

# How to Lose Some Weight

## A Practical Template Syndrome Decoding Attack

Sebastian Bitzer  
TUM

Jeroen Delvaux  
TII

Elena Kirshanova  
TII

Sebastian Maaßen  
RUB

Alexander May  
RUB

Antonia Wachter-Zeh  
TUM

WCC 2024, Perugia



*TUM Uhrenturm*

# Code-based Cryptography

 McEliece (1978). [A Public-Key Cryptosystem based on Algebraic Coding Theory.](#)

→ 40 years later: BIKE, HQC, Classic McEliece

# Code-based Cryptography

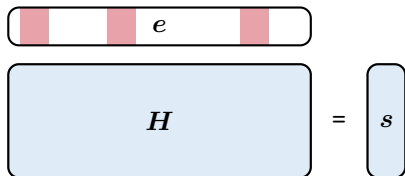
McEliece (1978). [A Public-Key Cryptosystem based on Algebraic Coding Theory.](#)

→ 40 years later: BIKE, HQC, Classic McEliece

## Syndrome Decoding Problem

Given:  $H \in \mathbb{F}_2^{r \times n}$ ,  $s \in \mathbb{F}_2^r$ ,  $w \in \mathbb{N}$ .

Find:  $e \in \mathbb{F}_2^n$  with  $He = s$  and  $\text{wt}(e) = w$ .



# Code-based Cryptography

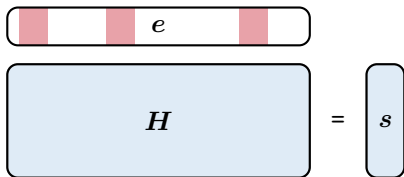
McEliece (1978). *A Public-Key Cryptosystem based on Algebraic Coding Theory.*

→ 40 years later: BIKE, HQC, Classic McEliece

## Syndrome Decoding Problem

Given:  $H \in \mathbb{F}_2^{r \times n}$ ,  $s \in \mathbb{F}_2^r$ ,  $w \in \mathbb{N}$ .

Find:  $e \in \mathbb{F}_2^n$  with  $He = s$  and  $\text{wt}(e) = w$ .



## Example

$n = 2197$ ,  $r = 439$ ,  $w = 37$  requires  $\sim 2^{88}$  operations

# Code-based Cryptography

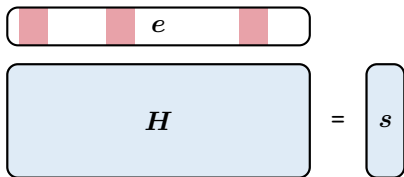
McEliece (1978). *A Public-Key Cryptosystem based on Algebraic Coding Theory.*

→ 40 years later: BIKE, HQC, Classic McEliece

## Syndrome Decoding Problem

Given:  $H \in \mathbb{F}_2^{r \times n}$ ,  $s \in \mathbb{F}_2^r$ ,  $w \in \mathbb{N}$ ,  $\text{Hint}(e)$ .

Find:  $e \in \mathbb{F}_2^n$  with  $He = s$  and  $\text{wt}(e) = w$ .



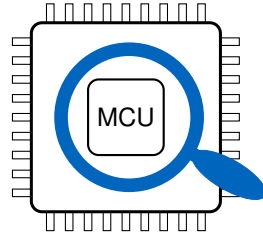
## Example

$n = 2197$ ,  $r = 439$ ,  $w = 37$  requires  $\sim 2^{88}$  operations

# Can You Give Me a Hint?

Implementations leak information:

- Timing
- Power consumption



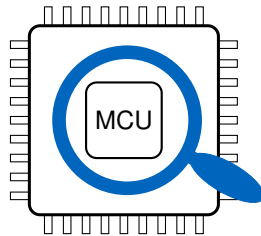
# Can You Give Me a Hint?

Implementations leak information:

- Timing
- Power consumption

Can be translated into

- Error positions
- Block weights



Horlemann, Puchinger, Renner, Schamberger, Wachter-Zeh (2021). [ISD with Hints](#).

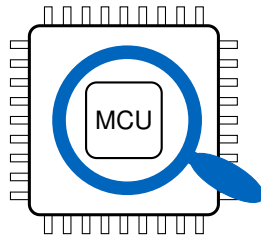
# Can You Give Me a Hint?


Implementations leak information:

- Timing
- Power consumption

Can be translated into

- Error positions
- Block weights



 Horlemann, Puchinger, Renner, Schamberger, Wachter-Zeh (2021). [ISD with Hints](#).

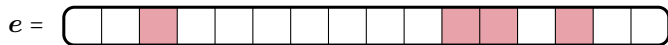
**Contribution:** Improved solver, noisy hints, and explicit implementation



# Known Block Weights

Motivation → Blockwise operations

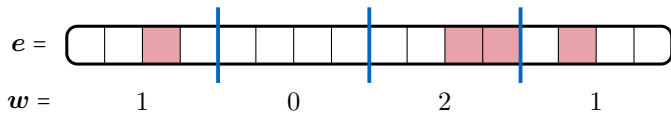
→ Dependence on block weight



# Known Block Weights

Motivation → Blockwise operations

→ Dependence on block weight



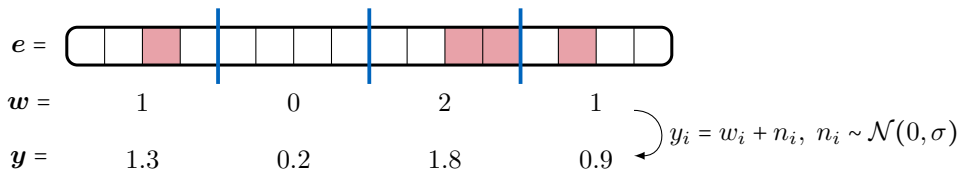
## Example

$n = 2197$  consists of  $m = 69$  blocks of  $b_i = 32$  bits

# Known Block Weights

Motivation → Blockwise operations

→ Dependence on block weight



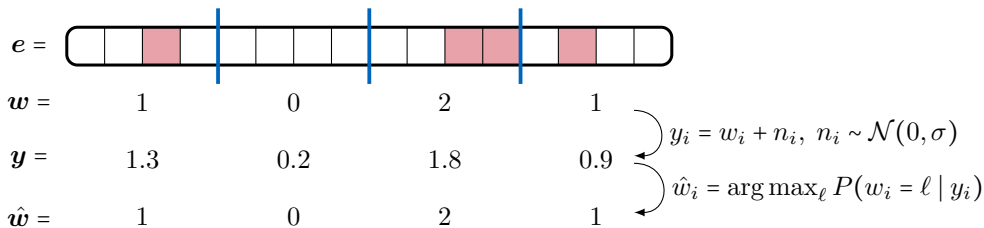
## Example

$n = 2197$  consists of  $m = 69$  blocks of  $b_i = 32$  bits

# Known Block Weights

Motivation → Blockwise operations

→ Dependence on block weight



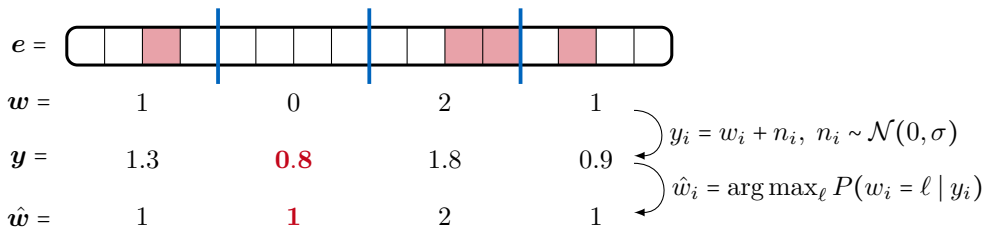
## Example

$n = 2197$  consists of  $m = 69$  blocks of  $b_i = 32$  bits

# Known Block Weights

Motivation → Blockwise operations

→ Dependence on block weight

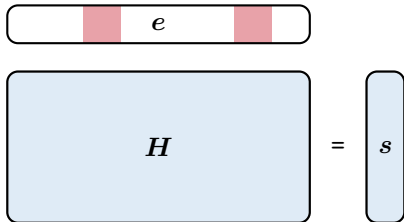


## Example

$n = 2197$  consists of  $m = 69$  blocks of  $b_i = 32$  bits

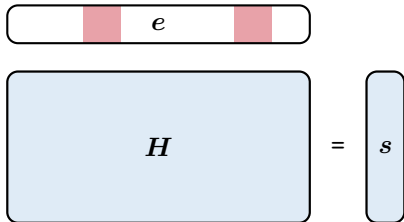
# Solving SDP

- Prange (1962)
  - ⋮
  - Stern (1989)
  - ⋮
  - BJMM (2012)
  - ⋮
  - CDMT (2024)
- } Information Set  
Decoding (ISD)



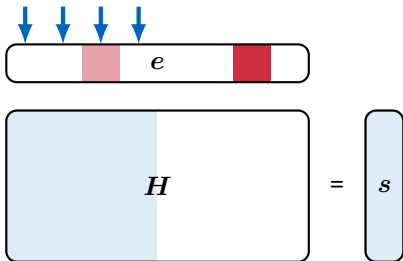
# Solving SDP

- Prange (1962)
  - $\vdots$
  - Stern (1989)
  - $\vdots$
  - BJMM (2012)
  - $\vdots$
  - CDMT (2024)
- } Information Set  
Decoding (ISD)



# Solving SDP

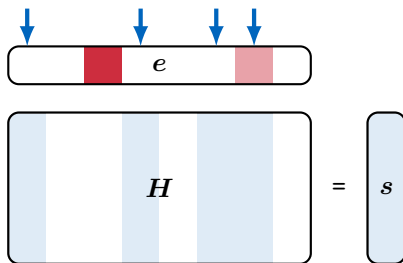
- **Prange** (1962)
  - $\vdots$
  - Stern (1989)
  - $\vdots$
  - BJMM (2012)
  - $\vdots$
  - CDMT (2024)
- } Information Set Decoding (ISD)





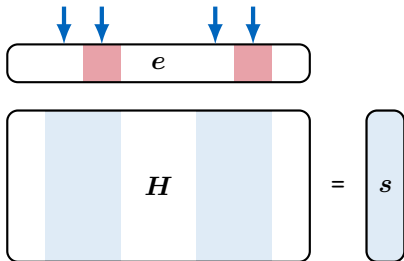
# Solving SDP

- Prange (1962)
  - Stern (1989)
  - BJMM (2012)
  - CDMT (2024)
- } Information Set Decoding (ISD)



# Solving SDP

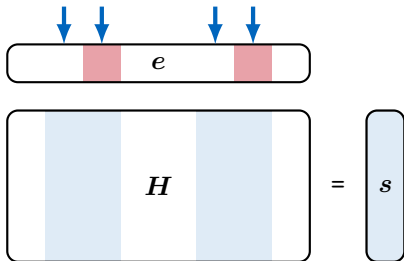
- Prange (1962)
  - Stern (1989)
  - BJMM (2012)
  - CDMT (2024)
- } Information Set Decoding (ISD)



# Solving SDP

- Prange (1962)
- Stern (1989)
- BJMM (2012)
- CDMT (2024)

Information Set  
Decoding (ISD)

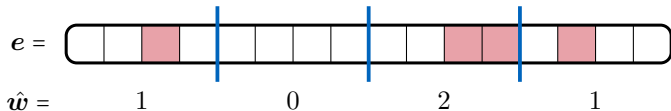


Cost

$$C_{\text{Prange}} = \text{Poly}(n) \cdot \frac{\binom{n}{w}}{\binom{w}{r}}$$

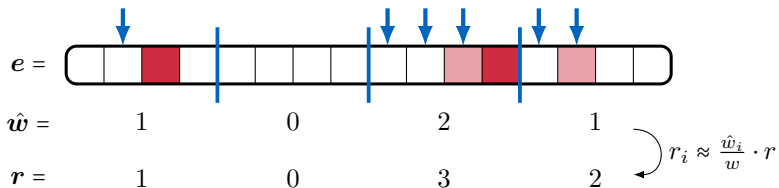
# Information Set Decoding with Hints

Horlemann, Puchinger, Renner, Schamberger, Wachter-Zeh (2021). [ISD with Hints](#).



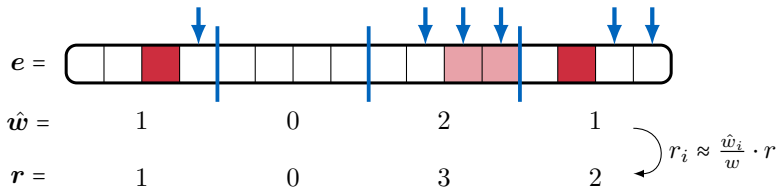
# Information Set Decoding with Hints

Horlemann, Puchinger, Renner, Schamberger, Wachter-Zeh (2021). [ISD with Hints](#).



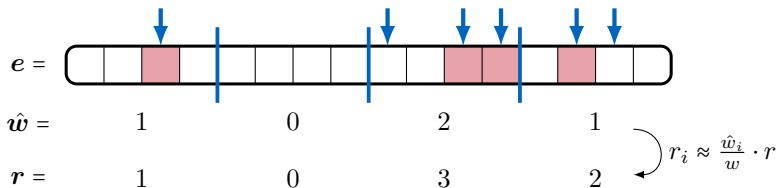
# Information Set Decoding with Hints

Horlemann, Puchinger, Renner, Schamberger, Wachter-Zeh (2021). [ISD with Hints](#).



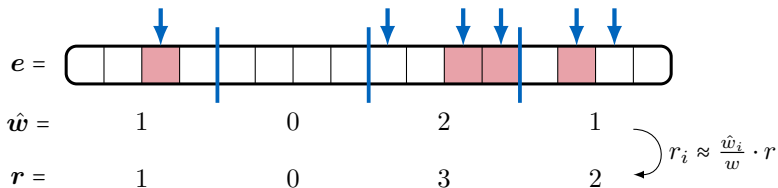
# Information Set Decoding with Hints

Horlemann, Puchinger, Renner, Schamberger, Wachter-Zeh (2021). [ISD with Hints](#).



# Information Set Decoding with Hints

Horlemann, Puchinger, Renner, Schamberger, Wachter-Zeh (2021). [ISD with Hints](#).



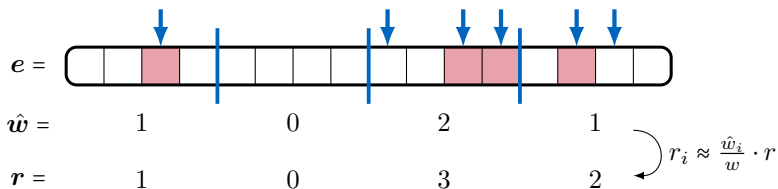
Cost

$$C_{\text{Hints}} = \text{Poly}(n) \cdot \prod_{i=1}^m \frac{\binom{b_i}{w_i}}{\binom{r_i}{w_i}}$$



# Information Set Decoding with Hints

Horlemann, Puchinger, Renner, Schamberger, Wachter-Zeh (2021). [ISD with Hints](#).



Cost

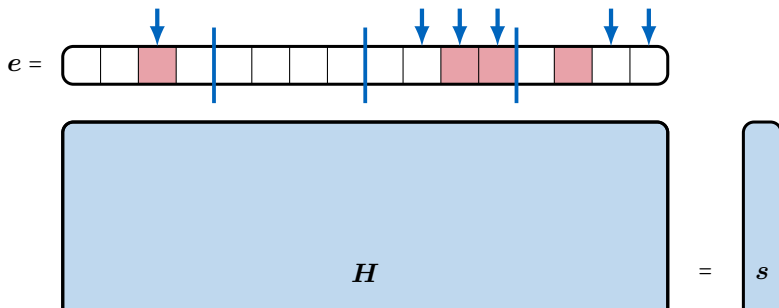
$$C_{\text{Hints}} = \text{Poly}(n) \cdot \prod_{i=1}^m \frac{\binom{b_i}{w_i}}{\binom{r_i}{w_i}}$$

Example

Decoder lost some weight, runs in  $2^{36}$  iterations

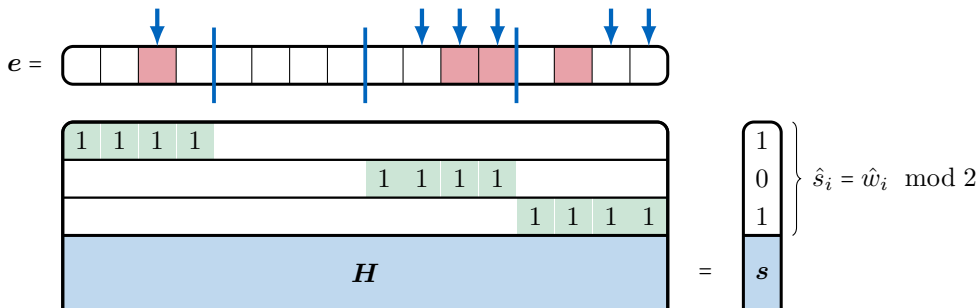
# Improved Solver

Esser, Santini (2023). [Asymptotics and Improvements of Regular Syndrome Decoding Attacks.](#)



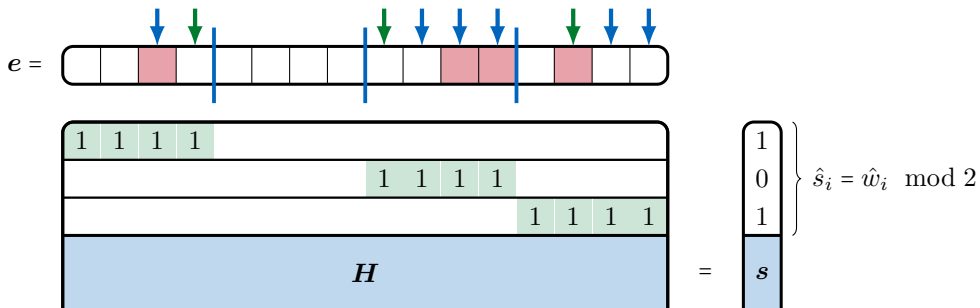
# Improved Solver

Esser, Santini (2023). *Asymptotics and Improvements of Regular Syndrome Decoding Attacks.*



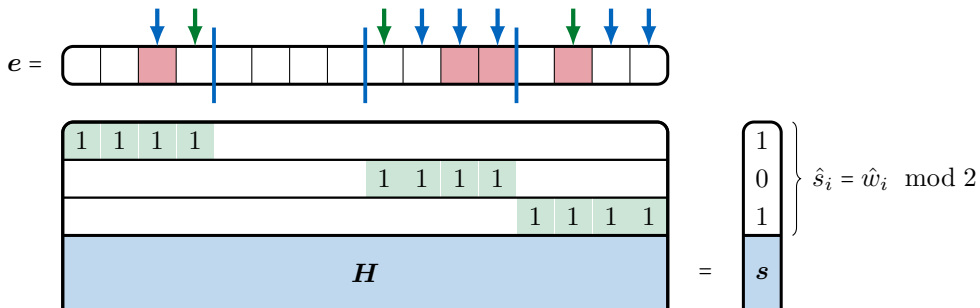
# Improved Solver

Esser, Santini (2023). [Asymptotics and Improvements of Regular Syndrome Decoding Attacks.](#)



# Improved Solver

Esser, Santini (2023). *Asymptotics and Improvements of Regular Syndrome Decoding Attacks.*

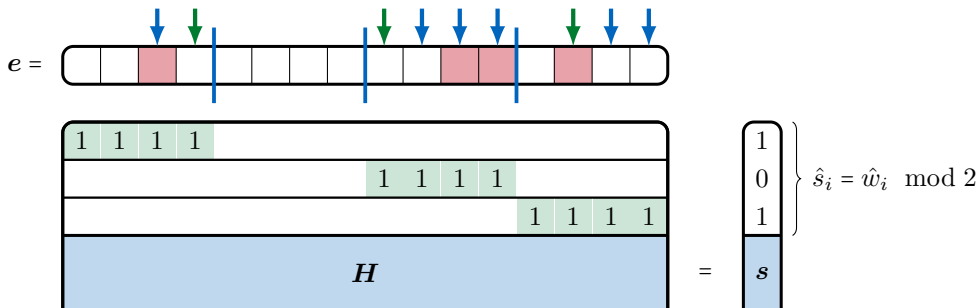


## Example

$r$  increased by  $\sim 29$ ;  $2^{32}$  instead of  $2^{87}$  ( $2^{36}$ ) iterations

# Improved Solver

Esser, Santini (2023). *Asymptotics and Improvements of Regular Syndrome Decoding Attacks.*



## Example

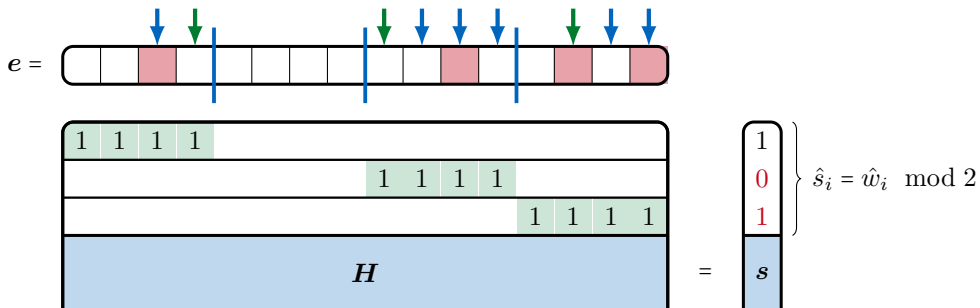
$r$  increased by  $\sim 29$ ;  $2^{32}$  instead of  $2^{87}$  ( $2^{36}$ ) iterations

## Issue

Noise resilience

# Improved Solver

Esser, Santini (2023). *Asymptotics and Improvements of Regular Syndrome Decoding Attacks.*



## Example

$r$  increased by  $\sim 29$ ;  $2^{32}$  instead of  $2^{87}$  ( $2^{36}$ ) iterations

## Issue

Noise resilience

# Complexity vs Noise

Increase noise resilience → Checksum  $\sum_i \hat{w}_i \stackrel{?}{=} w$

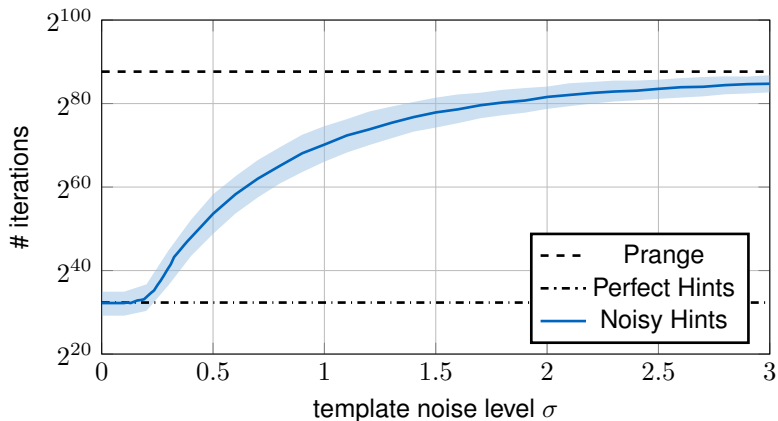
→ Detect unreliable  $\hat{w}_i$  using measurement  $\mathbf{y}$



# Complexity vs Noise

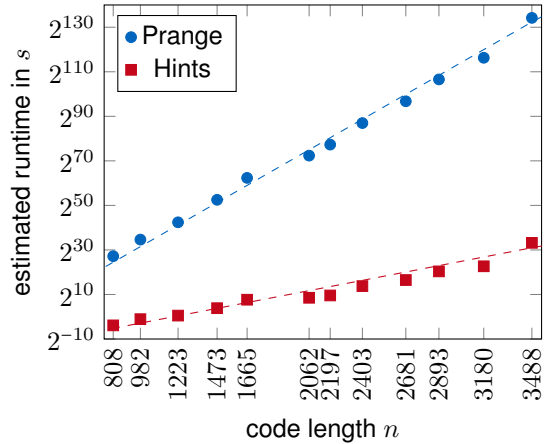
Increase noise resilience → Checksum  $\sum_i \hat{w}_i \stackrel{?}{=} w$

→ Detect unreliable  $\hat{w}_i$  using measurement  $y$



# Explicit Attack

- Weight computation on ARM Cortex-M4
- Template attack using ChipWhisperer
- ISD on two AMD EPYC 7742 CPUs

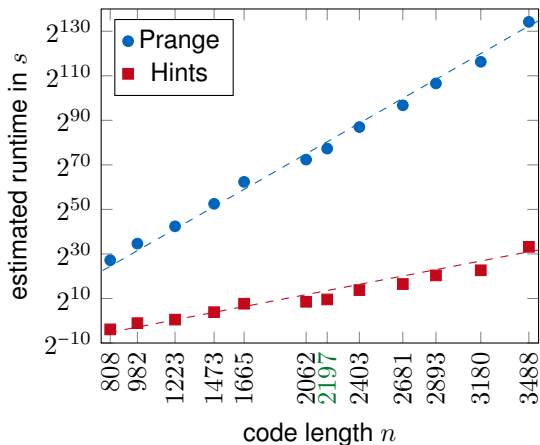


# Explicit Attack

- Weight computation on ARM Cortex-M4
- Template attack using ChipWhisperer
- ISD on two AMD EPYC 7742 CPUs

## Example

$n = 2197$ :  $|\{i \mid \hat{w}_i \neq w_i\}| \approx 1$ , ISD in 10 s



# Conclusion

Solving SDP with hints:

- 😊 Increase parity-check matrix, decrease cost
- 😊 Error-prone hints
- 😊 Explicit implementation of attack

eprint 2024/621



# Conclusion

Solving SDP with hints:

- 😊 Increase parity-check matrix, decrease cost
- 😊 Error-prone hints
- 😊 Explicit implementation of attack

Can one

- ❓ derive other hints?
- ❓ find further applications?

eprint 2024/621



# Conclusion

Solving SDP with hints:

- 😊 Increase parity-check matrix, decrease cost
- 😊 Error-prone hints
- 😊 Explicit implementation of attack

Can one

- 🤔 derive other hints?
- 🤔 find further applications?

eprint 2024/621



Thank you!  
Questions?