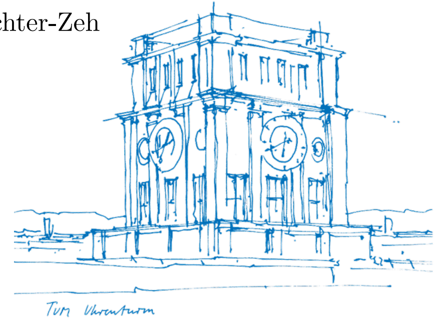
HQC Beyond the BSC – Towards Error Structure-Aware Decoding

Marco Baldi, Sebastian Bitzer, Paolo Santini, Antonia Wachter-Zeh

Technical University of Munich
Università Politecnica delle Marche

ITG AIT



Post-Quantum Cryptography

Post-Quantum Cryptography

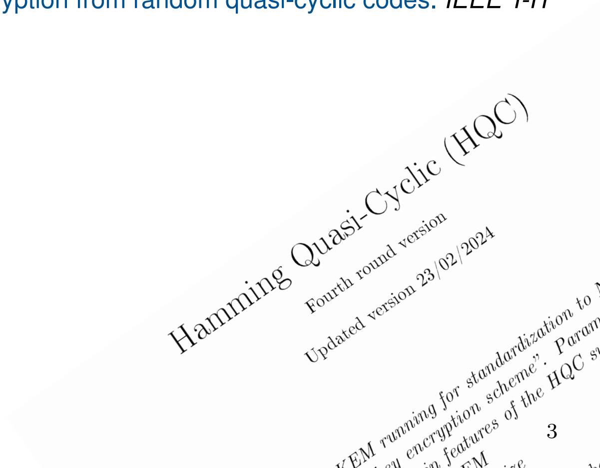
Hamming Quasi-Cyclic (HQC)

Aguilar-Melchor, C., et al. (2017). Hamming quasi-cyclic (HQC). *NIST PQC*

Aguilar-Melchor, C., et al. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*

Hamming Quasi-Cyclic (HQC)

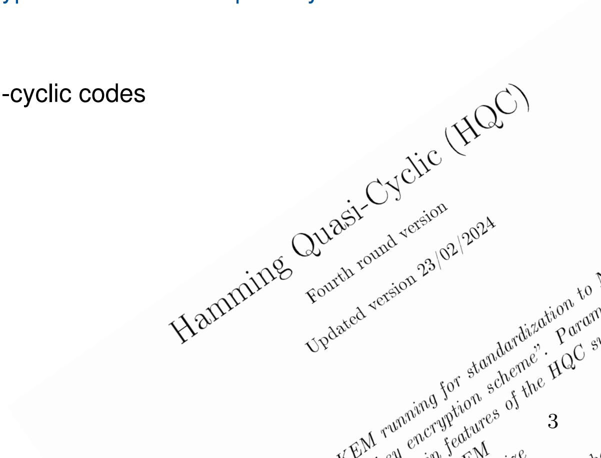
- Aguilar-Melchor, C., et al. (2017). Hamming quasi-cyclic (HQC). *NIST PQC*
- Aguilar-Melchor, C., et al. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*



Hamming Quasi-Cyclic (HQC)

- Aguilar-Melchor, C., et al. (2017). Hamming quasi-cyclic (HQC). *NIST PQC*
- Aguilar-Melchor, C., et al. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*

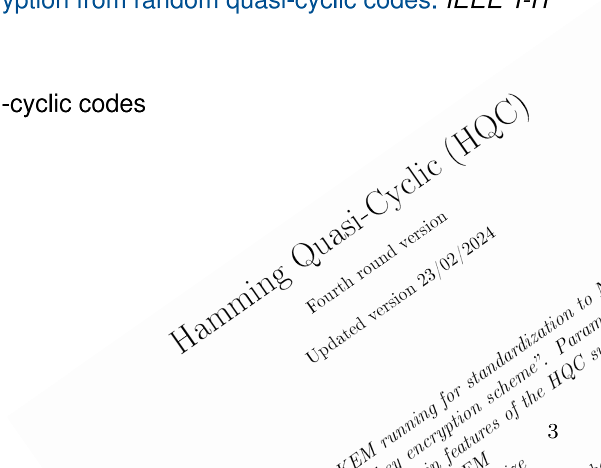
- Based on hardness of decoding random quasi-cyclic codes
- No hidden code structure
- Precise DFR analysis


Hamming Quasi-Cyclic (HQC)
Fourth round version
Updated version 23/02/2024

Hamming Quasi-Cyclic (HQC)

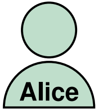
- Aguilar-Melchor, C., et al. (2017). Hamming quasi-cyclic (HQC). *NIST PQC*
- Aguilar-Melchor, C., et al. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*

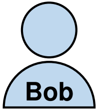
- Based on hardness of decoding random quasi-cyclic codes
- No hidden code structure
- Precise DFR analysis


Hamming Quasi-Cyclic (HQC)
Fourth round version
Updated version 23/02/2024

HQC in a Nutshell

HQC in a Nutshell



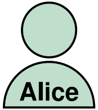


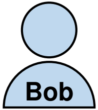
$\boldsymbol{u}_1, \boldsymbol{u}_2 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_u

$\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$

$$\xrightarrow{\quad (\boldsymbol{h}, \boldsymbol{s}) \quad}$$

HQC in a Nutshell





$\boldsymbol{u}_1, \boldsymbol{u}_2 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_u

$\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$

$\xrightarrow{(\boldsymbol{h}, \boldsymbol{s})}$

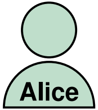
$\boldsymbol{c} \leftarrow \mathcal{C}.\textsf{Enc}(\boldsymbol{m})$

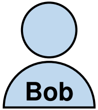
$\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_r

$\xleftarrow{(\boldsymbol{t}_1, \boldsymbol{t}_2)}$

$(\boldsymbol{t}_1, \boldsymbol{t}_2) \leftarrow (\boldsymbol{c} + \boldsymbol{s}\boldsymbol{r}_2 + \boldsymbol{r}_3, \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2)$

HQC in a Nutshell





Alice:

$\boldsymbol{u}_1, \boldsymbol{u}_2 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_u

$\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$

$\xrightarrow{(\boldsymbol{h}, \boldsymbol{s})}$

Bob:

$\boldsymbol{c} \leftarrow \mathcal{C}.\textsf{Enc}(\boldsymbol{m})$

$\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_r

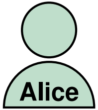
$(\boldsymbol{t}_1, \boldsymbol{t}_2) \leftarrow (\boldsymbol{c} + \boldsymbol{s}\boldsymbol{r}_2 + \boldsymbol{r}_3, \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2)$

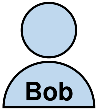
$\xleftarrow{(\boldsymbol{t}_1, \boldsymbol{t}_2)}$

Alice:

$\hat{\boldsymbol{m}} \leftarrow \mathcal{C}.\textsf{Dec}(\boldsymbol{t}_1 - \boldsymbol{t}_2\boldsymbol{u}_2)$

HQC in a Nutshell





Alice:

$\boldsymbol{u}_1, \boldsymbol{u}_2 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_u

$\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$

$\xrightarrow{(\boldsymbol{h}, \boldsymbol{s})}$

Bob:

$\boldsymbol{c} \leftarrow \mathcal{C}.\textsc{Enc}(\boldsymbol{m})$

$\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_r

$(\boldsymbol{t}_1, \boldsymbol{t}_2) \leftarrow (\boldsymbol{c} + \boldsymbol{s}\boldsymbol{r}_2 + \boldsymbol{r}_3, \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2)$

$\xleftarrow{(\boldsymbol{t}_1, \boldsymbol{t}_2)}$

Alice:

$\hat{\boldsymbol{m}} \leftarrow \mathcal{C}.\textsc{Dec}(\boldsymbol{t}_1 - \boldsymbol{t}_2\boldsymbol{u}_2)$

$\mathcal{C}$ needs to decode $\boldsymbol{t}_1 - \boldsymbol{t}_2\boldsymbol{u}_2 = \boldsymbol{c} + \underbrace{\boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3}_{\text{error } \boldsymbol{e}}$

A First Look at the Error

- $P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$
- $\rho = P(e_i = 1)$ simple

A First Look at the Error

- $P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$
- $\rho = P(e_i = 1)$ simple

BSC Approximation

Under the independence assumption,

$$P(|\boldsymbol{e}| = w) \approx \binom{n}{w}\rho^w(1-\rho)^{n-w}.$$

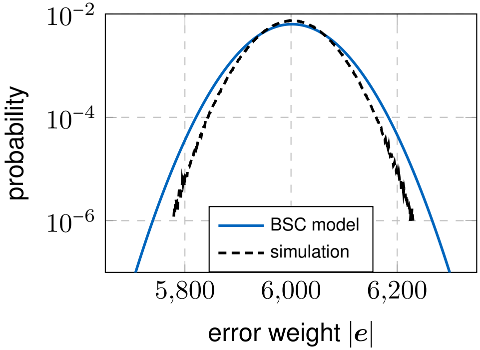
A First Look at the Error

- $P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$
- $\rho = P(e_i = 1)$ simple

BSC Approximation

Under the independence assumption,

$$P(|\boldsymbol{e}| = w) \approx \binom{n}{w}\rho^w(1-\rho)^{n-w}.$$



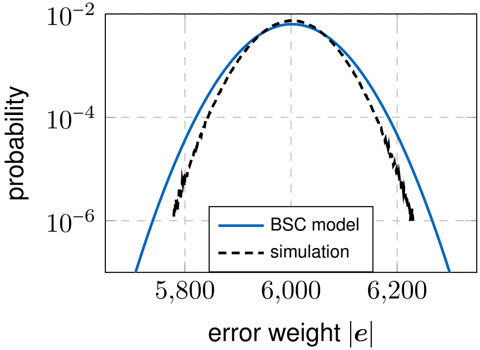
A First Look at the Error

- $P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$
- $\rho = P(e_i = 1)$ simple

BSC Approximation

Under the independence assumption,

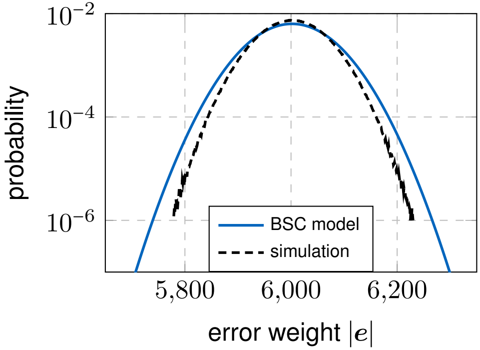
$$P(|\boldsymbol{e}| = w) \approx \binom{n}{w}\rho^w(1-\rho)^{n-w}.$$



Seems conservative but not precise!

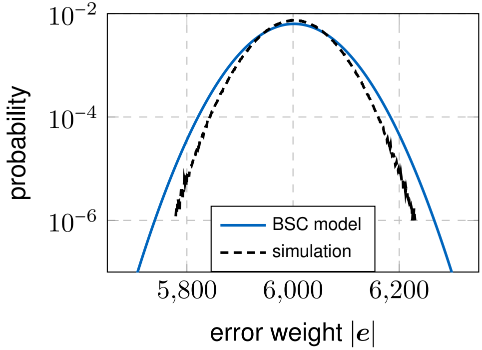
A Closer Look at the Error

- Consider $\boldsymbol{a} = \boldsymbol{u} \cdot \boldsymbol{r} = \sum_{\ell \in \mathrm{supp}(\boldsymbol{u})} x^{\ell} \cdot \boldsymbol{r}(x)$



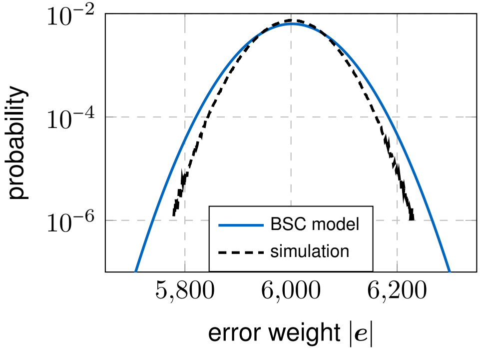
A Closer Look at the Error

- Consider $\boldsymbol{a} = \boldsymbol{u} \cdot \boldsymbol{r} = \sum_{\ell \in \mathrm{supp}(\boldsymbol{u})} x^{\ell} \cdot \boldsymbol{r}(x)$
- b_i = # ones added in i-th position



A Closer Look at the Error

- Consider $\boldsymbol{a} = \boldsymbol{u} \cdot \boldsymbol{r} = \sum_{\ell \in \mathrm{supp}(\boldsymbol{u})} x^{\ell} \cdot \boldsymbol{r}(x)$
- b_i = # ones added in i-th position
- $a_i = b_i \mod 2$
- $\sum_i b_i = |\boldsymbol{u}| \cdot |\boldsymbol{r}|$



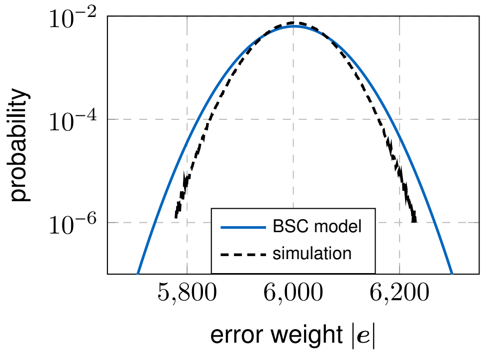
A Closer Look at the Error

- Consider $\boldsymbol{a} = \boldsymbol{u} \cdot \boldsymbol{r} = \sum_{\ell \in \mathrm{supp}(\boldsymbol{u})} x^{\ell} \cdot \boldsymbol{r}(x)$
- b_i = # ones added in i-th position
- $a_i = b_i \mod 2$
- $\sum_i b_i = |\boldsymbol{u}| \cdot |\boldsymbol{r}|$

Proposed Approximation

Assume $b_0, \ldots, b_{n-1}$ indep. hypergeometric, let $a_i = b_i \mod 2$:

$$P(|\boldsymbol{u} \cdot \boldsymbol{r}| = w) \approx P\left(\sum_i a_i \mid \sum_i b_i = |\boldsymbol{u}| \cdot |\boldsymbol{r}|\right).$$



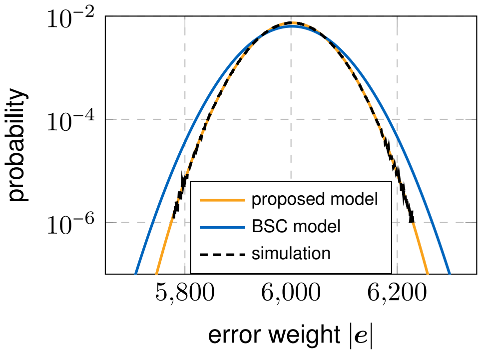
A Closer Look at the Error

- Consider $\boldsymbol{a} = \boldsymbol{u} \cdot \boldsymbol{r} = \sum_{\ell \in \mathrm{supp}(\boldsymbol{u})} x^{\ell} \cdot \boldsymbol{r}(x)$
- b_i = # ones added in i-th position
- $a_i = b_i \mod 2$
- $\sum_i b_i = |\boldsymbol{u}| \cdot |\boldsymbol{r}|$

Proposed Approximation

Assume $b_0, \ldots, b_{n-1}$ indep. hypergeometric, let $a_i = b_i \mod 2$:

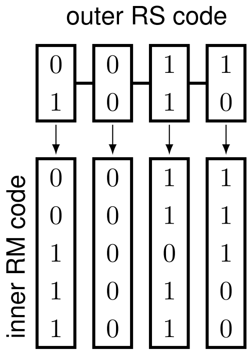
$$P(|\boldsymbol{u} \cdot \boldsymbol{r}| = w) \approx P\left(\sum_i a_i \mid \sum_i b_i = |\boldsymbol{u}| \cdot |\boldsymbol{r}|\right).$$



Tensor Product Code in HQC

Encoder

1. Encode outer RS code
2. Encode inner RM code



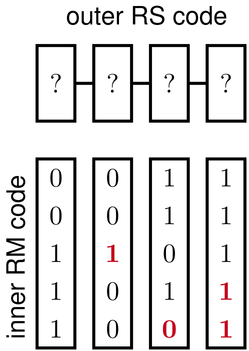
Decoder

1. Decode inner RM code
2. Decode outer RS code

Tensor Product Code in HQC

Encoder

1. Encode outer RS code
2. Encode inner RM code



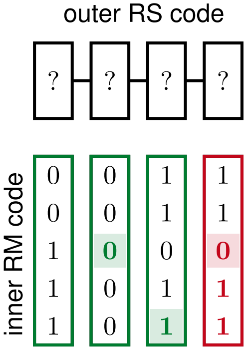
Decoder

1. Decode inner RM code
2. Decode outer RS code

Tensor Product Code in HQC

Encoder

1. Encode outer RS code
2. Encode inner RM code



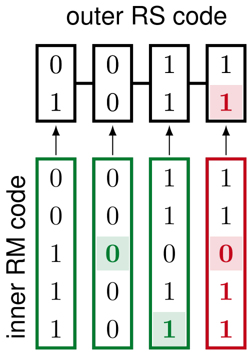
Decoder

1. Decode inner RM code
2. Decode outer RS code

Tensor Product Code in HQC

Encoder

1. Encode outer RS code
2. Encode inner RM code



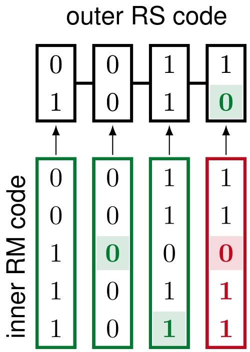
Decoder

1. Decode inner RM code
2. Decode outer RS code

Tensor Product Code in HQC

Encoder

1. Encode outer RS code
2. Encode inner RM code



Decoder

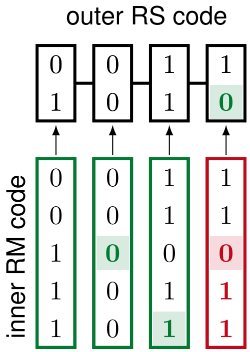
1. Decode inner RM code
2. Decode outer RS code

Simple DFR analysis under independence assumption ✓

Tensor Product Code in HQC

Encoder

1. Encode outer RS code
2. Encode inner RM code



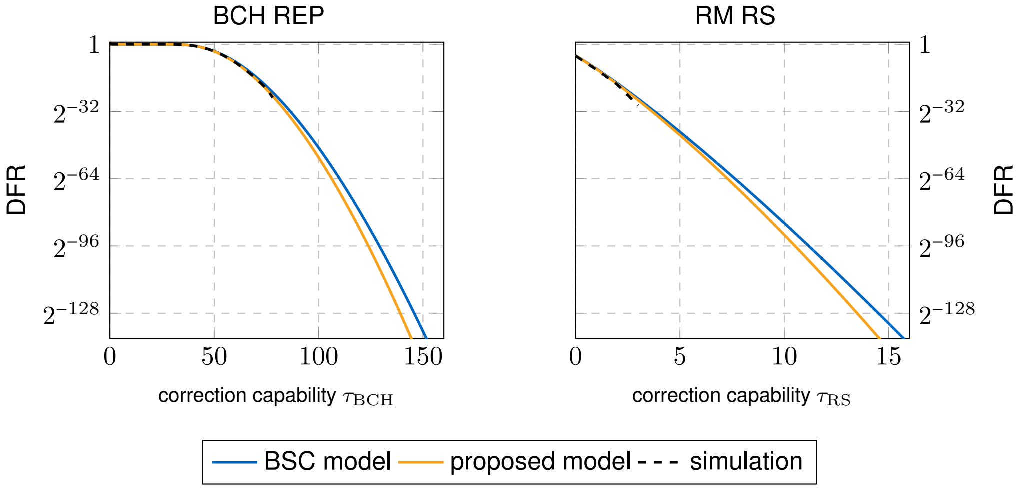
Decoder

1. Decode inner RM code
2. Decode outer RS code

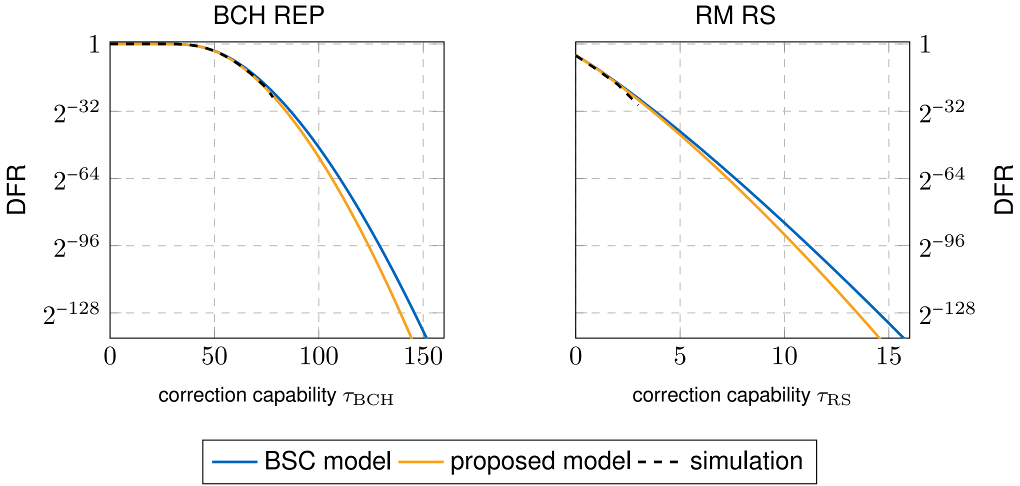
Simple DFR analysis under independence assumption ✓

Modified analysis for arbitrary error weight distribution ✓

DFR Comparison



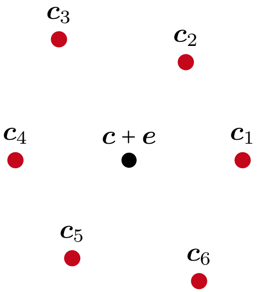
DFR Comparison



So much effort for such a small improvement?

Beyond the BSC

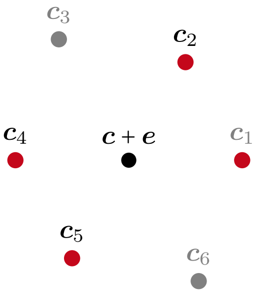
plausible for BSC



Beyond the BSC

plausible for BSC

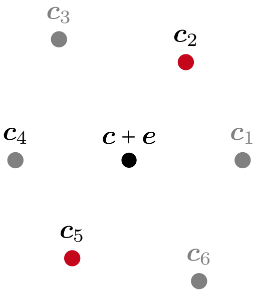
for proposed model



Beyond the BSC

plausible for BSC

for proposed model

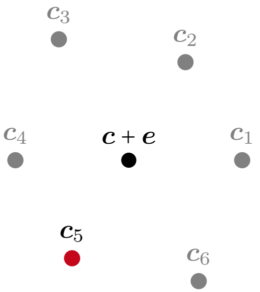


$$e = u_1 r_2 + u_2 r_1 + r_3$$

Beyond the BSC

plausible for BSC

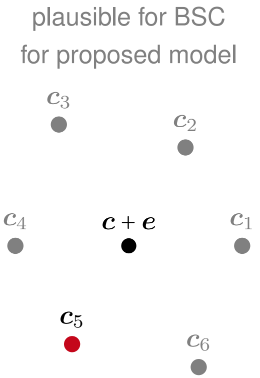
for proposed model



$$\boldsymbol{e} = \boldsymbol{u}_1 \boldsymbol{r}_2 + \boldsymbol{u}_2 \boldsymbol{r}_1 + \boldsymbol{r}_3$$

with known $\boldsymbol{u}_1, \boldsymbol{u}_2$

Beyond the BSC



$\boldsymbol{e} = \boldsymbol{u}_1 \boldsymbol{r}_2 + \boldsymbol{u}_2 \boldsymbol{r}_1 + \boldsymbol{r}_3$

with known $\boldsymbol{u}_1, \boldsymbol{u}_2$

GV-like Bound

There exist codes of length

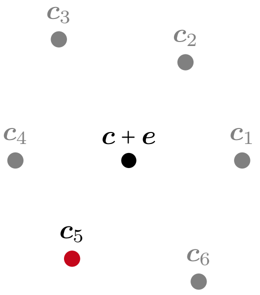
$$n \leq \lambda + 2w_u \log_2\left(\frac{n \cdot e}{w_u}\right) + 6w_r \log_2\left(\frac{n \cdot e}{2w_r}\right) + \log_2(w_r)$$

that can guarantee correct decryption.

Beyond the BSC

plausible for BSC

for proposed model



$$\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$$

with known $\boldsymbol{u}_1, \boldsymbol{u}_2$

GV-like Bound

There exist codes of length

$$n \le \lambda + 2w_u \log_2\left(\frac{n \cdot e}{w_u}\right) + 6w_r \log_2\left(\frac{n \cdot e}{2w_r}\right) + \log_2(w_r)$$

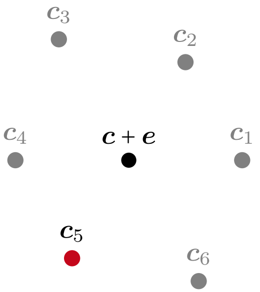
that can guarantee correct decryption.

	length	error model	decoder
HQC	17669	BSC	multistage

Beyond the BSC

plausible for BSC

for proposed model



$$\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$$

with known $\boldsymbol{u}_1, \boldsymbol{u}_2$

GV-like Bound

There exist codes of length

$$n \leq \lambda + 2w_u \log_2\left(\frac{n \cdot e}{w_u}\right) + 6w_r \log_2\left(\frac{n \cdot e}{2w_r}\right) + \log_2(w_r)$$

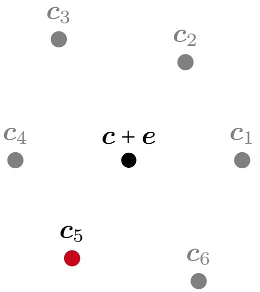
that can guarantee correct decryption.

	length	error model	decoder
HQC	17669	BSC	multistage
SPB	≥ 13438	BSC	ML

Beyond the BSC

plausible for BSC

for proposed model



$$\boldsymbol{e} = \boldsymbol{u}_1 \boldsymbol{r}_2 + \boldsymbol{u}_2 \boldsymbol{r}_1 + \boldsymbol{r}_3$$

with known $\boldsymbol{u}_1, \boldsymbol{u}_2$

GV-like Bound

There exist codes of length

$$n \leq \lambda + 2w_u \log_2\left(\frac{n \cdot e}{w_u}\right) + 6w_r \log_2\left(\frac{n \cdot e}{2w_r}\right) + \log_2(w_r)$$

that can guarantee correct decryption.

	length	error model	decoder
HQC	17669	BSC	multistage
SPB	≥ 13438	BSC	ML
GVB	≤ 3800	structured	???

Conclusion

The structure of the HQC error enables

- ☺ tighter DFR estimates
- ☺ short codes with structure-aware decoder

Conclusion

The structure of the HQC error enables

- ☺ tighter DFR estimates
- ☺ short codes with structure-aware decoder

Can one

- ? obtain a provable DFR analysis?
- ? construct codes with efficient, structure-aware decoder?

Conclusion

The structure of the HQC error enables

- ☺ tighter DFR estimates
- ☺ short codes with structure-aware decoder

Can one

- ? obtain a provable DFR analysis?
- ? construct codes with efficient, structure-aware decoder?

Thank you!

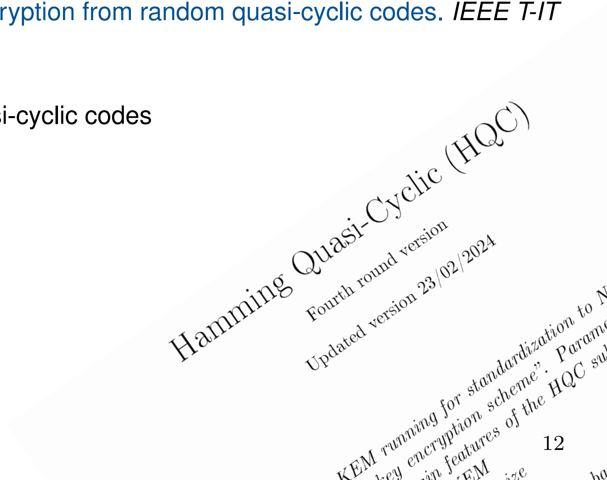
Questions?

Post-Quantum Cryptography

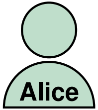
Hamming Quasi-Cyclic (HQC)

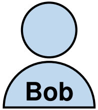
- Aguilar-Melchor, C., et al. (2017). Hamming quasi-cyclic (HQC). *NIST PQC*
- Aguilar-Melchor, C., et al. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*

- Based on hardness of decoding random quasi-cyclic codes
- No hidden code structure
- Precise DFR analysis


Hamming Quasi-Cyclic (HQC)
Fourth round version
Updated version 23/02/2024

HQC in a Nutshell





Alice:

$\boldsymbol{h} \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$

$\boldsymbol{u}_1, \boldsymbol{u}_2 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_u

$\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$

$\xrightarrow{(\boldsymbol{h}, \boldsymbol{s})}$

Bob:

$\boldsymbol{c} \leftarrow \mathcal{C}.\textsc{Enc}(\boldsymbol{m})$

$\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \xleftarrow{\$} \mathbb{F}_2[x]/(x^n - 1)$ of wt w_r

$(\boldsymbol{t}_1, \boldsymbol{t}_2) \leftarrow (\boldsymbol{c} + \boldsymbol{s}\boldsymbol{r}_2 + \boldsymbol{r}_3, \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2)$

$\xleftarrow{(\boldsymbol{t}_1, \boldsymbol{t}_2)}$

Alice:

$\hat{\boldsymbol{m}} \leftarrow \mathcal{C}.\textsc{Dec}(\boldsymbol{t}_1 - \boldsymbol{t}_2\boldsymbol{u}_2)$

$\mathcal{C}$ needs to decode $\boldsymbol{t}_1 - \boldsymbol{t}_2\boldsymbol{u}_2 = \boldsymbol{c} + \underbrace{\boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3}_{\text{error } \boldsymbol{e}}$

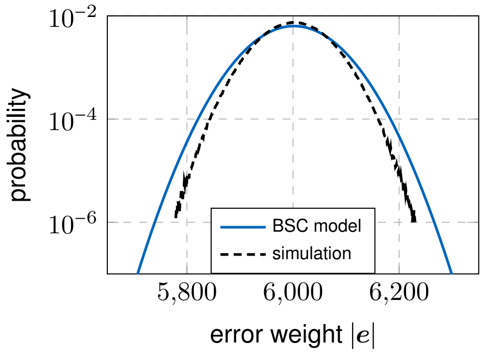
A First Look at the Error

- $P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$
- $\rho = P(e_i = 1)$ simple

BSC Approximation

Under the independence assumption,

$$P(|\boldsymbol{e}| = w) \approx \binom{n}{w}\rho^w(1-\rho)^{n-w}.$$



Seems conservative but not precise!

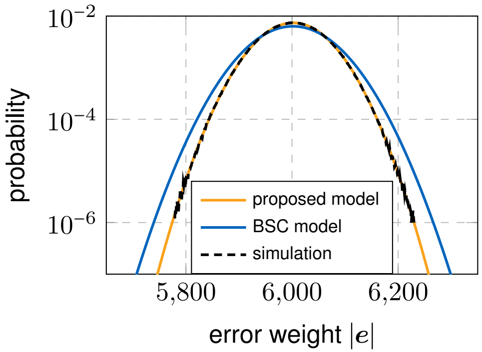
A Closer Look at the Error

- Consider $\boldsymbol{a} = \boldsymbol{u} \cdot \boldsymbol{r} = \sum_{\ell \in \mathrm{supp}(\boldsymbol{u})} x^{\ell} \cdot \boldsymbol{r}(x)$
- b_i = # ones added in i-th position
- $a_i = b_i \mod 2$
- $\sum_i b_i = |\boldsymbol{u}| \cdot |\boldsymbol{r}|$

Proposed Approximation

Assume $b_0, \dots, b_{n-1}$ indep. hypergeometric, let $a_i = b_i \mod 2$:

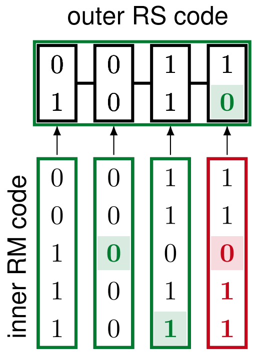
$$P(|\boldsymbol{u} \cdot \boldsymbol{r}| = w) \approx P\left(\sum_i a_i \mid \sum_i b_i = |\boldsymbol{u}| \cdot |\boldsymbol{r}|\right).$$



Tensor Product Code in HQC

Encoder

1. Encode outer RS code
2. Encode inner RM code



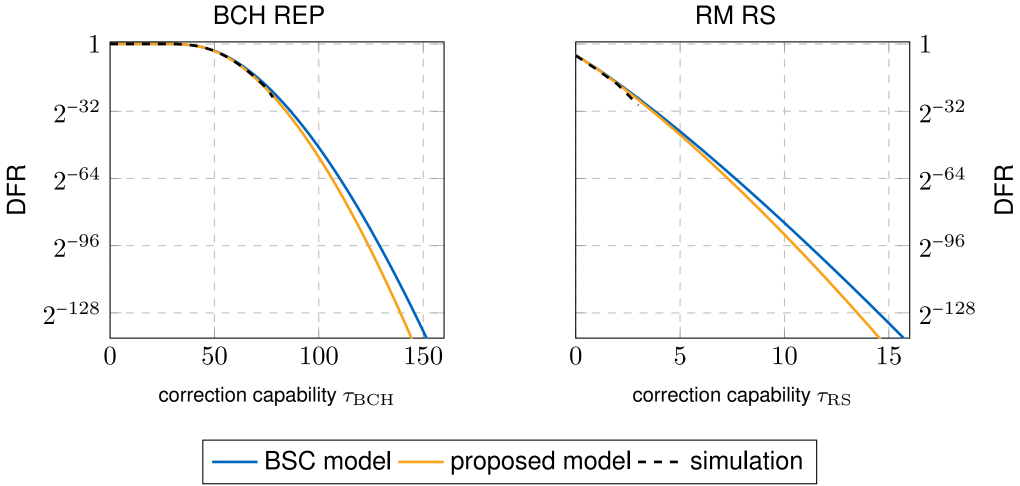
Decoder

1. Decode inner RM code
2. Decode outer RS code

Simple DFR analysis under independence assumption ✓

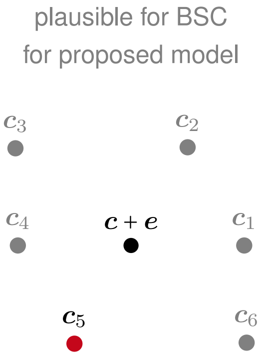
Modified analysis for arbitrary error weight distribution ✓

DFR Comparison



So much fuss for such a small improvement?

Beyond the BSC



$$e = u_1 r_2 + u_2 r_1 + r_3$$

with known u_1, u_2

GV-like Bound

There exist codes of length

$$n \leq \lambda + 2w_u \log_2\left(\frac{n \cdot e}{w_u}\right) + 6w_r \log_2\left(\frac{n \cdot e}{2w_r}\right) + \log_2(w_r)$$

that can guarantee correct decryption.

	length	error model	decoder
HQC	17669	BSC	multistage
SPB	≥ 13438	BSC	ML
GVB	≤ 3800	structured	???

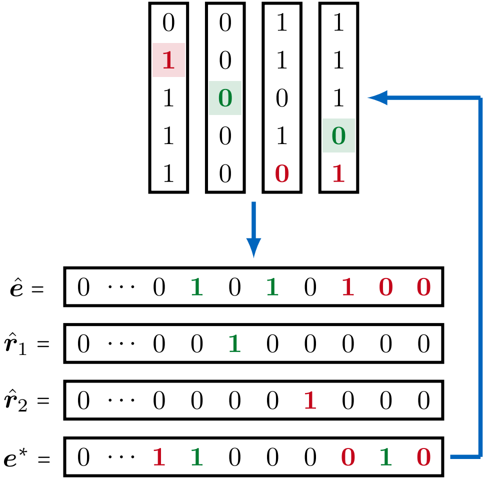
Error Structure-Aware Decoding

Remember: $\boldsymbol{e} = \boldsymbol{u}_1 \cdot \boldsymbol{r}_2 + \boldsymbol{u}_2 \cdot \boldsymbol{r}_1 + \boldsymbol{r}_3$

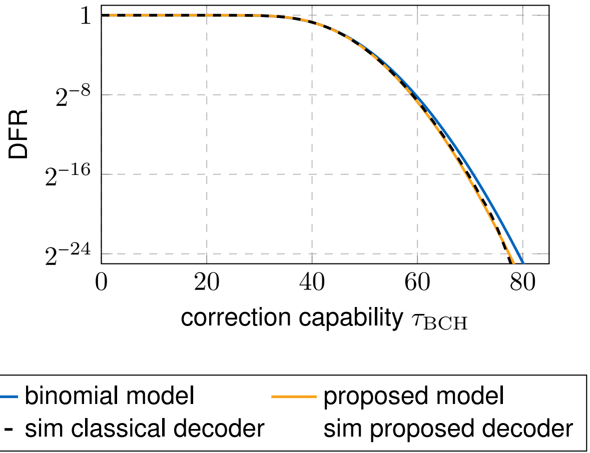
Proposed Decoder

1. Decode inner codewords, get $\hat{e}$.
2. Estimate $\hat{\boldsymbol{r}}_1, \hat{\boldsymbol{r}}_2$ using $\hat{e}, \boldsymbol{u}_1, \boldsymbol{u}_2$.
3. Estimate error $\boldsymbol{e}^* = \boldsymbol{u}_1 \cdot \hat{\boldsymbol{r}}_2 + \boldsymbol{u}_2 \cdot \hat{\boldsymbol{r}}_1$.
4. Decode $\boldsymbol{t}_1 + \boldsymbol{t}_2 \boldsymbol{u}_2 - \boldsymbol{e}^* = \boldsymbol{c} + \boldsymbol{e} - \boldsymbol{e}^*$.

$\Rightarrow$ error weight reduced if $\hat{\boldsymbol{r}}_1 \approx \boldsymbol{r}_1$ and $\hat{\boldsymbol{r}}_2 \approx \boldsymbol{r}_2$

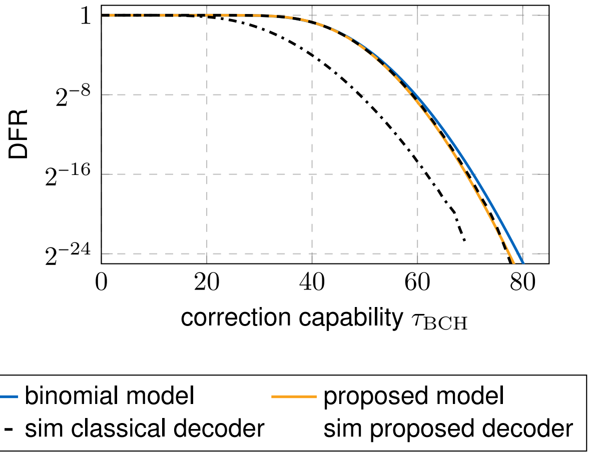


Decoding Performance Results



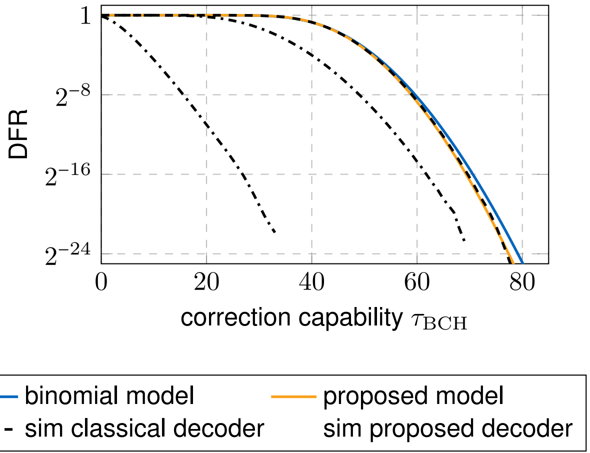
Considerable improvements conceivable ✓

Decoding Performance Results



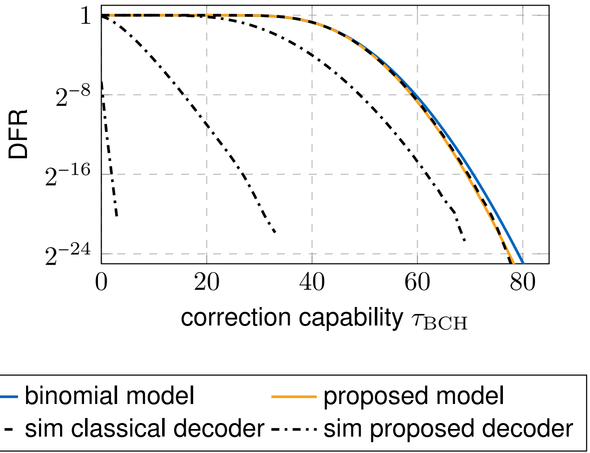
Considerable improvements conceivable ✓

Decoding Performance Results



Considerable improvements conceivable ✓

Decoding Performance Results



Considerable improvements conceivable ✓

Conclusion

The structure of the HQC error enables
- ☺ tighter DFR estimates
- ☺ short codes with structure-aware decoder
- ☺ improved decoding performance in practice

Can one
- ? obtain a provable DFR analysis?
- ? construct codes with efficient, structure-aware decoder?
- ? provide DFR analysis for the proposed decoder?

Thank you!

Questions?