HQC-SSD (Hamming Quasi-Cyclic Shamir Shared Decoding)

HQC-SSD
team-thqc@lists.recherche.enac.fr

Jean-Christophe Deneuville[2] Nathan Maillet[1,3] Vincent Migliore[3] Cyrius Nugier[2]

[1] EDF R&D, France
[2] Fédération ENAC ISAE-SUPAERO ONERA, France
[3] LAAS–CNRS / INSA-Toulouse, France



2026-10-13 @ NIST TCPT3

THQC (Threshold Hamming Quasi-Cyclic) OR HQC-SSD (Shamir Shared Decoding)

to be determined...

In a nutshell, our proposed submission will:

- depart from NIST PQC HQC (selected 03/25 to be FIPS 207);
- use multi-party decryption, hence decoding;
- with the decryption key split/shared among participating parties (Shamir secret sharing);
- thresholdize to get T honest parties out of N correctly decrypt.

Let $\boldsymbol{G} \in \mathbb{F}_2^{k \times n}$ be a generator matrix of a **any** code $\mathcal{C}$ capable of correcting up to t errors (using **public** decoding algorithm $\mathcal{D}_{\mathcal{C}}$).





$\boldsymbol{x}, \boldsymbol{y} \xleftarrow{\$} \mathcal{S}_w^n(\mathbb{F}_2)$

$\mathsf{seed}_{\boldsymbol{h}} \xleftarrow{\$} \{0,1\}^{\lambda}, \boldsymbol{h} \xleftarrow{\mathsf{seed}_{\boldsymbol{h}}} \mathbb{F}_2^n,$

$\boldsymbol{s} \leftarrow \boldsymbol{x} + \boldsymbol{h}\boldsymbol{y}$

$\mathsf{pk}=(\mathsf{seed}_{\boldsymbol{h}}, \boldsymbol{s})$ ⟶

message $\boldsymbol{m} \in \mathbb{F}_2^k$

$\boldsymbol{r}_1, \boldsymbol{r}_1, \xleftarrow{\$} \mathcal{S}_{w_r}^n(\mathbb{F}_2), \boldsymbol{e} \xleftarrow{\$} \mathcal{S}_{w_e}^n(\mathbb{F}_2)$

$\boldsymbol{u}, \boldsymbol{v}$ ⟵

$\boldsymbol{u} = \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2 \in \mathbb{F}_2^n$

$\boldsymbol{v} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{s}\boldsymbol{r}_2 + \boldsymbol{e} \in \mathbb{F}_2^n$

$\boldsymbol{m} \leftarrow \mathcal{D}_{\mathcal{C}}(\boldsymbol{v} - \boldsymbol{u}\boldsymbol{y})$

HQC parameters [GAA+26]

Instance	Security	n_1	n_2	n	k	ω	$\omega_r = \omega_e$	DFR
HQC-1	NIST-1	46	384	17 669	128	67	76	$< 2^{-127}$
HQC-3	NIST-3	56	640	35 851	192	101	114	$< 2^{-192}$
HQC-5	NIST-5	90	640	57 637	256	132	150	$< 2^{-256}$

Instance	Security	$\lvert\mathbf{ek}_{\mathrm{KEM}}\rvert$	$\lvert\mathbf{dk}_{\mathrm{KEM}}\rvert$	$\lvert\mathbf{c}_{\mathrm{KEM}}\rvert$	$\lvert K\rvert$
HQC-1	NIST-1	2 241	32	4 433	32
HQC-3	NIST-3	4 514	32	8 978	32
HQC-5	NIST-5	7 237	32	14 421	32

Multi-Party Threshold Protocol

- **Shamir secret sharing** of the key: Each bit y_i of y is shared in N elements in $\mathbb{F}_{2^m}$. Given a polynomial f of degree T such that $f(0) = y_i$, the shares are the evaluations of f in $(\alpha_1, \cdots, \alpha_N)$ where α has maximal multiplicative order. Each party p is given the share of each bit y_i corresponding to α_p. A share of a variable v is noted $[v]$
- **Computation**: Parties synchronously alternate rounds of
  - local (linear over shares) computation operations
  - communication either via an established, confidential and authenticated channels to each other party, or via a broadcast channel
- **Recomposition**: When at least T parties centralize their results (e.g. through a trusted third party), interpolation allows to determine the polynomial f and evaluate $f(0)$ as a bit of the result

Experimental Setup

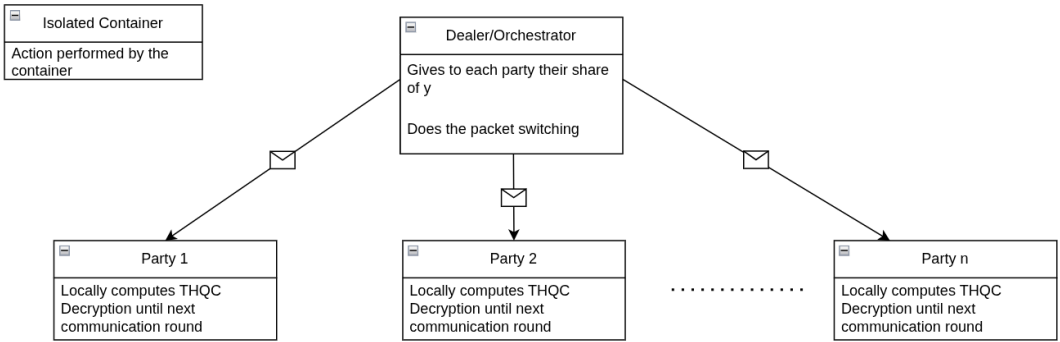


Figure: Distribution of the secret's shares to each party

Experimental Setup

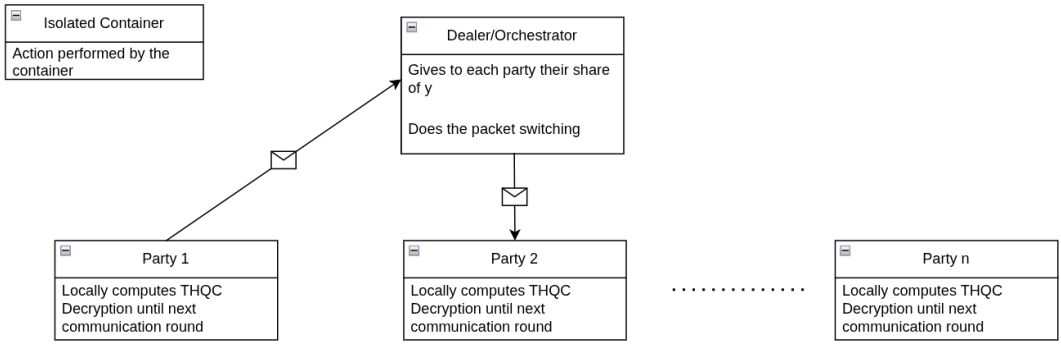


Figure: Disclosure of an element of $\mathbb{F}_2^m$ to a single party

Experimental Setup

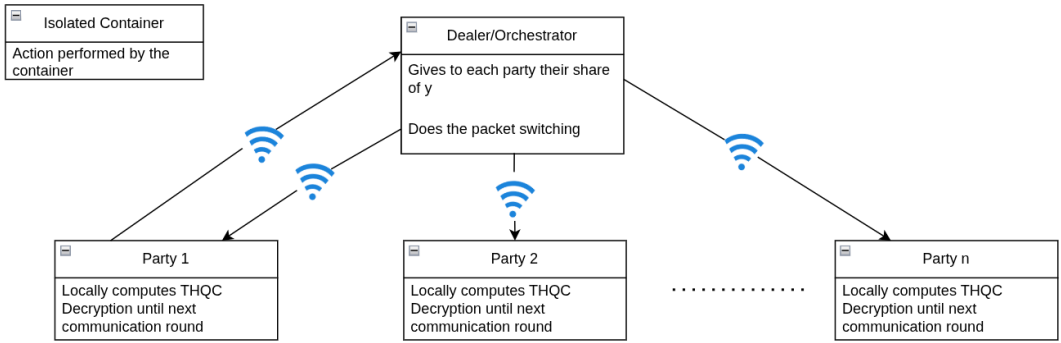
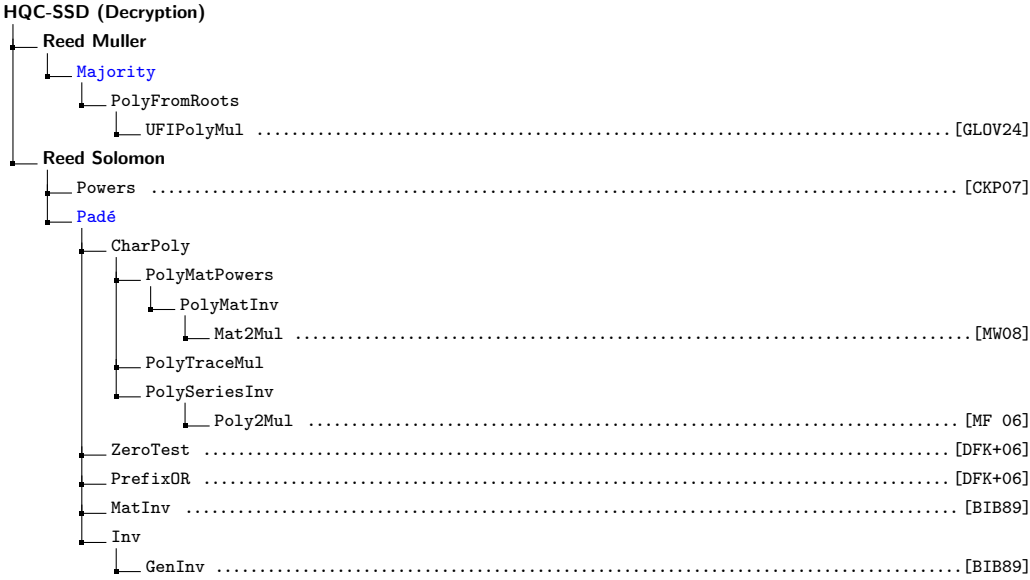


Figure: Disclosure of an element of $\mathbb{F}_2^m$ to each party (broadcast)

Protocol stack



- **Majority** First computes $[P] = \left[\prod_0^{n-1}(X - y_i)\right] = \prod_0^{n-1}(X - [y_i])$. P has $X^{n-\mathrm{HW}(y)}$ as a factor, thus, it follows that $r = 1 - \prod_0^{n/2}(1 - [P_i])$ tells if the first half of coefficients of $[P]$ are 0 and therefore if $\mathrm{HW}(y) \leq \lceil n/2 \rceil$

- **Padé** Takes as input shares of the syndrome polynomial $[S] = \left[\sum_0^{n-1} y_i X^i\right] = \sum_0^{n-1}[y_i]X^i$
  The protocol computes the shares of the error polynomial σ as the solution of the (δ, δ)-Padé approximant problem for S

  The $(k, n-k)$-Padé approximant problem for f aims to find two polynomials $(r, t) \in \mathbb{F}[X]^2$ such that:

  $$\frac{r}{t} = f \mod X^n,\ \deg(r) \leq k,\ \deg(t) \leq n-k,\ \text{and } t(0) \neq 0$$

  Finally, zero-testing reveals the location of the errors and Forney's algorithm returns the values of the errors, allowing for correction.

Security model

The current proposed protocol has IND-CPA security.
To reach IND-CCA security, one could transform HQC's decryption as such:

IND-CPA HQC Decryption

$u, v \leftarrow c$

$m \leftarrow C.Decode(v - u \cdot y)$

return m

$\xrightarrow{\text{FO transform}}$

IND-CCA2 HQC Decryption

$u, v, salt \leftarrow c$

$m' \leftarrow C.Decode(v - u \cdot y)$

$c' \leftarrow HQC.PKE.Encrypt(m', salt)$

return m if $c = c'$ else $f(c)$

FO transform [FO99, HHK17]

Using this transform would require a threshold re-encryption, or at least a threshold seed expansion in the random oracle model.

Security model

The current proposed protocol has IND-CPA security.
To reach IND-CCA security, one could transform HQC's decryption as such:

IND-CPA HQC Decryption

$u, v \leftarrow c$
$m \leftarrow C.Decode(v - u \cdot y)$
return m

$\xrightarrow{\text{NY transform}}$

IND-CCA HQC Decryption

$u_0, v_0 \leftarrow c_0$
$u_1, v_1 \leftarrow c_1$
$m \leftarrow C.Decode(v_0 - u_0 \cdot y)$
return m if $\mathcal{V}(c_0, c_1)$ else $\perp$

NY transform [NY90]

This transform requires to encrypt twice with a nul-DFR (Decryption Failure Rate) version of HQC, with consistence verified by a ZKP-verifier $\mathcal{V}$.
Depending on the proof, it can achieve an IND-CCA1 scheme or an IND-CCA2 scheme [Sah99].
The redudant encryption may be disposed of if the PKE version of HQC is proven OW-CPA [GLOV26].

Expected Parameter Sets

Four parameter sets for each NIST category (I, III, V).

- **NIST-HQC-SSD** Equivalent to HQC.KEM ($n = 17669$), matching KATs. Not threshold friendly (RS decoding complexity in $\mathcal{O}(\delta^{4.5})$ due to the use of Padé)
- **DFRλ-HQC-SSD** Closest to HQC.KEM while threshold friendly. δ minimized, weights unbalanced, ciphertext compression, at the cost of slightly increasing n (≈ 20000 for Cat. I)
- **SCA-HQC-SSD** Optimized for local computation performance, disregarding communication complexity. A (N, T) MPC protocol would be resistant in the t-probing model with $(N - T)$ probes, which is important for HQC as most decryption operations may leak key information [BMG+25, MNMD25].
- **DFR0-HQC-SSD** Allows NY transform. n greatly increases in order for noise to always be less than the code capacity ($46000 - 82000$ depending on desired δ)

N2 and S2 schemes submitted

Scheme	Security	Identifiable abort	Robustness	Computation	Indistinguishability	PQC	Round
NIST-HQC-SSD	Adaptive	Yes	Yes	$O(N)$	?	Yes	Constant
DFRλ-HQC-SSD	Adaptive	Yes	Yes	$O(N)$	?	Yes	Constant
SCA-HQC-SSD	Adaptive	Yes	Yes	$O(N)$	?	Yes	Constant
DFR0-HQC-SSD	Adaptive	Yes	Yes	$O(N)$	?	Yes	Constant
Amber-I	Adaptive	?	No	$O(1)$	IND-CCA	Yes	?
Amber-II	Static	?	Yes	$O(T)$	IND-CCA	Yes	?
CGGMP-II	?	Yes	?	?	?	No	?
PQarrot	Static	No	?	$O(T^2)$	?	Yes	Linear
SplitKey (Split-Decryption)	Static	?	?	?	?	No	?
Holocron	Static	?	?	?	?	Yes	Constant

Table: Comparative properties of N2 and S2 schemes altogether

Future directions

- In order to use the FO transform, implement a threshold-friendly hash function, maybe ChaCha20 as a hash?
- Find other code families with friendlier decoding? Maybe keep RS codes but change decoder? Berlekamp Welsh is more threshold friendly, but is not currently constant-round, so it may be an alternative for low numbers of participants (lower than 2^{RM_k})
- Open question : bitwise sharing has huge performance costs, maybe codes over $\mathbb{F}_{2^k}$ or over $\mathbb{F}_p$ with $p \lesssim 2^k$ can be more friendly (despite being maybe longer)?

References I



Carlos Aguilar Melchor, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor.

Efficient encryption from random quasi-cyclic codes.
IEEE Trans. Information Theory, 64(5):3927–3943, 2018.



Chloé Baïsse, Antoine Moran, Guillaume Goy, Julien Maillard, Nicolas Aragon, Philippe Gaborit, Maxime Lecomte, and Antoine Loiseau.

Secret and shared keys recovery on hamming quasi-cyclic with sasca.
Designs, Codes and Cryptography, pages 1–21, 2025.



Eiichiro Fujisaki and Tatsuaki Okamoto.

Secure integration of asymmetric and symmetric encryption schemes.
In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, pages 537–554, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.



Philippe Gaborit, Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Jerome Lacan, Jean-Marc Robert, Pascal Veron, Paulo Barreto, Shay Gueron, Tim Güneysu, Rafael Misoczki, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, Santosh Ghosh, and Jan Richter-Brockmann.
HQC.
Technical report, National Institute of Standards and Technology, 2026.
version of October 2026, available at `https://pqc-hqc.org/doc/hqc_specifications_2026_10_12.pdf`.



Pascal Giorgi, Fabien Laguillaumie, Lucas Ottow, and Damien Vergnaud.

Threshold Niederreiter: chosen-ciphertext security and improved distributed decoding.
Designs, Codes and Cryptography, 94(3):64, February 2026.



Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz.

A modular analysis of the fujisaki-okamoto transformation.
In Yael Tauman Kalai and Leonid Reyzin, editors, *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 341–371. Springer, 2017.



Nathan Maillet, Cyrius Nugier, Vincent Migliore, and Jean-Christophe Deneuville.

Key recovery from side-channel power analysis attacks on non-simd hqc decryption.
In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025*, pages 70–102, Cham, 2025. Springer Nature Switzerland.

References II



Moni Naor and Moti Yung.

Public-key cryptosystems provably secure against chosen ciphertext attacks.
In *22nd Annual ACM Symposium on Theory of Computing*, pages 427–437, Baltimore, MD, USA, May 14–16, 1990. ACM Press.



A. Sahai.

Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security.
In *40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039)*, pages 543–553, 1999.