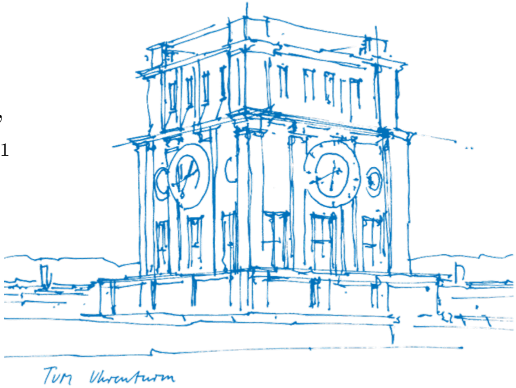
Generic Decoding of Restricted Errors

Sebastian Bitzer[1], Alessio Pavoni[2], Violetta Weger[1], Paolo Santini[2], Marco Baldi[2], Antonia Wachter-Zeh[1]

[1]Technical University of Munich

[2]Università Politecnica delle Marche

June 26, 2023



Outline

The Restricted Syndrome Decoding Problem

Restricted Syndrome Decoding Problem (R-SDP)

Given: parity-check matrix $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, weight t, $g \in \mathbb{F}_p$ of order z and $\mathbb{E} = \{g^0, \dots, g^{z-1}\} \subset \mathbb{F}_p^*$.

Find: error $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ such that $\boldsymbol{H}\boldsymbol{e}^\top = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = t$.

The Restricted Syndrome Decoding Problem

Restricted Syndrome Decoding Problem (R-SDP)

Given: parity-check matrix $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, weight t, $g \in \mathbb{F}_p$ of order z and $\mathbb{E} = \{g^0, \dots, g^{z-1}\} \subset \mathbb{F}_p^*$.

Find: error $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ such that $\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = t$.

- NP-hard, not only for $z = p - 1$

The Restricted Syndrome Decoding Problem

Restricted Syndrome Decoding Problem (R-SDP)

Given: parity-check matrix $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, weight t,
$g \in \mathbb{F}_p$ of order z and $\mathbb{E} = \{g^0, \dots, g^{z-1}\} \subset \mathbb{F}_p^*$.

Find: error $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ such that $\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = t$.

- NP-hard, not only for $z = p - 1$
- Restriction of error guarantees unique solution for increased weight

The Restricted Syndrome Decoding Problem

Restricted Syndrome Decoding Problem (R-SDP)

Given: parity-check matrix $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, weight t,
$g \in \mathbb{F}_p$ of order z and $\mathbb{E} = \{g^0, \ldots, g^{z-1}\} \subset \mathbb{F}_p^*$.

Find: error $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ such that $\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = t$.

- NP-hard, not only for $z = p - 1$
- Restriction of error guarantees unique solution for increased weight
- Recent proposals use R-SDP to achieve compact sizes, e.g.,

Baldi, M., et al. (2023). Zero knowledge protocols and signatures from the restricted syndrome decoding problem. *ePrint*

The Restricted Syndrome Decoding Problem

Restricted Syndrome Decoding Problem (R-SDP)

Given: parity-check matrix $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, weight t,
$g \in \mathbb{F}_p$ of order z and $\mathbb{E} = \{g^0, \ldots, g^{z-1}\} \subset \mathbb{F}_p^*$.

Find: error $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ such that $\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = t$.

- NP-hard, not only for $z = p - 1$
- Restriction of error guarantees unique solution for increased weight
- Recent proposals use R-SDP to achieve compact sizes, e.g.,
  - Baldi, M., et al. (2023). Zero knowledge protocols and signatures from the restricted syndrome decoding problem. *ePrint*

Due to suboptimal solvers or due to hardness of problem?

The Restricted Syndrome Decoding Problem

Restricted Syndrome Decoding Problem (R-SDP)

Given: parity-check matrix $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, weight t,
$g \in \mathbb{F}_p$ of order z and $\mathbb{E} = \{g^0, \ldots, g^{z-1}\} \subset \mathbb{F}_p^*$.

Find: error $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ such that $\boldsymbol{H}\boldsymbol{e}^\mathsf{T} = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = t$.

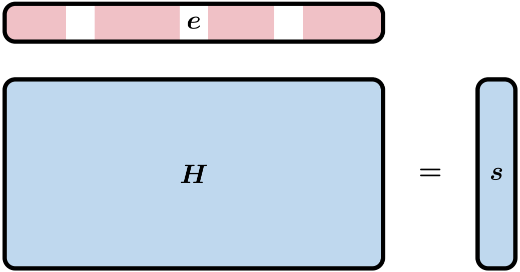
- NP-hard, not only for $z = p - 1$
- Restriction of error guarantees unique solution for increased weight
- Recent proposals use R-SDP to achieve compact sizes, e.g.,
  Baldi, M., et al. (2023). Zero knowledge protocols and signatures from the restricted syndrome decoding problem. *ePrint*

Due to suboptimal solvers or due to hardness of problem?

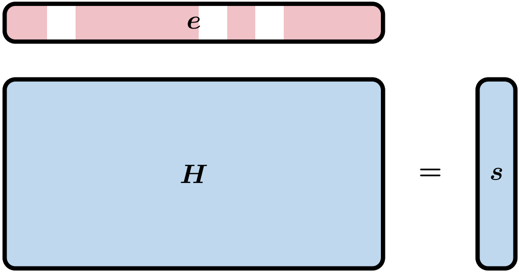
Improved solvers using the representation technique[1]

[1] Howgrave-Graham, N., & Joux, A. (2010). New generic algorithms for hard knapsacks. *Eurocrypt*

The General Framework

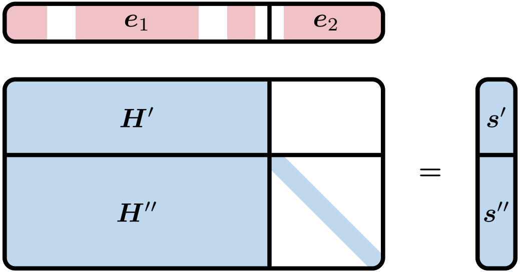


The General Framework



1. Random permutation

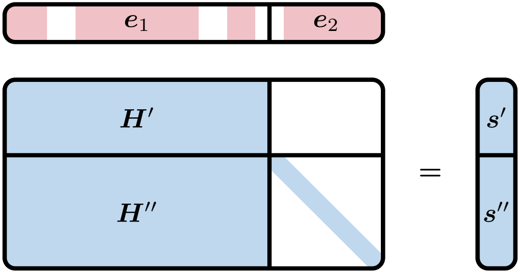
The General Framework



1. Random permutation
2. Quasi-systematic form[2]

[2] Finiasz, M., & Sendrier, N. (2009). Security bounds for the design of code-based cryptosystems. *Asiacrypt*

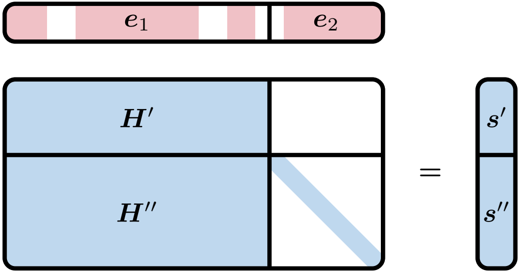
The General Framework



1. Random permutation
2. Quasi-systematic form[2]
3. Enumerate e_1

[2] Finiasz, M., & Sendrier, N. (2009). Security bounds for the design of code-based cryptosystems. *Asiacrypt*

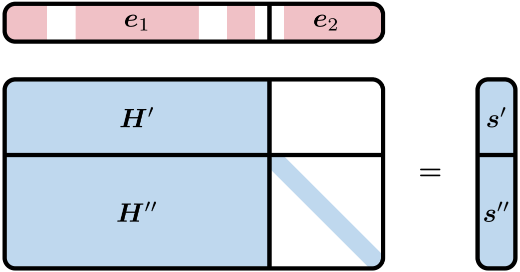
The General Framework



1. Random permutation
2. Quasi-systematic form[2]
3. Enumerate e_1
4. Check corresponding e_2

[2] Finiasz, M., & Sendrier, N. (2009). Security bounds for the design of code-based cryptosystems. *Asiacrypt*

The General Framework

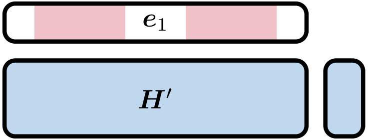


1. Random permutation
2. Quasi-systematic form[2]
3. Enumerate e_1
4. Check corresponding e_2

$\Rightarrow$ cost $= \frac{\text{enumeration cost}}{\text{success probability}}$

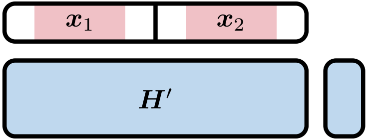
[2] Finiasz, M., & Sendrier, N. (2009). Security bounds for the design of code-based cryptosystems. *Asiacrypt*

A Meet-in-the-Middle Strategy

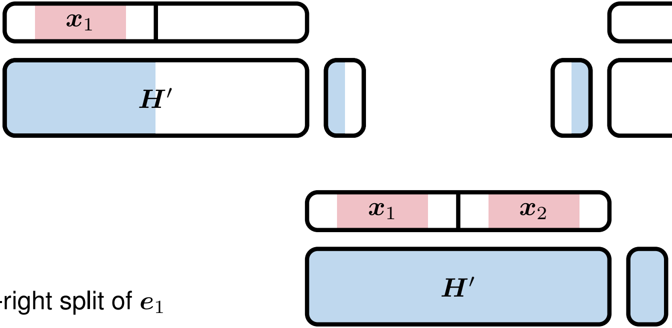


A Meet-in-the-Middle Strategy

- Left-right split of e_1

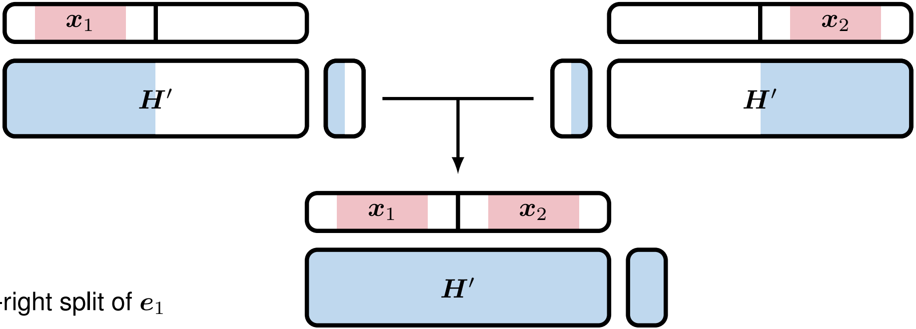


A Meet-in-the-Middle Strategy



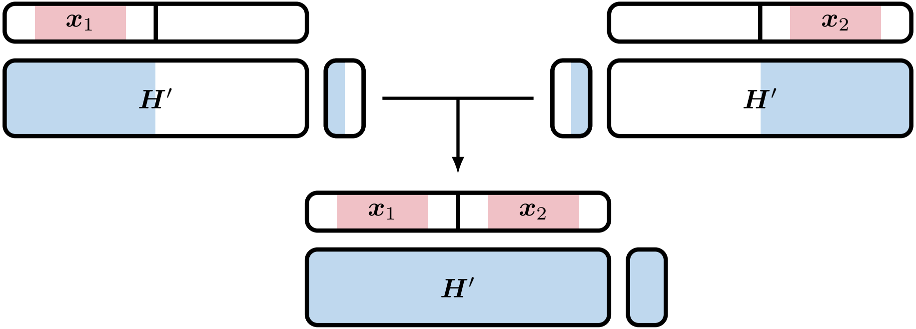
- Left-right split of e_1
- Enumerate x_1, x_2

A Meet-in-the-Middle Strategy

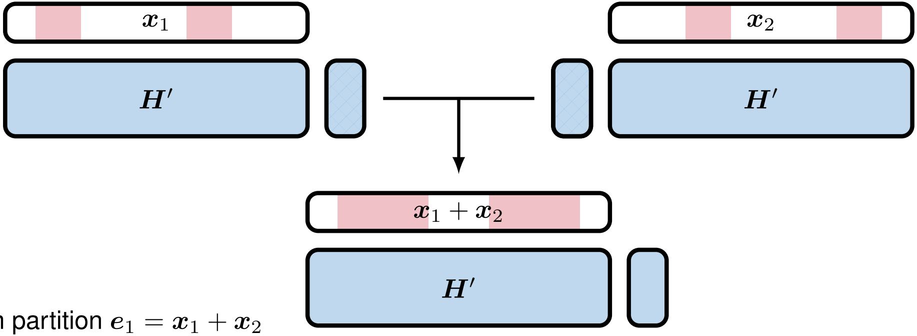


- Left-right split of e_1
- Enumerate x_1, x_2
- Collisions solve small instance

The Representation Technique

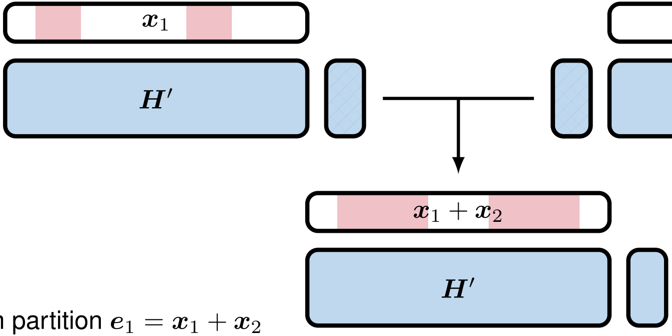


The Representation Technique



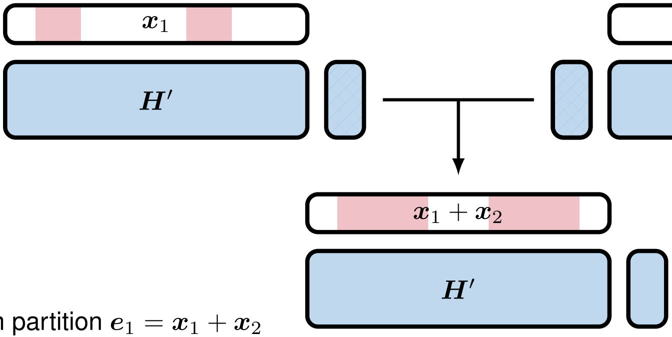
- Sum partition $\boldsymbol{e}_1 = \boldsymbol{x}_1 + \boldsymbol{x}_2$

The Representation Technique



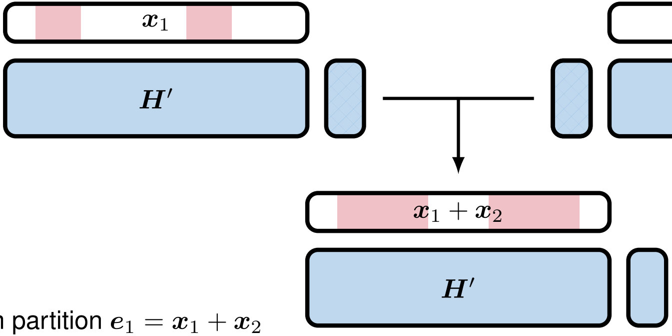
- Sum partition $\boldsymbol{e}_1 = \boldsymbol{x}_1 + \boldsymbol{x}_2$
- Multiple representations

The Representation Technique



- Sum partition $\boldsymbol{e}_1 = \boldsymbol{x}_1 + \boldsymbol{x}_2$
- Multiple representations
- Enumerate only fraction

The Representation Technique



- Sum partition $e_1 = x_1 + x_2$
- Multiple representations
- Enumerate only fraction

Search space for x_1, x_2?

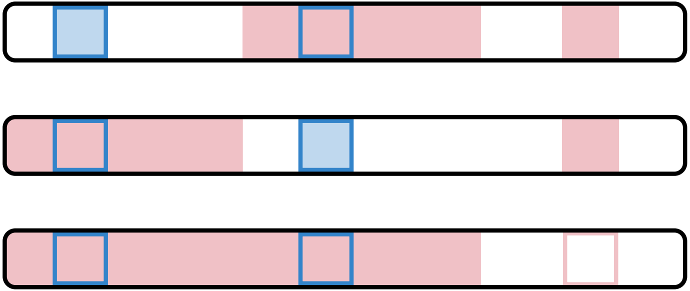
The Search Space for $\boldsymbol{x}_1$, $\boldsymbol{x}_2$

The Search Space for $\boldsymbol{x}_1, \boldsymbol{x}_2$

- Split support[3]

[3] Howgrave-Graham, N., & Joux, A. (2010). New generic algorithms for hard knapsacks. *Eurocrypt*

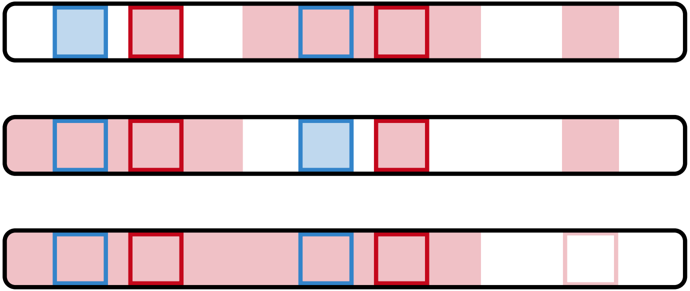
The Search Space for $\boldsymbol{x}_1$, $\boldsymbol{x}_2$



- Split support[3]
- Overlaps[4] to 0 for even z

[3] Howgrave-Graham, N., & Joux, A. (2010). New generic algorithms for hard knapsacks. *Eurocrypt*
[4] Becker, A., Coron, J.-S., & Joux, A. (2011). Improved generic algorithms for hard knapsacks. *Eurocrypt*

The Search Space for $\boldsymbol{x}_1$, $\boldsymbol{x}_2$

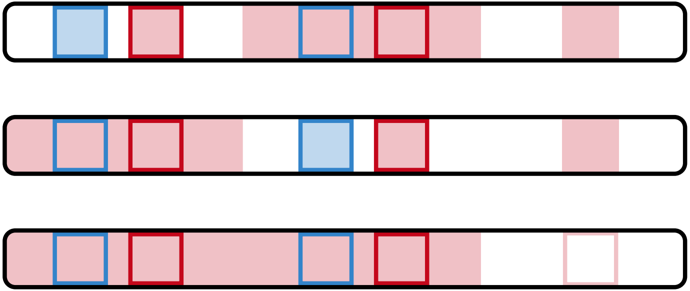


- Split support[3]
- Overlaps[4] to 0 for even z
- Additional overlaps to $\mathbb{E}$

[3] Howgrave-Graham, N., & Joux, A. (2010). New generic algorithms for hard knapsacks. *Eurocrypt*

[4] Becker, A., Coron, J.-S., & Joux, A. (2011). Improved generic algorithms for hard knapsacks. *Eurocrypt*

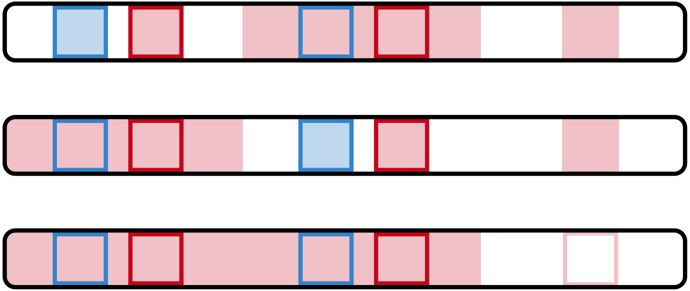
The Search Space for $\boldsymbol{x}_1, \boldsymbol{x}_2$



- Split support[3]
- Overlaps[4] to 0 for even z
- Additional overlaps to $\mathbb{E}$
- "$\mathbb{E} + \mathbb{E} = \mathbb{E}$"-representations

[3] Howgrave-Graham, N., & Joux, A. (2010). New generic algorithms for hard knapsacks. *Eurocrypt*
[4] Becker, A., Coron, J.-S., & Joux, A. (2011). Improved generic algorithms for hard knapsacks. *Eurocrypt*

The Search Space for $\boldsymbol{x}_1$, $\boldsymbol{x}_2$

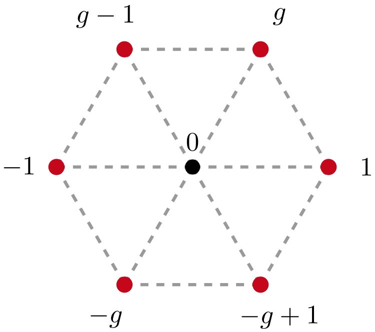


- Split support[3]
- Overlaps[4] to 0 for even z
- Additional overlaps to $\mathbb{E}$
- "$\mathbb{E} + \mathbb{E} = \mathbb{E}$"-representations

Performance highly dependent on structure of $\mathbb{E}$

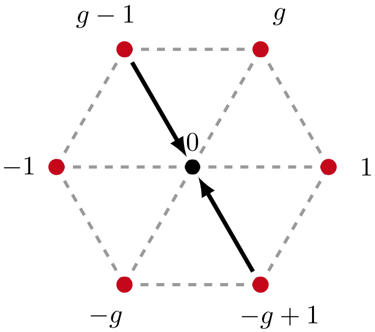
[3] Howgrave-Graham, N., & Joux, A. (2010). New generic algorithms for hard knapsacks. *Eurocrypt*
[4] Becker, A., Coron, J.-S., & Joux, A. (2011). Improved generic algorithms for hard knapsacks. *Eurocrypt*

$z = 6$: Many Symmetries[5]



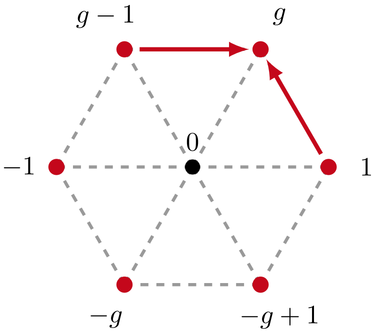
[5] Thiers, J.-P., & Freudenberger, J. (2021). Codes over Eisenstein integers for the Niederreiter cryptosystem. *ICCE*

$z = 6$: Many Symmetries[5]



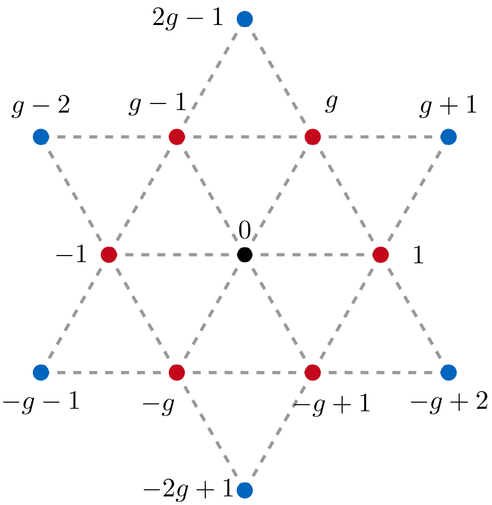
[5]Thiers, J.-P., & Freudenberger, J. (2021). Codes over Eisenstein integers for the Niederreiter cryptosystem. *ICCE*

$z = 6$: Many Symmetries[5]



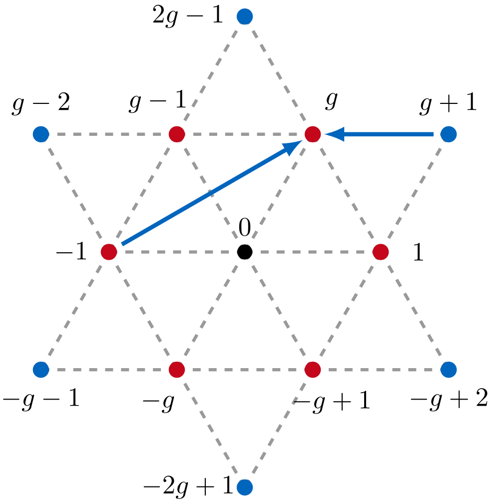
[5] Thiers, J.-P., & Freudenberger, J. (2021). Codes over Eisenstein integers for the Niederreiter cryptosystem. *ICCE*

$z = 6$: Many Symmetries[5]



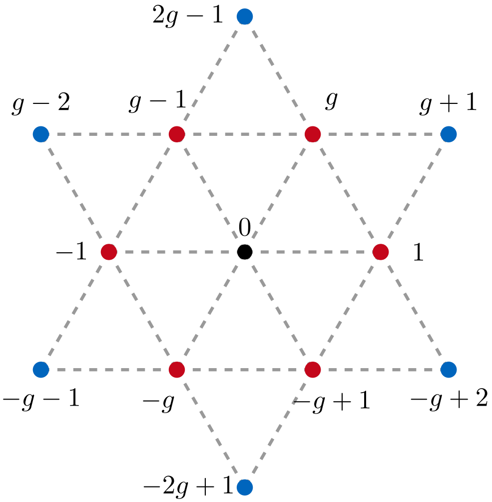
[5] Thiers, J.-P., & Freudenberger, J. (2021). Codes over Eisenstein integers for the Niederreiter cryptosystem. *ICCE*

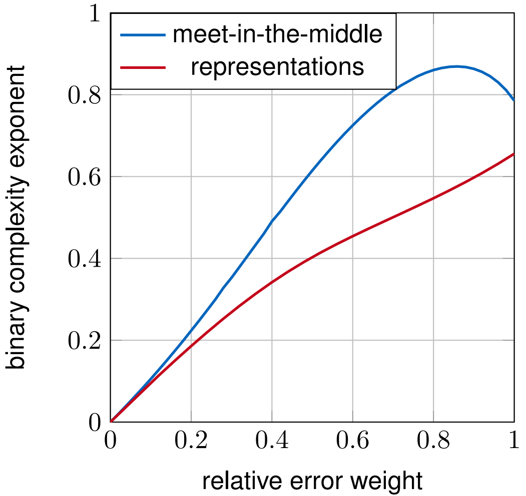
$z = 6$: Many Symmetries[5]



[5]Thiers, J.-P., & Freudenberger, J. (2021). Codes over Eisenstein integers for the Niederreiter cryptosystem. *ICCE*

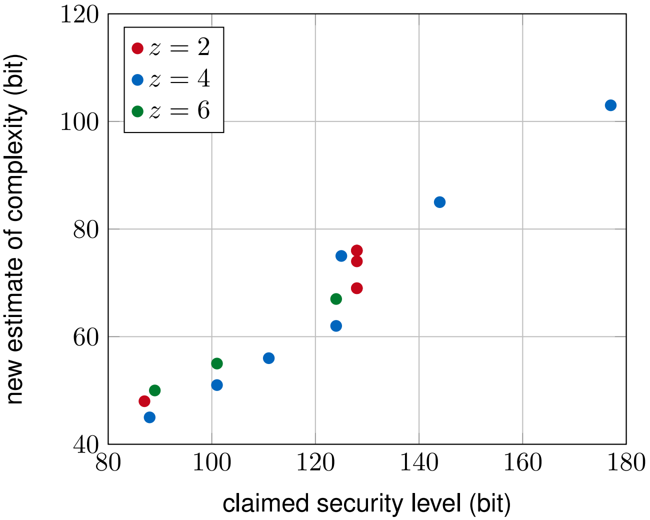
$z = 6$: Many Symmetries[5]





[5] Thiers, J.-P., & Freudenberger, J. (2021). Codes over Eisenstein integers for the Niederreiter cryptosystem. *ICCE*

Overview of Results



Conclusion

Summary

- Restricted decoding problem
- Representation technique for R-SDP
- Improvement for $z \in \{2, 4, 6\}$

Conclusion

Summary

- Restricted decoding problem
- Representation technique for R-SDP
- Improvement for $z \in \{2, 4, 6\}$

Open Questions

- Further combinatorial tricks
- Algebraic attacks
- Secure McEliece-like constructions

Conclusion

Summary

- Restricted decoding problem
- Representation technique for R-SDP
- Improvement for $z \in \{2, 4, 6\}$

Open Questions

- Further combinatorial tricks
- Algebraic attacks
- Secure McEliece-like constructions

CROSS

https://cross-crypto.com

Conclusion

Summary

- Restricted decoding problem
- Representation technique for R-SDP
- Improvement for $z \in \{2, 4, 6\}$

Open Questions

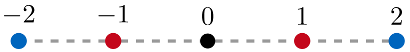
- Further combinatorial tricks
- Algebraic attacks
- Secure McEliece-like constructions

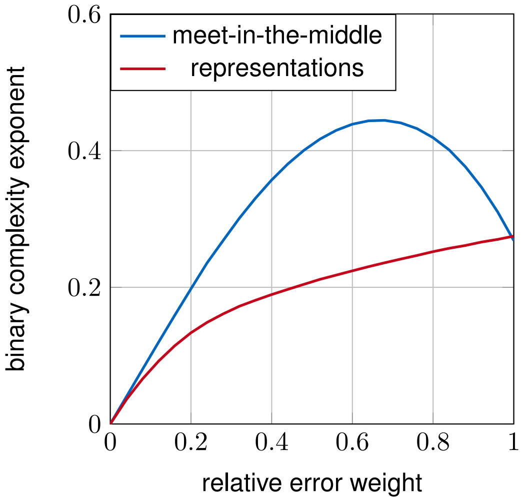
CROSS

https://cross-crypto.com

Thank you! Questions?

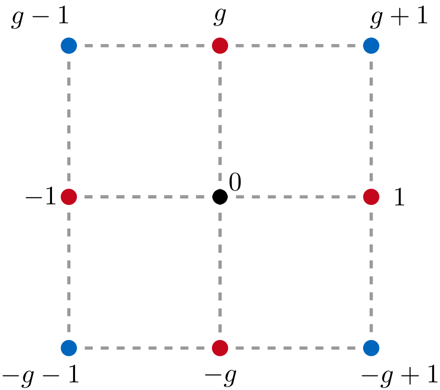
$z = 2$: Simple Structure[6]

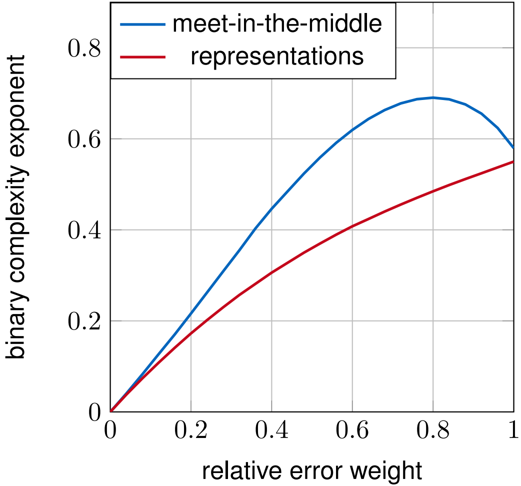




[6] Baldi, M., Chiaraluce, F., & Santini, P. (2021). Code-based signatures without trapdoors through restricted vectors. *Cryptology ePrint Archive*

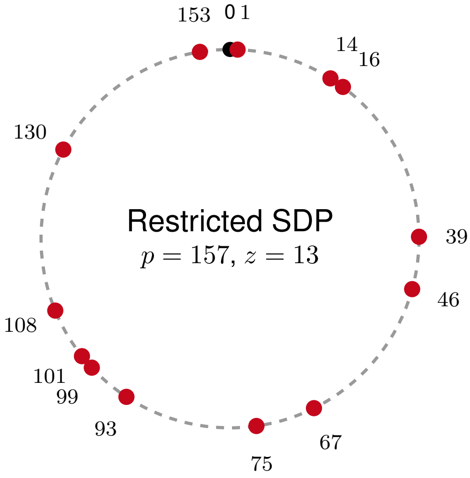
$z = 4$: Gaussian Integers[7]

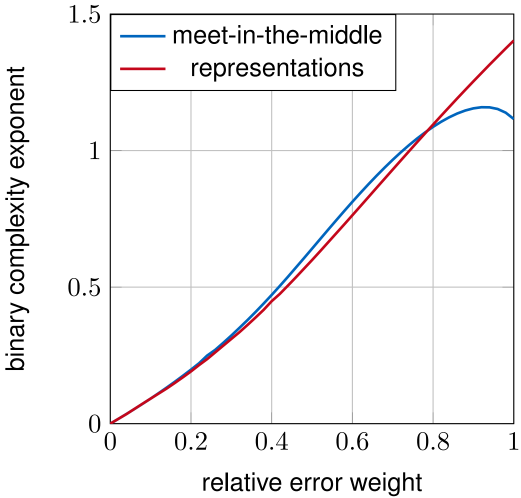




[7] Freudenberger, J., & Thiers, J.-P. (2021). A new class of q-ary codes for the McEliece cryptosystem. *Cryptography*

$z = 13$: Few Symmetries[8]





[8] Baldi, M., et al. (2023). Zero knowledge protocols and signatures from the restricted syndrome decoding problem. *ePrint*