation)



Theorem

HQC is IND-CPA under 2-DQCSD and 3-DQCSD.

2-Decisional Quasi-Cyclic Syndrome Decoding and 3-DQCSD Problems

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{x}, \mathbf{y}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\mathbf{s} = \begin{pmatrix} \mathbf{I}_n & \mathbf{h} \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{h} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{s} \end{pmatrix} \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{e} \\ \mathbf{r}_2 \end{pmatrix}$

HQC Instantiation

HQC is a generic framework to build efficient and secure code-based cryptosystems

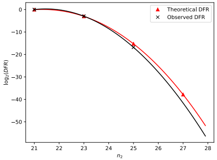
Proposed instantiation:

- BCH codes tensored with repetition codes
  - Efficient decoding
  - Accurate DFR estimates

Time in ms
Intel® Core™ i7-4770 CPU @ 3.4GHz

Instance	KeyGen	Encaps	Decaps
Strength 1	0.17-0.19	0.36-0.40	0.57-0.63
Strength 3	0.37-0.43	0.77-0.89	1.13-1.28
Strength 5	0.65-0.82	1.38-1.76	1.96-2.50

(Number of cycles available in supporting documentation)



Theorem

HQC is IND-CPA under 2-DQCSD and 3-DQCSD.

2-Decisional Quasi-Cyclic Syndrome Decoding and 3-DQCSD Problems

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{x}, \mathbf{y}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\mathbf{s} = \begin{pmatrix} \mathbf{I}_n & \mathbf{h} \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{h} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{s} \end{pmatrix} \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{e} \\ \mathbf{r}_2 \end{pmatrix}$

HQC Instantiation

HQC is a generic framework to build efficient and secure code-based cryptosystems

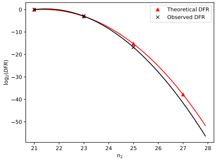
Proposed instantiation:

- BCH codes tensored with repetition codes
  - Efficient decoding
  - Accurate DFR estimates

Time in ms
Intel® Core™ i7-4770 CPU @ 3.4GHz

Instance	KeyGen	Encaps	Decaps
Strength 1	0.17-0.19	0.36-0.40	0.57-0.63
Strength 3	0.37-0.43	0.77-0.89	1.13-1.28
Strength 5	0.65-0.82	1.38-1.76	1.96-2.50

(Number of cycles available in supporting documentation)



Theorem

HQC is IND-CPA under 2-DQCSD and 3-DQCSD.

2-Decisional Quasi-Cyclic Syndrome Decoding and 3-DQCSD Problems

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{x}, \mathbf{y}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\mathbf{s} = \begin{pmatrix} \mathbf{I}_n & \mathbf{h} \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$

Instance: $\mathbf{h}, \mathbf{s} \in \mathbb{F}_2^n$

Decide: $\exists ?(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e}) \in \mathcal{S}_w^n(\mathbb{F}_2)$ s.t. $\begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{h} \\ \mathbf{0} & \mathbf{I}_n & \mathbf{s} \end{pmatrix} \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{e} \\ \mathbf{r}_2 \end{pmatrix}$

Outline

Parameters

All sizes in **bytes**

NIST Cat.	Instance	pk size sizeof($\mathbf{h}, \mathbf{s}$) (sizeof($\text{seed}_{\mathbf{h}}, \mathbf{s}$))	sk size sizeof($\mathbf{x}, \mathbf{y}$) (sizeof(seed_{sk}))	ct size	DFR
1	Basic-I	5,558 (2,819)	252 (40)	5,622	2^{-64}
	Basic-III	6,170 (3,125)	252 (40)	6,234	2^{-128}
3	Advanced-I	10,150 (5,115)	404 (40)	10,214	2^{-64}
	Advanced-III	11,688 (5,884)	404 (40)	11,752	2^{-192}
5	Paranoiac-I	14,754 (7,417)	532 (40)	14,818	2^{-64}
	Paranoiac-IV	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])

Best known quantum attack: ISD with [Gro96] $\rightarrow$ work factor $\sqrt{\binom{n}{2w}/\binom{n-k}{2w}}$

Outline

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
- Attacks on Hamming metric are well understood (50+ years)
- Easy to understand

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

Pros and cons

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

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
- Attacks on Hamming metric are well understood (50+ years)
- Easy to understand

Thank you for your attention.

HQC official website and updates:
https://pqc-hqc.org/

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.

Michael Alekhnovich.
More on average case vs approximation complexity.
In *44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA, Proceedings*, pages 298–307, 2003.

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.

Qian Guo, Thomas Johansson, and Paul Stankovski.
A key recovery attack on mdpc with cca security using decoding errors.
In *22nd Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT), 2016*, 2016.

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.

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz.
A modular analysis of the fujisaki-okamoto transformation.
Cryptology ePrint Archive, Report 2017/604, 2017.
http://eprint.iacr.org/2017/604.

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

HQC official website and updates:

https://pqc-hqc.org/