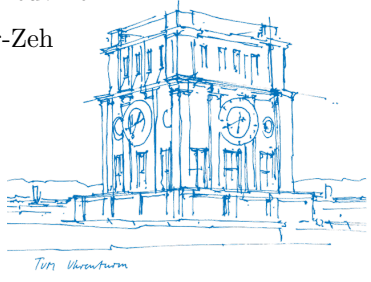
HQC Beyond the Standard: Ciphertext Compression & Refined DFR Analysis

Sebastian Bitzer Emma Munisamy Jean-Christophe Deneuville
Bharath Purtipli Stefan Ritterhoff Antonia Wachter-Zeh

Eurocrypt 2026



NIST's Favorite KEMs

HQC	KYBER

- Alekhnovich, More on Average Case vs Approximation Complexity
- Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

NIST's Favorite KEMs

	HQC	KYBER

- Alekhnovich, More on Average Case vs Approximation Complexity
- Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Metric	Hamming	Euclidean

NIST's Favorite KEMs

	HQC	KYBER

- Alekhnovich, More on Average Case vs Approximation Complexity
- Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Metric	Hamming	Euclidean
Ciphertext size	4.4 kB	0.8 kB

NIST's Favorite KEMs

	HQC	KYBER

- Alekhnovich, More on Average Case vs Approximation Complexity
- Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Metric	Hamming	Euclidean
Ciphertext size	~~4.4 kB~~	0.8 kB
	4.2 kB (-5 %)	

NIST's Favorite KEMs

	HQC	KYBER

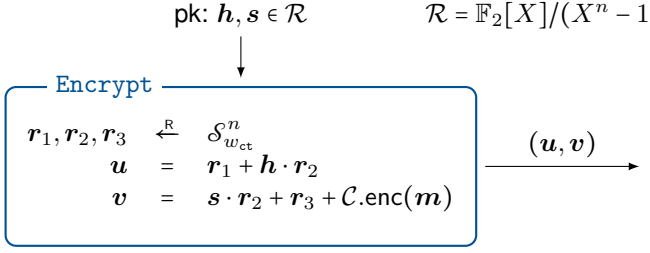
- Alekhnovich, More on Average Case vs Approximation Complexity
- Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Metric	Hamming	Euclidean
Ciphertext size	~~4.4 kB~~	0.8 kB
	4.2 kB (-5 %)	

This work: ➔ DFR analysis ➔ Hamming-metric compression

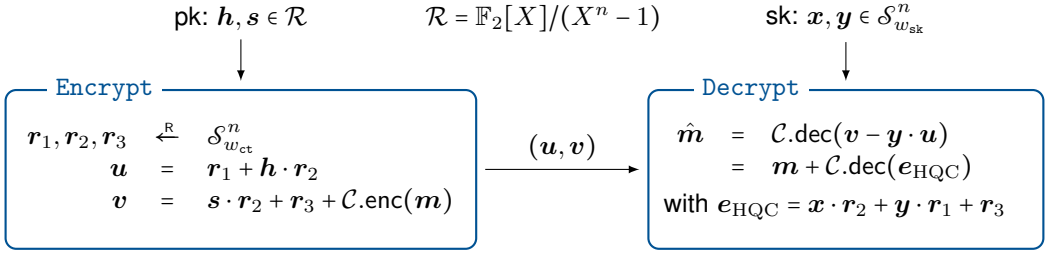
HQC Essentials

Aguilar-Melchor et al. Efficient Encryption From Random Quasi-Cyclic Codes



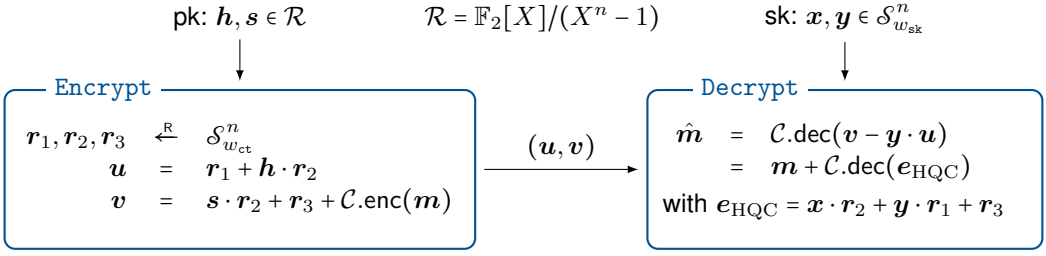
HQC Essentials

Aguilar-Melchor et al. Efficient Encryption From Random Quasi-Cyclic Codes



HQC Essentials

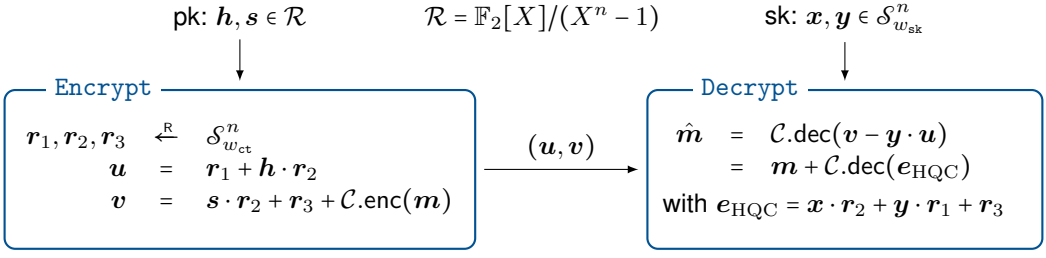
Aguilar-Melchor et al. Efficient Encryption From Random Quasi-Cyclic Codes



➔ DFR analysis: Assure $\Pr[\mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}}) \neq \boldsymbol{0}] \leq 2^{-\lambda}$

HQC Essentials

Aguilar-Melchor et al. Efficient Encryption From Random Quasi-Cyclic Codes



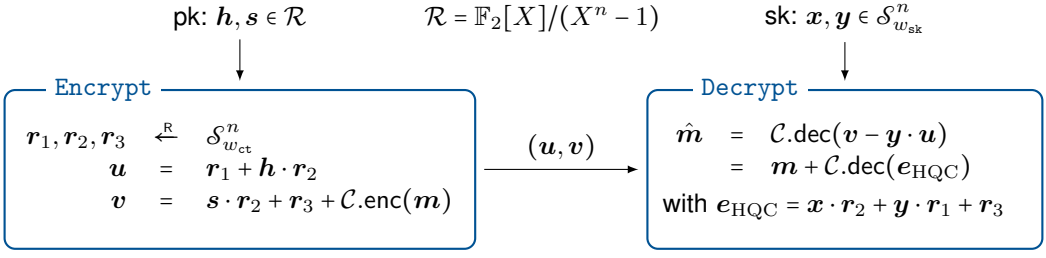
➔ DFR analysis: Assure $\Pr[\mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}}) \neq \boldsymbol{0}] \leq 2^{-\lambda}$

? Bound $\mathcal{F}_{\mathcal{C}} \triangleq \{\boldsymbol{e} : \mathcal{C}.\mathsf{dec}(\boldsymbol{e}) = \boldsymbol{0}\}$

? Model for $\boldsymbol{e}_{\mathrm{HQC}}$

HQC Essentials

Aguilar-Melchor et al. Efficient Encryption From Random Quasi-Cyclic Codes



➔ DFR analysis: Assure $\Pr[\mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}}) \neq \boldsymbol{0}] \leq 2^{-\lambda}$

☺ Bound $\mathcal{F}_{\mathcal{C}} \triangleq \{\boldsymbol{e} : \mathcal{C}.\mathsf{dec}(\boldsymbol{e}) = \boldsymbol{0}\}$

? Model for $\boldsymbol{e}_{\mathrm{HQC}}$

Error Models

$$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$$

Error Models

$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

$$\left(\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2)\right)_i \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})$$

Error Models

$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

$$\left(\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2)\right)_i \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})$$

Model 1

Independence assumption:

$$\boldsymbol{e}_{\mathrm{HQC}}^{(1)} \sim \mathrm{Bern}(p^\star)^n$$

Error Models

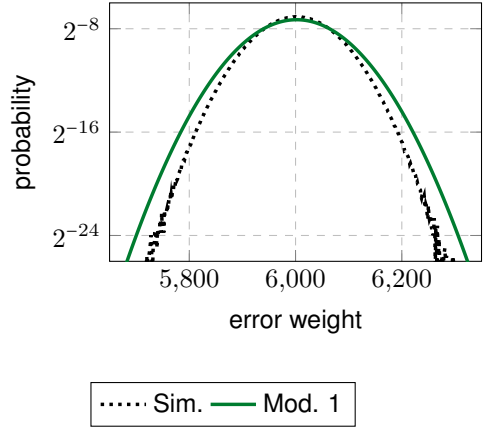
$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

$$(\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})$$

Model 1

Independence assumption:

$$\boldsymbol{e}^{(1)}_{\mathrm{HQC}} \sim \mathrm{Bern}(p^\star)^n$$



Error Models

$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

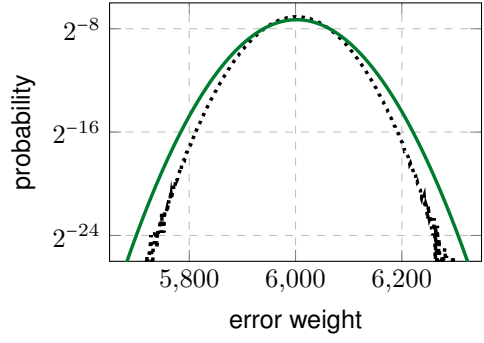
$$(\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})$$

Model 1

Independence assumption:

$$\boldsymbol{e}^{(1)}_{\mathrm{HQC}} \sim \mathrm{Bern}(p^\star)^n$$

Gaborit et al. HQC – Round 4



Error Models

Sendrier, Vasseur On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders

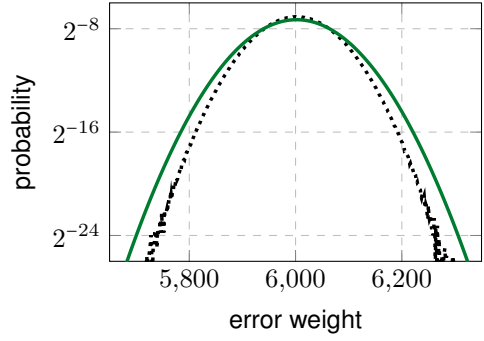
$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

$$(\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})$$
$$\textstyle\sum_i (\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i = w_{\mathtt{ct}} \cdot w_{\mathtt{sk}}$$

Model 1

Independence assumption:

$$\boldsymbol{e}^{(1)}_{\mathrm{HQC}} \sim \mathrm{Bern}(p^\star)^n$$



Gaborit et al. HQC – Round 4

Error Models

Sendrier, Vasseur On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders

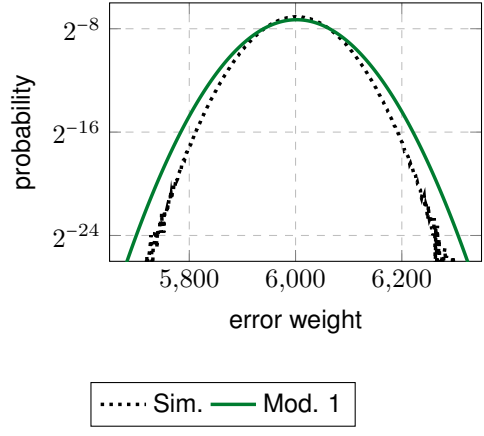
$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

$$(\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})$$
$$\textstyle\sum_i (\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i = w_{\mathtt{ct}} \cdot w_{\mathtt{sk}}$$

Model 2

$\boldsymbol{t}_j \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})^n \mid \sum_i t_{j,i} = w_{\mathtt{sk}} \cdot w_{\mathtt{ct}}$:

$$\boldsymbol{e}^{(2)}_{\mathrm{HQC}} = \boldsymbol{t}_1 \bmod 2 + \boldsymbol{t}_2 \bmod 2 + \boldsymbol{r}_3$$



Error Models

Sendrier, Vasseur On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders

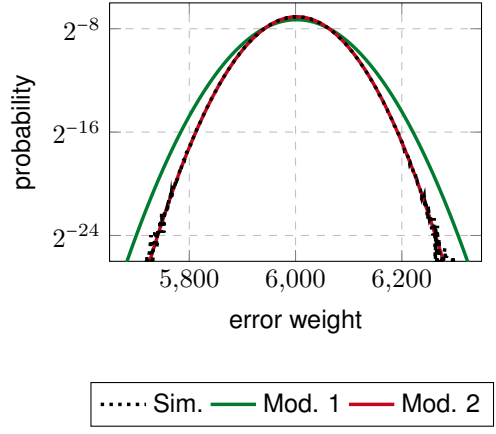
$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

$$(\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})$$
$$\textstyle\sum_i (\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i = w_{\mathtt{ct}} \cdot w_{\mathtt{sk}}$$

Model 2

$\boldsymbol{t}_j \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})^n \mid \sum_i t_{j,i} = w_{\mathtt{sk}} \cdot w_{\mathtt{ct}}$:

$$\boldsymbol{e}^{(2)}_{\mathrm{HQC}} = \boldsymbol{t}_1 \bmod 2 + \boldsymbol{t}_2 \bmod 2 + \boldsymbol{r}_3$$



Error Models

Sendrier, Vasseur On the Decoding Failure Rate of QC-MDPC Bit-Flipping Decoders

$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

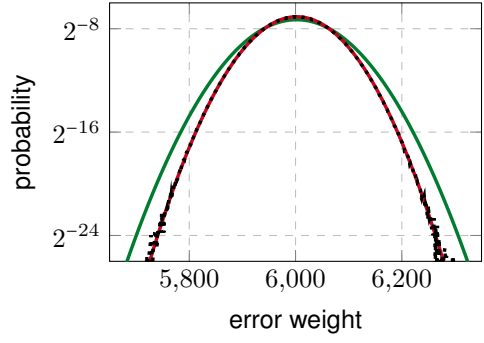
$$(\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})$$
$$\textstyle\sum_i (\mathbb{Z}(\boldsymbol{x}) \cdot \mathbb{Z}(\boldsymbol{r}_2))_i = w_{\mathtt{ct}} \cdot w_{\mathtt{sk}}$$

Model 2

$\boldsymbol{t}_j \sim \mathrm{Hyp}(n, w_{\mathtt{sk}}, w_{\mathtt{ct}})^n \mid \sum_i t_{j,i} = w_{\mathtt{sk}} \cdot w_{\mathtt{ct}}$:

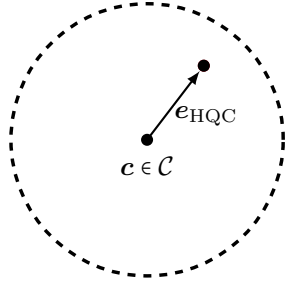
$$\boldsymbol{e}^{(2)}_{\mathrm{HQC}} = \boldsymbol{t}_1 \bmod 2 + \boldsymbol{t}_2 \bmod 2 + \boldsymbol{r}_3$$

➔ NIST 1: DFR bound $2^{-132.9}$ to $2^{-145.1}$



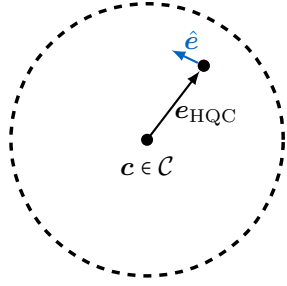
Lossy Source Coding: More Noise, Less Bits

`Decrypt:` $\hat{\boldsymbol{m}} = \mathcal{C}.\mathsf{dec}(\boldsymbol{v} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}})$



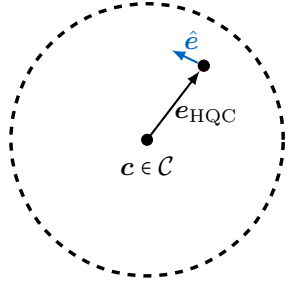
Lossy Source Coding: More Noise, Less Bits

Decrypt: $\hat{\boldsymbol{m}} = \mathcal{C}.\mathsf{dec}(\boldsymbol{v} - \boldsymbol{y}\cdot\boldsymbol{u} + \hat{\boldsymbol{e}}) = \boldsymbol{m} + \mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$



Lossy Source Coding: More Noise, Less Bits

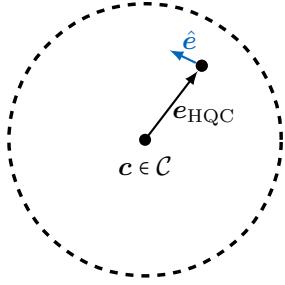
Decrypt: $\hat{\boldsymbol{m}} = \mathcal{C}.\mathsf{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$



Lossy Source Coding: More Noise, Less Bits

`Decrypt:` $\hat{\boldsymbol{m}} = \mathcal{C}.\mathsf{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$

Shannon, Mathematical Theory of Communication



Lossy Source Coding: More Noise, Less Bits

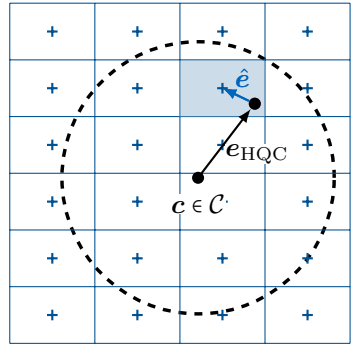
Decrypt: $\hat{\boldsymbol{m}} = \mathcal{C}.\mathsf{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$

Shannon, Mathematical Theory of Communication

Quantizer $\mathcal{Q}$:

$$\boldsymbol{v} \in \mathbb{F}_2^n \xrightarrow[\mathcal{Q}.\mathsf{dec}]{\mathtt{comp}} \boldsymbol{v}' \in \mathbb{F}_2^{k_{\mathcal{Q}}} \xrightarrow[\mathcal{Q}.\mathsf{enc}]{\mathtt{decomp}} \hat{\boldsymbol{v}} = \boldsymbol{v} + \hat{\boldsymbol{e}} \in \mathcal{Q}$$

$$\hat{\boldsymbol{e}} \in \mathcal{F}_{\mathcal{Q}}$$



Lossy Source Coding: More Noise, Less Bits

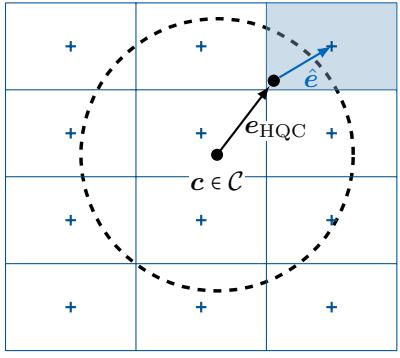
Decrypt: $\hat{\boldsymbol{m}} = \mathcal{C}.\mathsf{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$

Shannon, Mathematical Theory of Communication

Quantizer $\mathcal{Q}$:

$$\boldsymbol{v} \in \mathbb{F}_2^n \xrightarrow[\mathcal{Q}.\mathsf{dec}]{\mathtt{comp}} \boldsymbol{v}' \in \mathbb{F}_2^{k_{\mathcal{Q}}} \xrightarrow[\mathcal{Q}.\mathsf{enc}]{\mathtt{decomp}} \hat{\boldsymbol{v}} = \boldsymbol{v} + \hat{\boldsymbol{e}} \in \mathcal{Q}$$

$$\hat{\boldsymbol{e}} \in \mathcal{F}_{\mathcal{Q}}$$



Lossy Source Coding: More Noise, Less Bits

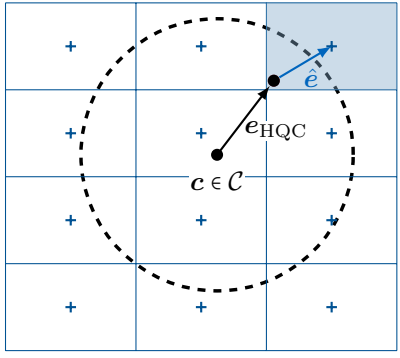
Decrypt: $\hat{\boldsymbol{m}} = \mathcal{C}.\mathrm{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathrm{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$

Shannon, Mathematical Theory of Communication

Quantizer $\mathcal{Q}$:

$$\boldsymbol{v} \in \mathbb{F}_2^n \xrightarrow[\mathcal{Q}.\mathrm{dec}]{\mathrm{comp}} \boldsymbol{v}' \in \mathbb{F}_2^{k_\mathcal{Q}} \xrightarrow{\mathrm{decomp}}_{\mathcal{Q}.\mathrm{enc}} \hat{\boldsymbol{v}} = \boldsymbol{v} + \hat{\boldsymbol{e}} \in \mathcal{Q}$$

$$\hat{\boldsymbol{e}} \in \mathcal{F}_\mathcal{Q}$$



Sphere-Packing Bound

$$k_\mathcal{Q} \geq n - \log_2\left(c \cdot \sum_{\ell=0}^{w_{\max}} \binom{n}{\ell}\right) \quad \text{for} \quad |\hat{\boldsymbol{e}}| \leq w_{\max}$$

Lossy Source Coding: More Noise, Less Bits

Decrypt: $\hat{\boldsymbol{m}} = \mathcal{C}.\mathrm{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathrm{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$

Shannon, Mathematical Theory of Communication

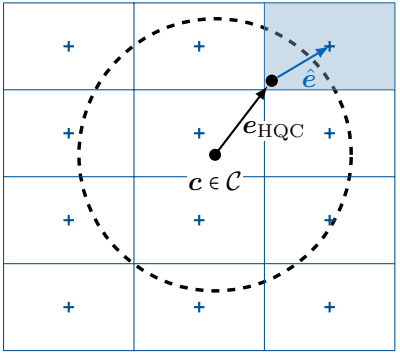
Quantizer $\mathcal{Q}$:

$$\boldsymbol{v} \in \mathbb{F}_2^n \xrightarrow[\mathcal{Q}.\mathrm{dec}]{\mathrm{comp}} \boldsymbol{v}' \in \mathbb{F}_2^{k_\mathcal{Q}} \xrightarrow[\mathcal{Q}.\mathrm{enc}]{\mathrm{decomp}} \hat{\boldsymbol{v}} = \boldsymbol{v} + \hat{\boldsymbol{e}} \in \mathcal{Q}$$

$$\hat{\boldsymbol{e}} \in \mathcal{F}_\mathcal{Q}$$

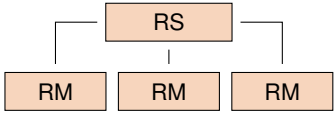
Sphere-Packing Bound

$$k_\mathcal{Q} \geq n - \log_2\left(c \cdot \sum_{\ell=0}^{w_{\max}} \binom{n}{\ell}\right) \quad \text{for} \quad |\hat{\boldsymbol{e}}| \leq w_{\max}$$

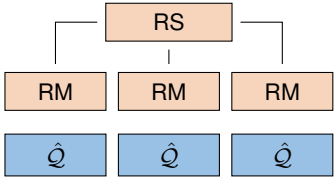


Advanced $\mathcal{Q}$: LDPC, Polar

Aligning Compression and Error Correction

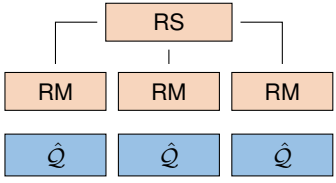


Aligning Compression and Error Correction



Aligning Compression and Error Correction

Shannon, Coding Theorems for a Discrete Source with a Fidelity Criterion

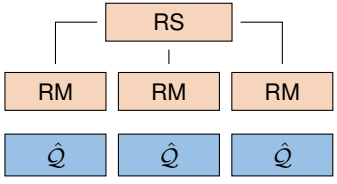


Direct-Product $\mathcal{Q} = \hat{\mathcal{Q}}^{\times n_{\mathrm{RS}}}$

- ☺ Hamming, Golay codes
- ☺ $\hat{\boldsymbol{e}} = (\hat{\boldsymbol{e}}_1, \ldots, \hat{\boldsymbol{e}}_{n_{\mathrm{RS}}}) \xleftarrow{\mathrm{R}} \mathcal{F}_{\hat{\mathcal{Q}}}^{\times n_{\mathrm{RS}}}$

Aligning Compression and Error Correction

Shannon, Coding Theorems for a Discrete Source with a Fidelity Criterion



Direct-Product $\mathcal{Q} = \hat{\mathcal{Q}}^{\times n_{\mathrm{RS}}}$

- ☺ Hamming, Golay codes
- ☺ $\hat{\boldsymbol{e}} = (\hat{\boldsymbol{e}}_1, \ldots, \hat{\boldsymbol{e}}_{n_{\mathrm{RS}}}) \xleftarrow{\mathrm{R}} \mathcal{F}_{\hat{\mathcal{Q}}}^{\times n_{\mathrm{RS}}}$

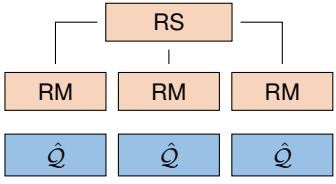
RM Failure Probability

For $\boldsymbol{e} \xleftarrow{\mathrm{R}} \mathcal{S}_w^{n_{\mathrm{RM}}}$, $\hat{\boldsymbol{e}} \xleftarrow{\mathrm{R}} \mathcal{F}_{\hat{\mathcal{Q}}}$:

$$\Pr[\boldsymbol{e} + \hat{\boldsymbol{e}} \notin \mathcal{F}_{\mathrm{RM}}]$$

Aligning Compression and Error Correction

Shannon, Coding Theorems for a Discrete Source with a Fidelity Criterion



Direct-Product $\mathcal{Q} = \hat{\mathcal{Q}}^{\times n_{\mathrm{RS}}}$

- ☺ Hamming, Golay codes
- ☺ $\hat{\boldsymbol{e}} = (\hat{\boldsymbol{e}}_1, \ldots, \hat{\boldsymbol{e}}_{n_{\mathrm{RS}}}) \xleftarrow{\mathrm{R}} \mathcal{F}_{\hat{\mathcal{Q}}}^{\times n_{\mathrm{RS}}}$

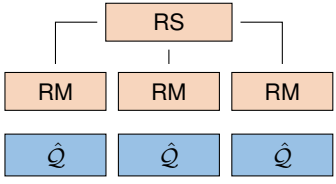
RM Failure Probability

For $\boldsymbol{e} \xleftarrow{\mathrm{R}} \mathcal{S}_w^{n_{\mathrm{RM}}}$, $\hat{\boldsymbol{e}} \xleftarrow{\mathrm{R}} \mathcal{F}_{\hat{\mathcal{Q}}}$:

$$\Pr[\boldsymbol{e} + \hat{\boldsymbol{e}} \notin \mathcal{F}_{\mathrm{RM}}] \leq \sum_{\boldsymbol{c} \in \mathrm{RM} \setminus \{\boldsymbol{0}\}} \Pr[\mathcal{E}_{\boldsymbol{c}}] + \frac{\Pr[\mathcal{T}_{\boldsymbol{c}}]}{2}$$

Aligning Compression and Error Correction

Shannon, Coding Theorems for a Discrete Source with a Fidelity Criterion



Direct-Product $\mathcal{Q} = \hat{\mathcal{Q}}^{\times n_{\mathrm{RS}}}$

- ☺ Hamming, Golay codes
- ☺ $\hat{\boldsymbol{e}} = (\hat{\boldsymbol{e}}_1, \ldots, \hat{\boldsymbol{e}}_{n_{\mathrm{RS}}}) \xleftarrow{\mathrm{R}} \mathcal{F}_{\hat{\mathcal{Q}}}^{\times n_{\mathrm{RS}}}$

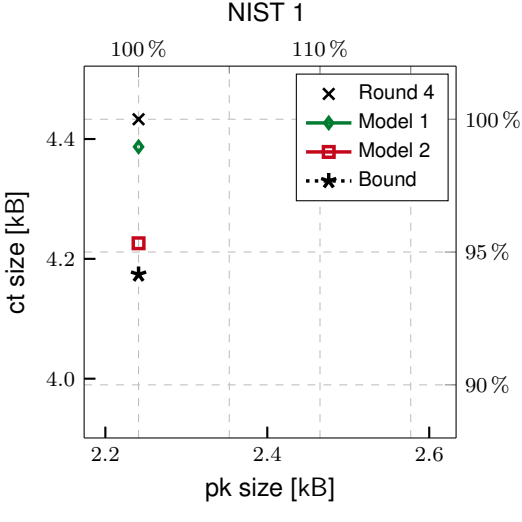
RM Failure Probability

For $\boldsymbol{e} \xleftarrow{\mathrm{R}} \mathcal{S}_w^{n_{\mathrm{RM}}}$, $\hat{\boldsymbol{e}} \xleftarrow{\mathrm{R}} \mathcal{F}_{\hat{\mathcal{Q}}}$:

$$\Pr[\boldsymbol{e} + \hat{\boldsymbol{e}} \notin \mathcal{F}_{\mathrm{RM}}] \leq \sum_{\boldsymbol{c} \in \mathrm{RM} \setminus \{\boldsymbol{0}\}} \Pr[\mathcal{E}_{\boldsymbol{c}}] + \frac{\Pr[\mathcal{T}_{\boldsymbol{c}}]}{2}$$

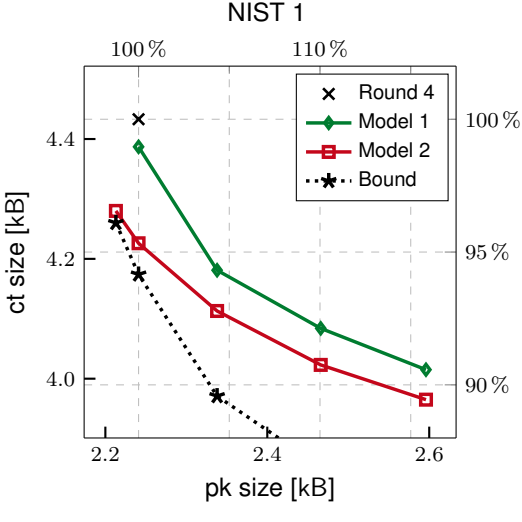
$$\mathcal{E}_{\boldsymbol{c}} : |\boldsymbol{c} + \hat{\boldsymbol{e}} + \boldsymbol{e}| < |\hat{\boldsymbol{e}} + \boldsymbol{e}| \qquad \mathcal{T}_{\boldsymbol{c}} : |\boldsymbol{c} + \hat{\boldsymbol{e}} + \boldsymbol{e}| = |\hat{\boldsymbol{e}} + \boldsymbol{e}|$$

Summa Summarum



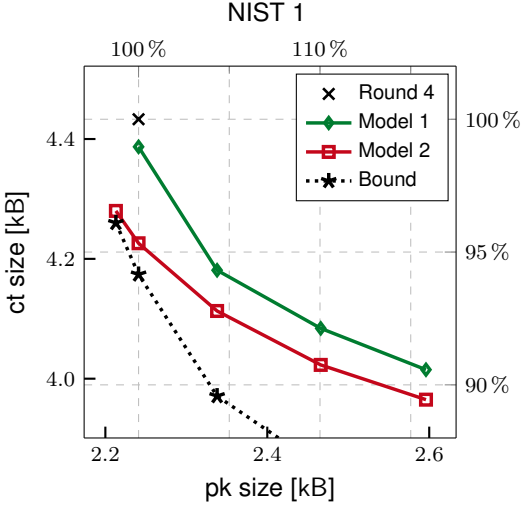
- ☺ Efficient direct-product $\mathcal{Q}$
- ☺ Error model with sum constraint
- ☺ Ciphertext size $-5\,\%$

Summa Summarum



- ☺ Efficient direct-product $\mathcal{Q}$
- ☺ Error model with sum constraint
- ☺ Ciphertext size $-5\,\%$ to $-10\,\%$

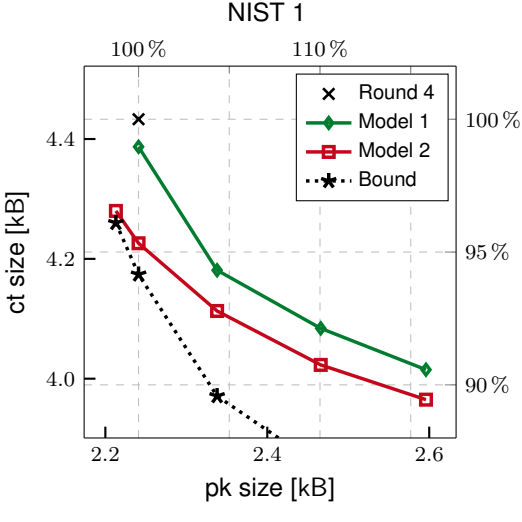
Summa Summarum



- ☺ Efficient direct-product $\mathcal{Q}$
- ☺ Error model with sum constraint
- ☺ Ciphertext size $-5\,\%$ to $-10\,\%$

- ? How far can we go?

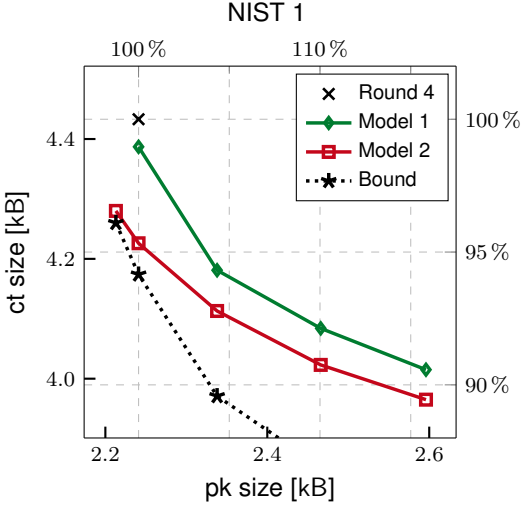
Summa Summarum



- ☺ Efficient direct-product $\mathcal{Q}$
- ☺ Error model with sum constraint
- ☺ Ciphertext size $-5\,\%$ to $-10\,\%$

- ? How far can we go?
- ? Hamming-metric LWR?

Summa Summarum



- ☺ Efficient direct-product $\mathcal{Q}$
- ☺ Error model with sum constraint
- ☺ Ciphertext size $-5\,\%$ to $-10\,\%$

- ? How far can we go?
- ? Hamming-metric LWR?

Thank you! Questions?