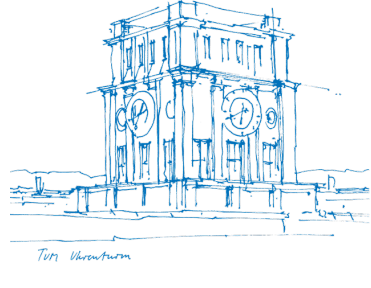
Code-Based Cryptography: Public-Key Encryption

Sebastian Bitzer

QSAFE



Code-Based Cryptography:

Public-Key Encryption


HQC Beyond the Standard: Ciphertext Compression and Refined DFR Analysis

Sebastian Bitzer[1], Jean-Christophe Deneuville[2], Emma Munisamy[1], Bharath Puttipli[1], Stefan Ritterhoff[1], and Antonia Wachter-Zeh[1]

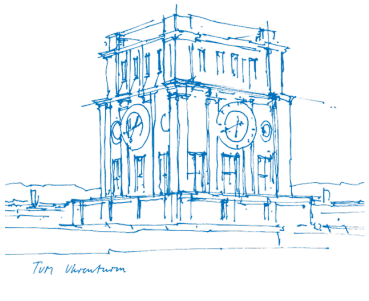
[1] Technical University of Munich, Munich, Germany

dération ENAC ISAE-SUPAERO ONERA, Université de Toulou

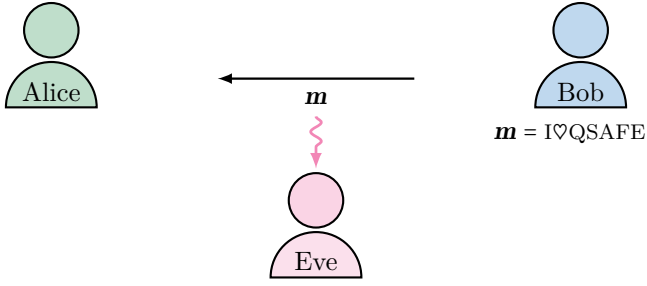
t. Hamming Quasi-Cyclic (HQC), recently
dization, does not employ ciphertext
counterpart Kyber. In lattice-ba
a standard post-processing
t-wise rounding. In
ed in code-base
ues to re

Sebastian Bitzer

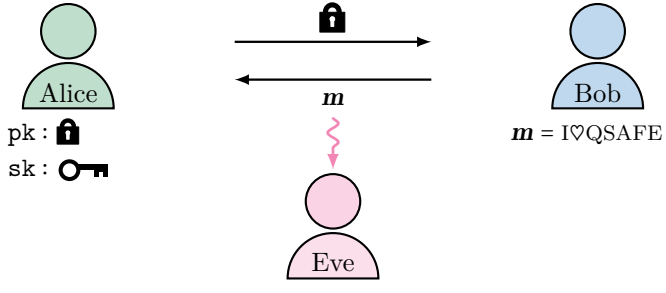
QSAFE



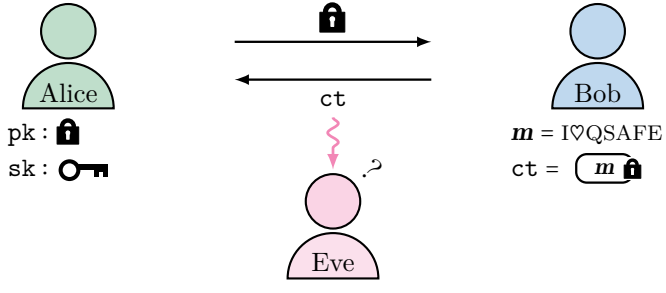
Public-Key Encryption: From Concept to Codes



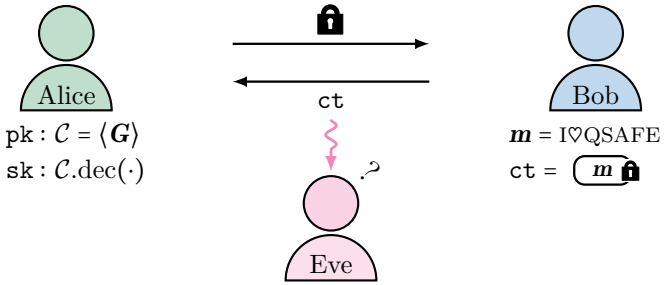
Public-Key Encryption: From Concept to Codes



Public-Key Encryption: From Concept to Codes



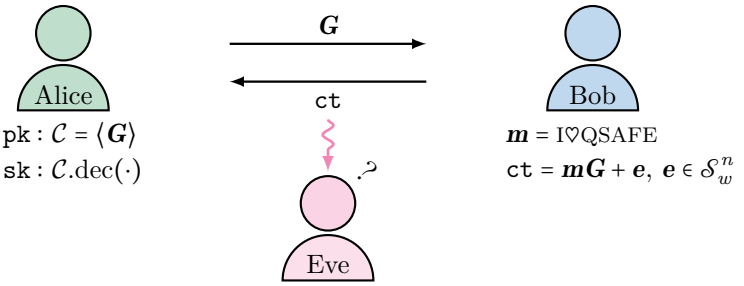
Public-Key Encryption: From Concept to Codes



Robert J. McEliece



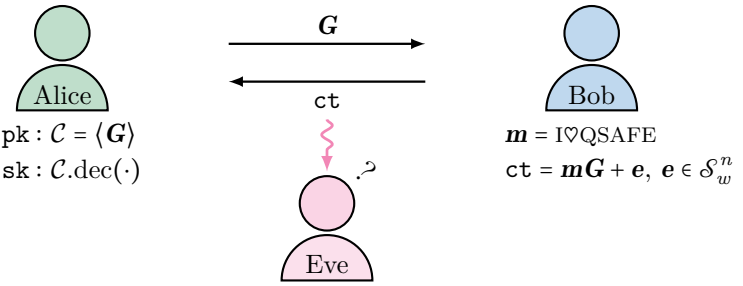
Public-Key Encryption: From Concept to Codes



Robert J. McEliece



Public-Key Encryption: From Concept to Codes



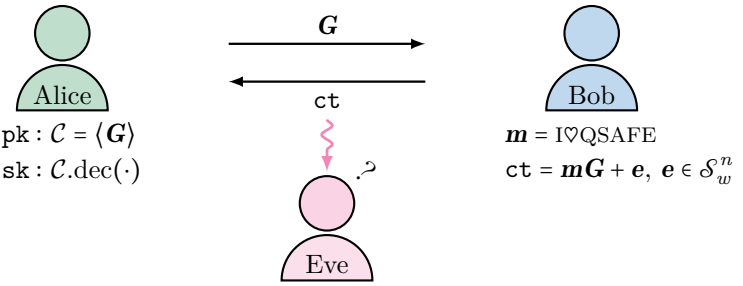
Robert J. McEliece



Decoding Random Code

Given: $\boldsymbol{G} \xleftarrow{\text{R}} \mathbb{F}_2^{k \times n}$, $\boldsymbol{y} \in \mathbb{F}_2^n$
Find: $\boldsymbol{m} \in \mathbb{F}_2^k, \boldsymbol{e} \in \mathcal{S}_w^n$ s.t. $\boldsymbol{mG} + \boldsymbol{e} = \boldsymbol{y}$

Public-Key Encryption: From Concept to Codes



Robert J. McEliece



Decoding Random Code

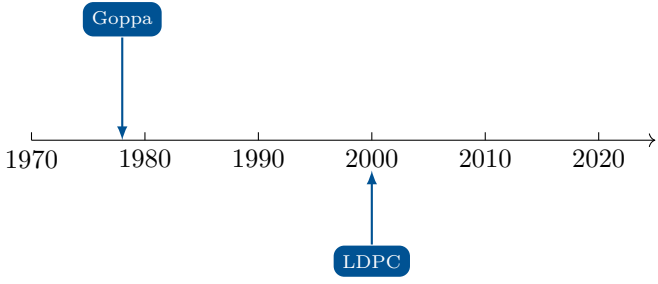
Given: $\boldsymbol{G} \xleftarrow{R} \mathbb{F}_2^{k \times n}$, $\boldsymbol{y} \in \mathbb{F}_2^n$
Find: $\boldsymbol{m} \in \mathbb{F}_2^k, \boldsymbol{e} \in \mathcal{S}_w^n$ s.t. $\boldsymbol{mG} + \boldsymbol{e} = \boldsymbol{y}$

Code Distinguishing

Given: $\mathcal{C} = \langle \boldsymbol{G} \rangle \subset \mathbb{F}_2^n$
Decide: $\mathcal{C}$ random?

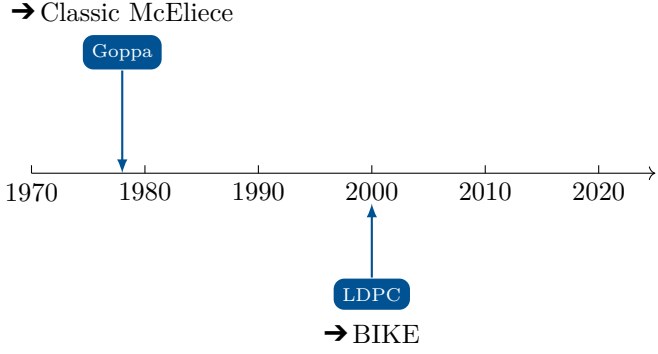
A Brief History of McEliece

- Weger et al., A Survey on Code-Based Cryptography
- Deneuville, Code-Based Post-Quantum Cryptography



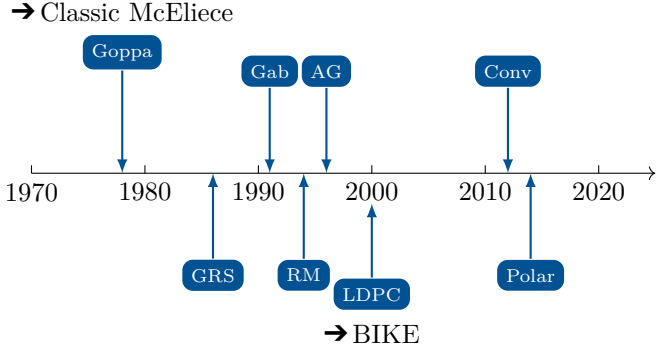
A Brief History of McEliece

- Weger et al., A Survey on Code-Based Cryptography
- Deneuville, Code-Based Post-Quantum Cryptography



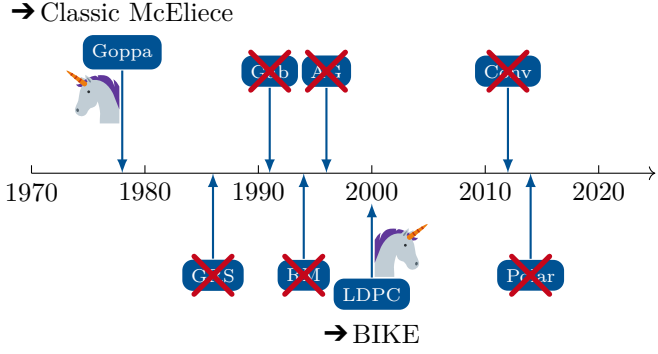
A Brief History of McEliece

- Weger et al., A Survey on Code-Based Cryptography
- Deneuville, Code-Based Post-Quantum Cryptography



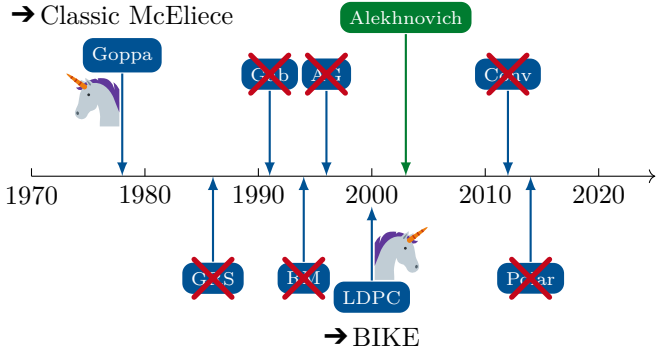
A Brief History of McEliece

- Weger et al., A Survey on Code-Based Cryptography
- Deneuville, Code-Based Post-Quantum Cryptography



A Brief History of McEliece

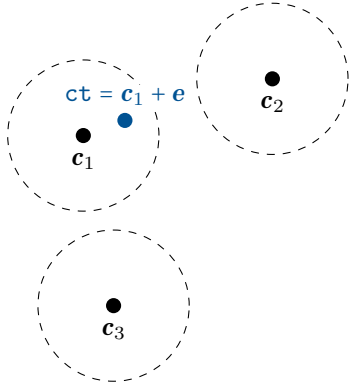
- Weger et al., A Survey on Code-Based Cryptography
- Deneuville, Code-Based Post-Quantum Cryptography



✕ secret structure recoverable

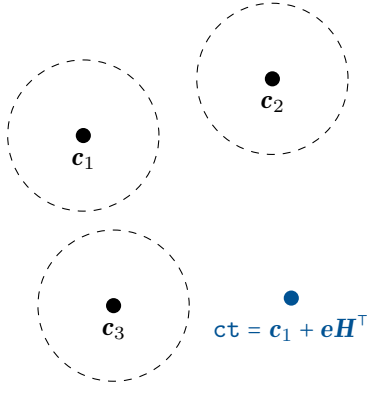
Encryption à la Alekhnovich

Alekhnovich, More on Average Case vs Approximation Complexity



Encryption à la Alekhnovich

Alekhnovich, More on Average Case vs Approximation Complexity

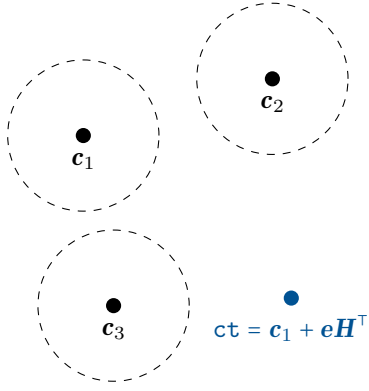


Encryption à la Alekhnovich

Alekhnovich, More on Average Case vs Approximation Complexity

Syndrome Decoding (SD)

$$\left\{(\boldsymbol{H}, \boldsymbol{e}\boldsymbol{H}^\top) : \boldsymbol{e} \xleftarrow{\mathrm{R}} \mathcal{S}_w^n\right\} \overset{c}{\approx} \left\{(\boldsymbol{H}, \boldsymbol{u}) : \boldsymbol{u} \xleftarrow{\mathrm{R}} \mathbb{F}_2^r\right\}$$

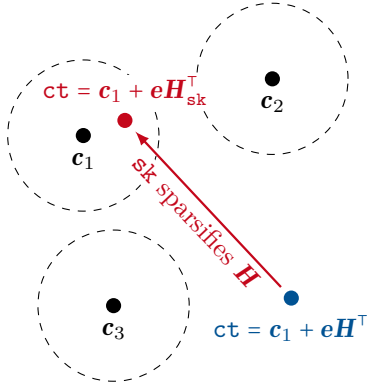


Encryption à la Alekhnovich

Alekhnovich, More on Average Case vs Approximation Complexity

Syndrome Decoding (SD)

$$\left\{(\boldsymbol{H}, \boldsymbol{e}\boldsymbol{H}^\intercal) : \boldsymbol{e} \xleftarrow{\mathrm{R}} \mathcal{S}_w^n\right\} \overset{c}{\approx} \left\{(\boldsymbol{H}, \boldsymbol{u}) : \boldsymbol{u} \xleftarrow{\mathrm{R}} \mathbb{F}_2^r\right\}$$

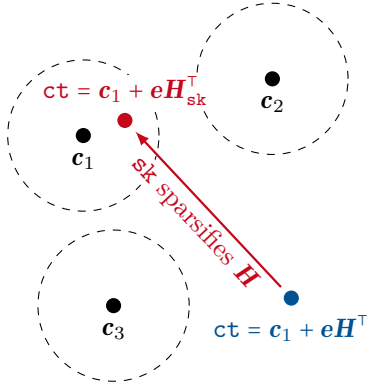


Encryption à la Alekhnovich

- Alekhnovich, More on Average Case vs Approximation Complexity
- Gaborit et al., Hamming Quasi-Cyclic (HQC)

Syndrome Decoding (SD)

$$\left\{(\boldsymbol{H}, \boldsymbol{e}\boldsymbol{H}^\top) : \boldsymbol{e} \xleftarrow{\text{R}} \mathcal{S}_w^n\right\} \overset{c}{\approx} \left\{(\boldsymbol{H}, \boldsymbol{u}) : \boldsymbol{u} \xleftarrow{\text{R}} \mathbb{F}_2^r\right\}$$



Encryption à la Alekhnovich

- Alekhnovich, More on Average Case vs Approximation Complexity
- Gaborit et al., Hamming Quasi-Cyclic (HQC)

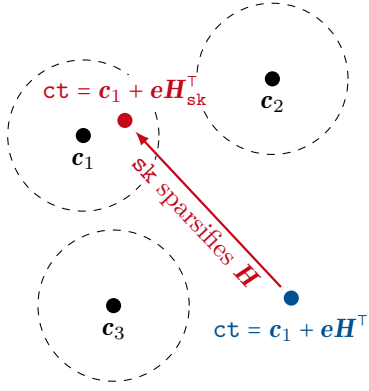
Syndrome Decoding (SD)

$$\left\{(\boldsymbol{H}, \boldsymbol{e}\boldsymbol{H}^\top) : \boldsymbol{e} \xleftarrow{R} \mathcal{S}_w^n\right\} \overset{c}{\approx} \left\{(\boldsymbol{H}, \boldsymbol{u}) : \boldsymbol{u} \xleftarrow{R} \mathbb{F}_2^r\right\}$$

$$\mathcal{R} \coloneqq \mathbb{F}_2[X]/(X^n - 1)$$

Quasi-Cyclic (QC) SD

$$\left\{(\boldsymbol{h}, \boldsymbol{e}_1 + \boldsymbol{e}_2\boldsymbol{h}) : \boldsymbol{e}_i \xleftarrow{R} \mathcal{S}_w^n\right\} \overset{c}{\approx} \left\{(\boldsymbol{h}, \boldsymbol{u}) : \boldsymbol{u} \xleftarrow{R} \mathcal{R}\right\}$$



HQC Essentials

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

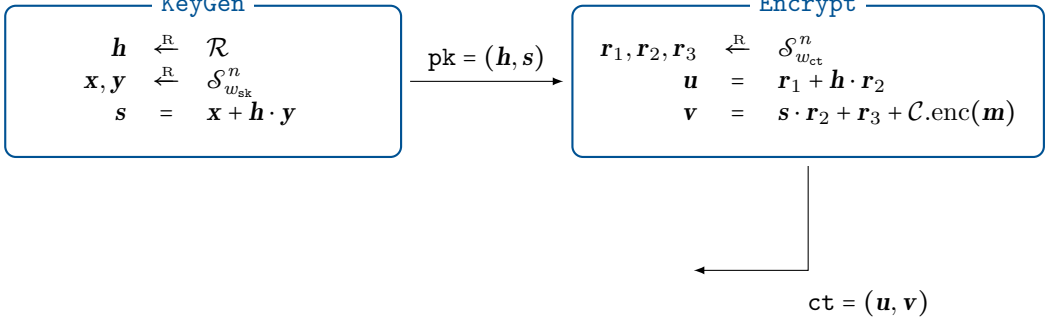
KeyGen

$$\begin{aligned} \boldsymbol{h} &\xleftarrow{R} \mathcal{R} \\ \boldsymbol{x}, \boldsymbol{y} &\xleftarrow{R} \mathcal{S}^n_{w_{\mathtt{sk}}} \\ \boldsymbol{s} &= \boldsymbol{x} + \boldsymbol{h} \cdot \boldsymbol{y} \end{aligned}$$

$$\xrightarrow{\mathtt{pk} = (\boldsymbol{h}, \boldsymbol{s})}$$

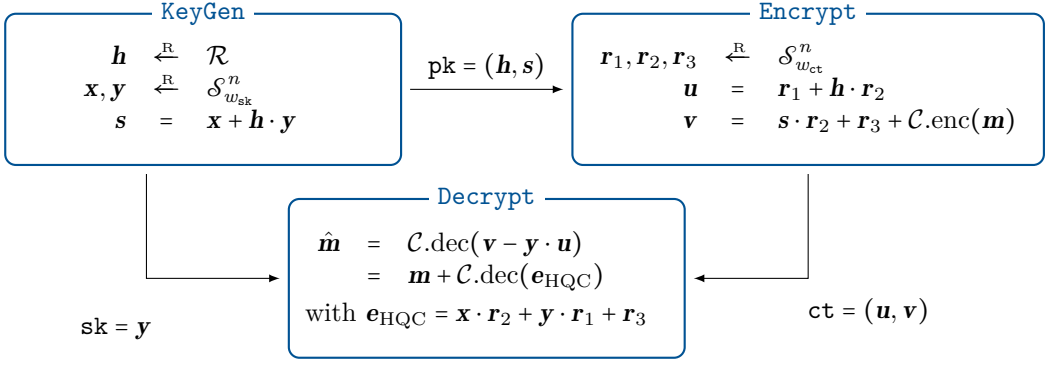
HQC Essentials

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



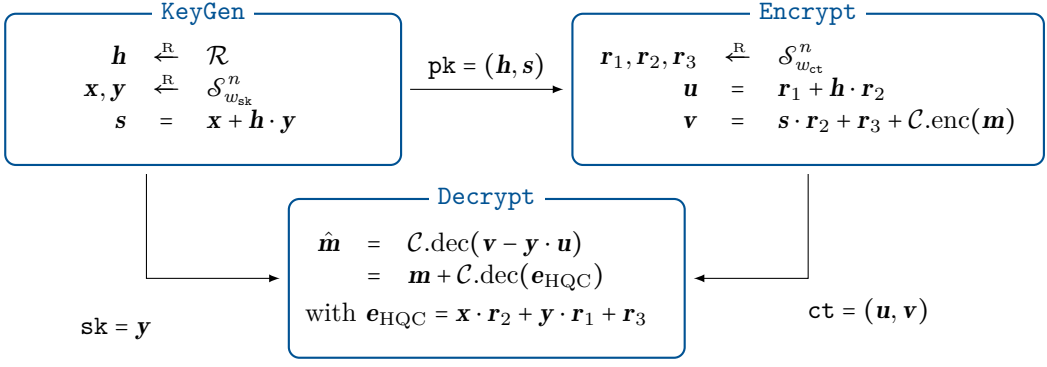
HQC Essentials

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



HQC Essentials

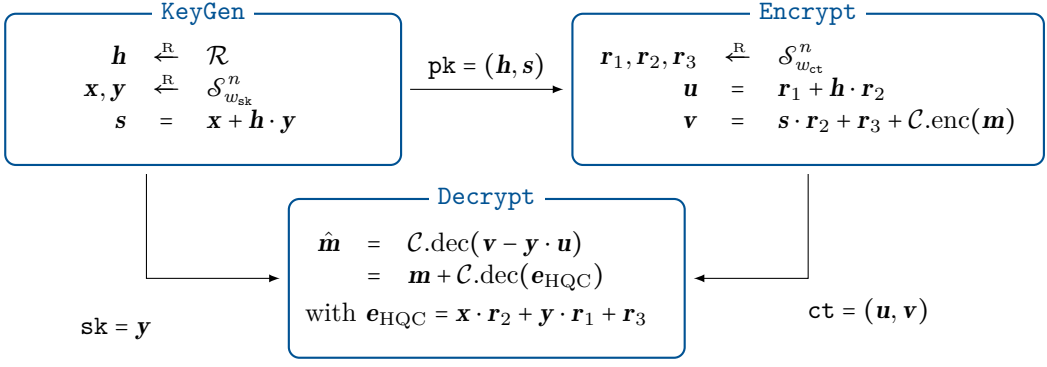
$$\mathcal{R} = \mathbb{F}_2[X]/(X^n - 1)$$



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

HQC Essentials

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



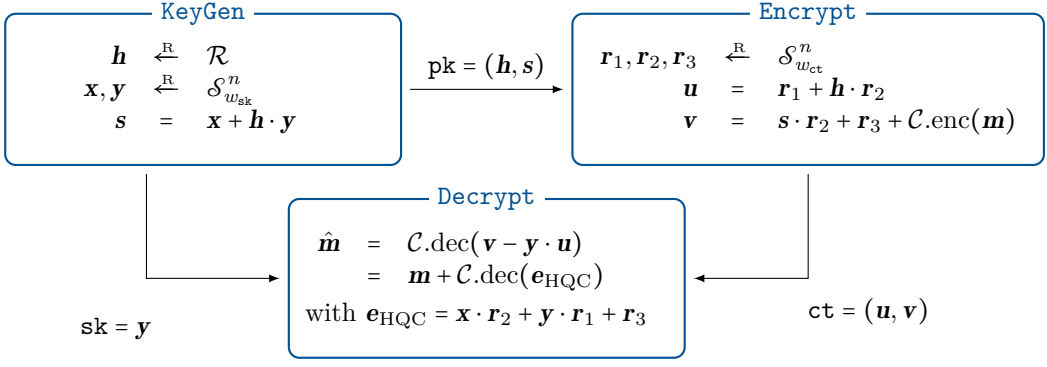
➔ DFR analysis: Assure $\Pr[\mathcal{C}.\mathrm{dec}(\boldsymbol{e}_{\mathrm{HQC}}) \neq \boldsymbol{0}] \leq 2^{-\lambda}$

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

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

HQC Essentials

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



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

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

? 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

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

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

Model 1

Independence assumption:

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

Error Models

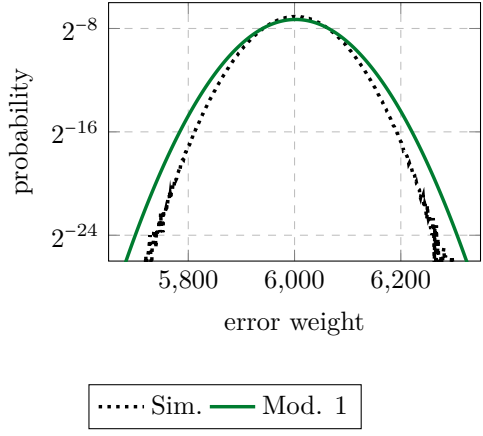
$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

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

Model 1

Independence assumption:

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



Error Models

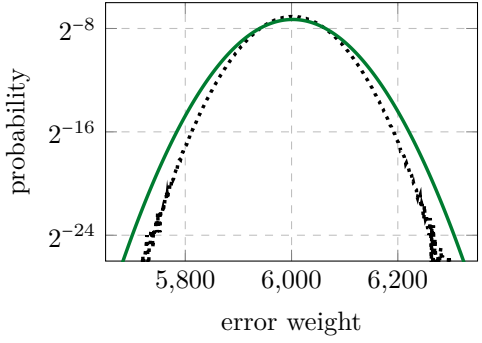
$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

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

Model 1

Independence assumption:

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



Gaborit et al. HQC – Round 4

Error Models

- Mesnard, Tillich, Vasseur, The Syndrome Weight Distribution in Quasi-Cyclic Codes
- Annechini, Barenghi, Pelosi, On the Decoding Failure Rate of HQC

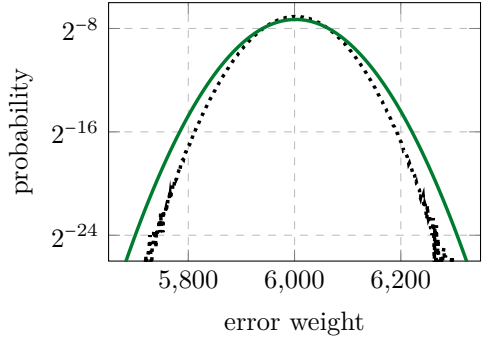
$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

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

Model 1

Independence assumption:

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



- Gaborit et al. HQC – Round 4

Error Models

- Mesnard, Tillich, Vasseur, The Syndrome Weight Distribution in Quasi-Cyclic Codes
- Annechini, Barenghi, Pelosi, On the Decoding Failure Rate of HQC

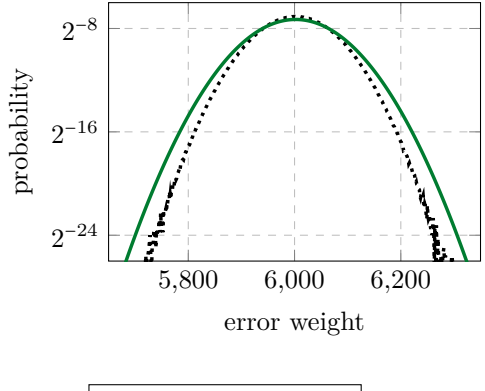
$\boldsymbol{e}_{\text{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

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

Model 2

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

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



Error Models

- Mesnard, Tillich, Vasseur, The Syndrome Weight Distribution in Quasi-Cyclic Codes
- Annechini, Barenghi, Pelosi, On the Decoding Failure Rate of HQC

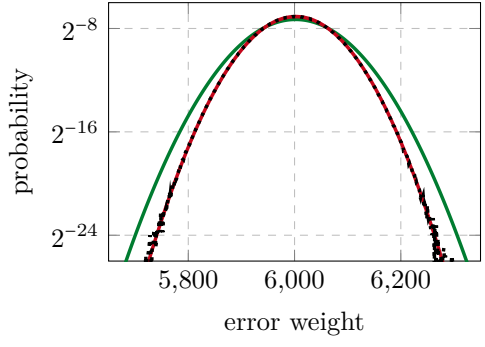
$\boldsymbol{e}_{\mathrm{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

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

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

- Mesnard, Tillich, Vasseur, The Syndrome Weight Distribution in Quasi-Cyclic Codes
- Annechini, Barenghi, Pelosi, On the Decoding Failure Rate of HQC

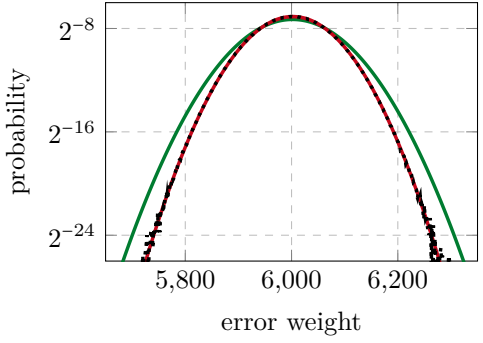
$\boldsymbol{e}_{\text{HQC}} = \boldsymbol{x} \cdot \boldsymbol{r}_2 + \boldsymbol{y} \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$:

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

Model 2

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

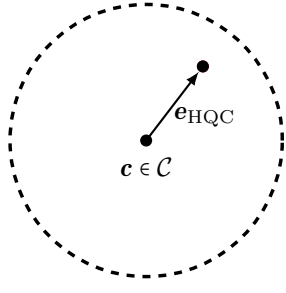
$$\boldsymbol{e}^{(2)}_{\text{HQC}} = \boldsymbol{t}_1 \bmod 2 + \boldsymbol{t}_2 \bmod 2 + \boldsymbol{r}_3$$



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

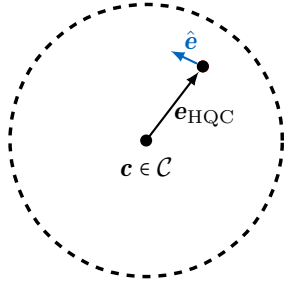
More Noise, Less Bits

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



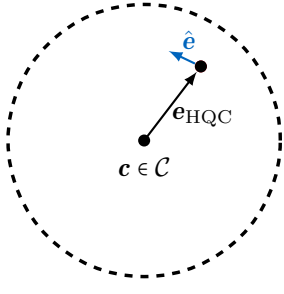
More Noise, Less Bits

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



More Noise, Less Bits

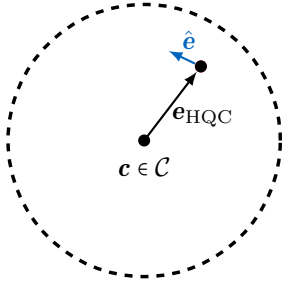
`Decrypt:` $\hat{\boldsymbol{m}} = \mathcal{C}.\mathrm{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathrm{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$



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



More Noise, Less Bits

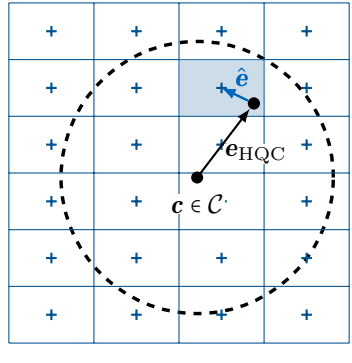
`Decrypt:` $\hat{\boldsymbol{m}} = \mathcal{C}.\mathrm{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathrm{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$

Shannon, Mathematical Theory of Communication

Quantizer $\mathcal{Q}$:

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

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



More Noise, Less Bits

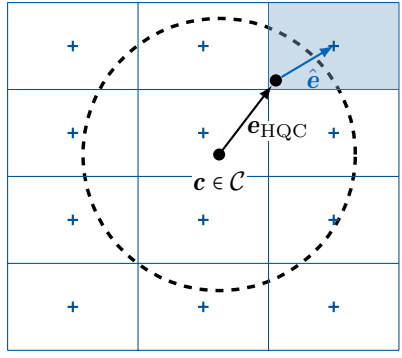
Decrypt: $\hat{\boldsymbol{m}} = \mathcal{C}.\mathrm{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathrm{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$

Shannon, Mathematical Theory of Communication

Quantizer $\mathcal{Q}$:

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

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



More Noise, Less Bits

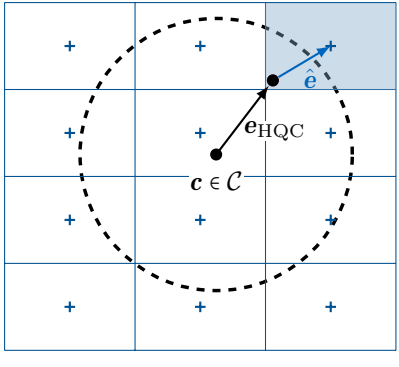
`Decrypt:` $\hat{\boldsymbol{m}} = \mathcal{C}.\mathrm{dec}(\hat{\boldsymbol{v}} - \boldsymbol{y} \cdot \boldsymbol{u}) = \boldsymbol{m} + \mathcal{C}.\mathrm{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \hat{\boldsymbol{e}})$

Shannon, Mathematical Theory of Communication

Quantizer $\mathcal{Q}$:

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

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



Sphere-Packing Bound

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

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

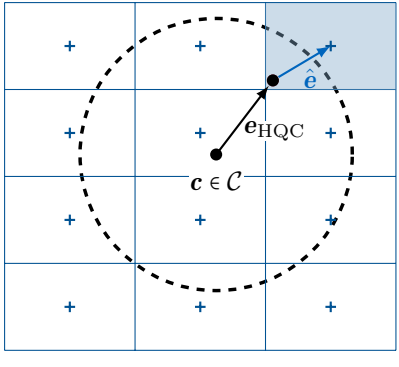
Quantizer $\mathcal{Q}$:

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

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

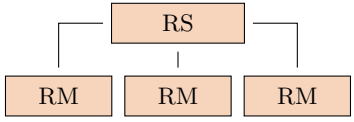
Sphere-Packing Bound

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

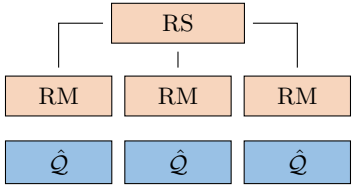


Advanced $\mathcal{Q}$: LDPC, Polar

Aligning Compression and Error Correction

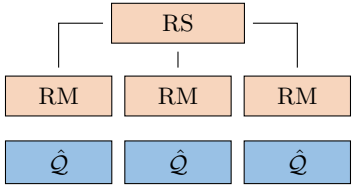


Aligning Compression and Error Correction



Aligning Compression and Error Correction

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

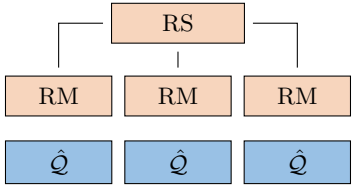


Direct-Product $\mathcal{Q} = \hat{\mathcal{Q}}^{\times n_{\mathrm{RS}}}$

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

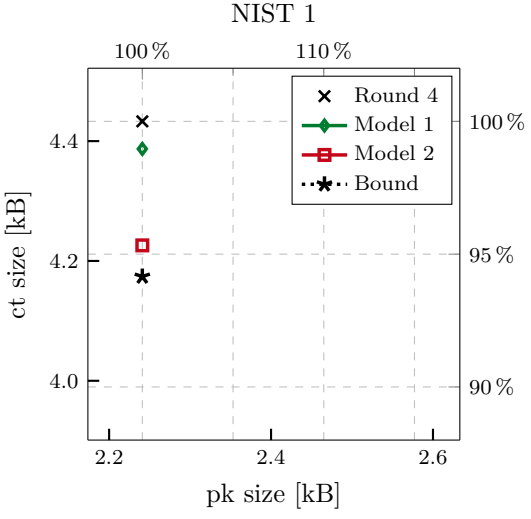
Aligning Compression and Error Correction

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



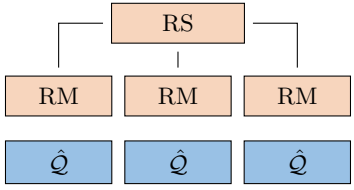
Direct-Product $\mathcal{Q} = \hat{\mathcal{Q}}^{\times n_{\mathrm{RS}}}$

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



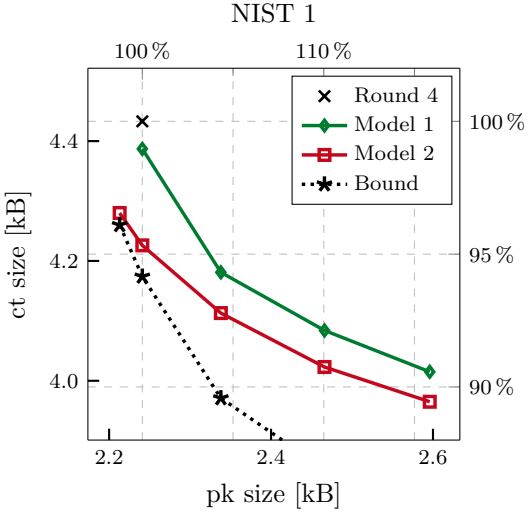
Aligning Compression and Error Correction

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



Conclusion

McEliece-like encryption:

- ➔ Requires hiding code structure

Hamming Quasi-Cyclic:

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

eprint.iacr.org/2025/2259



Conclusion

McEliece-like encryption:

- ➔ Requires hiding code structure

Hamming Quasi-Cyclic:

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

Open questions:

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

eprint.iacr.org/2025/2259

Conclusion

McEliece-like encryption:

- ➔ Requires hiding code structure

Hamming Quasi-Cyclic:

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

Open questions:

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

eprint.iacr.org/2025/2259

Thank you! Questions?