Punctured Syndrome Decoding Problem

Efficient Side-Channel Attacks Against *Classic McEliece*

Vincent Grosso Pierre-Louis Cayrel Brice Colombier Vlad-Florin Drăgoi

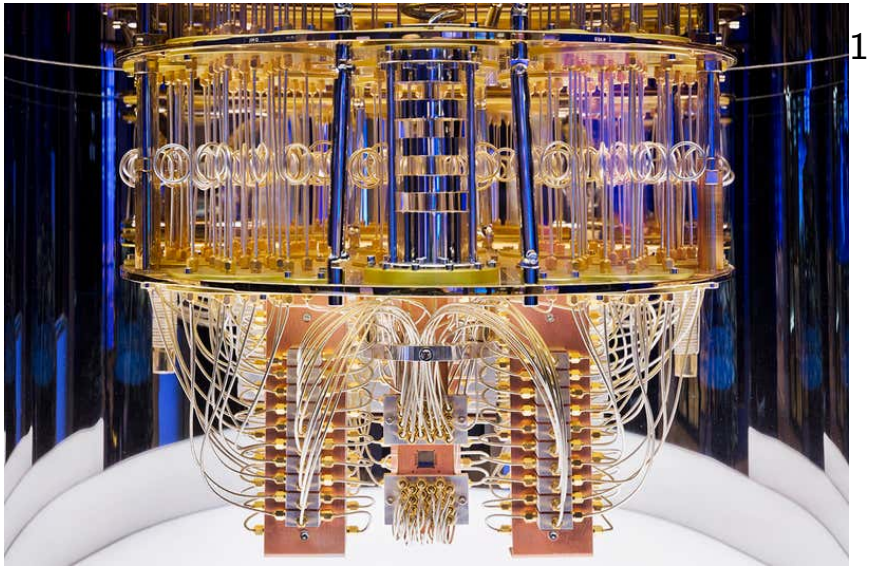
Université Jean Monnet Saint-Etienne, CNRS, Institut d Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, SAINT-ETIENNE, France

Faculty of Exact Sciences, Aurel Vlaicu University, Arad, Romania

LITIS, University of Rouen Normandie, Saint-Etienne du Rouvray, France

Introduction

Classic McEliece

 [1]

- Code-based candidate to the NIST PQC competition
- Key Encapsulation Mechanism from PKE à la Niederreiter
- Security based on the syndrome decoding problem

[1] Photo: IBM Research

Model encapsulation

Algorithm 1 *Classic McEliece* encapsulation

Require: A binary $(n-k, n)$ matrix $\boldsymbol{H}$ (public key)

Ensure: A session key K and a ciphertext $\boldsymbol{c}$

1: Generate a uniform random vector $\boldsymbol{e} \in \mathbb{F}_2^n$ with $\mathrm{HW}(\boldsymbol{e}) = t$.
2: Compute $\boldsymbol{c} \leftarrow \boldsymbol{H}\boldsymbol{e}$ ▷ target operation/encode
3: Compute $K \leftarrow \mathrm{H}(1 \,\|\, \boldsymbol{e} \,\|\, \boldsymbol{c})$ ▷ session key
4: **return** $(\boldsymbol{c}, K)$

Model encapsulation

Algorithm 1 *Classic McEliece* encapsulation

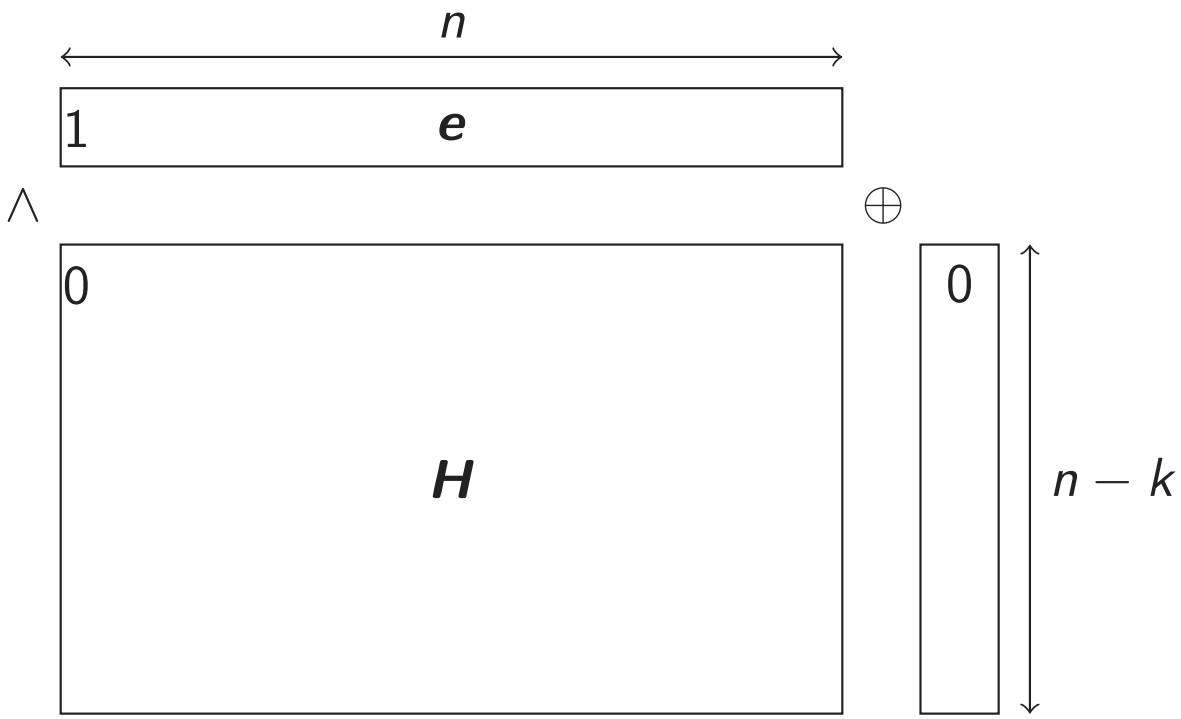
Require: A binary $(n-k, n)$ matrix $\boldsymbol{H}$ (public key)

Ensure: A session key K and a ciphertext $\boldsymbol{c}$

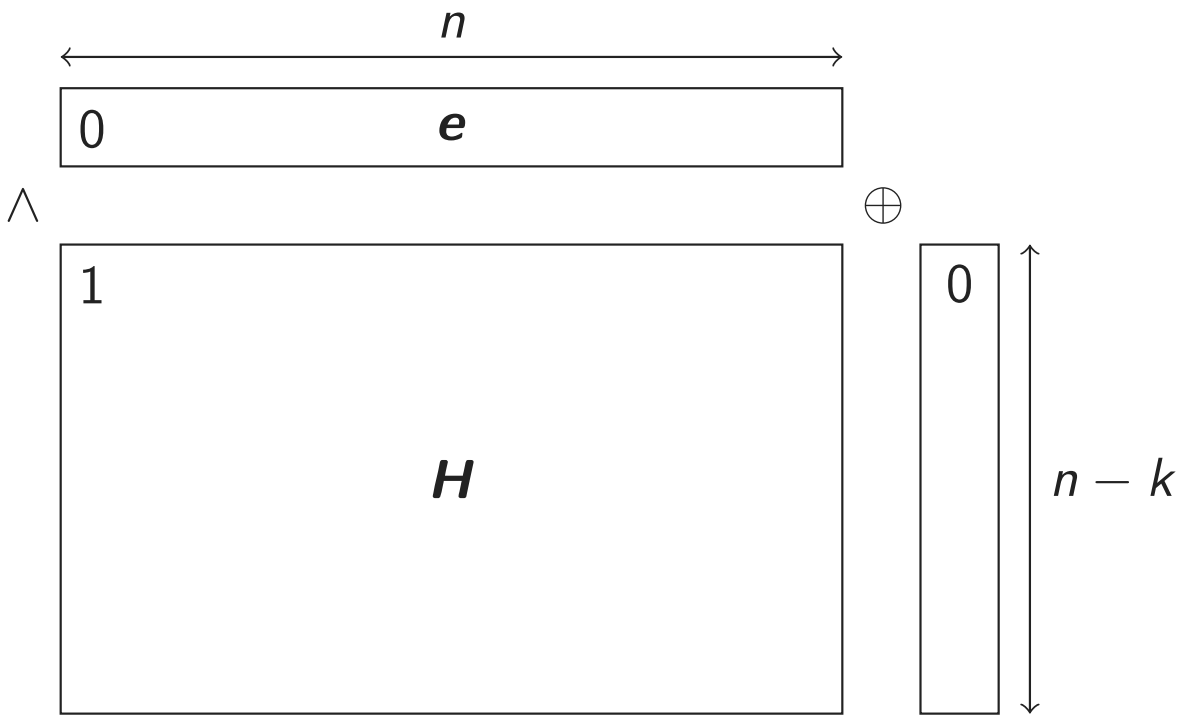
1: Generate a uniform random vector $\boldsymbol{e} \in \mathbb{F}_2^n$ with $\mathrm{HW}(\boldsymbol{e}) = t$.
2: Compute $\boldsymbol{c} \leftarrow \boldsymbol{H}\boldsymbol{e}$ ▷ target operation/encode
3: Compute $K \leftarrow \mathrm{H}(1 \,\|\, \boldsymbol{e} \,\|\, \boldsymbol{c})$ ▷ session key
4: **return** $(\boldsymbol{c}, K)$

$\boldsymbol{e}$ recovered $\Rightarrow$ confidentiality over

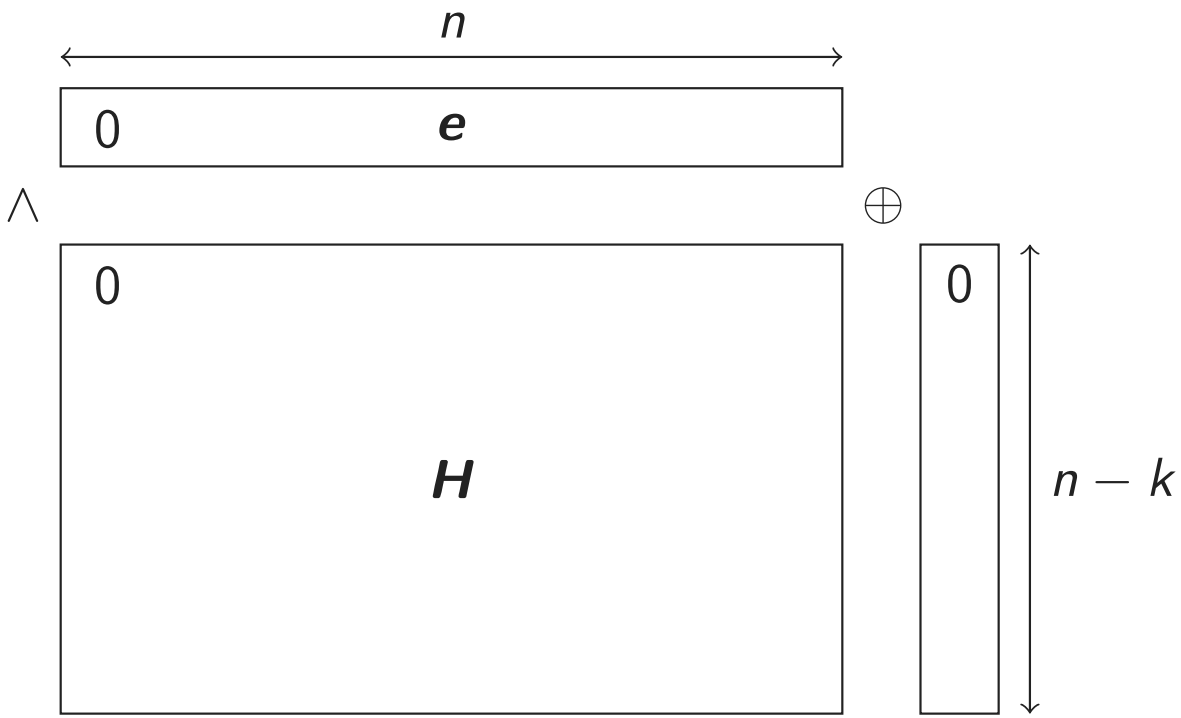
Binary matrix-vector product



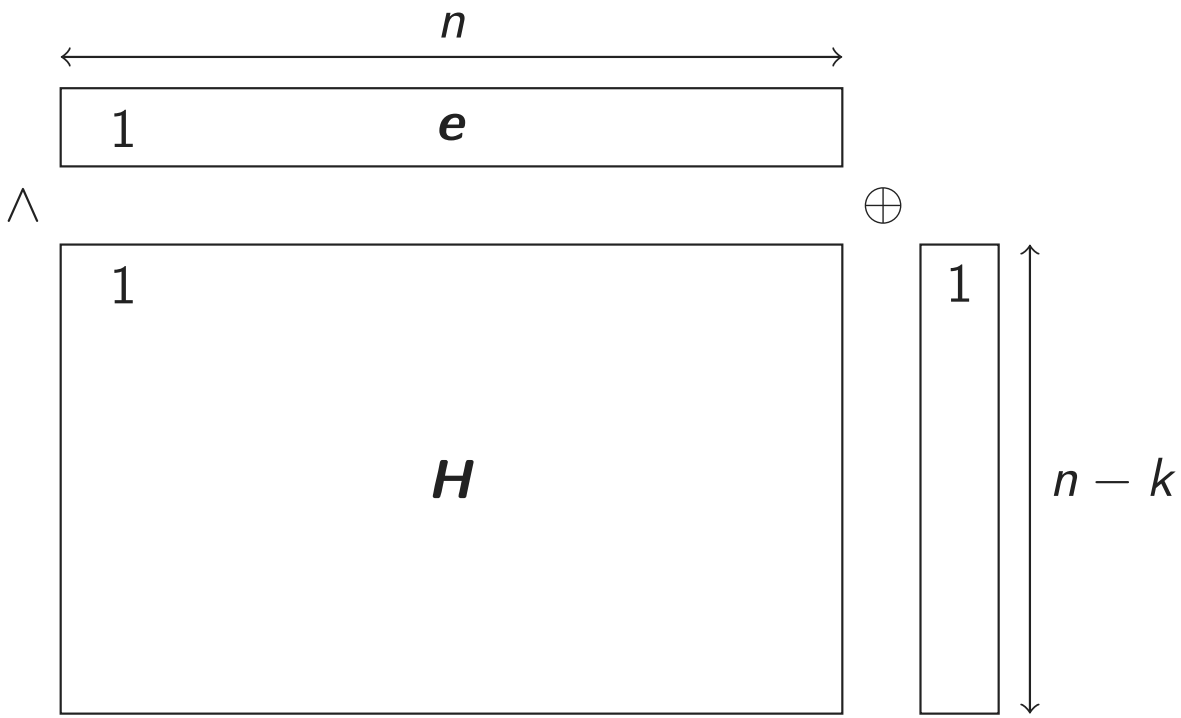
Binary matrix-vector product



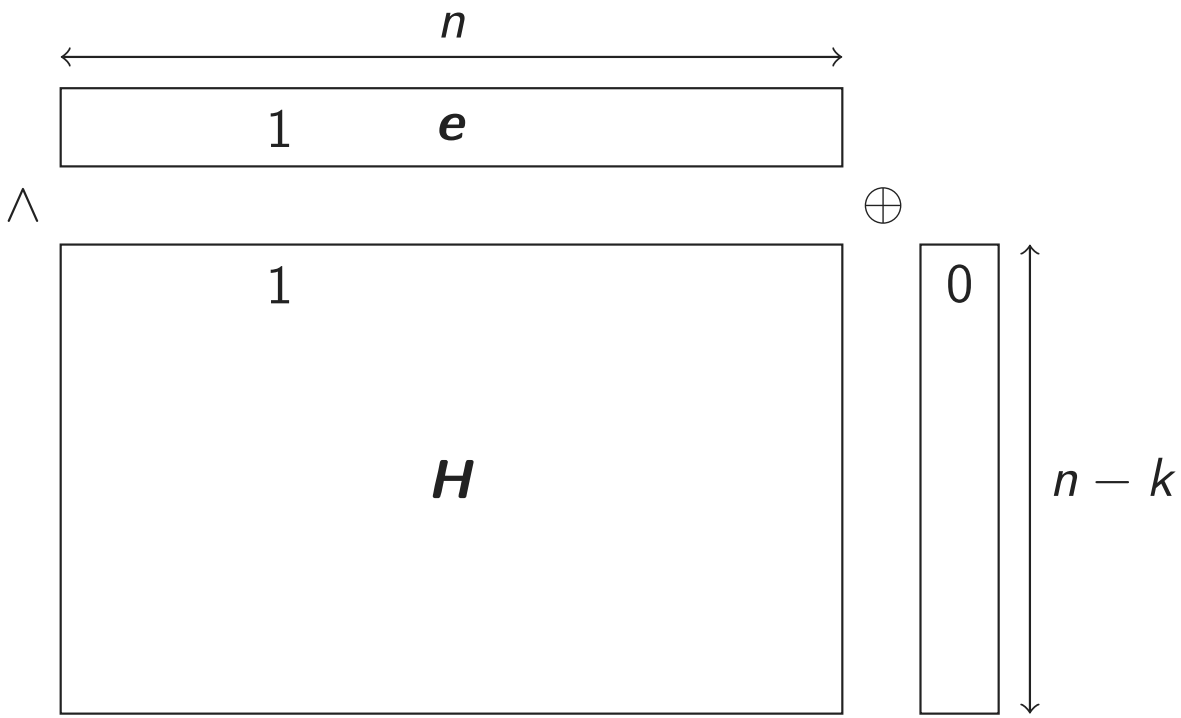
Binary matrix-vector product



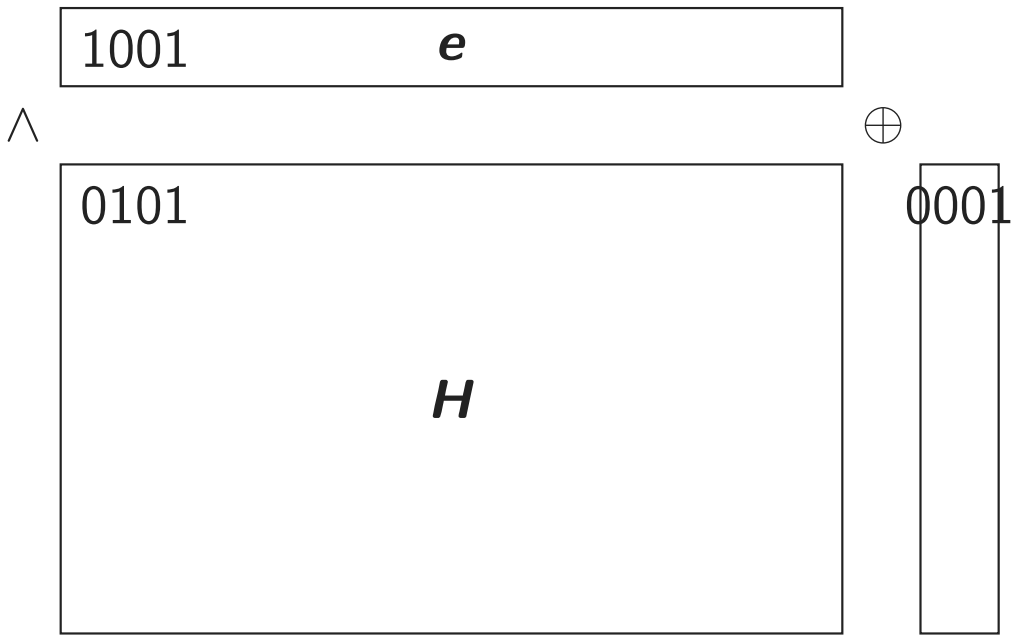
Binary matrix-vector product



Binary matrix-vector product

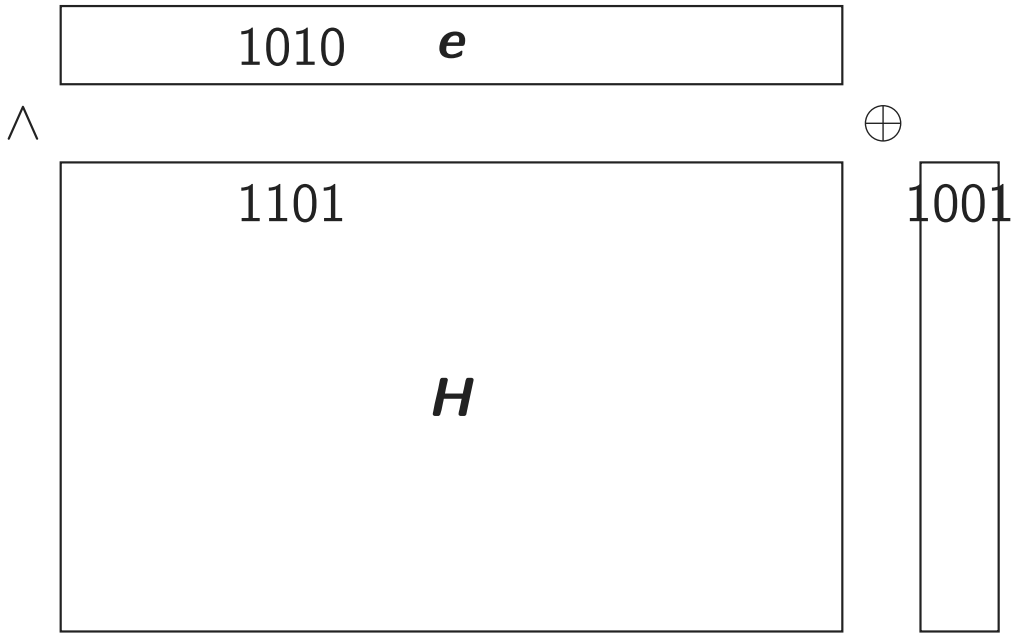


Packed binary matrix-vector product



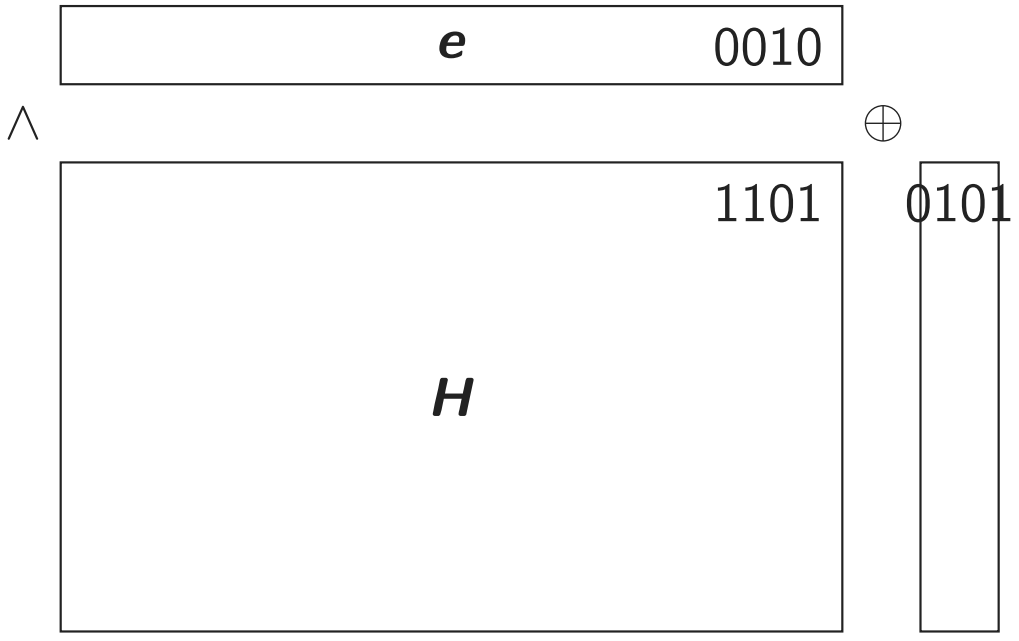
Main idea: use parallelism and register size w

Packed binary matrix-vector product



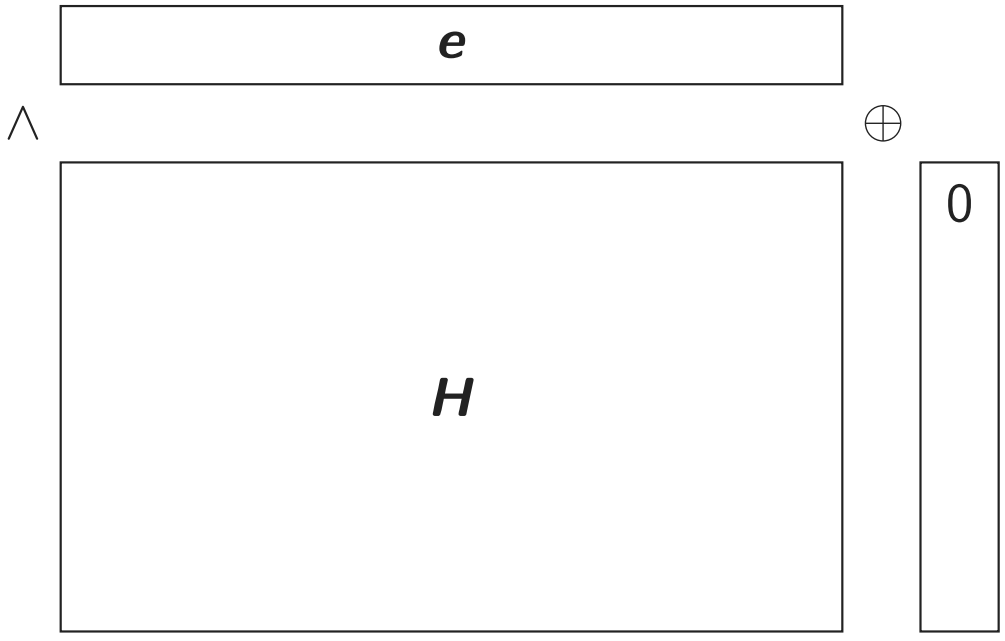
Main idea: use parallelism and register size w

Packed binary matrix-vector product



Main idea: use parallelism and register size w

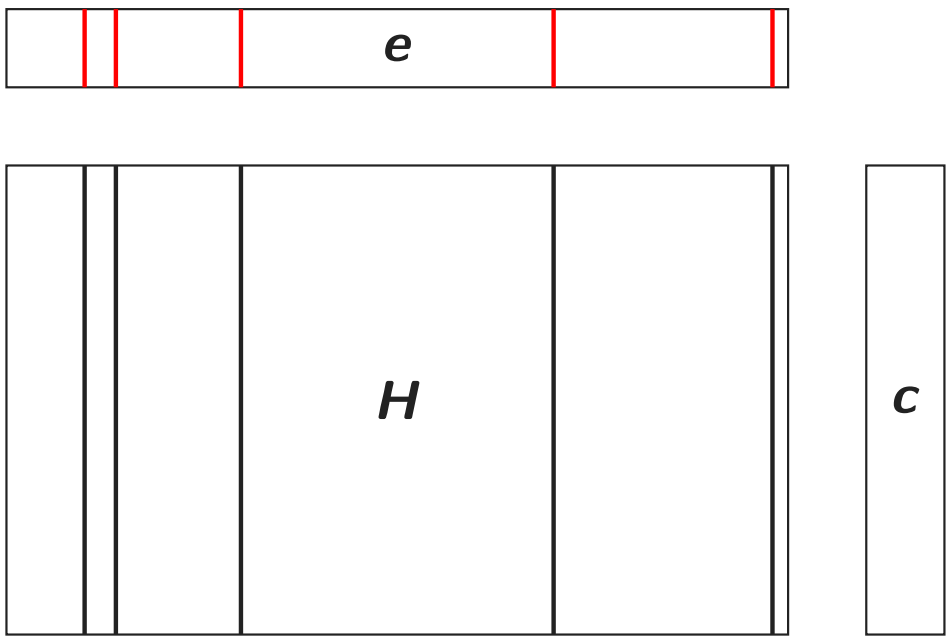
Packed binary matrix-vector product



Main idea: use parallelism and register size w

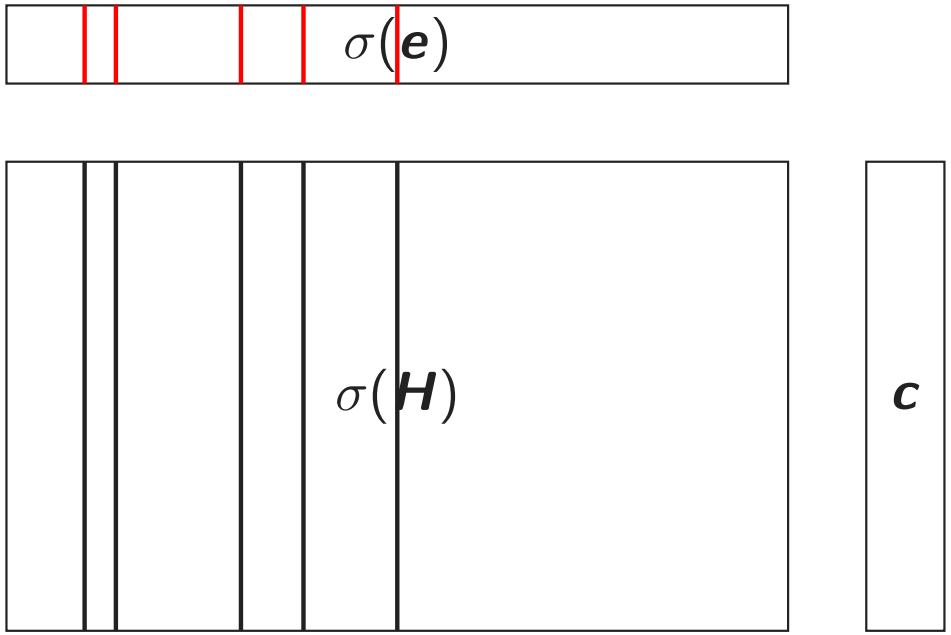
Security

- From $\boldsymbol{c}$ and $\boldsymbol{H}$ hard to find $\boldsymbol{e}$ of weight t, s.t. $\boldsymbol{He} = \boldsymbol{c}$



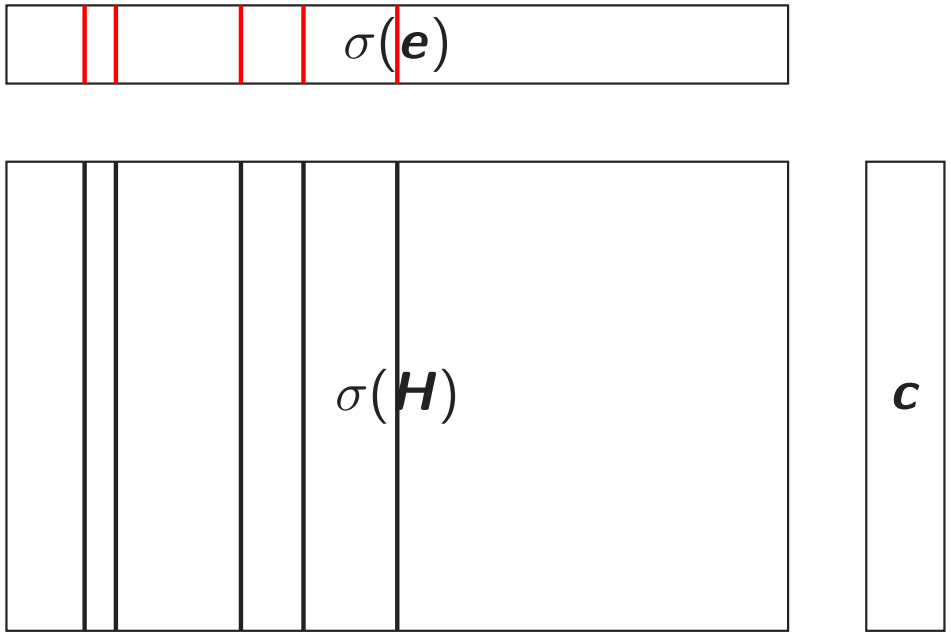
Security

- From $\boldsymbol{c}$ and $\boldsymbol{H}$ hard to find $\boldsymbol{e}$ of weight t, s.t. $\boldsymbol{He} = \boldsymbol{c}$
- Information Set Decoding strategy [Pra62]: find columns in the support of the vector $\boldsymbol{e}$ and perform Gaussian elimination



Security

- From $\boldsymbol{c}$ and $\boldsymbol{H}$ hard to find $\boldsymbol{e}$ of weight t, s.t. $\boldsymbol{He} = \boldsymbol{c}$
- Information Set Decoding strategy [Pra62]: find columns in the support of the vector $\boldsymbol{e}$ and perform Gaussian elimination



- Improvements allow some omissions on the left part

Previous physical attacks

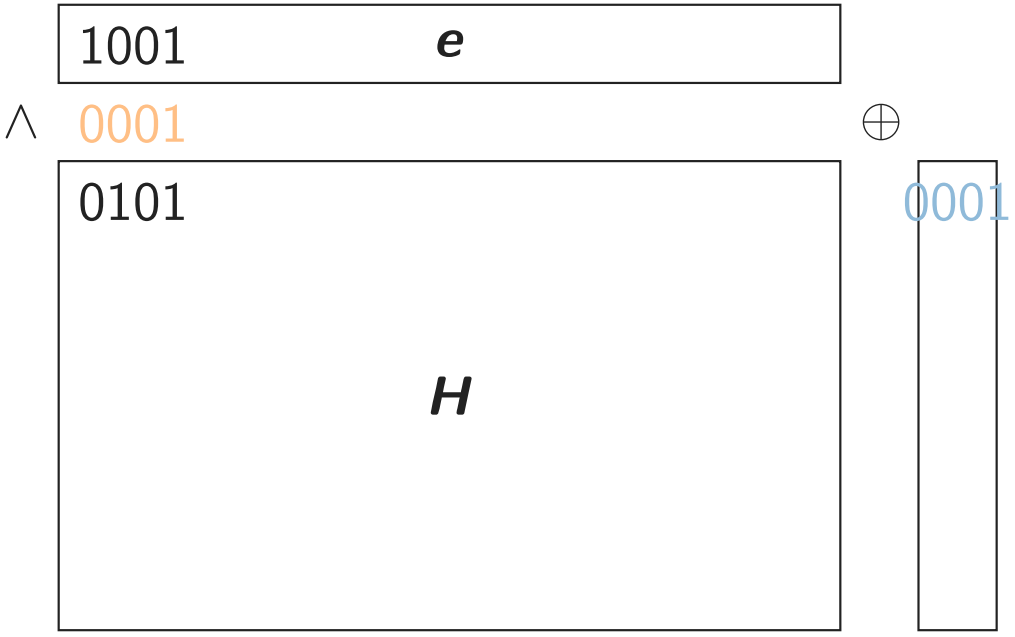
- Fault attacks [CCD+21]:
  - change field operations from XOR to add in $\mathbb{N}$
  - use ILP to solve the $\mathbb{N}$ – SDP
  - limited to schoolbook multiplication (not packed)
- Side-channel attacks [CDCG22]:
  - recover the Hamming weights of intermediate results
  - combine information to obtain an erroneous $\mathbb{N}$ – SDP
  - use quantitative group testing and ISD

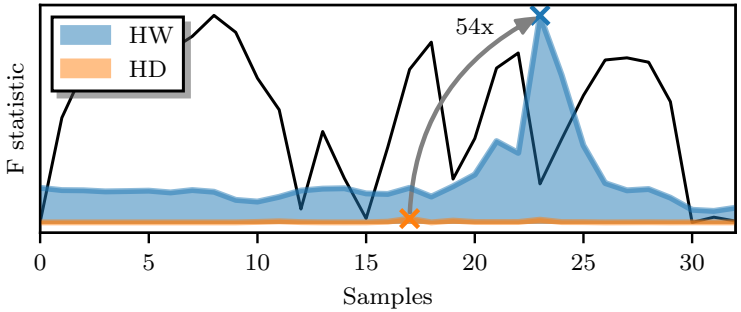
Application range

	$w = 1$	$w = 8$	$w = 32$	$w = 64$
Fault attack				
Side-channel attack				
small noise	N/A			
medium noise	N/A			
large noise	N/A			

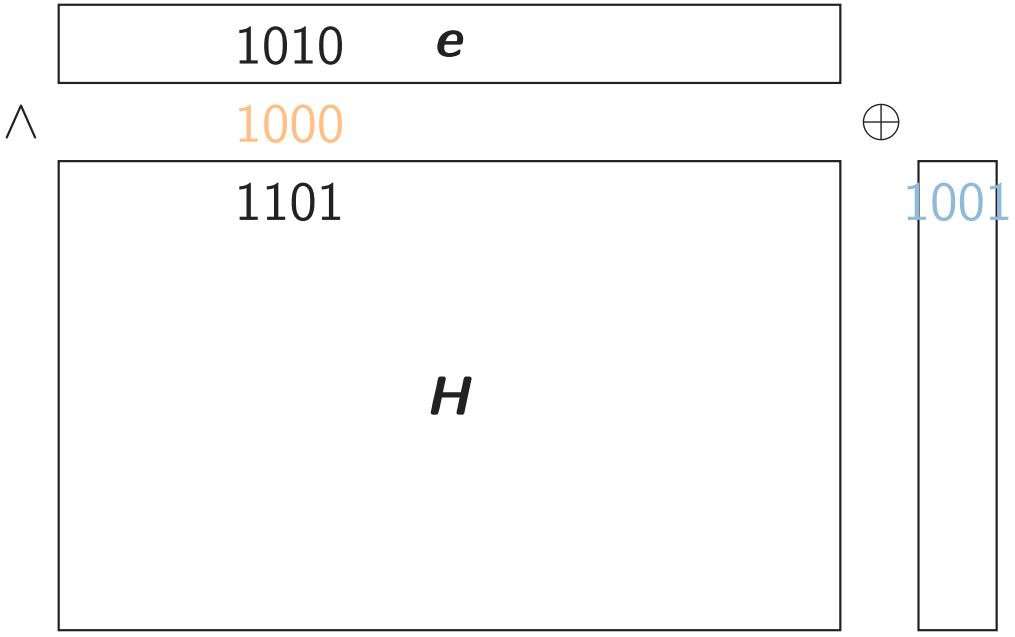
Errors analysis

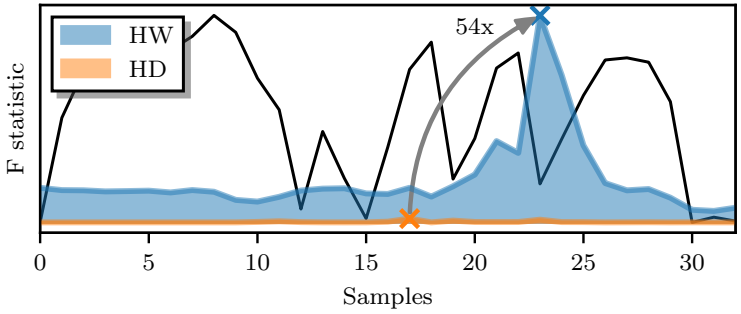
Available leakages





Available leakages

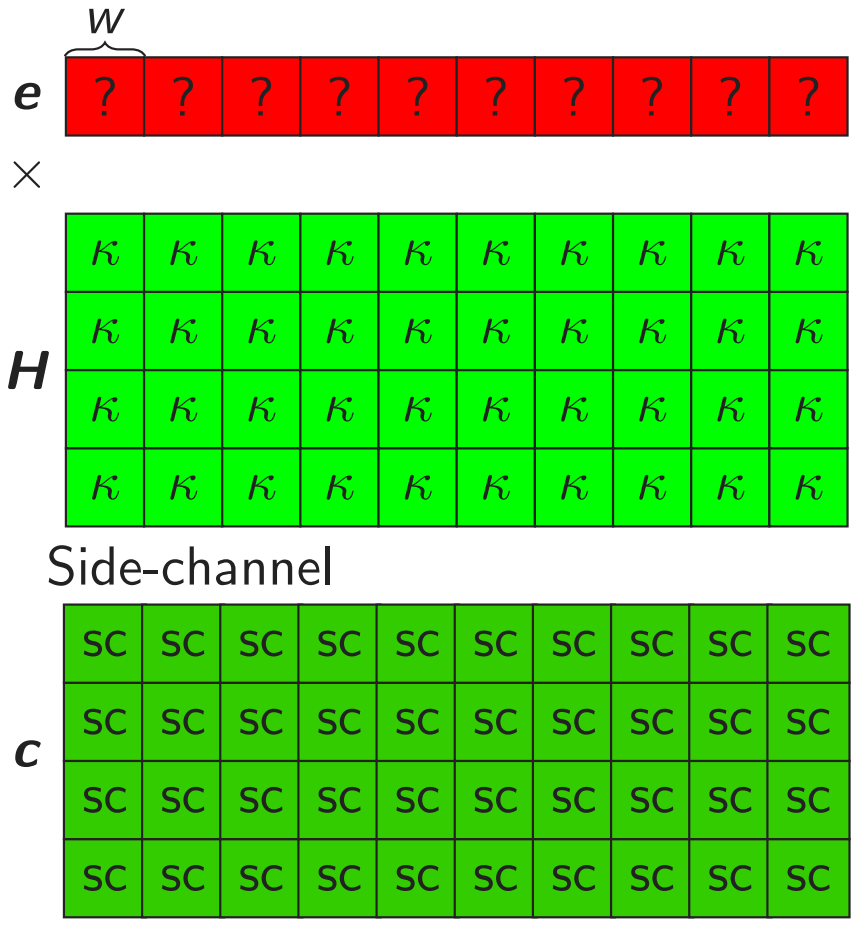




$$\widetilde{s_i} = \sum_{j=1}^{\frac{n}{w}} |\widetilde{\mathrm{HW}}(\boldsymbol{b}_{i,j-1}) - \widetilde{\mathrm{HW}}(\boldsymbol{b}_{i,j})|$$

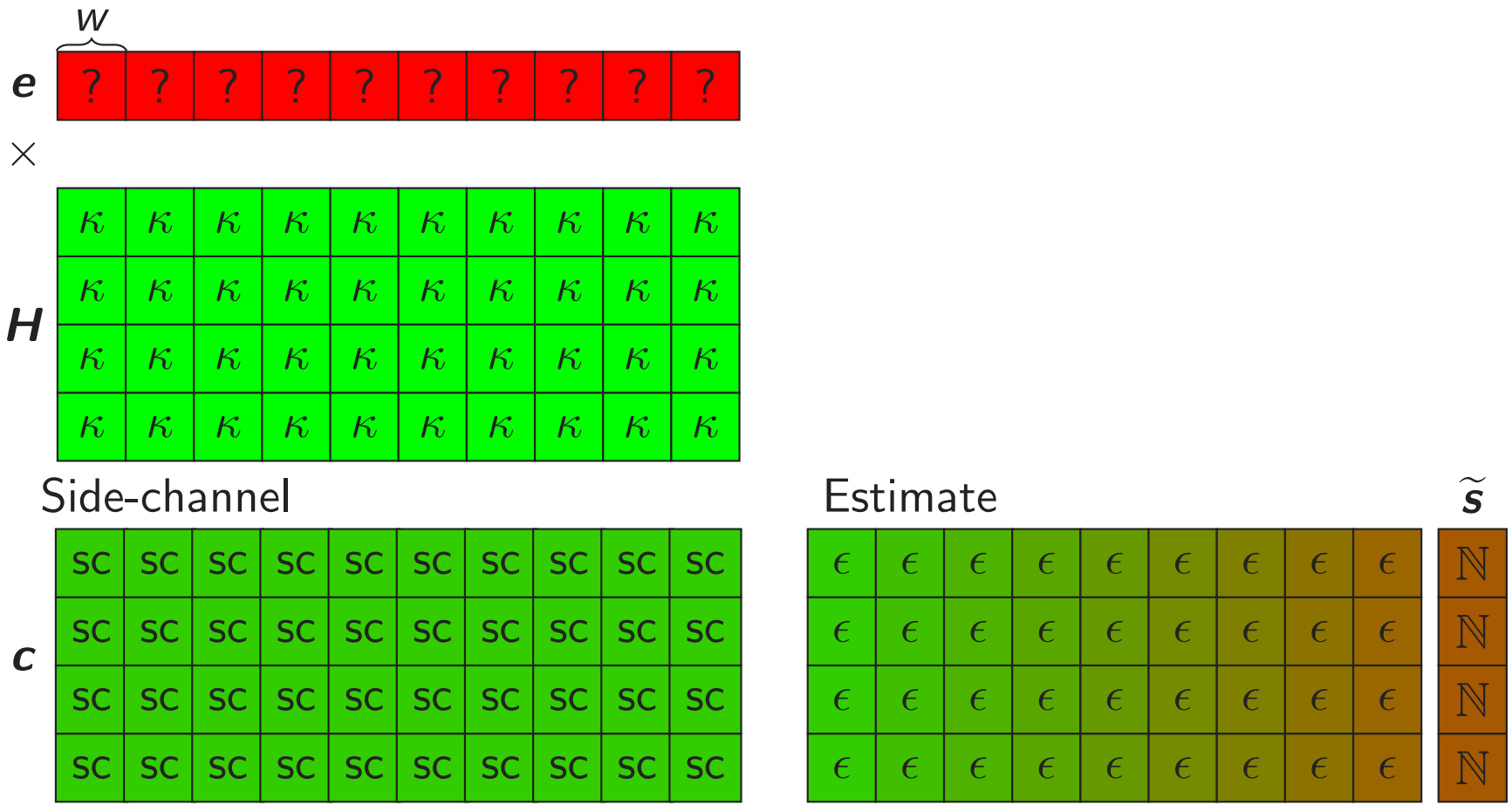
Limitations of previous side-channel attack: estimation

Limitations of previous side-channel attack: estimation



- Side-channel error

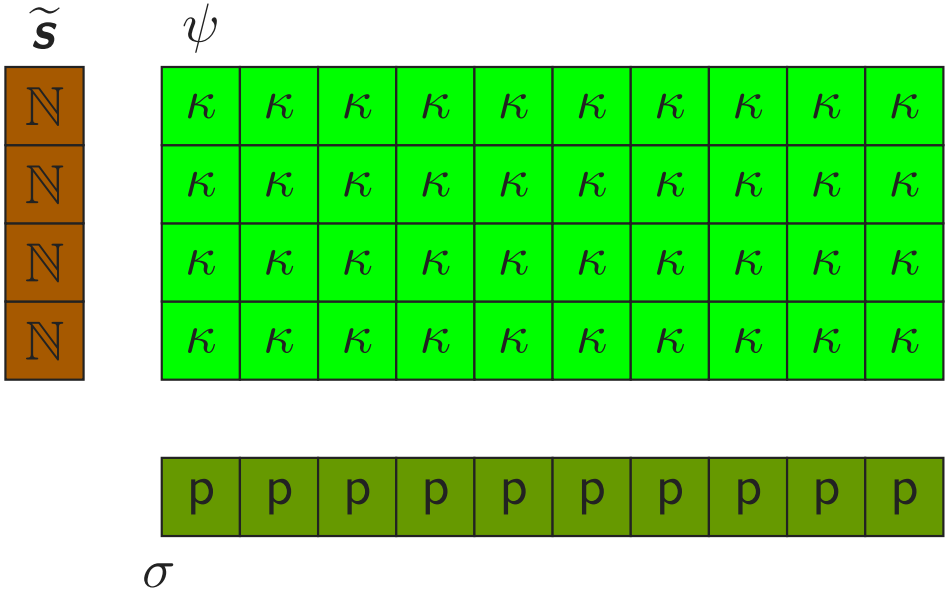
Limitations of previous side-channel attack: estimation



- Side-channel error
- Double cancellation (Hamming weight to Hamming distance), affects several coordinates of $\widetilde{s}$

Limitations of previous side-channel attack: score computation

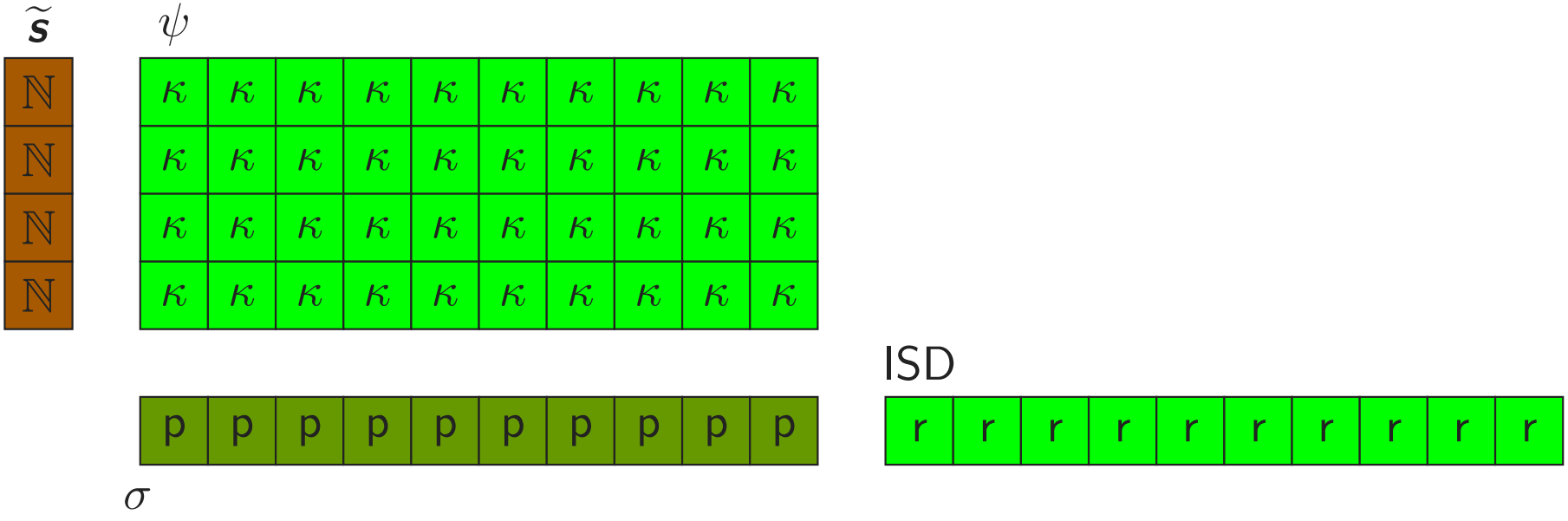
$$\forall j \in [\![1, n]\!], \quad \psi_j(\widetilde{\boldsymbol{s}}) = \boldsymbol{H}_{.,j} \cdot \widetilde{\boldsymbol{s}} + (1 - \boldsymbol{H}_{.,j}) \cdot (\boldsymbol{t} - \widetilde{\boldsymbol{s}})$$



- Error on one coordinate of the syndrome impacts the score of all columns

Limitations of previous side-channel attack: score computation

$$\forall j \in [\![1, n]\!], \quad \psi_j(\widetilde{\boldsymbol{s}}) = \boldsymbol{H}_{.,j} \cdot \widetilde{\boldsymbol{s}} + (1 - \boldsymbol{H}_{.,j}) \cdot (\boldsymbol{t} - \widetilde{\boldsymbol{s}})$$



- Error on one coordinate of the syndrome impacts the score of all columns

Punctured Matrices

New methods: key idea

- Columns that do not belong to the support of $\boldsymbol{e}$ **do not impact** the $\boldsymbol{c}$ computation
- Divide-and-conquer approach
  - Double cancellation limited impact
  - Better resistance to local error

Punctured block

$$\mathrm{HW}(\boldsymbol{e}) << n$$

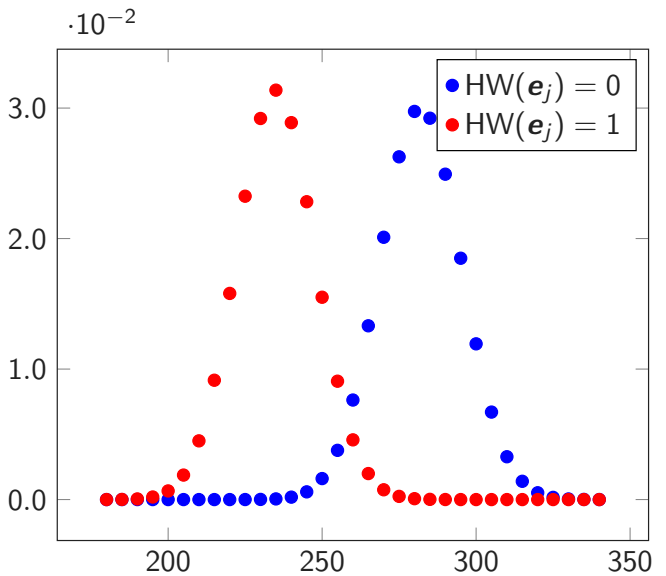
- If a block $\boldsymbol{e}_i = 0 \Rightarrow$ the intermediate results should not change for every row
- If a block $\boldsymbol{e}_i \neq 0 \Rightarrow$ the intermediate results should change for half of the rows
- Probability of a block $\boldsymbol{e}_i = 0$ decrease with the register size w

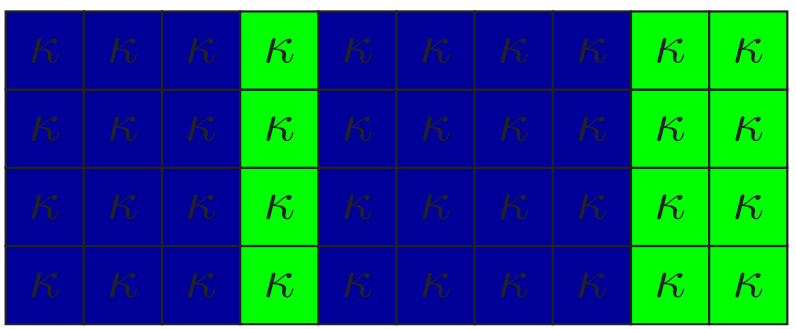
	$w = 8$	$w = 32$	$w = 64$
$(n, k, t) = (3488, 2720, 64)$	0.86	0.55	0.30
$(n, k, t) = (8192, 6528, 128)$	0.88	0.60	0.37

Distribution $e_i = 0$ or $\neq 0$

$$\#0 \in |\widetilde{\mathrm{HW}}(\boldsymbol{b}_{i,j-1}) - \widetilde{\mathrm{HW}}(\boldsymbol{b}_{i,j})|$$

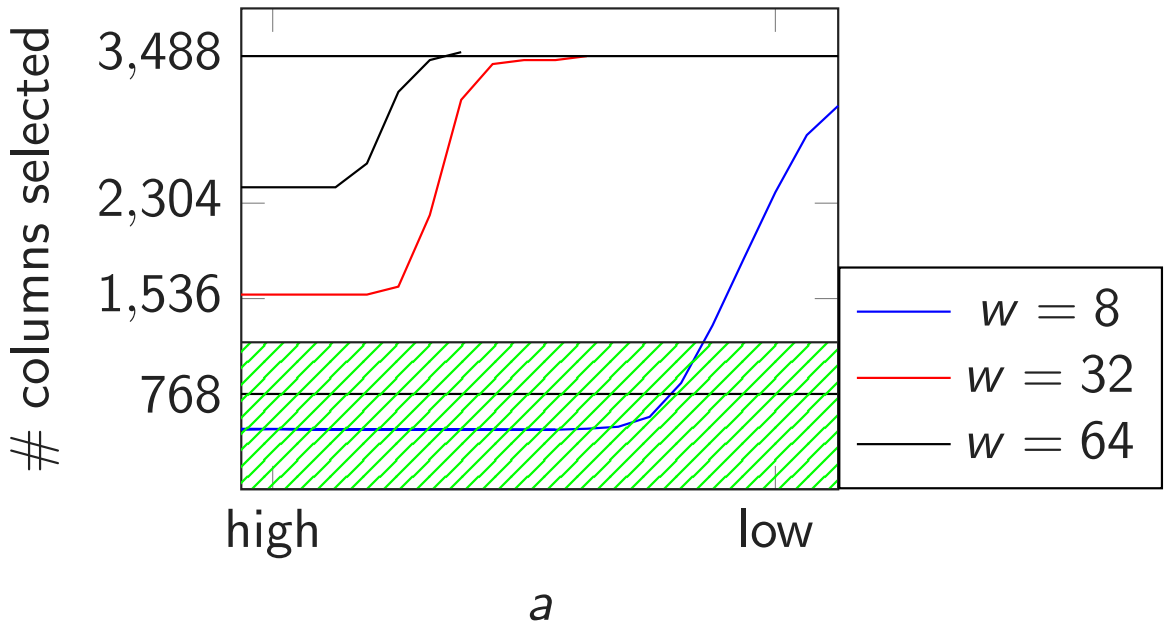
	$\mathrm{HW}(\boldsymbol{e}_j) = 0$	$\mathrm{HW}(\boldsymbol{e}_j) = 1$
First column	$\mathcal{B}(n-k, a)$	$\mathcal{B}\left(n-k, \frac{1+a}{4}\right)$
Other columns	$\mathcal{B}\left(n-k, a^2 + \frac{(1-a)^2}{2}\right)$	$\mathcal{B}\left(n-k, \frac{1+a^2}{4}\right)$





T-test separation plus feature selection

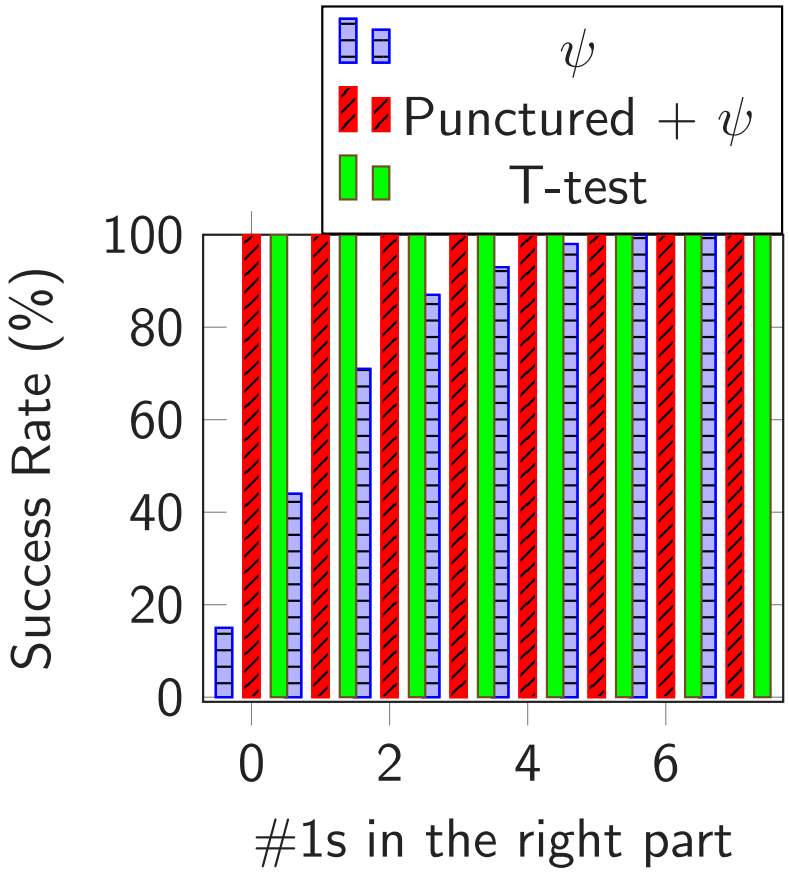
- For large register size, the puncture method does not remove enough columns
- System too large for efficient ISD



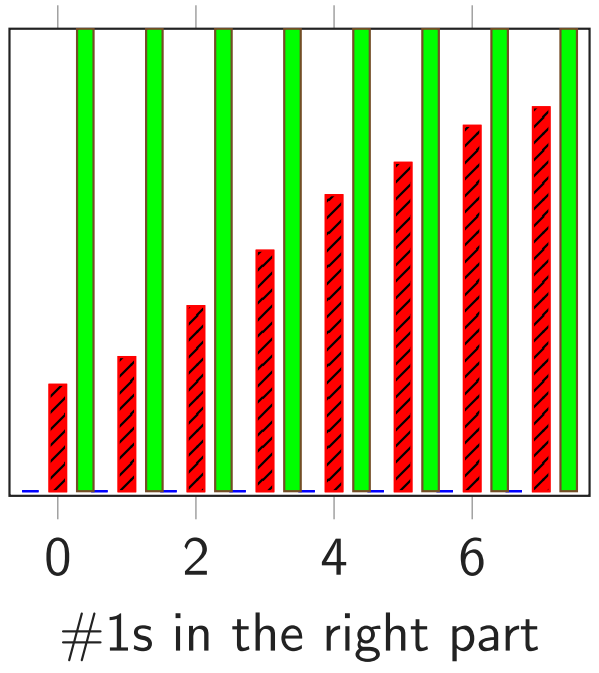
- Use the knowledge of the columns of the public matrix $\boldsymbol{H}$
- Perform feature selection via T-test

Results

Noise impact

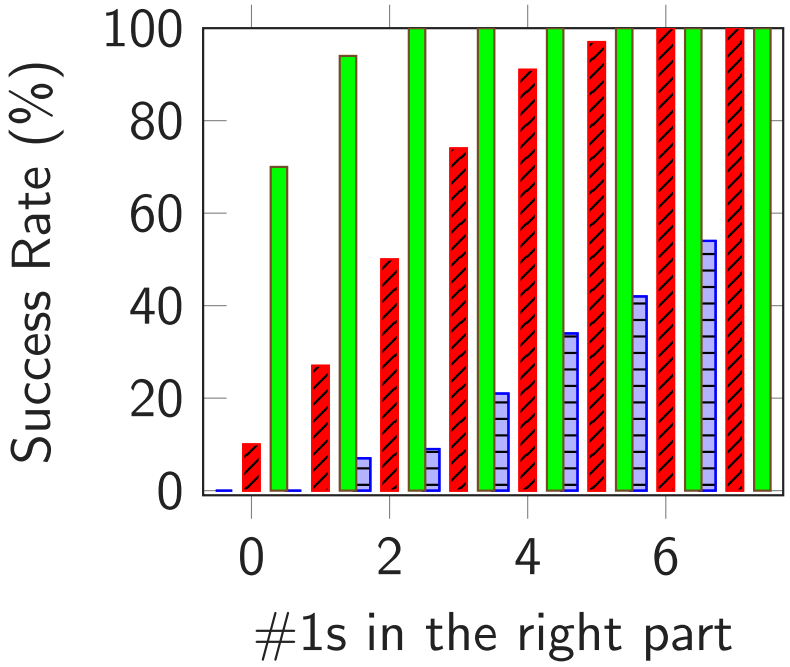


Medium noise, medium accuracy

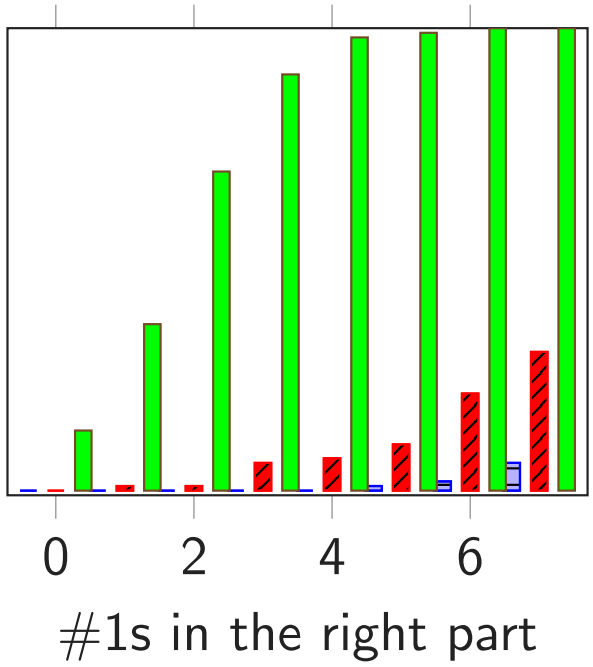


High noise, low accuracy

Register size impact

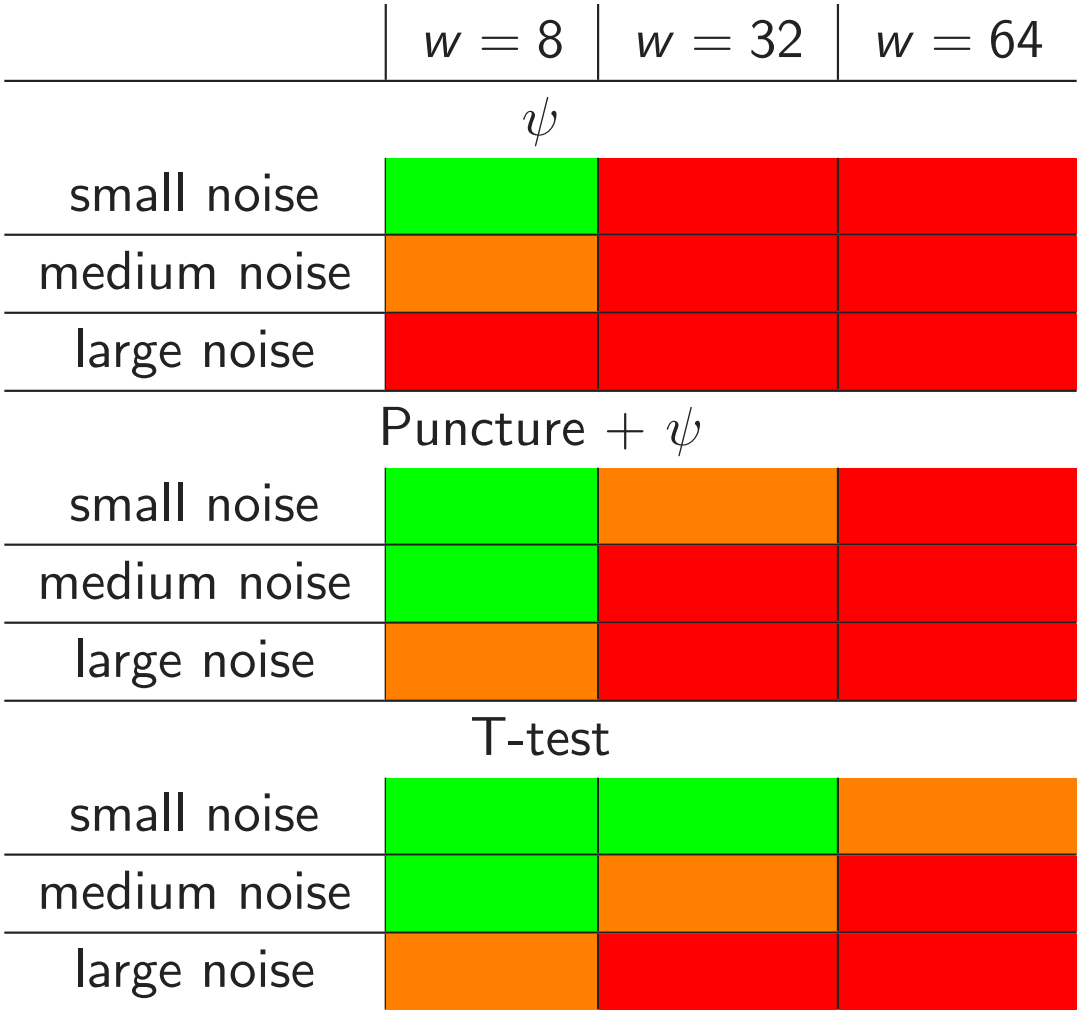


$w = 32$



$w = 64$

Application range



Conclusion

- More efficient attacks for large noise/large register
- Divide-and-conquer approach
- Exploit knowledge of the public matrix
- Algebraic attack to exploit leakages from different steps in the KEM (matrix-vector product + hashing+ generate $\boldsymbol{e}$)
- Unprofiled attack
- Masking countermeasure (no more low-weight)
- Long-term secret attack

Thanks for your attention!

References i

Pierre-Louis Cayrel, Brice Colombier, Vlad-Florin Dragoi, Alexandre Menu, and Lilian Bossuet.

Message-recovery laser fault injection attack on the Classic McEliece cryptosystem.

In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 438–467. Springer, 2021.

References ii

Brice Colombier, Vlad-Florin Dragoi, Pierre-Louis Cayrel, and Vincent Grosso.
Profiled side-channel attack on cryptosystems based on the binary syndrome decoding problem.
IEEE Trans. Inf. Forensics Secur., 17:3407–3420, 2022.

Eugene Prange.
The use of information sets in decoding cyclic codes.
IRE Trans. Inf. Theory, 8(5):5–9, 1962.