Code-Based Cryptography

Error-Correcting Codes and Cryptography

I. Márquez-Corbella

informatiques mathématiques

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. **Encoding (Linear Transformation)**
4. Parity Checking
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. Goppa Codes
9. McEliece Cryptosystem

Encoder - Linear Transformation

$\{\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_q^k\} \implies$ There are q^k possible messages

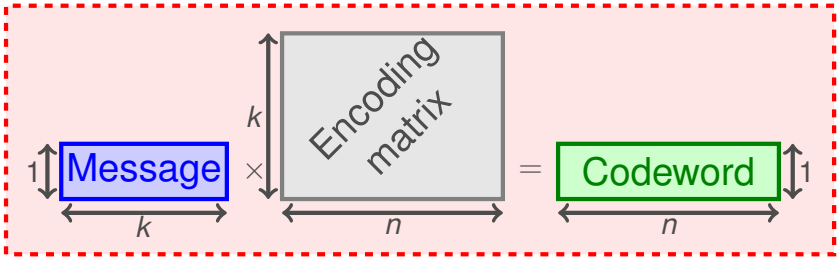
Message Space
$\mathbf{m} \in \mathbb{F}_q^k$

Encoder - Linear Transformation

$\{\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_q^k\} \Longrightarrow$ There are q^k possible messages

Encoder - Linear Transformation

$\{\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_q^k\} \Longrightarrow$ There are q^k possible messages



Linear Codes

Image of the **message space** through a **linear transformation** → **Linear code** $\mathcal{C}$ over $\mathbb{F}_q$ $=$ **Vector subspace** of $\mathbb{F}_q^n$

Linear Codes

Image of the **message space** through a **linear transformation** ⇢ **Linear code $\mathcal{C}$** over $\mathbb{F}_q$ $=$ **Vector subspace** of $\mathbb{F}_q^n$

1. $\mathcal{C}$ is closed under addition.

$$\forall \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C} \implies \mathbf{c}_1 + \mathbf{c}_2 \in \mathcal{C}$$

Linear Codes

Image of the **message space** through a **linear transformation** ⇢ **Linear code $\mathcal{C}$ over $\mathbb{F}_q$** $=$ **Vector subspace of $\mathbb{F}_q^n$**

1. $\mathcal{C}$ is closed under addition.
2. $\mathcal{C}$ is closed under scalar multiplication.

$$\forall \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C} \implies \mathbf{c}_1 + \mathbf{c}_2 \in \mathcal{C}$$

$$\forall \lambda \in \mathbb{F}_q,\ \forall \mathbf{c} \in \mathcal{C} \implies \lambda \mathbf{c} \in \mathcal{C}$$

Linear Codes

Image of the **message space** through a **linear transformation** → **Linear code $\mathcal{C}$ over $\mathbb{F}_q$** = **Vector subspace of $\mathbb{F}_q^n$**

1. $\mathcal{C}$ is closed under addition.
2. $\mathcal{C}$ is closed under scalar multiplication.
3. The zero vector is always a codeword.

$$\forall \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C} \implies \mathbf{c}_1 + \mathbf{c}_2 \in \mathcal{C}$$

$$\forall \lambda \in \mathbb{F}_q,\ \forall \mathbf{c} \in \mathcal{C} \implies \lambda \mathbf{c} \in \mathcal{C}$$

$$(0, \ldots, 0) \in \mathcal{C}$$

Generator Matrix - Linear Codes

A **basis** of a vector space V
is **linearly independent**
and **spans** V

Generator Matrix - Linear Codes

A **basis** of a vector space V is **linearly independent** and **spans** V

The **encoding matrix** is a **basis** for $\mathcal{C}$

Generator Matrix - Linear Codes

A **basis** of a vector space V is **linearly independent** and **spans** V

The **encoding matrix** is a **basis** for $\mathcal{C}$

Generator matrix for $\mathcal{C}$

Generator Matrix - Linear Codes

A **basis** of a vector space V is **linearly independent** and **spans** V

The **encoding matrix** is a **basis** for $\mathcal{C}$

Generator matrix for $\mathcal{C}$

A code can have more than one generator matrix!
But all have rank k

Generator Matrix - Linear Codes

A **basis** of a vector space V is **linearly independent** and **spans** V

The **encoding matrix** is a **basis** for $\mathcal{C}$

Generator matrix for $\mathcal{C}$

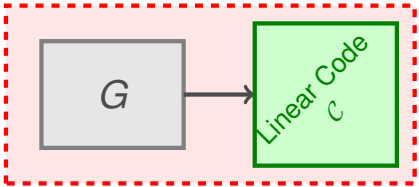
A code can have more than one generator matrix!
But all have rank k

Parameters of a linear code

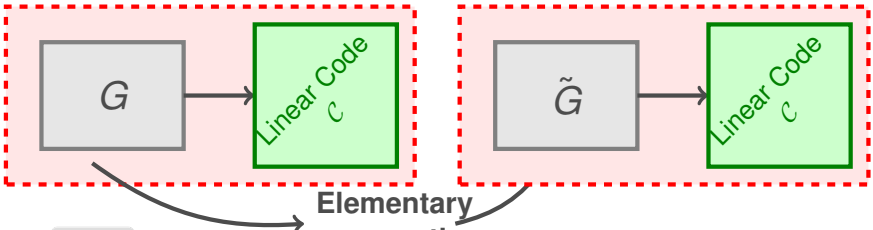
If $\mathcal{C}$ is a k-dimensional vector space of $\mathbb{F}_q^n$ then,

$\mathcal{C}$ is an $[n, k]_q$ code

Generator Matrix - Standard Form



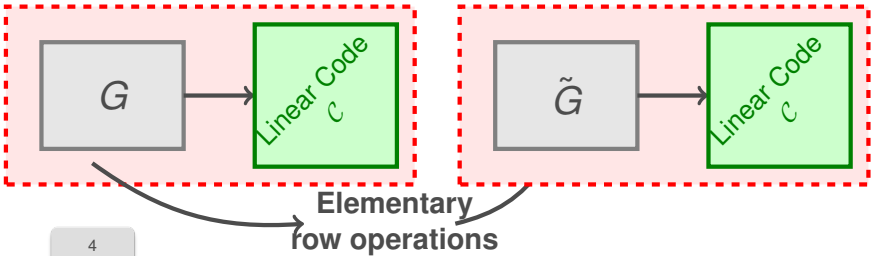
Generator Matrix - Standard Form



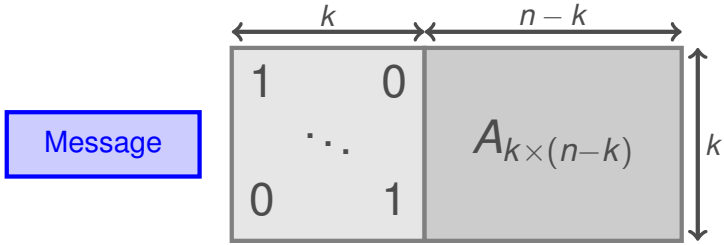
Generator Matrix - Standard Form

$$G = \begin{array}{c} \overset{k}{\longleftrightarrow} \quad \overset{n-k}{\longleftrightarrow} \\ \left[\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & A_{k\times(n-k)} \\ 0 & & 1 & \end{array}\right] \end{array} \quad \updownarrow k$$

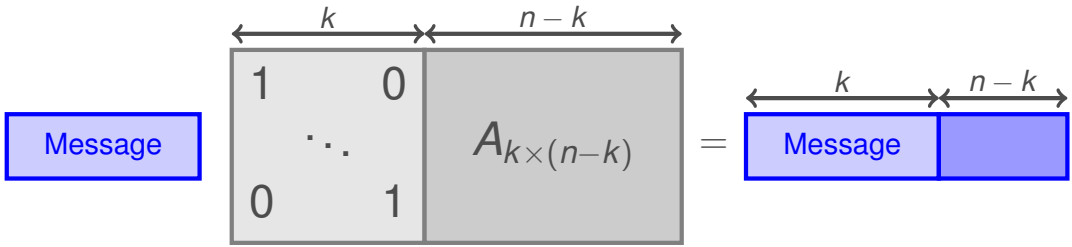
Generator Matrix in Standard Form



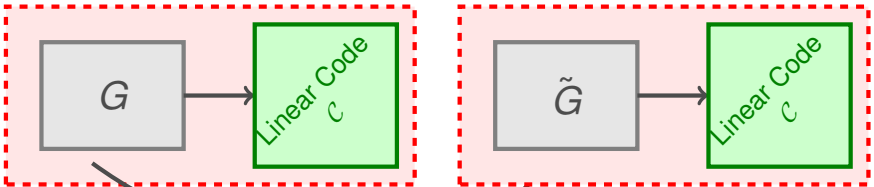
Generator Matrix - Standard Form



Generator Matrix - Standard Form



Generator Matrix in Standard Form



Number of codewords

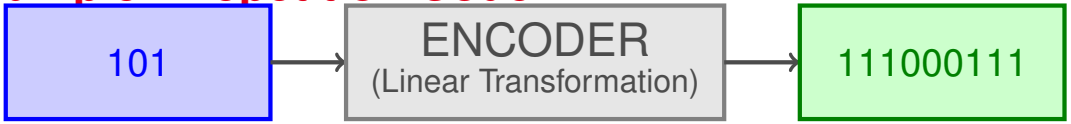
$$\{\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_q^k\} \Longrightarrow \text{There are } q^k \text{ possible messages}$$

Number of codewords

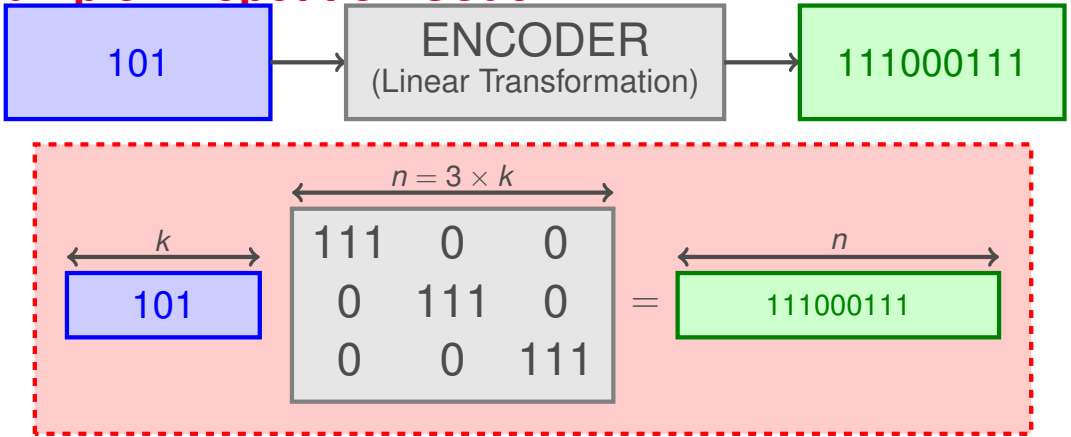
$\{\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_q^k\} \Longrightarrow$ There are q^k possible messages

$\mathcal{C}$ has q^k codewords

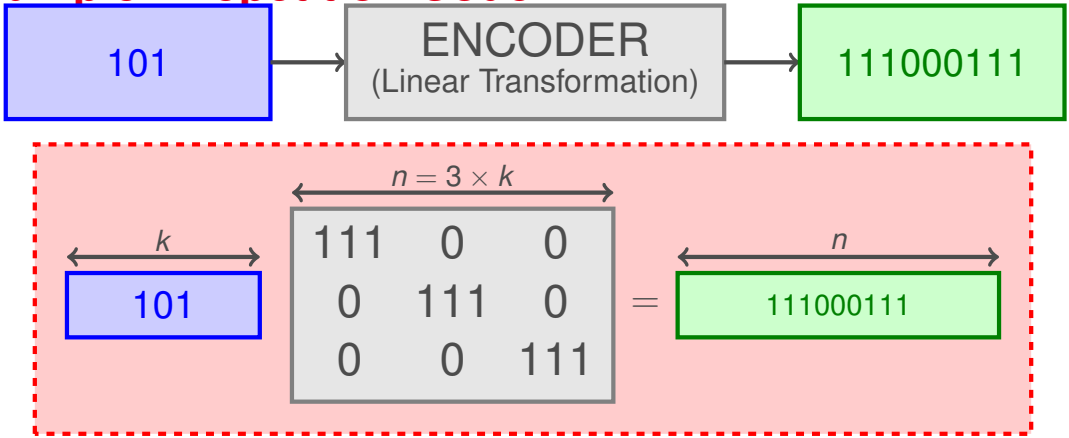
Example - Repetition Code



Example - Repetition Code

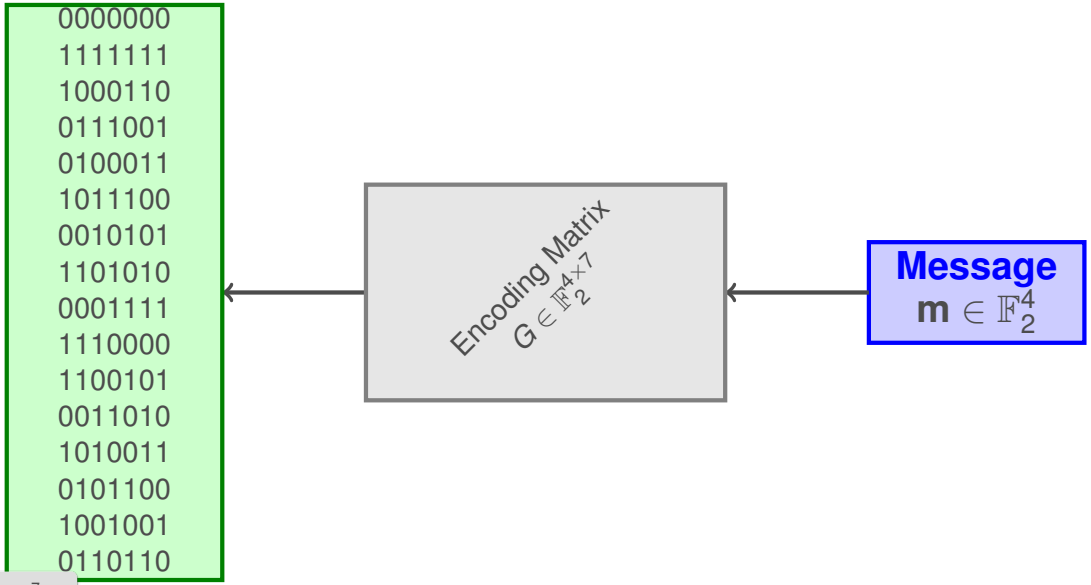


Example - Repetition Code

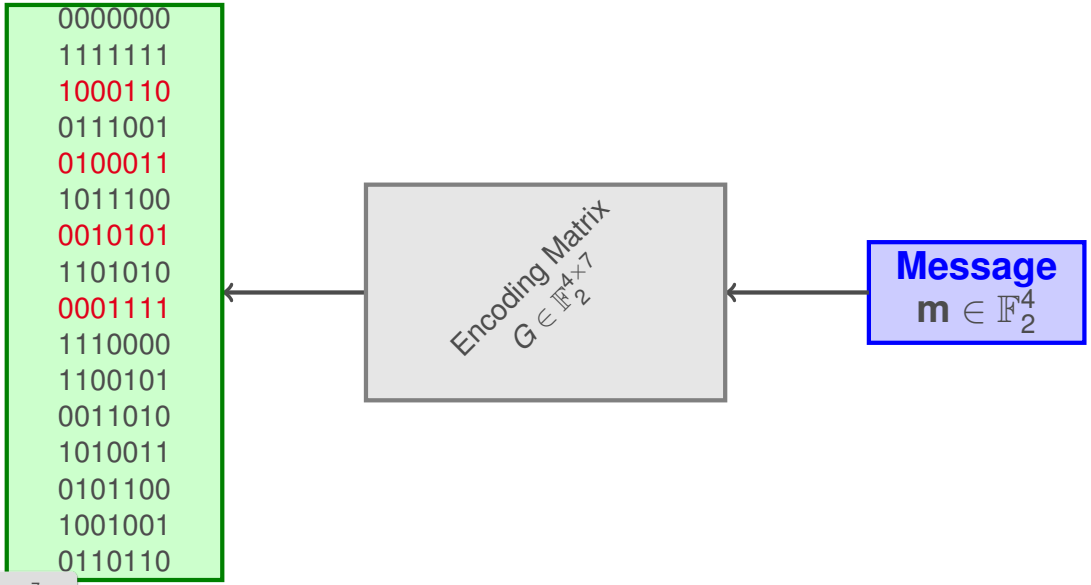


The 3-repetition code is an $[n, 1]_q$ code.

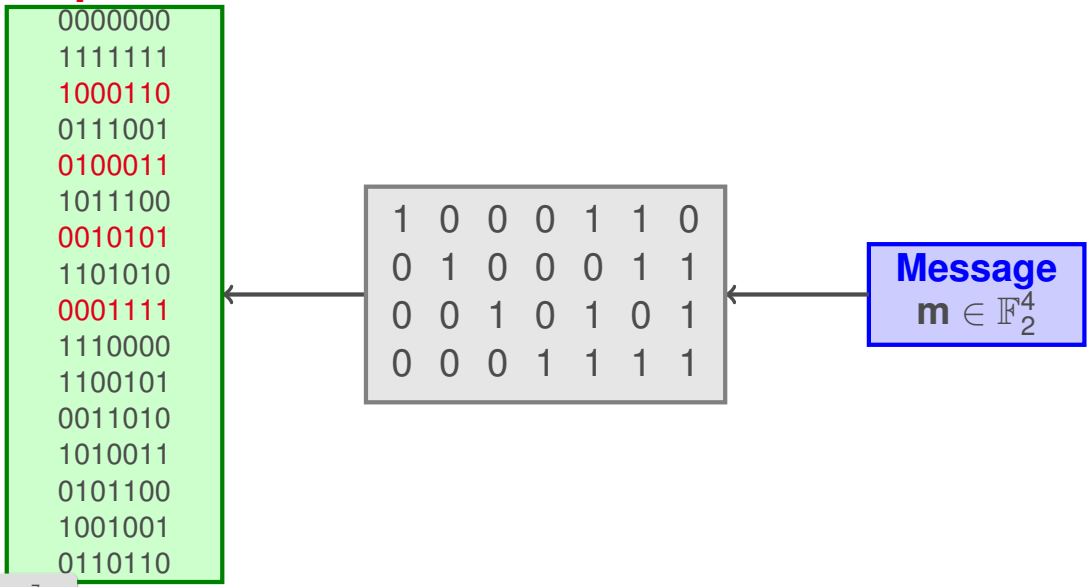
Example


0000000
1111111
1000110
0111001
0100011
1011100
0010101
1101010
0001111
1110000
1100101
0011010
1010011
0101100
1001001
0110110
Encoding Matrix
$G \in \mathbb{F}_2^{4\times 7}$
Message
$\mathbf{m} \in \mathbb{F}_2^4$

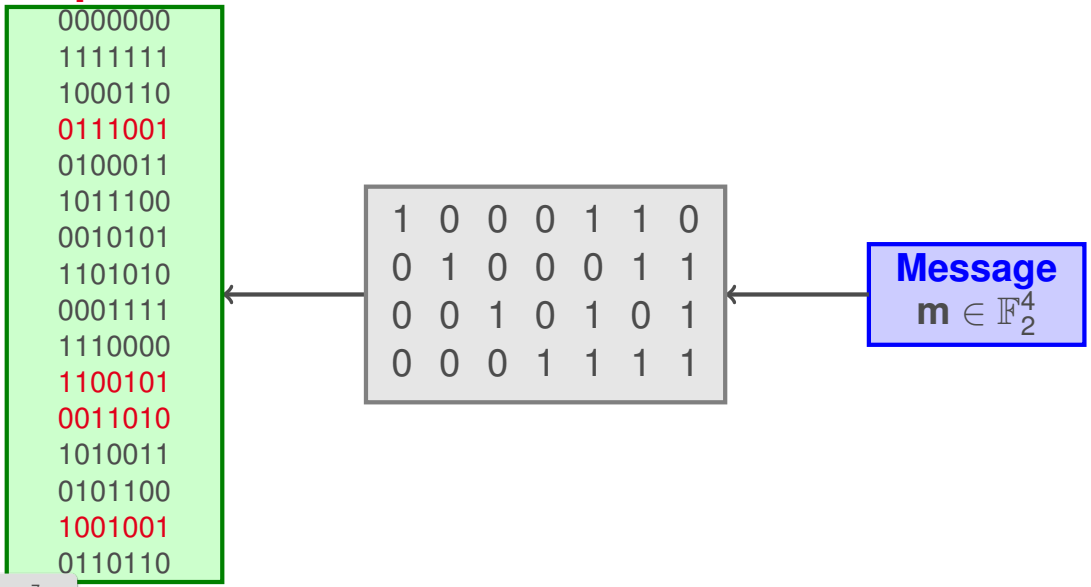
Example


0000000
1111111
1000110
0111001
0100011
1011100
0010101
1101010
0001111
1110000
1100101
0011010
1010011
0101100
1001001
0110110
Encoding Matrix
$G \in \mathbb{F}_2^{4\times 7}$
Message
$\mathbf{m} \in \mathbb{F}_2^4$

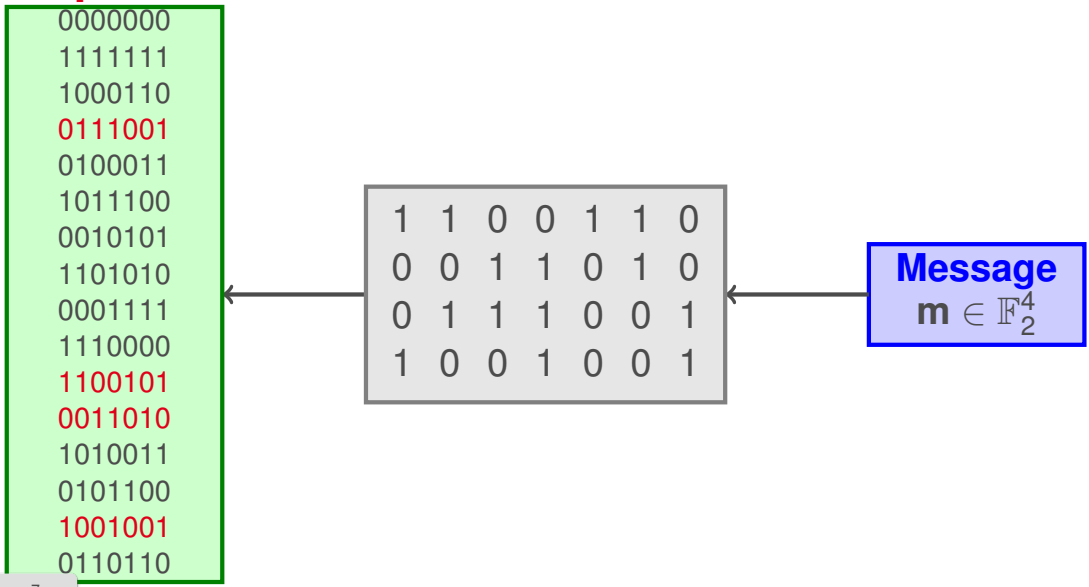
Example


0000000
1111111
1000110
0111001
0100011
1011100
0010101
1101010
0001111
1110000
1100101
0011010
1010011
0101100
1001001
0110110
1 0 0 0 1 1 0
0 1 0 0 0 1 1
0 0 1 0 1 0 1
0 0 0 1 1 1 1
Message
$\mathbf{m} \in \mathbb{F}_2^4$

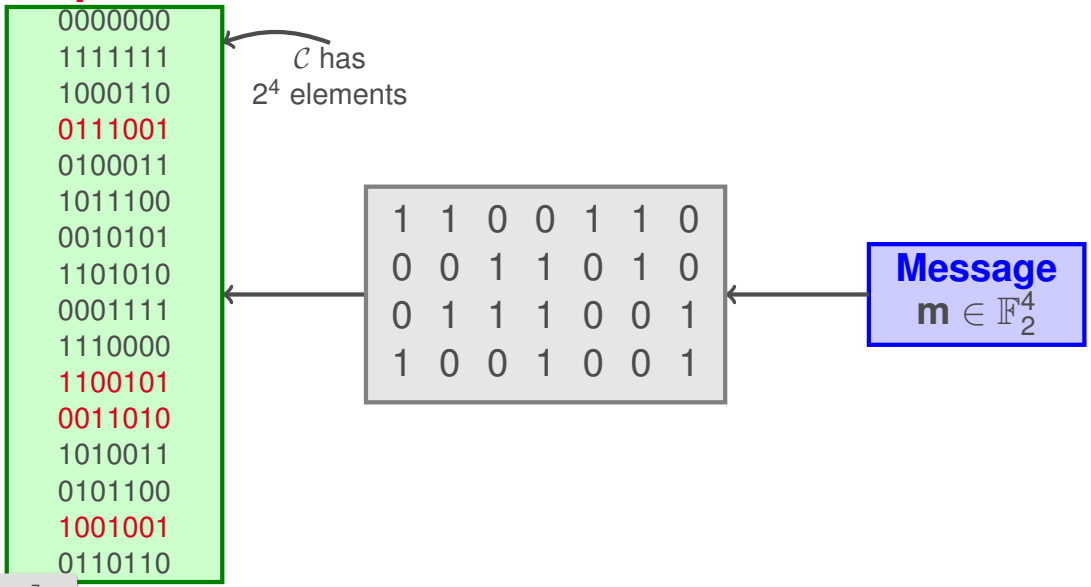
Example


0000000
1111111
1000110
0111001
0100011
1011100
0010101
1101010
0001111
1110000
1100101
0011010
1010011
0101100
1001001
0110110
1 0 0 0 1 1 0
0 1 0 0 0 1 1
0 0 1 0 1 0 1
0 0 0 1 1 1 1
Message
$\mathbf{m} \in \mathbb{F}_2^4$

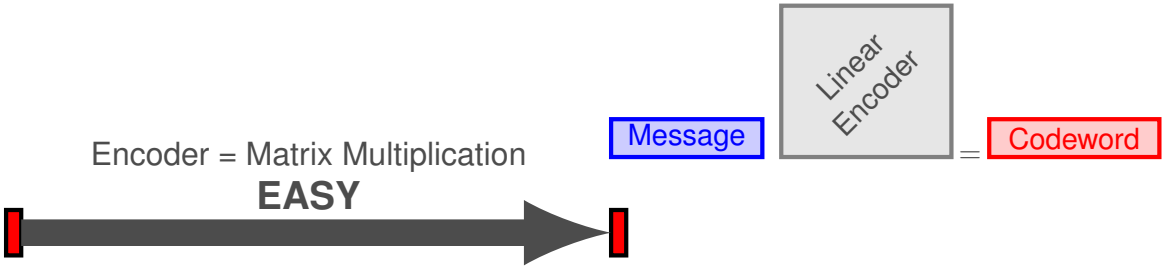
Example


0000000
1111111
1000110
0111001
0100011
1011100
0010101
1101010
0001111
1110000
1100101
0011010
1010011
0101100
1001001
0110110
1 1 0 0 1 1 0
0 0 1 1 0 1 0
0 1 1 1 0 0 1
1 0 0 1 0 0 1
Message
$\mathbf{m} \in \mathbb{F}_2^4$

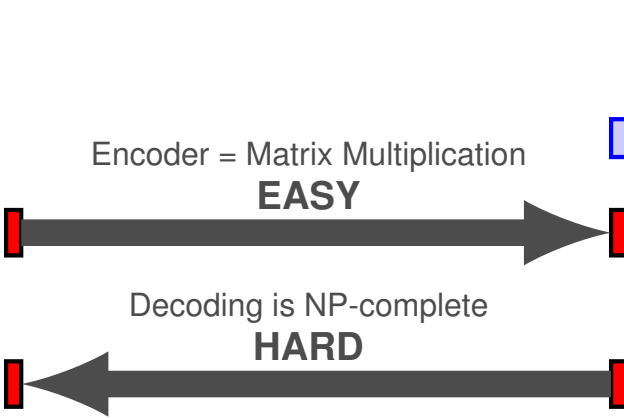
Example


0000000
1111111
1000110
0111001
0100011
1011100
0010101
1101010
0001111
1110000
1100101
0011010
1010011
0101100
1001001
0110110
$\mathcal{C}$ has
2^4 elements
1 1 0 0 1 1 0
0 0 1 1 0 1 0
0 1 1 1 0 0 1
1 0 0 1 0 0 1
Message
$\mathbf{m} \in \mathbb{F}_2^4$

Trapdoor one-way functions - Decoder



Trapdoor one-way functions - Decoder



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.

Trapdoor one-way functions - Decoder

Encoder = Matrix Multiplication

EASY

Decoding is NP-complete

HARD

Efficient decoder for certain families of codes

EASY(with TRAPDOOR information)

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.

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. Encoding (Linear Transformation)
4. **Parity Checking**
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. Goppa Codes
9. McEliece Cryptosystem