HQC and Ciphertext Quantization

6G Future Lab Bavaria Speaker Series

Bharath Purtipli, Antonia Wachter-Zeh
Technical University of Munich
Institute for Communications Engineering

October 14, 2025

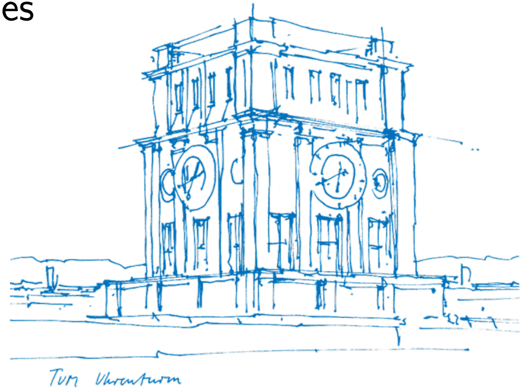


Table of Contents

HQC is . . .

- Hamming Quasi-Cyclic (HQC) is a code-based public key encryption.

HQC is . . .

- Hamming Quasi-Cyclic (HQC) is a code-based public key encryption.
- Standardized by NIST as a backup post-quantum cryptosystem.

HQC is . . .

- Hamming Quasi-Cyclic (HQC) is a code-based public key encryption.
- Standardized by NIST as a backup post-quantum cryptosystem.

Advantages	Disadvantages
Public code $\mathcal{C}$: Efficient decoder.	

HQC is ...

- Hamming Quasi-Cyclic (HQC) is a code-based public key encryption.
- Standardized by NIST as a backup post-quantum cryptosystem.

Advantages	Disadvantages
Public code $\mathcal{C}$: Efficient decoder.	
	Non-zero Decryption Failure Rate (DFR).

HQC is . . .

- Hamming Quasi-Cyclic (HQC) is a code-based public key encryption.
- Standardized by NIST as a backup post-quantum cryptosystem.

Advantages	Disadvantages
Public code $\mathcal{C}$: Efficient decoder.	
DFR is well understood and easily controlled.	Non-zero Decryption Failure Rate (DFR).

HQC is . . .

- Hamming Quasi-Cyclic (HQC) is a code-based public key encryption.
- Standardized by NIST as a backup post-quantum cryptosystem.

Advantages	Disadvantages
Public code $\mathcal{C}$: Efficient decoder.	Ciphertext length is large $\approx$ 4.4 kB.
DFR is well understood and easily controlled.	Non-zero Decryption Failure Rate (DFR).

HQC is . . .

- Hamming Quasi-Cyclic (HQC) is a code-based public key encryption.
- Standardized by NIST as a backup post-quantum cryptosystem.

Advantages	Disadvantages
Public code $\mathcal{C}$: Efficient decoder.	Ciphertext length is large $\approx 4.4\,\text{kB}$.
DFR is well understood and easily controlled.	Non-zero Decryption Failure Rate (DFR).

Goal: *Reduce ciphertext length using vector quantization such that DFR is negligible.*

Notation

Vector Space

$$\mathbb{F}_2^n$$

Polynomial Ring

$$\mathcal{R}_n = \mathbb{F}_2[x]/(x^n - 1)$$

Notation

Vector Space

$$\mathbb{F}_2^n$$

$$\mathbf{v} = (v_0, \ldots, v_{n-1})$$

Polynomial Ring

$$\mathcal{R}_n = \mathbb{F}_2[x]/(x^n - 1)$$

$$v(x) = \sum_{i=0}^{n-1} v_i x^i$$

Notation

Vector Space

$$\mathbb{F}_2^n$$

$$\mathbf{v} = (v_0, \ldots, v_{n-1})$$

$$\{\mathbf{v} \mid wt_{\mathrm{H}}(\mathbf{v}) = w\}$$

Polynomial Ring

$$\mathcal{R}_n = \mathbb{F}_2[x]/(x^n - 1)$$

$$v(x) = \sum_{i=0}^{n-1} v_i x^i$$

$$\mathcal{S}_w^n$$

Notation

Vector Space

$$\mathbb{F}_2^n$$

$$\mathbf{v} = (v_0, \ldots, v_{n-1})$$

$$\{\mathbf{v} \mid wt_{\mathrm{H}}(\mathbf{v}) = w\}$$

$$\mathbf{u} \cdot \mathbf{v}$$

Polynomial Ring

$$\mathcal{R}_n = \mathbb{F}_2[x]/(x^n - 1)$$

$$v(x) = \sum_{i=0}^{n-1} v_i x^i$$

$$\mathcal{S}_w^n$$

$$u(x)v(x) \mod x^n - 1$$

Notation

Vector Space	Polynomial Ring
$\mathbb{F}_2^n$	$\mathcal{R}_n = \mathbb{F}_2[x]/(x^n - 1)$
$\mathbf{v} = (v_0, \ldots, v_{n-1})$	$v(x) = \sum_{i=0}^{n-1} v_i x^i$
$\{\mathbf{v} \mid wt_{\mathrm{H}}(\mathbf{v}) = w\}$	$\mathcal{S}_w^n$
$\mathbf{u} \cdot \mathbf{v}$	$u(x)v(x) \mod x^n - 1$

Definition (Linear Code)

An (n, k) linear code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_2^n$ equipped with two functions -
$\mathcal{C}.\mathtt{enc} : \mathbf{m} \mapsto \mathbf{c} \in \mathcal{C}$

$\mathcal{C}.\mathtt{dec} : \mathbf{c} \in \mathcal{C} \mapsto \mathbf{m}$

Notation

Vector Space

$$\mathbb{F}_2^n$$

$$\mathbf{v} = (v_0, \ldots, v_{n-1})$$

$$\{\mathbf{v} \mid wt_{\mathrm{H}}(\mathbf{v}) = w\}$$

$$\mathbf{u} \cdot \mathbf{v}$$

Polynomial Ring

$$\mathcal{R}_n = \mathbb{F}_2[x]/(x^n - 1)$$

$$v(x) = \sum_{i=0}^{n-1} v_i x^i$$

$$\mathcal{S}_w^n$$

$$u(x)v(x) \mod x^n - 1$$

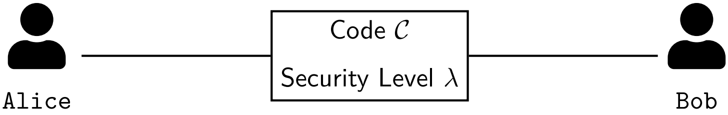
Definition (Linear Code)

An (n, k) linear code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_2^n$ equipped with two functions -
$\mathcal{C}.\mathtt{enc} : \mathbf{m} \mapsto \mathbf{c} \in \mathcal{C}$

$\mathcal{C}.\mathtt{dec} : \mathbf{c} + \mathbf{e} \in \mathbb{F}_2^n \mapsto \mathbf{m} + \mathcal{C}.\mathtt{dec}(\mathbf{e})$

HQC Primer

HQC Primer



HQC Primer

Code $\mathcal{C}$

Security Level λ

Alice

Bob

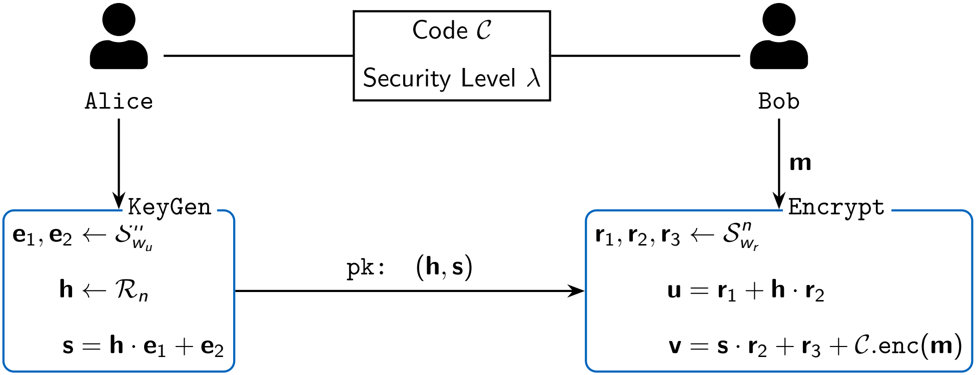
KeyGen

$$\mathbf{e}_1, \mathbf{e}_2 \leftarrow \mathcal{S}^n_{w_u}$$

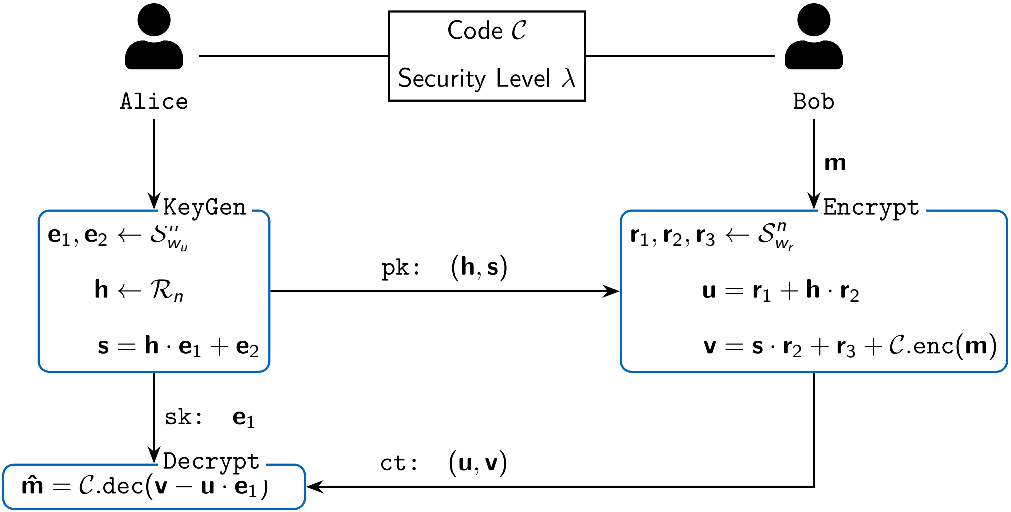
$$\mathbf{h} \leftarrow \mathcal{R}_n$$

$$\mathbf{s} = \mathbf{h} \cdot \mathbf{e}_1 + \mathbf{e}_2$$

HQC Primer

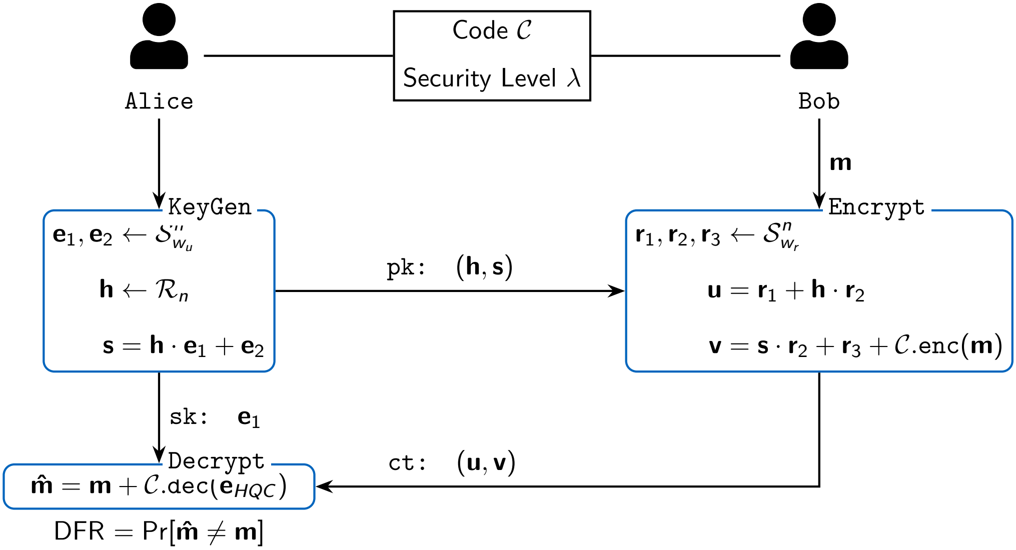

Code $\mathcal{C}$
Security Level λ
Alice
Bob
$\mathbf{m}$
KeyGen
$\mathbf{e}_1, \mathbf{e}_2 \leftarrow \mathcal{S}^n_{w_u}$
$\mathbf{h} \leftarrow \mathcal{R}_n$
$\mathbf{s} = \mathbf{h} \cdot \mathbf{e}_1 + \mathbf{e}_2$
pk: $(\mathbf{h}, \mathbf{s})$
Encrypt
$\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3 \leftarrow \mathcal{S}^n_{w_r}$
$\mathbf{u} = \mathbf{r}_1 + \mathbf{h} \cdot \mathbf{r}_2$
$\mathbf{v} = \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{r}_3 + \mathcal{C}.\mathtt{enc}(\mathbf{m})$

HQC Primer



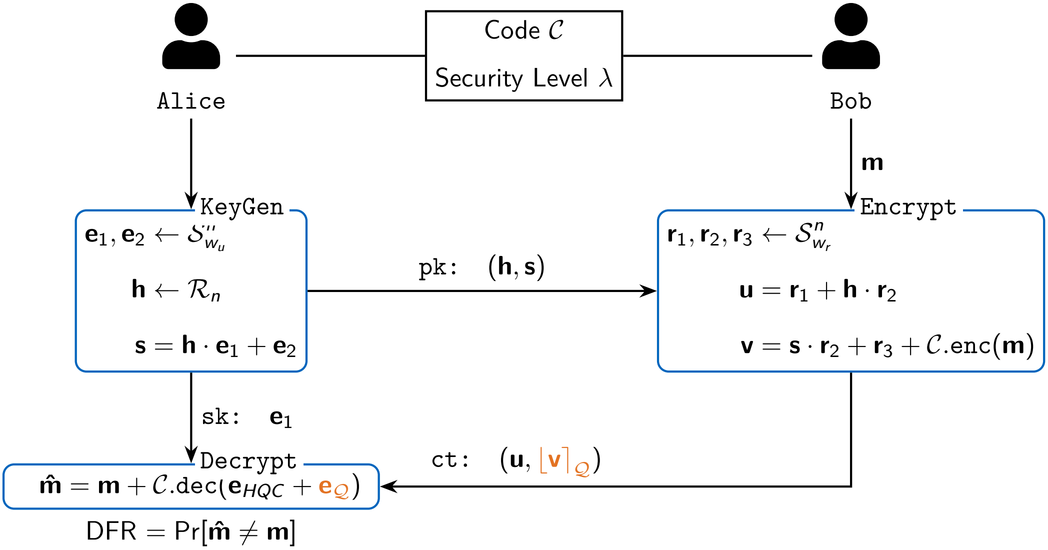
Code $\mathcal{C}$
Security Level λ
Alice
Bob
$\mathbf{m}$
KeyGen
$\mathbf{e}_1, \mathbf{e}_2 \leftarrow \mathcal{S}^n_{w_u}$
$\mathbf{h} \leftarrow \mathcal{R}_n$
$\mathbf{s} = \mathbf{h} \cdot \mathbf{e}_1 + \mathbf{e}_2$
pk: $(\mathbf{h}, \mathbf{s})$
Encrypt
$\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3 \leftarrow \mathcal{S}^n_{w_r}$
$\mathbf{u} = \mathbf{r}_1 + \mathbf{h} \cdot \mathbf{r}_2$
$\mathbf{v} = \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{r}_3 + \mathcal{C}.\mathtt{enc}(\mathbf{m})$
sk: $\mathbf{e}_1$
Decrypt
$\hat{\mathbf{m}} = \mathcal{C}.\mathtt{dec}(\mathbf{v} - \mathbf{u} \cdot \mathbf{e}_1)$
ct: $(\mathbf{u}, \mathbf{v})$

HQC Primer



Code $\mathcal{C}$
Security Level λ
Alice
Bob
$\mathbf{m}$
KeyGen
$\mathbf{e}_1, \mathbf{e}_2 \leftarrow \mathcal{S}^n_{w_u}$
$\mathbf{h} \leftarrow \mathcal{R}_n$
$\mathbf{s} = \mathbf{h} \cdot \mathbf{e}_1 + \mathbf{e}_2$
pk: $(\mathbf{h}, \mathbf{s})$
Encrypt
$\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3 \leftarrow \mathcal{S}^n_{w_r}$
$\mathbf{u} = \mathbf{r}_1 + \mathbf{h} \cdot \mathbf{r}_2$
$\mathbf{v} = \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{r}_3 + \mathcal{C}.\mathtt{enc}(\mathbf{m})$
sk: $\mathbf{e}_1$
ct: $(\mathbf{u}, \mathbf{v})$
Decrypt
$\hat{\mathbf{m}} = \mathbf{m} + \mathcal{C}.\mathtt{dec}(\mathbf{e}_{HQC})$
$\mathrm{DFR} = \Pr[\hat{\mathbf{m}} \neq \mathbf{m}]$

HQC Primer

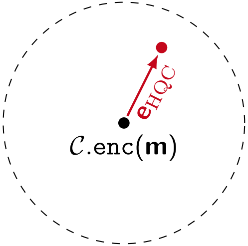


Code $\mathcal{C}$
Security Level λ
Alice
Bob
$\mathbf{m}$
KeyGen
$\mathbf{e}_1, \mathbf{e}_2 \leftarrow \mathcal{S}^{n}_{w_u}$
$\mathbf{h} \leftarrow \mathcal{R}_n$
$\mathbf{s} = \mathbf{h} \cdot \mathbf{e}_1 + \mathbf{e}_2$
pk: $(\mathbf{h}, \mathbf{s})$
Encrypt
$\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3 \leftarrow \mathcal{S}^{n}_{w_r}$
$\mathbf{u} = \mathbf{r}_1 + \mathbf{h} \cdot \mathbf{r}_2$
$\mathbf{v} = \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{r}_3 + \mathcal{C}.\mathtt{enc}(\mathbf{m})$
sk: $\mathbf{e}_1$
ct: $(\mathbf{u}, \lfloor \mathbf{v} \rceil_{\mathcal{Q}})$
Decrypt
$\hat{\mathbf{m}} = \mathbf{m} + \mathcal{C}.\mathtt{dec}(\mathbf{e}_{HQC} + \mathbf{e}_{\mathcal{Q}})$
$\mathrm{DFR} = \Pr[\hat{\mathbf{m}} \neq \mathbf{m}]$

What is Vector Quantization?

$$\begin{aligned}\lfloor\cdot\rceil_{\mathcal{Q}}: \quad & \mathbb{F}_2^n \to \mathcal{Q} \\ & \mathbf{v} \mapsto \lfloor\mathbf{v}\rceil_{\mathcal{Q}} = \mathbf{v} + \{\mathbf{v}\}_{\mathcal{Q}}\end{aligned}$$

$$n\,\text{bit} \to \rho n\,\text{bit}, \quad \rho < 1$$



What is Vector Quantization?

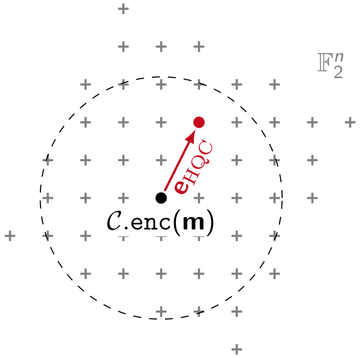
$$
\begin{aligned}
\lfloor\cdot\rceil_{\mathcal{Q}} : \quad & \mathbb{F}_2^n \to \mathcal{Q} \\
& \mathbf{v} \mapsto \lfloor\mathbf{v}\rceil_{\mathcal{Q}} = \mathbf{v} + \{\mathbf{v}\}_{\mathcal{Q}} \\
& n\,\text{bit} \to \rho n\,\text{bit}, \quad \rho < 1
\end{aligned}
$$

Theorem (Rate-Distortion Bound)

Compression by ρ creates average distortion

$$\mathbb{E}_{\mathbf{v}}\left[\frac{1}{n} wt_{\mathrm{H}}(\{\mathbf{v}\}_{\mathcal{Q}})\right] \geq H^{-1}(1-\rho)$$

[Shannon, 1948]



What is Vector Quantization?

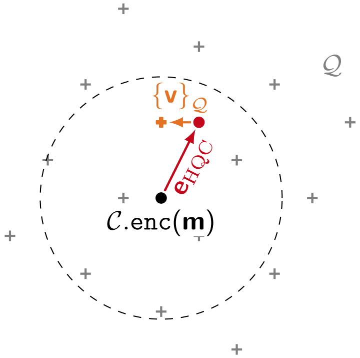
$$\begin{aligned} \lfloor\cdot\rceil_{\mathcal{Q}} : \quad & \mathbb{F}_2^n \to \mathcal{Q} \\ & \mathbf{v} \mapsto \lfloor \mathbf{v} \rceil_{\mathcal{Q}} = \mathbf{v} + \{\mathbf{v}\}_{\mathcal{Q}} \\ & n\,\text{bit} \to \rho n\,\text{bit}, \quad \rho < 1 \end{aligned}$$

Theorem (Rate-Distortion Bound)

Compression by ρ creates average distortion

$$\mathbb{E}_{\mathbf{v}}\left[\frac{1}{n} wt_{\mathrm{H}}(\{\mathbf{v}\}_{\mathcal{Q}})\right] \geq H^{-1}(1-\rho)$$

[Shannon, 1948]



What is Vector Quantization?

$$\begin{aligned} \lfloor\cdot\rceil_{\mathcal{Q}}: \quad & \mathbb{F}_2^n \to \mathcal{Q} \\ & \mathbf{v} \mapsto \lfloor\mathbf{v}\rceil_{\mathcal{Q}} = \mathbf{v} + \{\mathbf{v}\}_{\mathcal{Q}} \end{aligned}$$

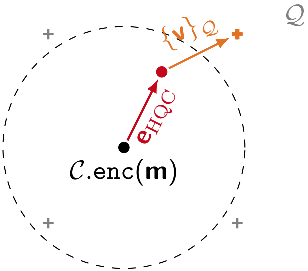
$$n\,\text{bit} \to \rho n\,\text{bit}, \quad \rho < 1$$

Theorem (Rate-Distortion Bound)

Compression by ρ creates average distortion

$$\mathbb{E}_{\mathbf{v}}\left[\frac{1}{n} wt_{\mathrm{H}}(\{\mathbf{v}\}_{\mathcal{Q}})\right] \geq H^{-1}(1-\rho)$$

[Shannon, 1948]



Polar Codes are Good Quantization Codes

[Korada and Urbanke, 2010]

SC decoding: approach rate-distortion bound asymptotically.

Polar Codes are Good Quantization Codes

[Korada and Urbanke, 2010]

SC decoding: approach rate-distortion bound asymptotically.

Complexity of encoding and decoding: $O(n \log n)$.

Polar Codes are Good Quantization Codes

[Korada and Urbanke, 2010]

SC decoding: approach rate-distortion bound asymptotically.

Complexity of encoding and decoding: $O(n \log n)$.

Distortion statistically close to Bernoulli$(p_{\mathcal{Q}})^n$.

$$\mathbf{c} \longrightarrow \boxed{\text{BSC}(p_{\mathcal{Q}})} \longrightarrow \lfloor \mathbf{c} \rceil_{\mathcal{Q}} = \mathbf{c} + \{\mathbf{c}\}_{\mathcal{Q}}$$

Polar Codes are Good Quantization Codes

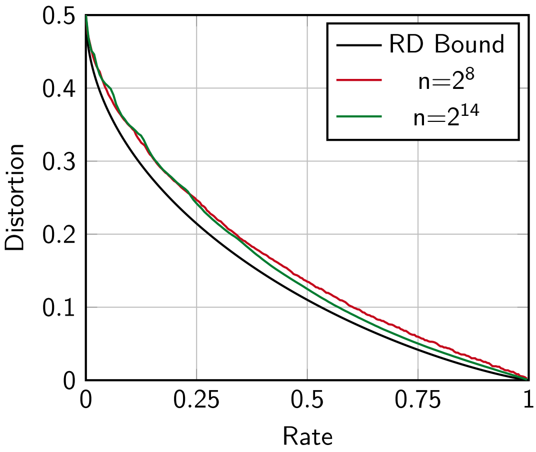
[Korada and Urbanke, 2010]

SC decoding: approach rate-distortion bound asymptotically.

Complexity of encoding and decoding: $O(n \log n)$.

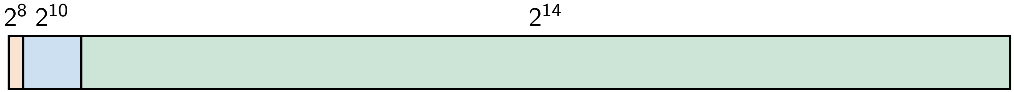
Distortion statistically close to Bernoulli$(p_{\mathcal{Q}})^n$.

$$\mathbf{c} \longrightarrow \boxed{\mathrm{BSC}(p_{\mathcal{Q}})} \longrightarrow \lfloor \mathbf{c} \rceil_{\mathcal{Q}} = \mathbf{c} + \{\mathbf{c}\}_{\mathcal{Q}}$$



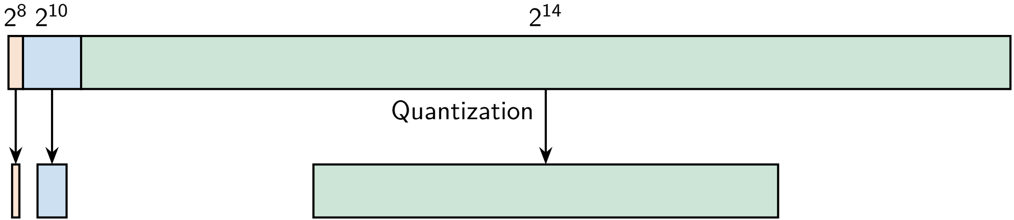
Quantization with Polar Codes (Black-Box Approach)

NIST 1 HQC Ciphertext **v** of length $n_\mathcal{C} = 17664$



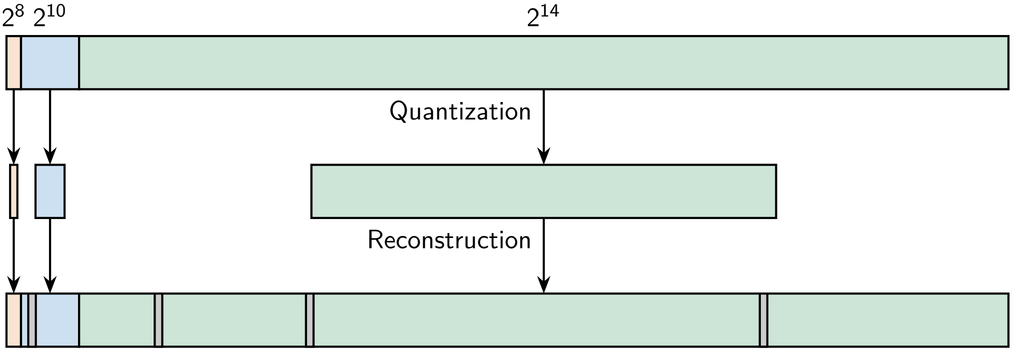
Quantization with Polar Codes (Black-Box Approach)

NIST 1 HQC Ciphertext $\mathbf{v}$ of length $n_{\mathcal{C}} = 17664$



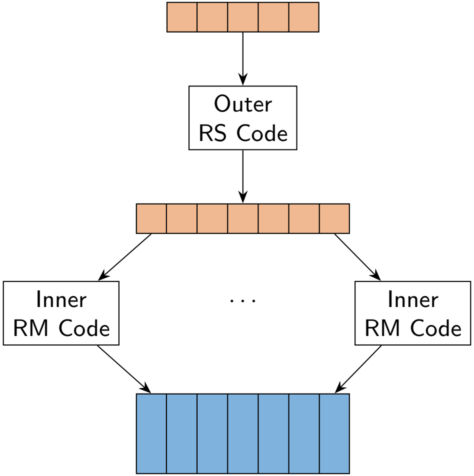
Quantization with Polar Codes (Black-Box Approach)

NIST 1 HQC Ciphertext $\mathbf{v}$ of length $n_{\mathcal{C}} = 17664$

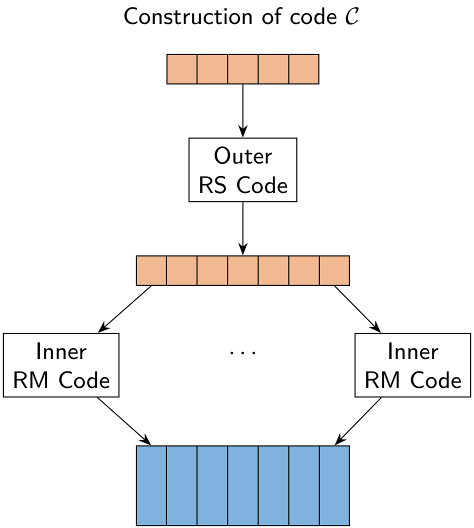


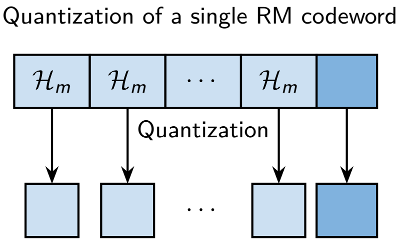
Aligned Quantization Code (White-Box Approach)

Construction of code $\mathcal{C}$



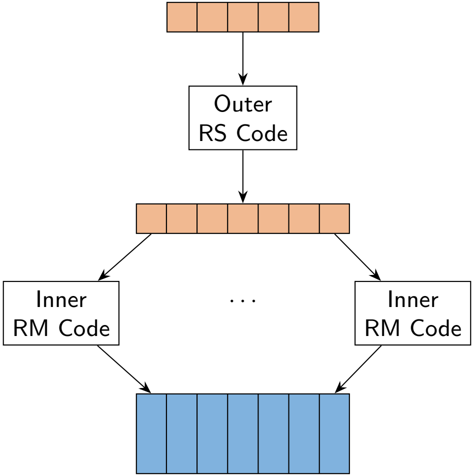
Aligned Quantization Code (White-Box Approach)



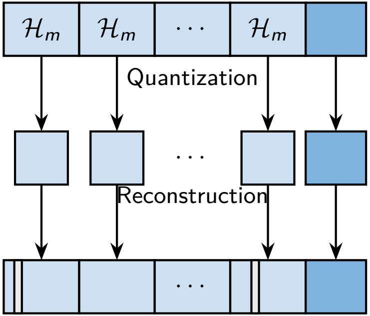


Aligned Quantization Code (White-Box Approach)

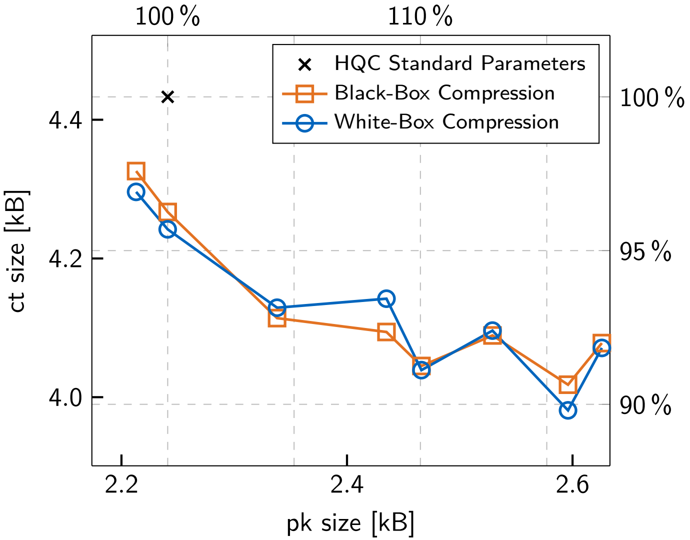
Construction of code $\mathcal{C}$



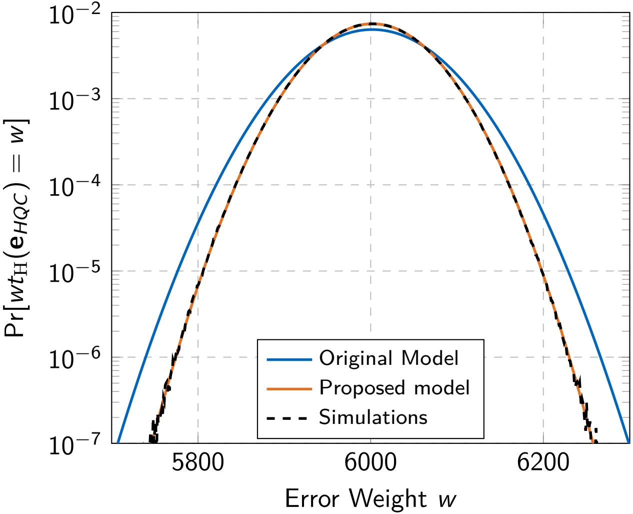
Quantization of a single RM codeword



Simulation Results



New Error Weight Model



In Conclusion

Summary

- Quantization can successfully reduce the ciphertext length of HQC upto 8%.
- But complexity of encryption and decryption increased 18%.

In Conclusion

Summary

- Quantization can successfully reduce the ciphertext length of HQC upto 8%.
- But complexity of encryption and decryption increased 18%.

Open Questions

- Other candidates for quantization code $\mathcal{Q}$?
- Better error-correcting code $\mathcal{C}$ with predictable DFR?

References I

Korada, S. B., & Urbanke, R. L. (2010). Polar codes are optimal for lossy source coding. *IEEE Transactions on Information Theory*, *56*(4), 1751–1768. https://doi.org/10.1109/TIT.2010.2040961

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system technical journal*, *27*(3), 379–423.