Code-Based Cryptography

McEliece Cryptosystem

I. Márquez-Corbella

2. McEliece Cryptosystem

1. Formal Definition
2. Security-Reduction Proof
3. **McEliece Assumptions**
4. Notions of Security
5. Critical Attacks - Semantic Secure Conversions
6. Reducing the Key Size
7. Reducing the Key Size - LDPC codes
8. Reducing the Key Size - MDPC codes
9. Implementation

McEliece Assumptions

The security of the McEliece Cryptosystem is based in two assumptions:

McEliece Assumptions

The security of the McEliece Cryptosystem is based in two assumptions:

Assumption 1: Decoding a random linear code is a difficult problem.

McEliece Assumptions

The security of the McEliece Cryptosystem is based in two assumptions:

Assumption 1: Decoding a random linear code is a difficult problem.

Assumption 2: The generator matrix of a Goppa code looks random.

Syndrome Decoder

Given an $[n,k]_q$ code $\mathcal{C}$ with parity check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$.
Let $\mathbf{y} \in \mathbb{F}_q^n$ be the **received word**.

Minimum Dist. Decoding (MDD):

Find $\mathbf{x} \in \mathcal{C}$
such that $d_H(\mathbf{y}, \mathbf{x})$ is minimized.

Syndrome Decoding (SD):

Find $\mathbf{e} \in \mathbb{F}_q^n$ with
$H\mathbf{e} = H\mathbf{y}$ and $\mathrm{w}_H(\mathbf{e})$ is minimized.

In a linear code:
$d_H(\mathbf{x}, \mathbf{y}) = \mathrm{w}_H(\mathbf{x} - \mathbf{y}) = \mathrm{w}_H(\mathbf{e})$
if $\mathbf{y} = \mathbf{c} + \mathbf{e}$, i.e. $H\mathbf{y} = H\mathbf{e}$

Syndrome Decoder

Given an $[n, k]_q$ code $\mathcal{C}$ with parity check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$.
Let $\mathbf{y} \in \mathbb{F}_q^n$ be the **received word**.

Minimum Dist. Decoding (MDD):

Find $\mathbf{x} \in \mathcal{C}$
such that $d_H(\mathbf{y}, \mathbf{x})$ is minimized.

Syndrome Decoding (SD):

Find $\mathbf{e} \in \mathbb{F}_q^n$ with
$H\mathbf{e} = H\mathbf{y}$ and $\mathrm{w}_H(\mathbf{e})$ is minimized.

In a linear code:
$d_H(\mathbf{x}, \mathbf{y}) = \mathrm{w}_H(\mathbf{x} - \mathbf{y}) = \mathrm{w}_H(\mathbf{e})$
if $\mathbf{y} = \mathbf{c} + \mathbf{e}$, i.e. $H\mathbf{y} = H\mathbf{e}$

Minimal codewords:
Consider $\mathbf{y} = \mathbf{0} \in \mathbb{F}_q^n$

Find $\mathbf{w} \in \mathcal{C}$ i.e. $H\mathbf{e} = \mathbf{0}$
and $\mathrm{w}_H(\mathbf{w})$ is minimized.

The Syndrome Decoding (SD) problem

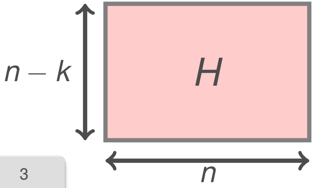
Assumption 1: Decoding a random linear code is a difficult problem.

The Syndrome Decoding (SD) problem

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Syndrome Decoding (SD) problem



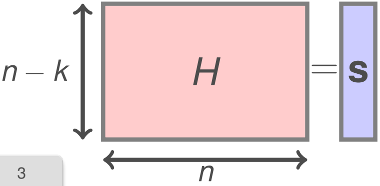
Input:

➜ A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Syndrome Decoding (SD) problem



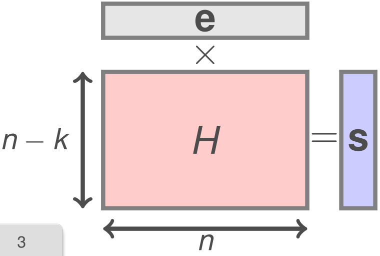
Input:

- A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Syndrome Decoding (SD) problem



Input:

- A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$
- A weight $w \in \mathbb{Z}$

The Syndrome Decoding (SD) problem

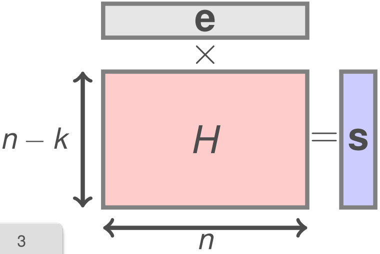
Assumption 1: Decoding a random linear code is a difficult problem.

The Syndrome Decoding (SD) problem

Output (Decision): Does $\mathbf{e} \in \mathbb{F}_2^n$ of $\mathrm{w}_H(\mathbf{e}) \leq w$ such that $\mathbf{e}H^T = \mathbf{s}$ exists? NP-complete

E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg.
On the Inherent Intractability of Certain Coding Problems.
IEEE Trans. Inf. Theory. Vol. 24, pp. 384-386, 1978.

A. Barg.
Complexity Issues in Coding Theory.
Chapter 7, in Handbock of Coding Theory, 1998.



Input:

- A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$
- A weight $w \in \mathbb{Z}$

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Syndrome Decoding (SD) problem

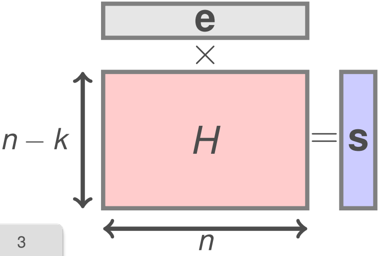
Output

(Decision): Does $\mathbf{e} \in \mathbb{F}_2^n$ of $\mathrm{w}_H(\mathbf{e}) \leq w$ such that $\mathbf{e}H^T = \mathbf{s}$ exists? NP-complete

(Computational): Find $\mathbf{e} \in \mathbb{F}_2^n$ of $\mathrm{w}_H(\mathbf{e}) \leq w$ such that $\mathbf{e}H^T = \mathbf{s}$ NP-difficult

E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg.
On the Inherent Intractability of Certain Coding Problems.
IEEE Trans. Inf. Theory. Vol. 24, pp. 384-386, 1978.

A. Barg.
Complexity Issues in Coding Theory.
Chapter 7, in Handbock of Coding Theory, 1998.



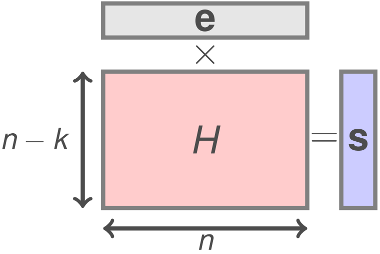
Input:

- A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$
- A weight $w \in \mathbb{Z}$

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Bounded-Distance Decoding problem

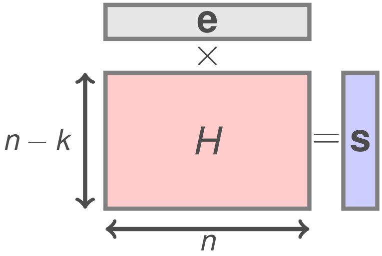


- A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$
- A weight $w \in \mathbb{Z}$

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Bounded-Distance Decoding problem



Input:

- A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$
- A weight $w \leq \dfrac{d-1}{2}$

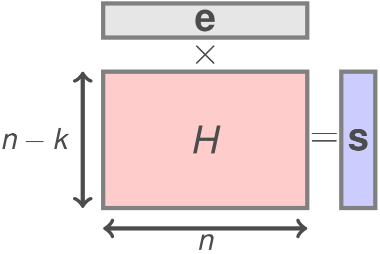
The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Bounded-Distance Decoding problem

(Computational): Find $\mathbf{e} \in \mathbb{F}_2^n$ of $\mathrm{w}_H(\mathbf{e}) \leq \frac{d-1}{2}$ such that $\mathbf{e}H^T = \mathbf{s}$

Conjectured NP-Hard



Input:

- ➜ A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- ➜ A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$
- ➜ A weight $w \leq \dfrac{d-1}{2}$

The Syndrome Decoding (SD) problem

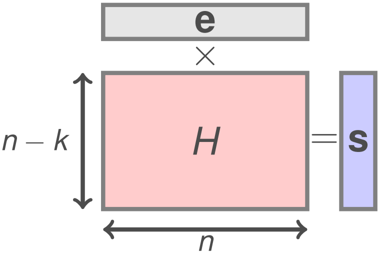
Assumption 1: Decoding a random linear code is a difficult problem.

The Bounded-Distance Decoding problem

(Computational): Find $\mathbf{e} \in \mathbb{F}_2^n$ of $w_H(\mathbf{e}) \leq \frac{d-1}{2}$ such that $\mathbf{e}H^T = \mathbf{s}$

Conjectured NP-Hard

A. Barg.
Complexity Issues in Coding Theory.
Chapter 7, in Handbock of Coding Theory, 1998.



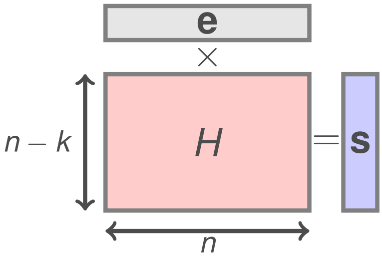
Input:

- A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$
- A weight $w \leq \dfrac{d-1}{2}$

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Goppa Parameterized Syndrome Decoding

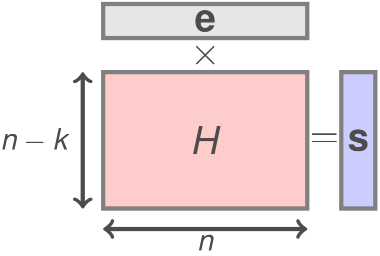


- ➜ A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$
- ➜ A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Goppa Parameterized Syndrome Decoding



Input:

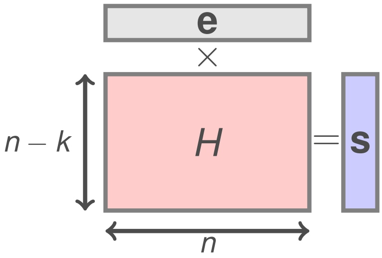
- ➜ A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ with $k = n - mt$ and $n = 2^m$
- ➜ A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$

The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Goppa Parameterized Syndrome Decoding

(Computational): Find $\mathbf{e} \in \mathbb{F}_2^n$ of $\mathrm{w}_H(\mathbf{e}) \leq \frac{n-k}{2}$ such that $\mathbf{e}H^T = \mathbf{s}$ NP-difficult



Input:

- ➜ A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ with $k = n - mt$ and $n = 2^m$
- ➜ A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$

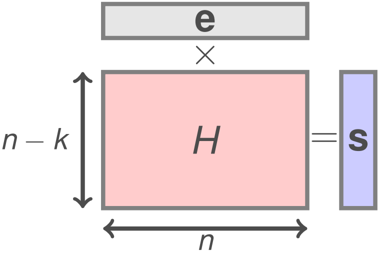
The Syndrome Decoding (SD) problem

Assumption 1: Decoding a random linear code is a difficult problem.

The Goppa Parameterized Syndrome Decoding

(Computational): Find $\mathbf{e} \in \mathbb{F}_2^n$ of $\mathrm{w}_H(\mathbf{e}) \leq \frac{n-k}{2}$ such that $\mathbf{e}H^T = \mathbf{s}$ NP-difficult

M. Finiasz.
Nouvelles constructions utilisant des codes correcteurs d'erreurs en cryptographie à clef publique.
PhD thesis, INRIA - Ecole Polytechnique, 2004



Input:

- A matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ with $k = n - mt$ and $n = 2^m$
- A syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$

Distinguisher for Goppa codes

Assumption 2: The generator matrix of a Goppa code looks random.

Distinguisher for Goppa codes

Assumption 2: The generator matrix of a Goppa code looks random.

$\mathcal{K}_{\text{Goppa}}$ $=$ All generator matrices of a $[n, k]$-binary Goppa code

Goppa Code Distinguishing (GCD) problem Conjectured NP-hard

INPUT: A matrix $G \in \mathbb{F}_2^{k \times n}$

OUTPUT: Is $G \in \mathcal{K}_{\text{Goppa}}$?

Distinguisher for Goppa codes

Assumption 2: The generator matrix of a Goppa code looks random.

$\mathcal{K}_{\text{Goppa}}$ = All generator matrices of a $[n, k]$-binary Goppa code

Goppa Code Distinguishing (GCD) problem Conjectured NP-hard

INPUT: A matrix $G \in \mathbb{F}_2^{k \times n}$

OUTPUT: Is $G \in \mathcal{K}_{\text{Goppa}}$?

1. There exists an efficient distinguisher for **high-rate** codes.

J. . Faugère, V. Gauthier-Umana, A. Otmani, L. Perret and J. P. Tillich
A Distinguisher for High-Rate McEliece Cryptosystems.
IEEE Trans. Inf. Theory. 59(10), pp. 6830-6844, 2013.

Distinguisher for Goppa codes

Assumption 2: The generator matrix of a Goppa code looks random.

$\mathcal{K}_{\mathrm{Goppa}}$ = All generator matrices of a $[n, k]$-binary Goppa code

Goppa Code Distinguishing (GCD) problem Conjectured NP-hard

INPUT: A matrix $G \in \mathbb{F}_2^{k \times n}$

OUTPUT: Is $G \in \mathcal{K}_{\mathrm{Goppa}}$?

1. There exists an efficient distinguisher for **high-rate** codes.

   J. . Faugère, V. Gauthier-Umana, A. Otmani, L. Perret and J. P. Tillich
   A Distinguisher for High-Rate McEliece Cryptosystems.
   IEEE Trans. Inf. Theory. 59(10), pp. 6830-6844, 2013.

2. **General case:** best-known attacks are based on the *support splitting algorithm* and have **exponential runtime**.

   P. Loidreau, N. Sendrier
   Weak keys in McEliece public-key cryptosystem.
   IEEE Trans. Inf. Theory 47(3):1207âĂŞ1212

McEliece Assumptions

We have seen that:

✔ The **general decoding problem** of a linear code whose parameters are those of a binary Goppa code is in the average case difficult.

✔ There exists no efficient distinguisher for Goppa codes

2. McEliece Cryptosystem

1. Formal Definition
2. Security-Reduction Proof
3. McEliece Assumptions
4. **Notions of Security**
5. Critical Attacks - Semantic Secure Conversions
6. Reducing the Key Size
7. Reducing the Key Size - LDPC codes
8. Reducing the Key Size - MDPC codes
9. Implementation