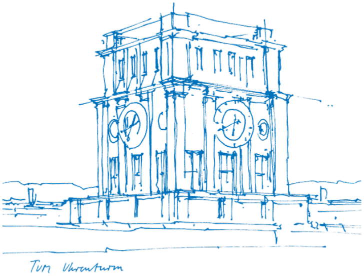
Ciphertext Compression for HQC

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

Zürich 2025



NIST's favourite KEMs

HQC	KYBER

Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

NIST's favourite KEMs

	HQC	KYBER
Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography		
Metric	Hamming	Euclidean

NIST's favourite KEMs

	HQC	KYBER
Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography		
Metric	Hamming	Euclidean

Later:

- Vadim Lyubashevsky, Kyber & More
- Jean-Christophe Deneuville, HQC & More

NIST's favourite KEMs

	HQC	KYBER
Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography		
Metric	Hamming	Euclidean
Ciphertext size	4.5 kB	0.8 kB

Later:

- Vadim Lyubashevsky, Kyber & More
- Jean-Christophe Deneuville, HQC & More

NIST's favourite KEMs

	HQC	KYBER
Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography		
Metric	Hamming	Euclidean
Ciphertext size	4.5 kB	0.8 kB
Compression	No	Yes, rounding

Later:

- Vadim Lyubashevsky, Kyber & More
- Jean-Christophe Deneuville, HQC & More

NIST's favourite KEMs

	HQC	KYBER
Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography		
Metric	Hamming	Euclidean
Ciphertext size	???	0.8 kB
Compression	???	Yes, rounding

Later:

- Vadim Lyubashevsky, Kyber & More
- Jean-Christophe Deneuville, HQC & More

This talk:

- → Hamming-metric compression
- → Reduce ciphertext size

HQC in a Nutshell

KeyGen

$$
\begin{aligned}
\boldsymbol{e}_1, \boldsymbol{e}_2 &\leftarrow \mathcal{S}_w^n \\
\boldsymbol{h} &\leftarrow \mathbb{F}_2[x]/(x^n - 1) \\
\boldsymbol{s} &= \boldsymbol{h} \cdot \boldsymbol{e}_1 + \boldsymbol{e}_2
\end{aligned}
$$

HQC in a Nutshell

KeyGen

$$\begin{aligned} \boldsymbol{e}_1, \boldsymbol{e}_2 &\leftarrow \mathcal{S}_w^n \\ \boldsymbol{h} &\leftarrow \mathbb{F}_2[x]/(x^n - 1) \\ \boldsymbol{s} &= \boldsymbol{h} \cdot \boldsymbol{e}_1 + \boldsymbol{e}_2 \end{aligned}$$

`pk`: $(\boldsymbol{h}, \boldsymbol{s})$

Encrypt

$$\begin{aligned} \boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 &\leftarrow \mathcal{S}_{w'}^n \\ \boldsymbol{y}_1 &= \boldsymbol{s} \cdot \boldsymbol{r}_2 + \boldsymbol{r}_3 + \mathcal{C}.\mathsf{enc}(\boldsymbol{m}) \\ \boldsymbol{y}_2 &= \boldsymbol{r}_1 + \boldsymbol{h} \cdot \boldsymbol{r}_2 \end{aligned}$$

HQC in a Nutshell

KeyGen

$$\begin{aligned} \boldsymbol{e}_1, \boldsymbol{e}_2 &\leftarrow \mathcal{S}_w^n \\ \boldsymbol{h} &\leftarrow \mathbb{F}_2[x]/(x^n - 1) \\ \boldsymbol{s} &= \boldsymbol{h} \cdot \boldsymbol{e}_1 + \boldsymbol{e}_2 \end{aligned}$$

pk: $(\boldsymbol{h}, \boldsymbol{s})$

Encrypt

$$\begin{aligned} \boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 &\leftarrow \mathcal{S}_{w'}^n \\ \boldsymbol{y}_1 &= \boldsymbol{s} \cdot \boldsymbol{r}_2 + \boldsymbol{r}_3 + \mathcal{C}.\mathtt{enc}(\boldsymbol{m}) \\ \boldsymbol{y}_2 &= \boldsymbol{r}_1 + \boldsymbol{h} \cdot \boldsymbol{r}_2 \end{aligned}$$

sk: $\boldsymbol{e}_1$

ct: $(\boldsymbol{y}_1, \boldsymbol{y}_2)$

Decrypt

$$\hat{\boldsymbol{m}} = \mathcal{C}.\mathtt{dec}(\boldsymbol{y}_1 - \boldsymbol{e}_1 \cdot \boldsymbol{y}_2)$$

HQC in a Nutshell

KeyGen

$$\begin{aligned} \mathbf{e}_1, \mathbf{e}_2 &\leftarrow \mathcal{S}_w^n \\ \mathbf{h} &\leftarrow \mathbb{F}_2[x]/(x^n - 1) \\ \mathbf{s} &= \mathbf{h} \cdot \mathbf{e}_1 + \mathbf{e}_2 \end{aligned}$$

pk: $(\mathbf{h}, \mathbf{s})$

Encrypt

$$\begin{aligned} \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3 &\leftarrow \mathcal{S}_{w'}^n \\ \mathbf{y}_1 &= \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{r}_3 + \mathcal{C}.\mathsf{enc}(\mathbf{m}) \\ \mathbf{y}_2 &= \mathbf{r}_1 + \mathbf{h} \cdot \mathbf{r}_2 \end{aligned}$$

sk: $\mathbf{e}_1$

ct: $(\mathbf{y}_1, \mathbf{y}_2)$

Decrypt

$$\hat{\mathbf{m}} = \mathbf{m} + \mathcal{C}.\mathsf{dec}(\mathbf{e}_{\mathrm{HQC}})$$

HQC in a Nutshell

KeyGen

$$\begin{aligned} \boldsymbol{e}_1, \boldsymbol{e}_2 &\leftarrow \mathcal{S}_w^n \\ \boldsymbol{h} &\leftarrow \mathbb{F}_2[x]/(x^n - 1) \\ \boldsymbol{s} &= \boldsymbol{h} \cdot \boldsymbol{e}_1 + \boldsymbol{e}_2 \end{aligned}$$

pk: $(\boldsymbol{h}, \boldsymbol{s})$

sk: $\boldsymbol{e}_1$

Encrypt

$$\begin{aligned} \boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 &\leftarrow \mathcal{S}_{w'}^n \\ \boldsymbol{y}_1 &= \boldsymbol{s} \cdot \boldsymbol{r}_2 + \boldsymbol{r}_3 + \mathcal{C}.\mathsf{enc}(\boldsymbol{m}) \\ \boldsymbol{y}_2 &= \boldsymbol{r}_1 + \boldsymbol{h} \cdot \boldsymbol{r}_2 \end{aligned}$$

ct: $(\boldsymbol{y}_1 + \boldsymbol{e}_{\mathcal{Q}}, \boldsymbol{y}_2)$

Decrypt

$$\hat{\boldsymbol{m}} = \boldsymbol{m} + \mathcal{C}.\mathsf{dec}(\boldsymbol{e}_{\mathrm{HQC}} + \boldsymbol{e}_{\mathcal{Q}})$$

HQC in a Nutshell

KeyGen

$$\begin{aligned} \mathbf{e}_1, \mathbf{e}_2 &\leftarrow \mathcal{S}_w^n \\ \mathbf{h} &\leftarrow \mathbb{F}_2[x]/(x^n - 1) \\ \mathbf{s} &= \mathbf{h} \cdot \mathbf{e}_1 + \mathbf{e}_2 \end{aligned}$$

pk: $(\mathbf{h}, \mathbf{s})$

sk: $\mathbf{e}_1$

Encrypt

$$\begin{aligned} \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3 &\leftarrow \mathcal{S}_{w'}^n \\ \mathbf{y}_1 &= \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{r}_3 + \mathcal{C}.\mathsf{enc}(\mathbf{m}) \\ \mathbf{y}_2 &= \mathbf{r}_1 + \mathbf{h} \cdot \mathbf{r}_2 \end{aligned}$$

ct: $(\lfloor \mathbf{y}_1 \rceil_{\mathcal{Q}}, \mathbf{y}_2)$

Decrypt

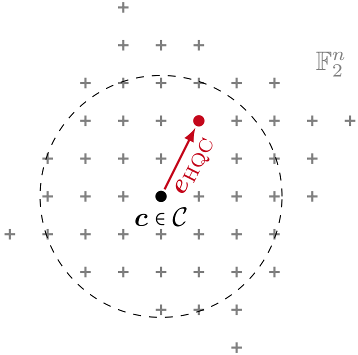
$$\hat{\mathbf{m}} = \mathbf{m} + \mathcal{C}.\mathsf{dec}(\mathbf{e}_{\mathrm{HQC}} + \mathbf{e}_{\mathcal{Q}})$$

Less Bits, More Noise

$$\lfloor \cdot \rceil_{\mathcal{Q}} : \quad \mathbb{F}_2^n \to \mathcal{Q}$$

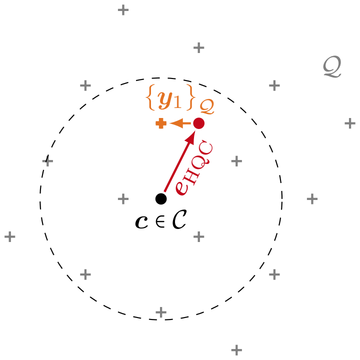
$$\boldsymbol{v} \mapsto \lfloor \boldsymbol{v} \rceil_{\mathcal{Q}} = \boldsymbol{v} + \{\boldsymbol{v}\}_{\mathcal{Q}}$$

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



Less Bits, More Noise

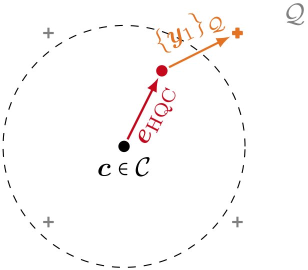
$$\lfloor \cdot \rceil_{\mathcal{Q}} : \quad \mathbb{F}_2^n \to \mathcal{Q}$$
$$\boldsymbol{v} \mapsto \lfloor \boldsymbol{v} \rceil_{\mathcal{Q}} = \boldsymbol{v} + \{\boldsymbol{v}\}_{\mathcal{Q}}$$
$$n\,\text{bit} \to \rho n\,\text{bit}, \quad \rho < 1$$



Less Bits, More Noise

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

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



Less Bits, More Noise

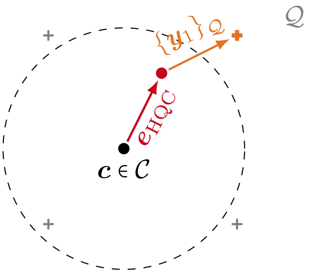
Claude E. Shannon, A Mathematical Theory of Communication

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

Rate-Distortion Bound (RDB)

Compression ρ implies average distortion

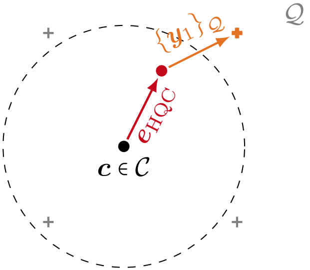
$$\mathbb{E}_{\boldsymbol{v}}\left[\tfrac{1}{n}\mathrm{wt}_{\mathrm{H}}(\{\boldsymbol{v}\}_{\mathcal{Q}})\right] \geq H^{-1}(1-\rho)$$



Less Bits, More Noise

Claude E. Shannon, A Mathematical Theory of Communication

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



Rate-Distortion Bound (RDB)

Compression ρ implies average distortion

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

Trade-off: ct size vs. pk size

Polar Codes are Good Quantizers

Korada, Urbanke, Polar Codes are Optimal for Lossy Source Coding

Polar Codes are Good Quantizers

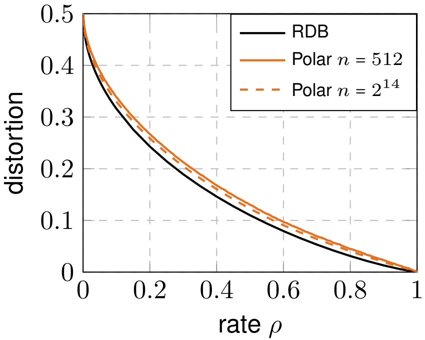
Korada, Urbanke, Polar Codes are Optimal for Lossy Source Coding

➔ Successive Cancellation (SC) decoding:
RDB for $n \to \infty$

Polar Codes are Good Quantizers

Korada, Urbanke, Polar Codes are Optimal for Lossy Source Coding

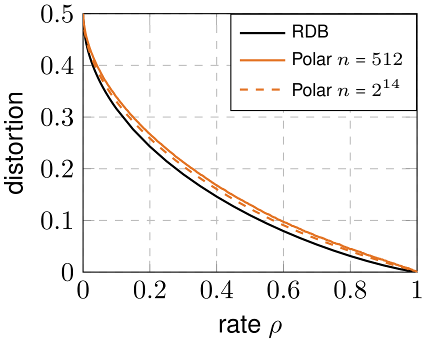
➔ Successive Cancellation (SC) decoding:
RDB for $n \to \infty$



Polar Codes are Good Quantizers

Korada, Urbanke, Polar Codes are Optimal for Lossy Source Coding

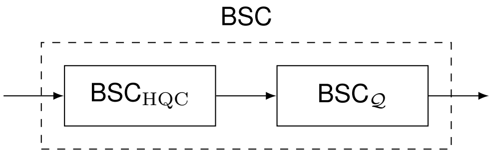
- Successive Cancellation (SC) decoding: RDB for $n \to \infty$
- Distortion statistically close to BSC

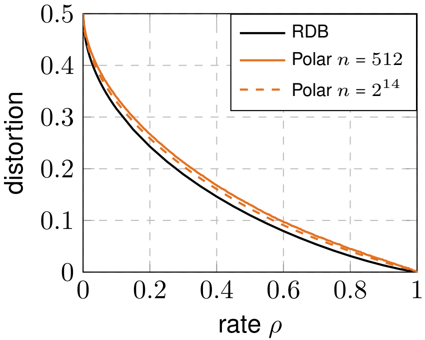


Polar Codes are Good Quantizers

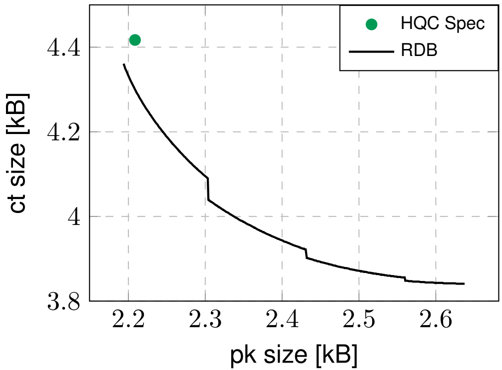
Korada, Urbanke, Polar Codes are Optimal for Lossy Source Coding

- Successive Cancellation (SC) decoding: RDB for $n \to \infty$
- Distortion statistically close to BSC

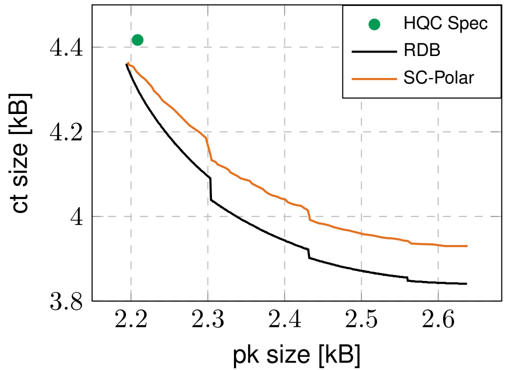




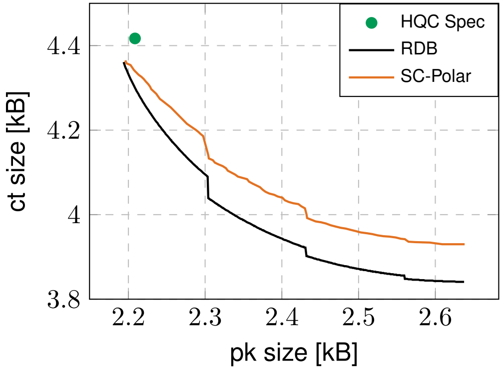
Polarizing Results



Polarizing Results



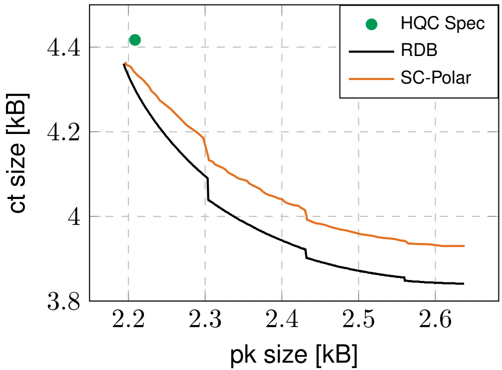
Polarizing Results



Optimize compression:

- Better code, better decoder
- More complex

Polarizing Results



Optimize compression:

- ☺ Better code, better decoder
- (!) More complex

Simplify compression:

- ☺ Low cost, rigorous analysis
- (!) Suboptimal compression

Keep It Short & Simple

Claude E. Shannon, Coding Theorems for a Discrete Source with a Fidelity Criterion

Direct Product $\mathcal{Q} \times \cdots \times \mathcal{Q}$

- ➔ $\mathcal{V}(\mathcal{Q}) = \{\boldsymbol{v} \in \mathbb{F}_2^n : \lfloor \boldsymbol{v} \rceil_{\mathcal{Q}} = \mathbf{0}\}$
- ➔ $\mathcal{V}(\mathcal{Q}^{\times m}) = \mathcal{V}(\mathcal{Q})^{\times m}$

Keep It Short & Simple

Claude E. Shannon, Coding Theorems for a Discrete Source with a Fidelity Criterion

Direct Product $\mathcal{Q} \times \cdots \times \mathcal{Q}$

- $\mathcal{V}(\mathcal{Q}) = \{\boldsymbol{v} \in \mathbb{F}_2^n : \lfloor \boldsymbol{v} \rceil_{\mathcal{Q}} = \boldsymbol{0}\}$
- $\mathcal{V}(\mathcal{Q}^{\times m}) = \mathcal{V}(\mathcal{Q})^{\times m}$

Golay Code

- $n = 23,\ \rho = \frac{12}{23}$
- $\mathcal{V}(\mathcal{Q}) = \{\boldsymbol{v} \in \mathbb{F}_2^n : \mathsf{wt}_{\mathrm{H}}(\boldsymbol{v}) \leq 3\}$

Keep It Short & Simple

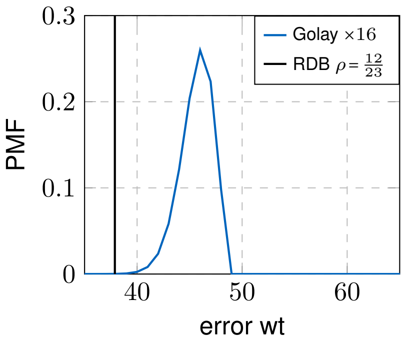
Claude E. Shannon, Coding Theorems for a Discrete Source with a Fidelity Criterion

Direct Product $\mathcal{Q} \times \cdots \times \mathcal{Q}$

- $\mathcal{V}(\mathcal{Q}) = \{\boldsymbol{v} \in \mathbb{F}_2^n : \lfloor \boldsymbol{v} \rceil_{\mathcal{Q}} = \mathbf{0}\}$
- $\mathcal{V}(\mathcal{Q}^{\times m}) = \mathcal{V}(\mathcal{Q})^{\times m}$

Golay Code

- $n = 23,\ \rho = \frac{12}{23}$
- $\mathcal{V}(\mathcal{Q}) = \{\boldsymbol{v} \in \mathbb{F}_2^n : \mathrm{wt}_{\mathrm{H}}(\boldsymbol{v}) \leq 3\}$



Keep It Short & Simple

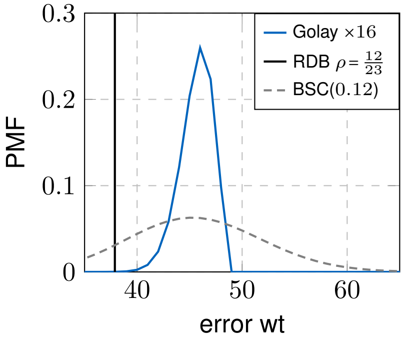
Claude E. Shannon, Coding Theorems for a Discrete Source with a Fidelity Criterion

Direct Product $\mathcal{Q} \times \cdots \times \mathcal{Q}$

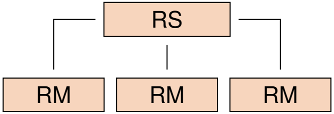
- $\mathcal{V}(\mathcal{Q}) = \{\boldsymbol{v} \in \mathbb{F}_2^n : \lfloor \boldsymbol{v} \rceil_{\mathcal{Q}} = \mathbf{0}\}$
- $\mathcal{V}(\mathcal{Q}^{\times m}) = \mathcal{V}(\mathcal{Q})^{\times m}$

Golay Code

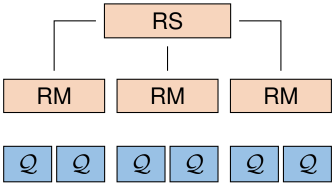
- $n = 23,\ \rho = \frac{12}{23}$
- $\mathcal{V}(\mathcal{Q}) = \{\boldsymbol{v} \in \mathbb{F}_2^n : \mathrm{wt_H}(\boldsymbol{v}) \leq 3\}$



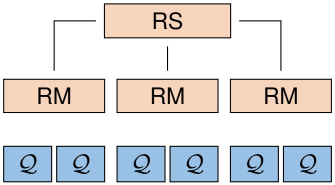
Aligning Compression and Error Correction



Aligning Compression and Error Correction



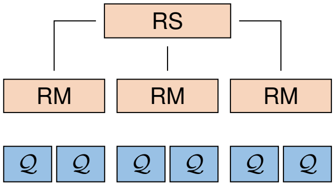
Aligning Compression and Error Correction



Quantization error

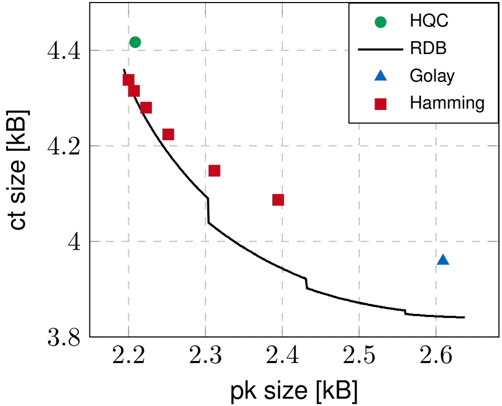
- ☺ Independent for each RM
- ☺ Evenly distributed

Aligning Compression and Error Correction

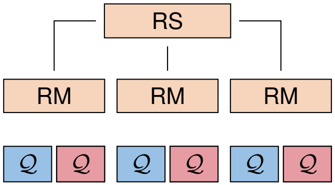


Quantization error

- ☺ Independent for each RM
- ☺ Evenly distributed

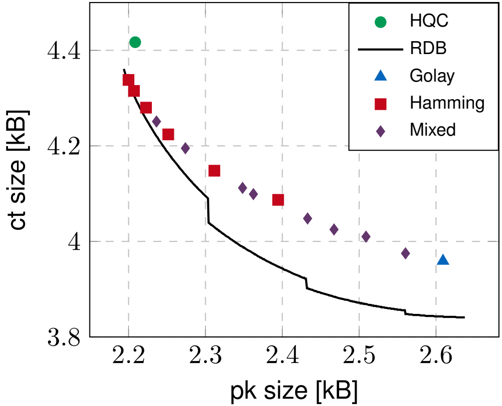


Aligning Compression and Error Correction

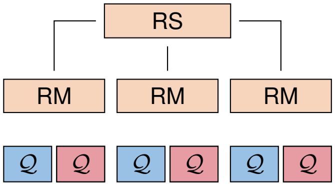


Quantization error

- ☺ Independent for each RM
- ☺ Evenly distributed

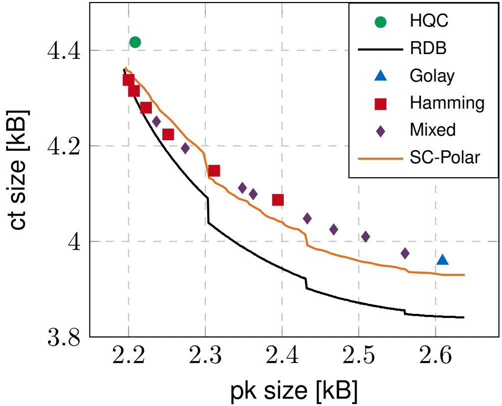


Aligning Compression and Error Correction



Quantization error

- ☺ Independent for each RM
- ☺ Evenly distributed



Conclusion

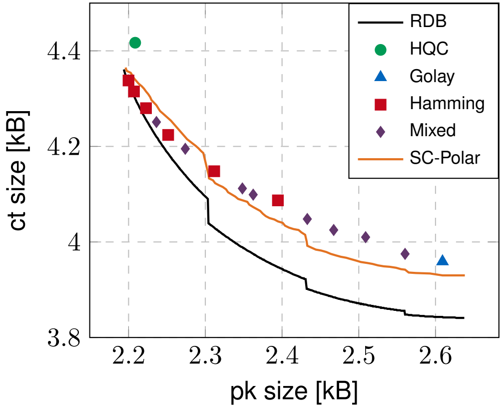
Ciphertext compression for HQC:

- ☺ Compression = decoding
- ☺ Precise control for short codes
- ☺ Ciphertext size $-10\,\%$

Conclusion

Ciphertext compression for HQC:

- ☺ Compression = decoding
- ☺ Precise control for short codes
- ☺ Ciphertext size $-10\,\%$



Conclusion

Ciphertext compression for HQC:

- ☺ Compression = decoding
- ☺ Precise control for short codes
- ☺ Ciphertext size $-10\,\%$

Thank you!

Questions?