# Syndrome Decoding with Hints

Letizia D'Achille[1] Andre Esser[2] Nicolai Kraus[1]

[1]Ruhr University Bochum, Germany
[2]Technology Innovation Institute, UAE

Selected Areas in Cryptography 2026
Ottawa, Canada, 27.08.2026

# Outline

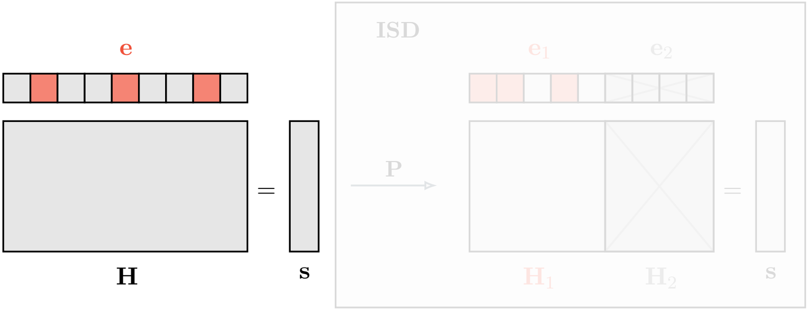
1. Preliminaries
   - Syndrome decoding and Information Set Decoding (ISD)
   - Approximate and perfect hints
2. Our contribution
   - From hints to reliabilities
   - Hint-ISD: biased permutations
3. Experiments and practical impact on HQC and McEliece

# Syndrome decoding problem and ISD

## Syndrome Decoding Problem (SDP)

Given $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_2^{n-k}$ and weight $t$, find

$$\mathbf{e} \in \mathbb{F}_2^n, \qquad |\mathbf{e}| = t, \qquad \mathbf{He} = \mathbf{s}.$$

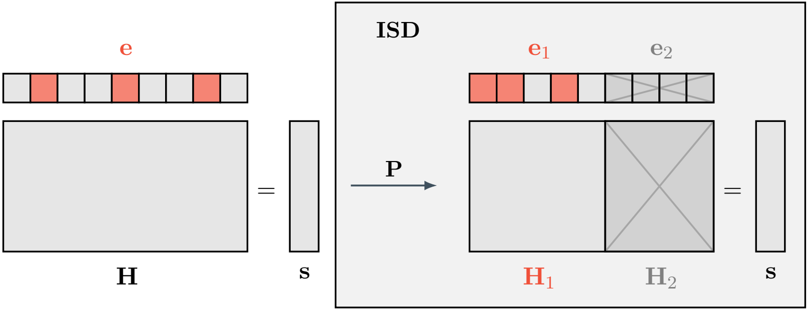


# Syndrome decoding problem and ISD

## Syndrome Decoding Problem (SDP)

Given $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_2^{n-k}$ and weight $t$, find

$$\mathbf{e} \in \mathbb{F}_2^n, \qquad |\mathbf{e}| = t, \qquad \mathbf{H}\mathbf{e} = \mathbf{s}.$$



# Hints

## Approximate hint

For a row $\mathbf{h}$ of $\mathbf{H}$, we obtain

$$\langle \mathbf{h}, \mathbf{e} \rangle + \varepsilon = z \in \mathbb{N}, \qquad \varepsilon \sim \mathcal{D}.$$

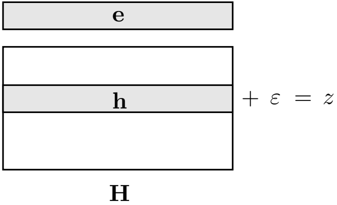
We call $(\mathbf{h}, z)$ an *approximate hint.*

## Perfect hint

Special case $\varepsilon = 0$:

$$\langle \mathbf{h}, \mathbf{e} \rangle = z \in \mathbb{N}.$$

We call $(\mathbf{h}, z)$ a *perfect hint.*



# Hints

## Approximate hint

For a row $\mathbf{h}$ of $\mathbf{H}$, we obtain

$$\langle \mathbf{h}, \mathbf{e} \rangle + \varepsilon = z \in \mathbb{N}, \qquad \varepsilon \sim \mathcal{D}.$$

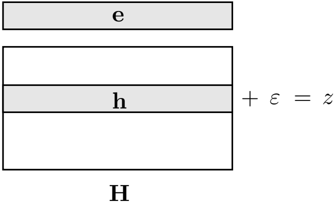
We call $(\mathbf{h}, z)$ an *approximate hint.*

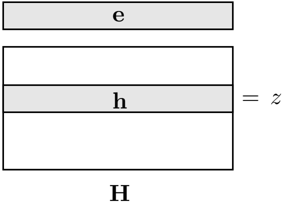
## Perfect hint

Special case $\varepsilon = 0$:

$$\langle \mathbf{h}, \mathbf{e} \rangle = z \in \mathbb{N}.$$

We call $(\mathbf{h}, z)$ a *perfect hint.*



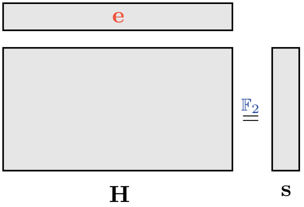
## Syndrome Decoding Problem

Given

- $(\mathbf{H}, \mathbf{s})$ an instance of SDP;

Find

$$\mathbf{e} \in \mathbb{F}_2^n, \qquad |\mathbf{e}| = t, \qquad \mathbf{H}\mathbf{e} = \mathbf{s} \text{ on } \mathbb{F}_2,$$



# SDP with Hints

## Syndrome Decoding Problem with Hints

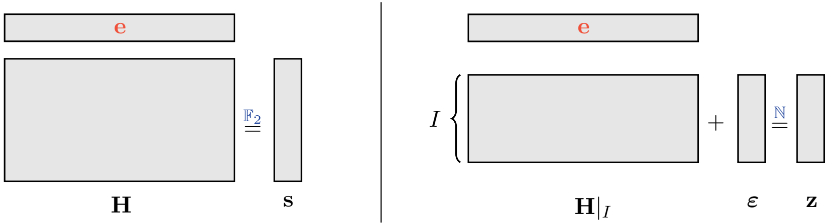
Given

- $(\mathbf{H}, \mathbf{s})$ an instance of SDP;
- hints $\langle \mathbf{h}, \mathbf{e} \rangle + \varepsilon = z$ for $\mathbf{h} \in I$, where $\varepsilon \sim \mathcal{D}$.

Find

$$\mathbf{e} \in \mathbb{F}_2^n, \qquad |\mathbf{e}| = t, \qquad \mathbf{He} = \mathbf{s} \text{ on } \mathbb{F}_2,$$

$$\mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon} = \mathbf{z} \text{ on } \mathbb{N}.$$



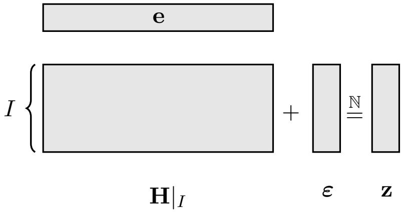
# Scoring and score distribution

## Goal

Use the hints

$$\mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon} = \mathbf{z}$$

to optimize the choice of $\mathbf{P}$.




## Score of a coordinate $i$ [FL20]

$$\psi_i(\mathbf{z}) = \langle \mathbf{h}_i|_I, \mathbf{z} \rangle + \langle \mathbf{1}^m - \mathbf{h}_i|_I, t\mathbf{1}^m - \mathbf{z} \rangle$$

**Intuition:** if $i \in \mathrm{Supp}(\mathbf{e})$, $\mathbf{h}_i|_I$ contributes to $\mathbf{z} \Rightarrow$ larger $\psi_i(\mathbf{z})$.

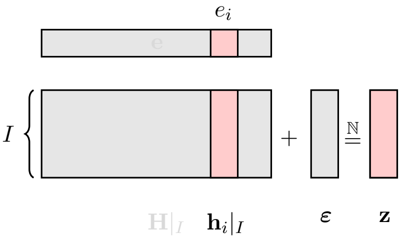
# Scoring and score distribution

**Goal**

Use the hints

$$\mathbf{H}|_I\mathbf{e} + \boldsymbol{\varepsilon} = \mathbf{z}$$

to optimize the choice of $\mathbf{P}$.




**Score of a coordinate $i$ [FL20]**

$$\psi_i(\mathbf{z}) = \langle \mathbf{h}_i|_I, \mathbf{z}\rangle + \langle \mathbf{1}^m - \mathbf{h}_i|_I, t\mathbf{1}^m - \mathbf{z}\rangle$$

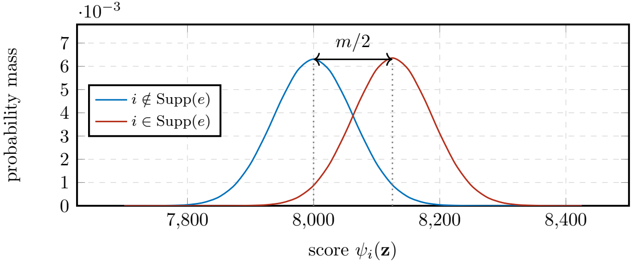
**Intuition:** if $i \in \mathrm{Supp}(\mathbf{e})$, $\mathbf{h}_i|_I$ contributes to $\mathbf{z} \Rightarrow$ larger $\psi_i(\mathbf{z})$.

# Scoring and score distribution

## Score of a coordinate $i$ [FL20]

We actually use for $|I| = m$

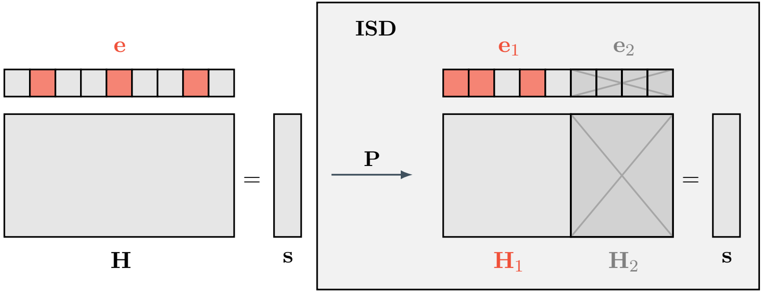
$$\psi_i(\mathbf{z}) = \langle \mathbf{h}_i|_I, \mathbf{z}\rangle + \langle \mathbf{1}^m - \mathbf{h}_i|_I, t\mathbf{1}^m - \mathbf{z}\rangle$$




**Key idea:** Larger score $\Rightarrow$ coordinate $i$ is more likely in $\mathrm{Supp}(\mathbf{e})$.

# Integrate ISD with reliabilities: Hint-ISD

**Recall: ISD chooses P at random**



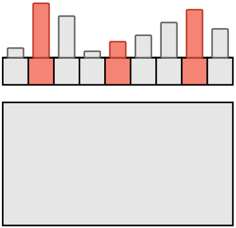
# Integrate ISD with reliabilities: Hint-ISD

Hints $\mathbf{z} = \mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon}$ → Scores $\psi_i(\mathbf{z})$ → Reliabilities $r_i$ → Hint-ISD

## Reliability

$$r_i := \Pr[i \in \mathrm{Supp}(\mathbf{e}) \mid \psi_i(\mathbf{z})]$$

$\mathbf{r}$



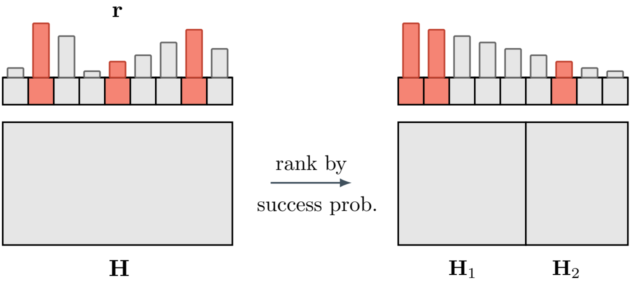
$\mathbf{H}$

$\xrightarrow{?}$

how to choose $\mathbf{P}$ from $\mathbf{r}$?

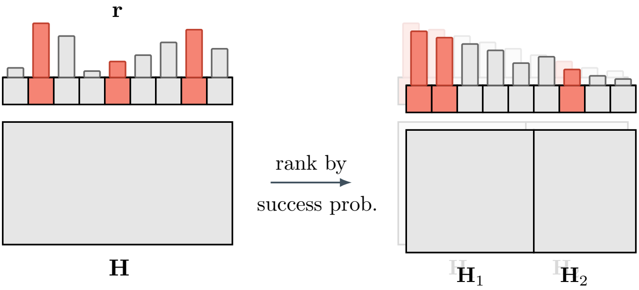
# Integrate ISD with reliabilities: Hint-ISD

Hints $\mathbf{z} = \mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon}$ → Scores $\psi_i(\mathbf{z})$ → Reliabilities $r_i$ → **Hint-ISD**



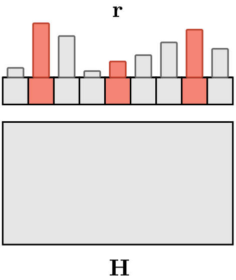
# Integrate ISD with reliabilities: Hint-ISD

Hints $\mathbf{z} = \mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon}$ → Scores $\psi_i(\mathbf{z})$ → Reliabilities $r_i$ → **Hint-ISD**

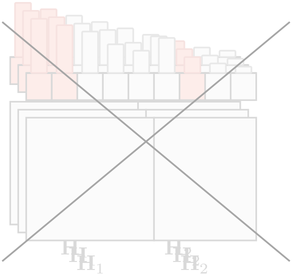


# Integrate ISD with reliabilities: Hint-ISD

Hints $\mathbf{z} = \mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon}$ → Scores $\psi_i(\mathbf{z})$ → Reliabilities $r_i$ → **Hint-ISD**




rank by → success prob.

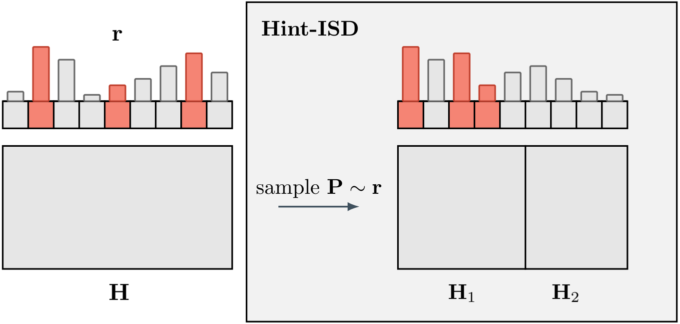



**exponentially many!**

**Open problem:** can this be done efficiently?

# Integrate ISD with reliabilities: Hint-ISD

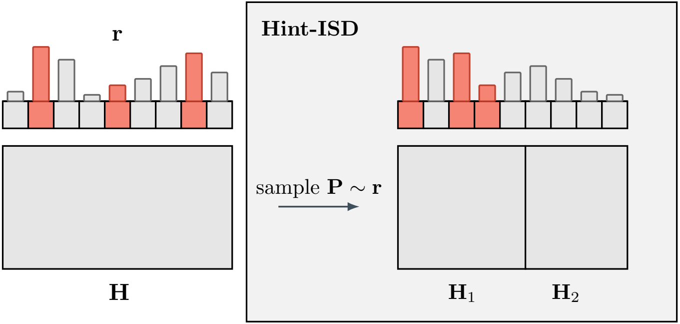
Hints $\mathbf{z} = \mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon}$ → Scores $\psi_i(\mathbf{z})$ → Reliabilities $r_i$ → **Hint-ISD**




**Feasible in practice!**

# Integrate ISD with reliabilities: Hint-ISD

Hints $\mathbf{z} = \mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon}$ → Scores $\psi_i(\mathbf{z})$ → Reliabilities $r_i$ → **Hint-ISD**

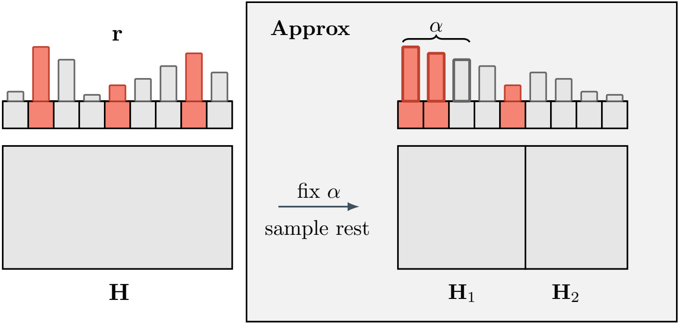



## Feasible in practice!

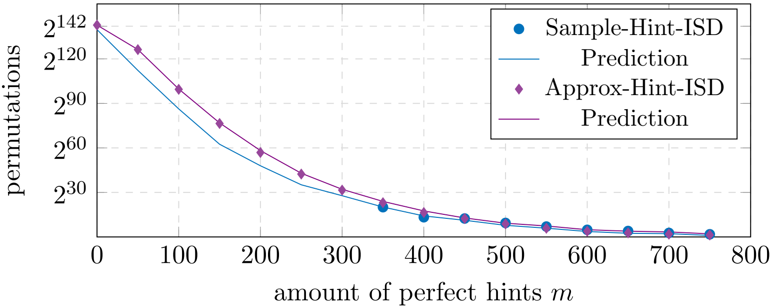
but estimating the running time requires knowing $\mathbf{e}$

# Integrate ISD with reliabilities: Hint-ISD

Hints $\mathbf{z} = \mathbf{H}|_I \mathbf{e} + \boldsymbol{\varepsilon}$ → Scores $\psi_i(\mathbf{z})$ → Reliabilities $r_i$ → **Hint-ISD**



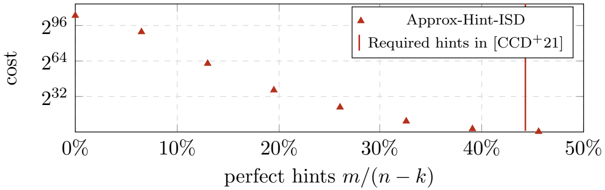
# Validating approximation



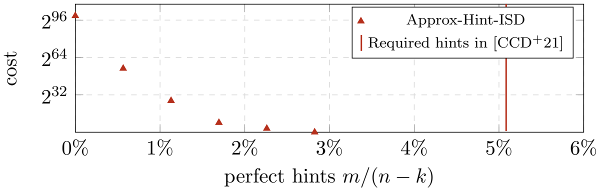

**Remark:** Hint-ISD can be integrated with any ISD variant.

# Practical results - Perfect hints

**McEliece.**




**HQC.**



# Conclusions

**Key takeaways.**

1. Scores can be converted into reliabilities.
2. Reliabilities can be integrated into ISD.
3. Hint-ISD gives non-trivial speedups for *any* hint exposure.
4. Hint-ISD interpolates between **classical ISD** and **polynomial-time decoding**.

**Additional results.**

- Lower bound on hints required for polynomial-time decoding.
- Stern-based Hint-ISD.
- Experiments for approximate hints.
- Analysis for systematic matrices.

`eprint.iacr.org/2026/341`

Pierre-Louis Cayrel, Brice Colombier, Vlad-Florin Drăgoi, Alexandre Menu, and Lilian Bossuet.
Message-recovery laser fault injection attack on the classic mceliece cryptosystem.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 438–467. Springer, 2021.

Brice Colombier, Vlad-Florin Drăgoi, Pierre-Louis Cayrel, and Vincent Grosso.
Profiled side-channel attack on cryptosystems based on the binary syndrome decoding problem.
*IEEE Transactions on Information Forensics and Security*, 17:3407–3420, 2022.

Uriel Feige and Amir Lellouche.
Quantitative group testing and the rank of random matrices.
*arXiv preprint arXiv:2006.09074*, 2020.