McEliece needs a Break – Solving McEliece-1284 and Quasi-Cyclic-2918 with Modern ISD

Andre Esser[1] Alexander May[2] Floyd Zweydinger[2]

03 June 2022

[1]Technology Innovation Institute, UAE

[2]Ruhr University Bochum, Germany

Motivation

- NIST Round 3 KEM selection
- McEliece, BIKE, HQC
- Exact security estimations needed

Motivation

- NIST Round 3 KEM selection
- McEliece, BIKE, HQC
- Exact security estimations needed

  Do we need to take modern ISD into account?

Motivation

- NIST Round 3 KEM selection
- McEliece, BIKE, HQC
- Exact security estimations needed

  Do we need to take modern ISD into account?

  What is the correct memory cost model for ISD?

Motivation

- NIST Round 3 KEM selection
- McEliece, BIKE, HQC
- Exact security estimations needed

  Do we need to take modern ISD into account?

  What is the correct memory cost model for ISD?

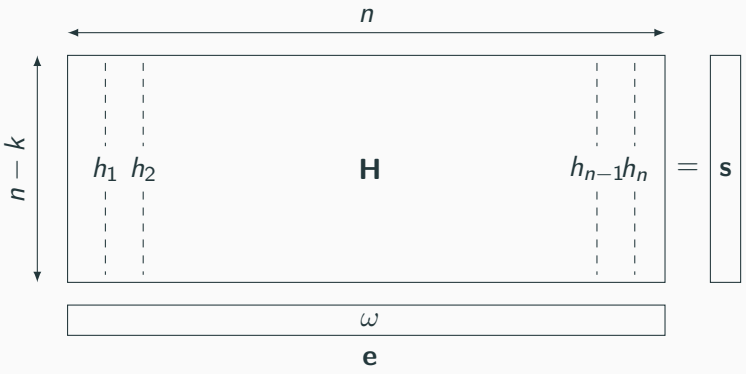
constant	log	cube-root
T	$T \cdot \log M$	$T \cdot \sqrt[3]{M}$

Results

- first public available implementation of the MMT/BJMM algorithm
- precise bit security extrapolations for code based crypto schemes

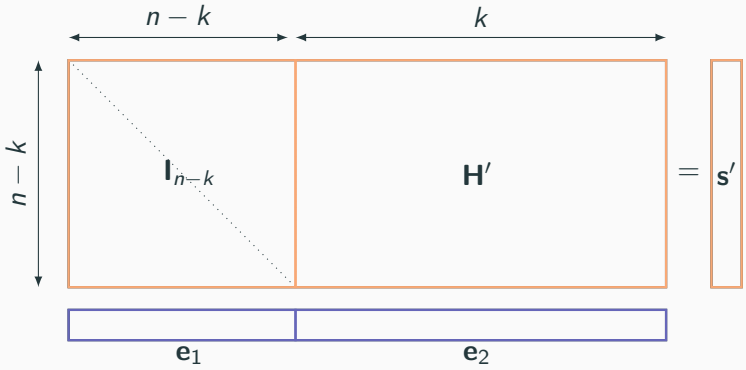
Information Set Decoding (ISD)

Syndrome Decoding Problem



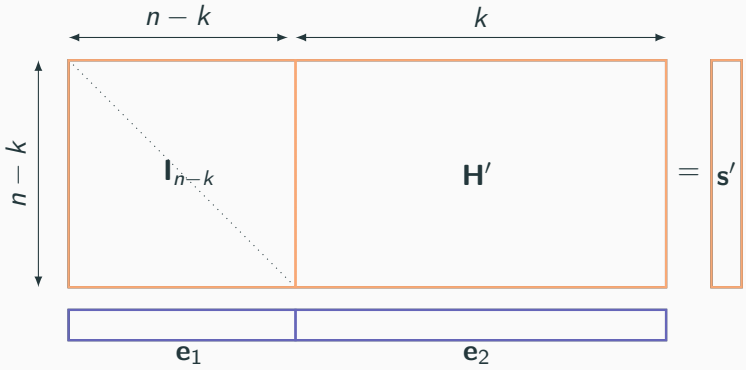
- **Given:** $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_2^{n-k}$ and $\omega \in \mathbb{N}$
- **Find:** $\mathbf{e} \in \mathbb{F}_2^n$ s.t. $\mathbf{He} = \mathbf{s}$, with $\mathrm{wt}(\mathbf{e}) = \omega$.

Information Set Decoding



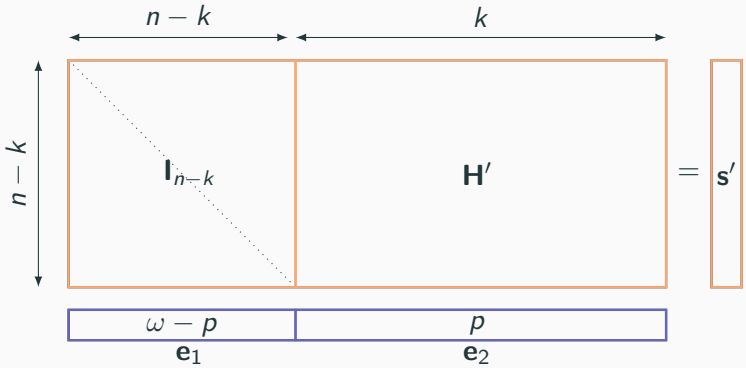
$$\mathbf{GHe} = (\mathbf{I}_{n-k}\mathbf{H}')(\mathbf{e}_1||\mathbf{e}_2)$$

Information Set Decoding



$$\mathbf{GHe} = (\mathbf{I}_{n-k}\mathbf{H}')(\mathbf{e}_1||\mathbf{e}_2) = \mathbf{e}_1 + \mathbf{H}'\mathbf{e}_2 = \mathbf{s}' = \mathbf{Gs}$$

Information Set Decoding

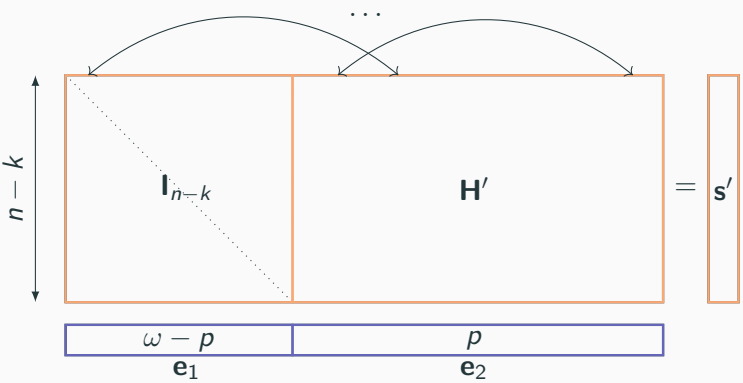


$$\mathbf{GHe} = (\mathbf{I}_{n-k}\mathbf{H}')(\mathbf{e}_1||\mathbf{e}_2) = \mathbf{e}_1 + \mathbf{H}'\mathbf{e}_2 = \mathbf{s}' = \mathbf{Gs}$$

$$\mathbf{H}'\mathbf{e}_2 + \mathbf{s}' = \mathbf{e}_1 \Leftrightarrow$$

$$\mathrm{wt}(\mathbf{H}'\mathbf{e}_2 + \mathbf{s}') = \omega - p$$

Information Set Decoding



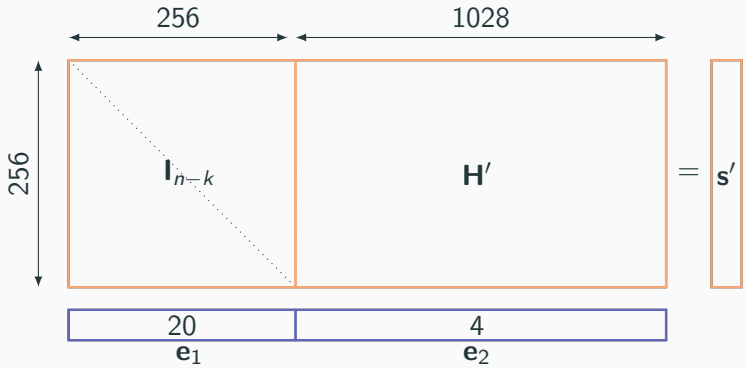
1) Permute
2) Gauß
3) Solve

$$\mathbf{GHe} = (\mathbf{I}_{n-k}\mathbf{H}')(\mathbf{e}_1||\mathbf{e}_2) = \mathbf{e}_1 + \mathbf{H}'\mathbf{e}_2 = \mathbf{s}' = \mathbf{Gs}$$

$$\mathbf{H}'\mathbf{e}_2 + \mathbf{s}' = \mathbf{e}_1 \Leftrightarrow$$

$$\mathrm{wt}(\mathbf{H}'\mathbf{e}_2 + \mathbf{s}') = \omega - p$$

Information Set Decoding



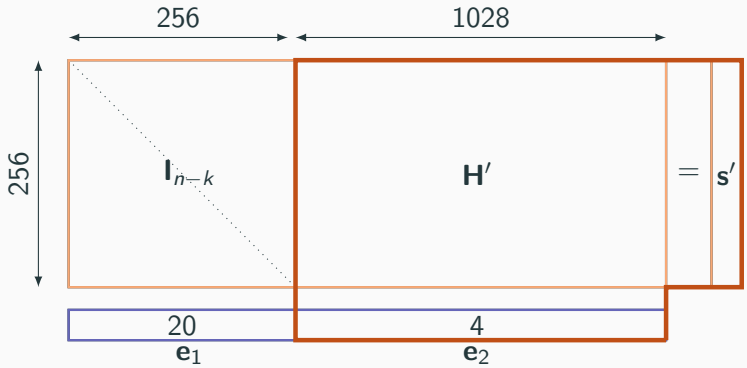
1) Permute
2) Gauß
3) Solve

$$\mathbf{GHe} = (\mathbf{I}_{n-k}\mathbf{H}')(\mathbf{e}_1||\mathbf{e}_2) = \mathbf{e}_1 + \mathbf{H}'\mathbf{e}_2 = \mathbf{s}' = \mathbf{Gs}$$

$$\mathbf{H}'\mathbf{e}_2 + \mathbf{s}' = \mathbf{e}_1 \Leftrightarrow$$

$$\mathrm{wt}(\mathbf{H}'\mathbf{e}_2 + \mathbf{s}') = \omega - p$$

Information Set Decoding

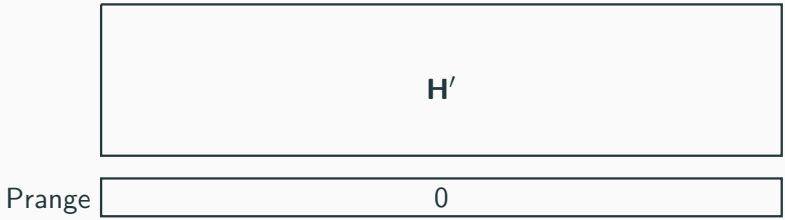


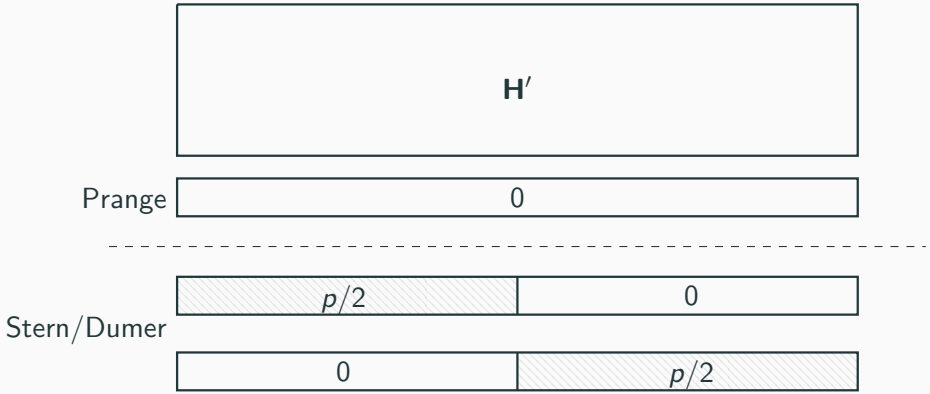
1) Permute
2) Gauß
3) Solve

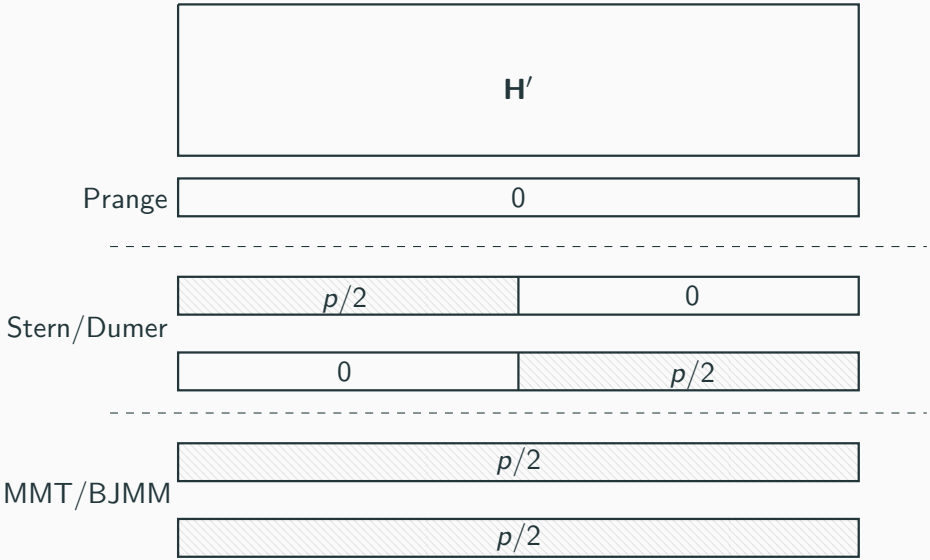
$$\mathbf{GHe} = (\mathbf{I}_{n-k}\mathbf{H}')(\mathbf{e}_1||\mathbf{e}_2) = \mathbf{e}_1 + \mathbf{H}'\mathbf{e}_2 = \mathbf{s}' = \mathbf{Gs}$$

$$\mathbf{H}'\mathbf{e}_2 + \mathbf{s}' = \mathbf{e}_1 \Leftrightarrow$$

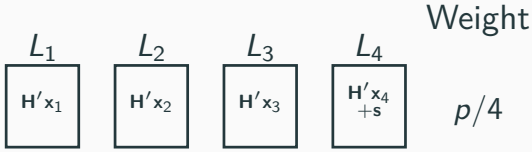
$$\mathrm{wt}(\mathbf{H}'\mathbf{e}_2 + \mathbf{s}') = \omega - p$$


$\mathbf{H}'$
Prange
0

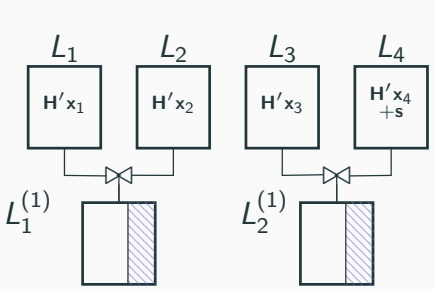

H′
Prange
0
p/2
0
Stern/Dumer
0
p/2


H′
Prange
0
Stern/Dumer
p/2
0
0
p/2
MMT/BJMM
p/2
p/2

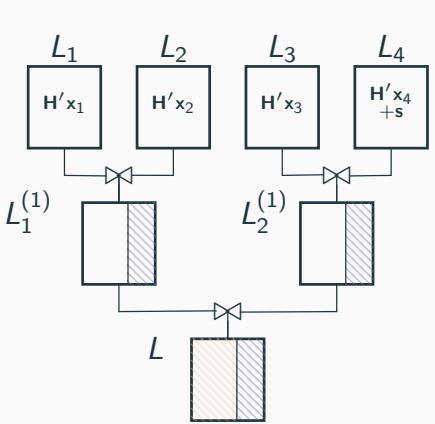
MMT/BJMM


Weight
L_1
L_2
L_3
L_4
$\mathbf{H}'\mathbf{x}_1$
$\mathbf{H}'\mathbf{x}_2$
$\mathbf{H}'\mathbf{x}_3$
$\mathbf{H}'\mathbf{x}_4 + \mathbf{s}$
$p/4$

MMT/BJMM


Weight
L_1
L_2
L_3
L_4
$\mathbf{H}'\mathbf{x}_1$
$\mathbf{H}'\mathbf{x}_2$
$\mathbf{H}'\mathbf{x}_3$
$\mathbf{H}'\mathbf{x}_4 + \mathbf{s}$
$p/4$
$L_1^{(1)}$
$L_2^{(1)}$
$p/2$

MMT/BJMM


Weight
L_1
L_2
L_3
L_4
$\mathbf{H}'\mathbf{x}_1$
$\mathbf{H}'\mathbf{x}_2$
$\mathbf{H}'\mathbf{x}_3$
$\mathbf{H}'\mathbf{x}_4 + \mathbf{s}$
$p/4$
$L_1^{(1)}$
$L_2^{(1)}$
$p/2$
L
p

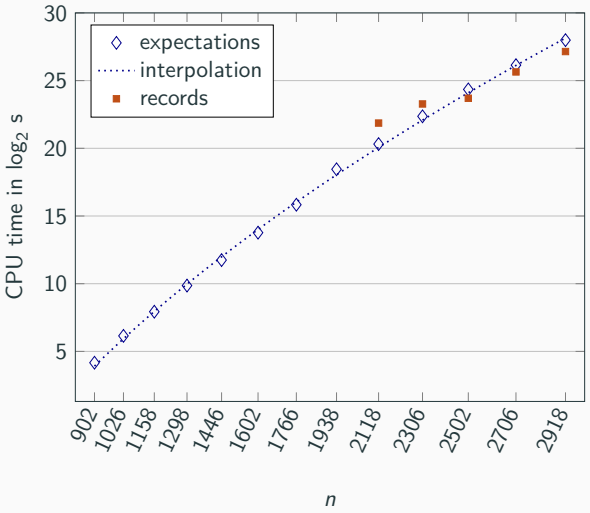
Results

Results

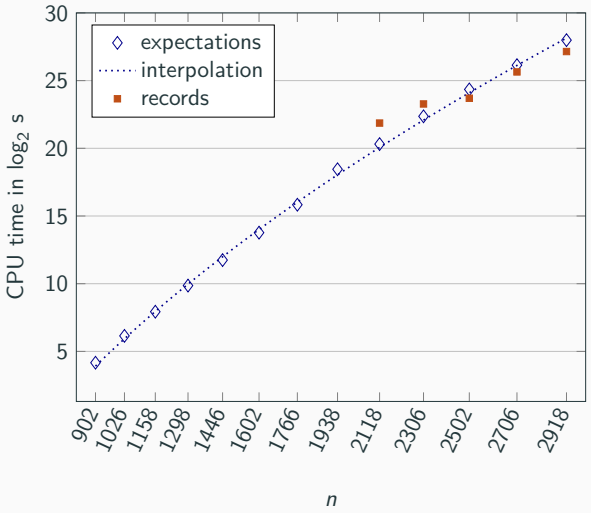
System	n	k	ω	time (days)	CPU years
McEliece	1223	979	23	2.45	1.71
	1284	1028	24	31.43	22.04
QC	2118	1059	46	0.08	0.05
	2306	1153	48	0.22	0.15
	2502	1459	50	0.30	0.21
	2706	1353	52	1.18	0.83
	2918	1459	54	3.33	2.33

https://decodingchallenge.org/

Results (Quasi-Cyclic)

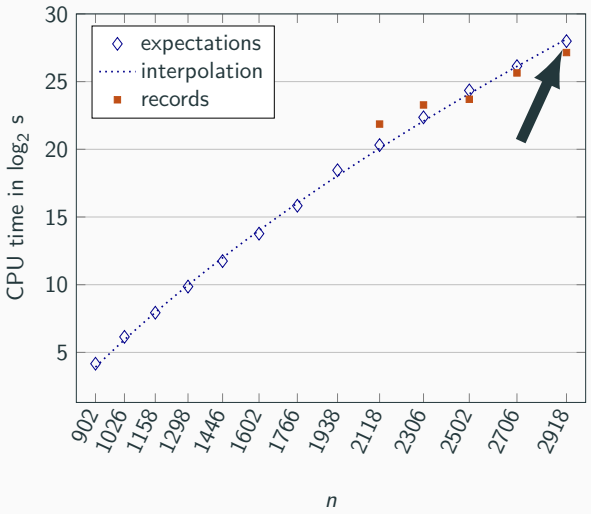


Results (Quasi-Cyclic)



$$\frac{\text{Exp. Perms.} \leftarrow \text{SD-Estimator}}{\text{Perms/second} \leftarrow \text{Implementation}}$$

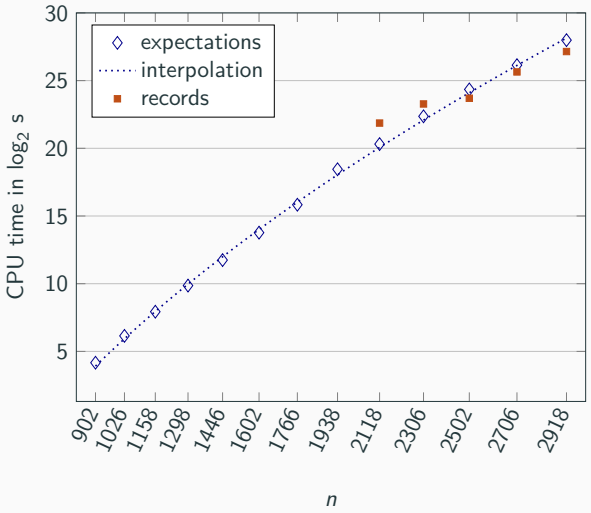
Results (Quasi-Cyclic)



$$\frac{\text{Exp. Perms.} \leftarrow \text{SD-Estimator}}{\text{Perms/second} \leftarrow \text{Implementation}}$$

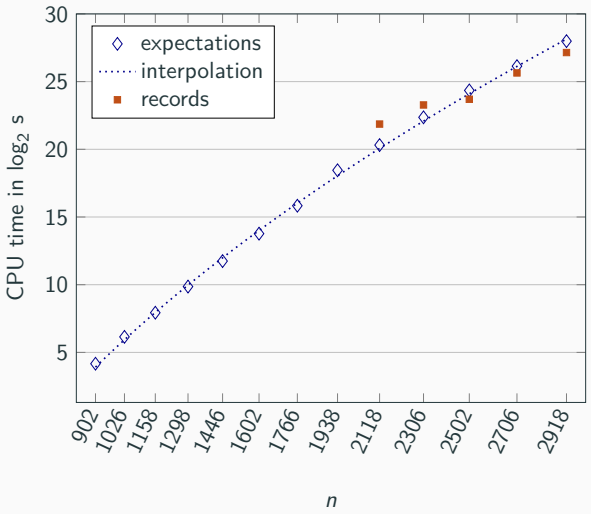
$$\frac{2^{31.9}}{2^{3.9}} = 2^{28}$$

Results (Quasi-Cyclic)



$\omega = \sqrt{n}$ and $k = n/2$

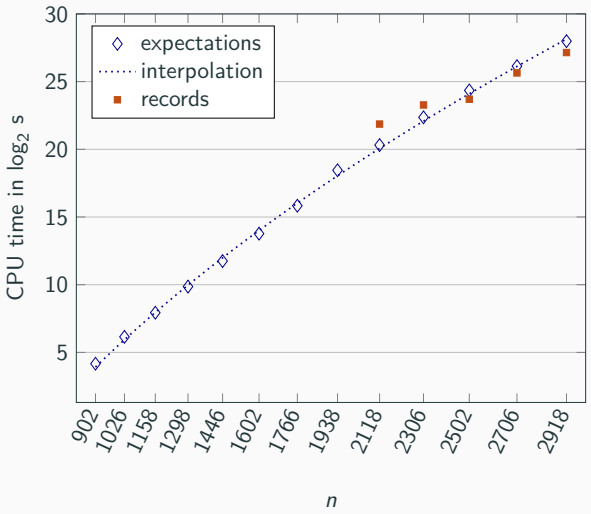
Results (Quasi-Cyclic)



$\omega = \sqrt{n}$ and $k = n/2$

$T(n) = 2^{\sqrt{n}}$

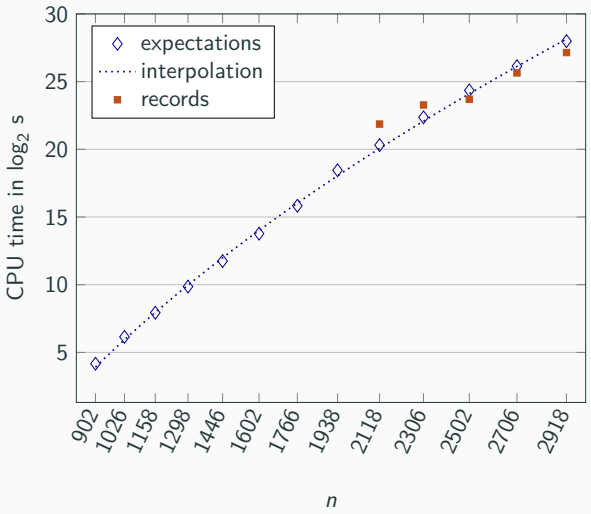
Results (Quasi-Cyclic)



$\omega = \sqrt{n}$ and $k = n/2$

$T_{\text{Prange}}(n) = 2^{(1+o(1))\sqrt{n}}$

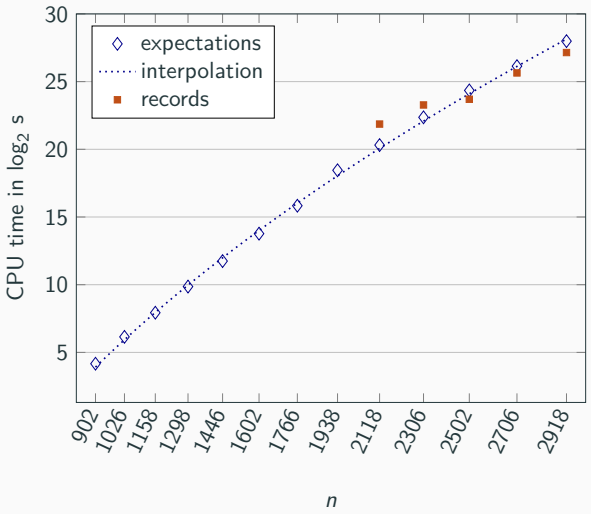
Results (Quasi-Cyclic)



$\omega = \sqrt{n}$ and $k = n/2$

$T_{\mathrm{BJMM}}(n) = 2^{(1\pm o(1))\sqrt{n}}$

Results (Quasi-Cyclic)

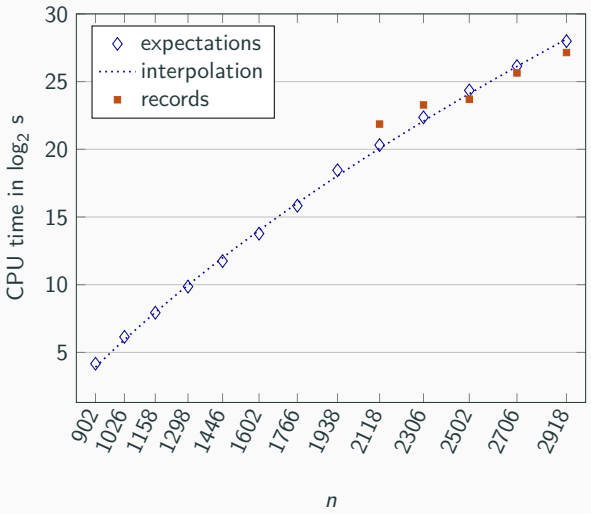


$\omega = \sqrt{n}$ and $k = n/2$

$T_{\mathrm{BJMM}}(n) = 2^{(1\pm o(1))\sqrt{n}}$

$f(n) = a \cdot \sqrt{n} + b$

Results (Quasi-Cyclic)

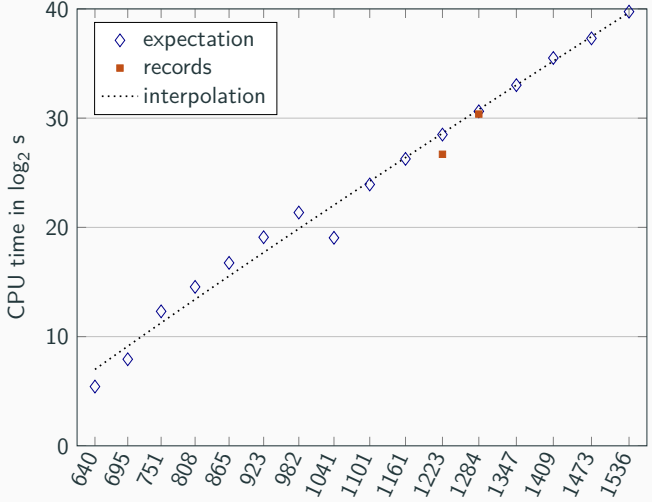


$\omega = \sqrt{n}$ and $k = n/2$

$T_{\mathrm{BJMM}}(n) = 2^{(1+o(1))\sqrt{n}}$

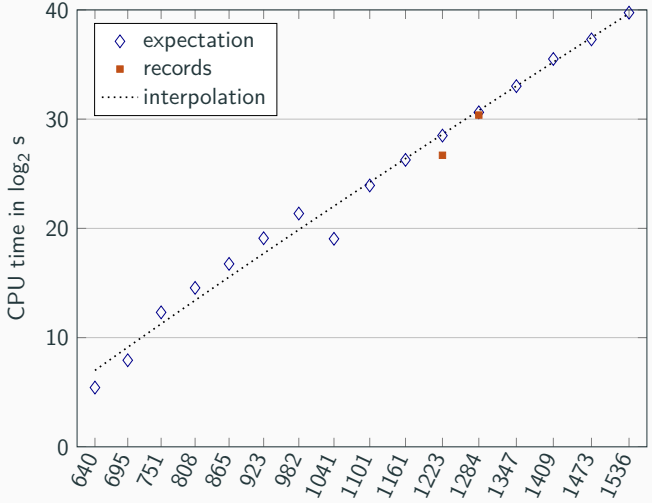
$f(n) = 1.01 \cdot \sqrt{n} - 26.42$

Results (McEliece)



$\omega = \frac{n}{\log_2(n)}$ and $k = \frac{4n}{5}$

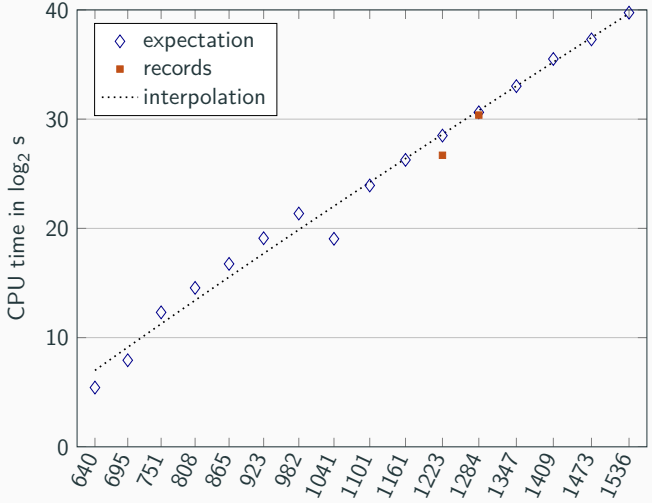
Results (McEliece)



$$\omega = \frac{n}{\log_2(n)} \text{ and } k = \frac{4n}{5}$$

$$T(n) = 2^{2.32\frac{n}{\log n}}$$

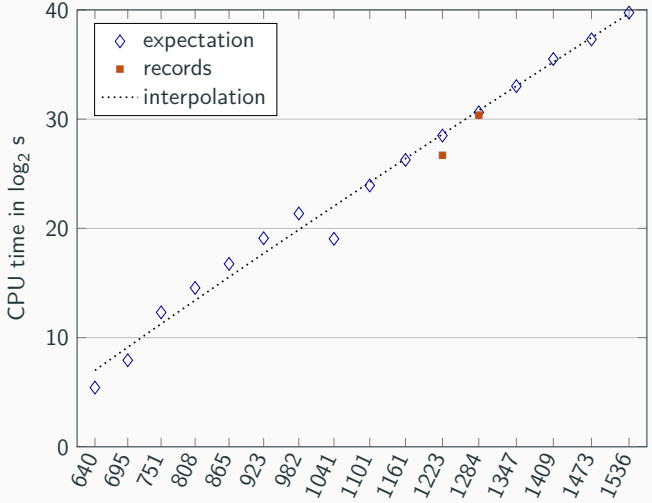
Results (McEliece)



$\omega = \frac{n}{\log_2(n)}$ and $k = \frac{4n}{5}$

$T_{\text{Prange}}(n) = 2^{2.32(1+o(1))\frac{n}{\log n}}$

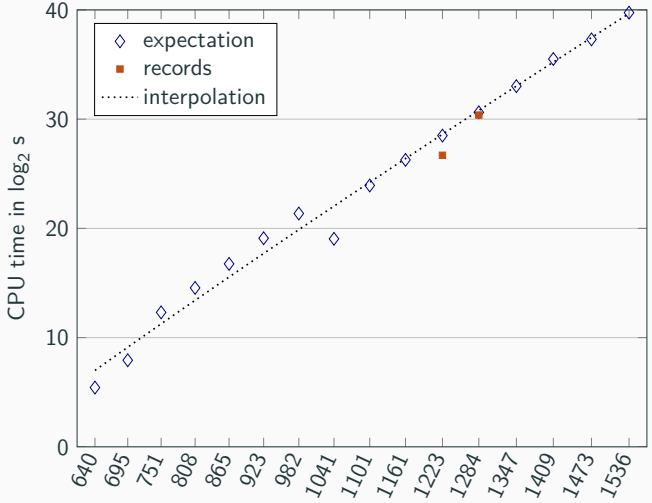
Results (McEliece)



$\omega = \frac{n}{\log_2(n)}$ and $k = \frac{4n}{5}$

$T_{\mathrm{BJMM}}(n) = 2^{2.32(1\pm o(1))\frac{n}{\log n}}$

Results (McEliece)

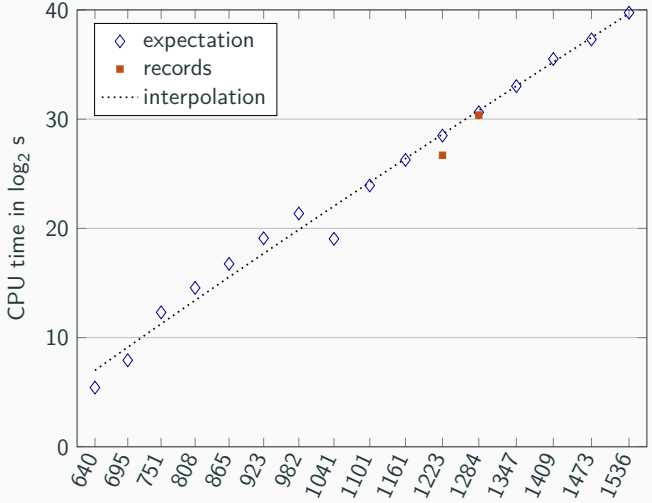


$\omega = \frac{n}{\log_2(n)}$ and $k = \frac{4n}{5}$

$T_{\mathrm{BJMM}}(n) = 2^{2.32(1\pm o(1))\frac{n}{\log n}}$

$f(n) = a \cdot \frac{n}{\log n} + b$

Results (McEliece)

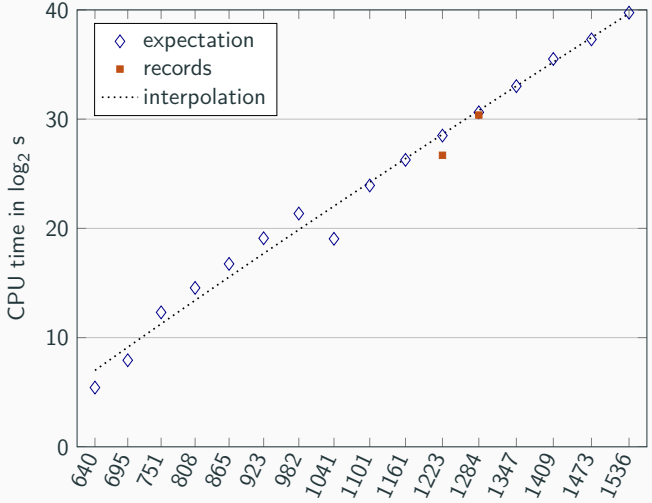


$\omega = \frac{n}{\log_2(n)}$ and $k = \frac{4n}{5}$

$T_{\mathrm{BJMM}}(n) = 2^{(2.32-o(1))\frac{n}{\log n}}$

$f(n) = 2.17 \cdot \frac{n}{\log n} - 22.97$

Results (McEliece)



$\omega = \frac{n}{\log_2(n)}$ and $k = \frac{4n}{5}$

$T_{\mathrm{BJMM}}(n) = 2^{(2.32-o(1))\frac{n}{\log n}}$

$f(n) = 2.17 \cdot \frac{n}{\log n} - 22.97$

constant	log	cube-root
T	$T \cdot \log M$	$T \cdot \sqrt[3]{M}$
2.04	2.13	2.24

Estimating Security

McEliece	$n = 3488$	$n = 4608$	$n = 6688$	$n = 6960$	$n = 8192$
	AES-128	AES-192	AES-256	AES-256	AES-256

Estimating Security

McEliece		$n = 3488$ AES-128	$n = 4608$ AES-192	$n = 6688$ AES-256	$n = 6960$ AES-256	$n = 8192$ AES-256
$\log(M)$	unlimited	**1**	**-23**	**-20**	**-21**	**18**

Estimating Security

McEliece		$n = 3488$ AES-128	$n = 4608$ AES-192	$n = 6688$ AES-256	$n = 6960$ AES-256	$n = 8192$ AES-256
$\log(M)$	unlimited	1	-23	-20	-21	18
	$M \leq 2^{80}$	2	-20	-10	- 9	24
	$M \leq 2^{60}$	5	-18	- 3	- 3	33

Estimating Security

McEliece		$n = 3488$ AES-128	$n = 4608$ AES-192	$n = 6688$ AES-256	$n = 6960$ AES-256	$n = 8192$ AES-256
$\log(M)$	unlimited	1	-23	-20	-21	18
	$M \leq 2^{80}$	2	-20	-10	- 9	24
	$M \leq 2^{60}$	5	-18	- 3	- 3	33
constant	unlimited	0	-24	-23	-23	6
$\sqrt[3]{M}$		10	-12	0	1	38

Estimating Security

BIKE / HQC	AES-128	AES-192	AES-256

Estimating Security

BIKE / HQC		AES-128	AES-192	AES-256
BIKE	constant	**3**	**2**	**5**
	$\log(M)$	**4**	**3**	**6**
	$\sqrt[3]{M}$	**5**	**5**	**9**

Estimating Security

BIKE / HQC		AES-128	AES-192	AES-256
BIKE	constant	**3**	**2**	**5**
	$\log(M)$	**4**	**3**	**6**
	$\sqrt[3]{M}$	**5**	**5**	**9**
HQC	constant	**1**	**4**	**2**
	$\log(M)$	**1**	**4**	**2**
	$\sqrt[3]{M}$	**3**	**7**	**5**

Conclusion

- BIKE/HQC are secure against modern ISD
- McEliece parameters below security level in certain models
  - AES-192 parameter-set should be readjusted
- log model is the best for ISD

Thank You!

https://eprint.iacr.org/2021/1634

https://github.com/FloydZ/decoding