

Code-Based Cryptography

Error-Correcting Codes and Cryptography

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

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

Message Space

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

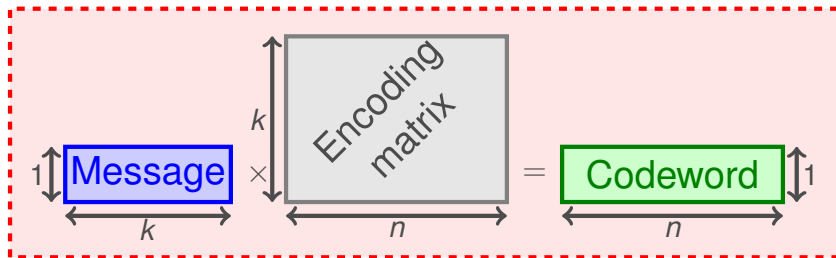
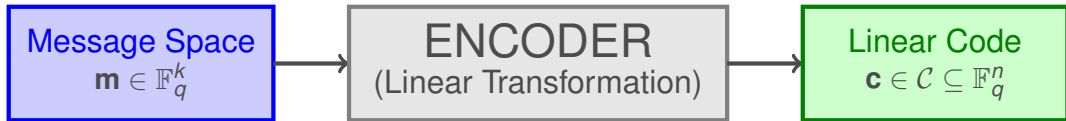
Encoder - Linear Transformation

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

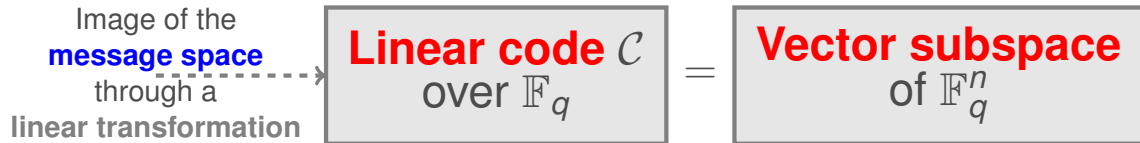


Encoder - Linear Transformation

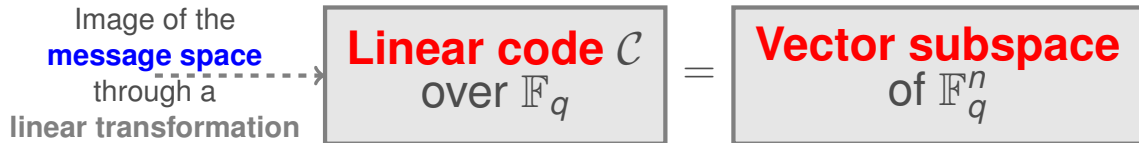
$\{\mathbf{m} = (m_1, \dots, m_k) \in \mathbb{F}_q^k\} \implies$ There are q^k possible messages
 \parallel



Linear Codes



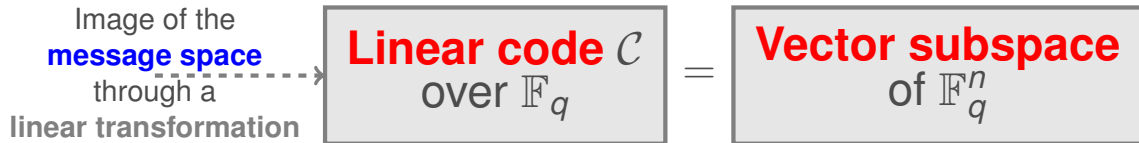
Linear Codes



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

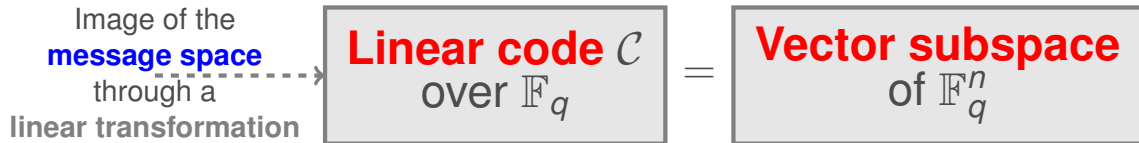


1. \mathcal{C} is closed under addition.
2. \mathcal{C} is closed under scalar multiplication.

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

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

Linear Codes



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

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

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

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

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}

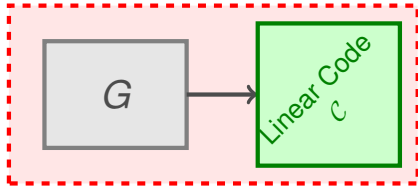
A code can have more than one generator matrix!
But all have rank k

Parameters of a linear code

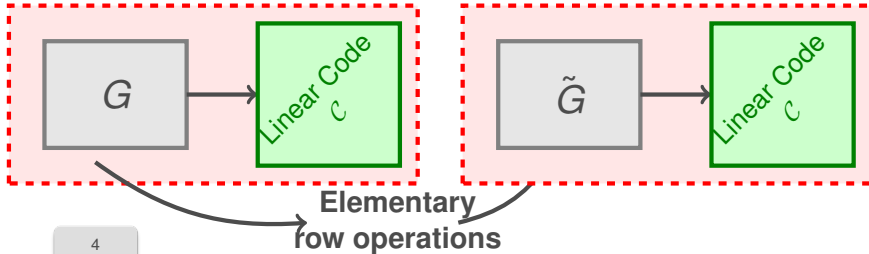
If \mathcal{C} is a k -dimensional vector space of \mathbb{F}_q^n then,

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

Generator Matrix - Standard Form



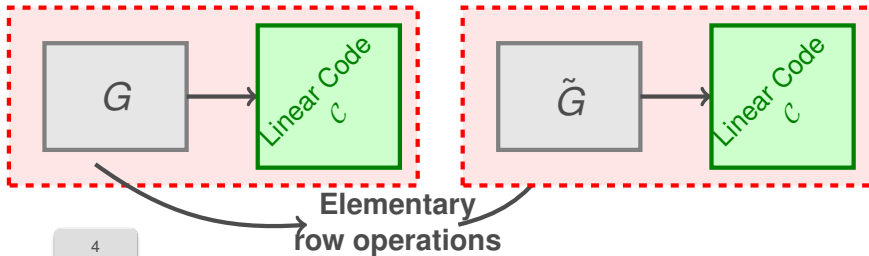
Generator Matrix - Standard Form



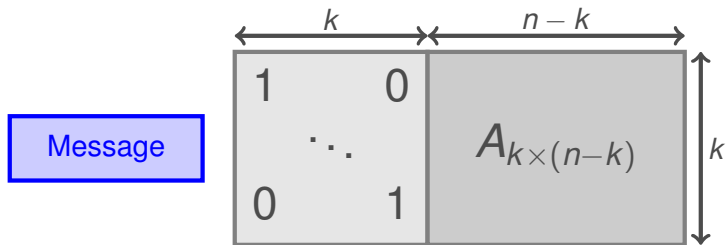
Generator Matrix - Standard Form

$$G = \begin{array}{|cc|c|} \hline \xrightarrow{k} & \xrightarrow{n-k} & \\ \hline 1 & 0 & \\ & \ddots & \\ 0 & 1 & \\ \hline \end{array} \begin{array}{c} A_{k \times (n-k)} \\ \xrightarrow{k} \end{array}$$

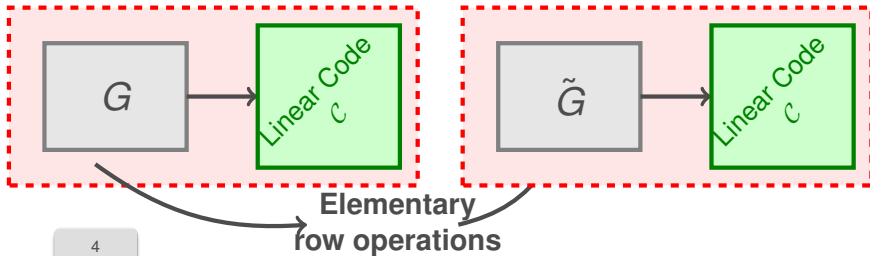
**Generator Matrix
in Standard Form**



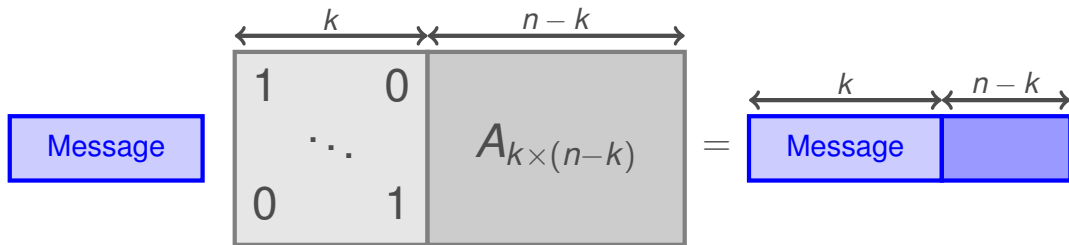
Generator Matrix - Standard Form



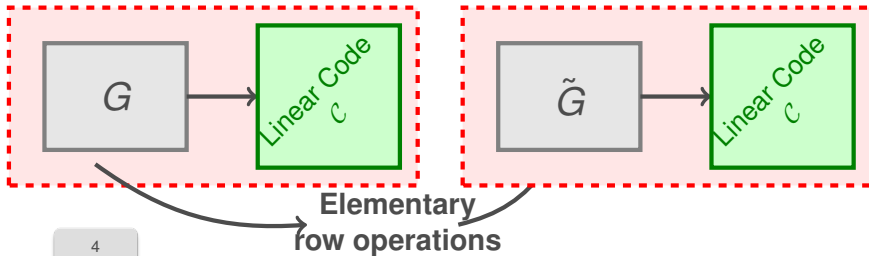
Generator Matrix
in Standard Form



Generator Matrix - Standard Form



**Generator Matrix
in Standard Form**



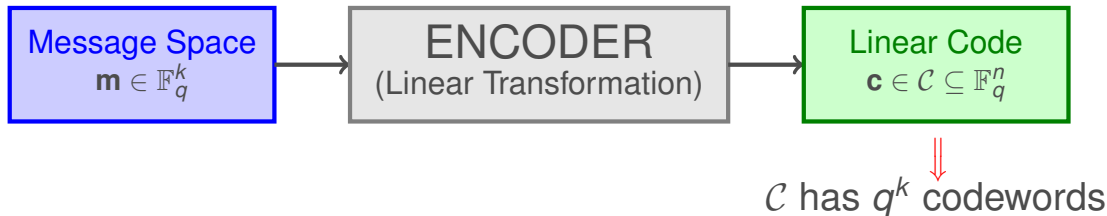
Number of codewords

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

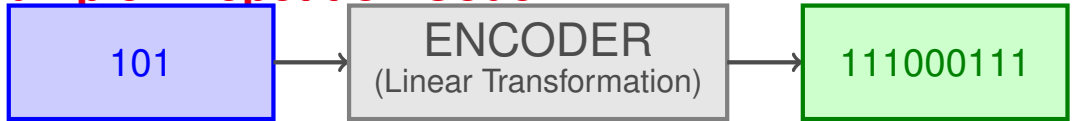


Number of codewords

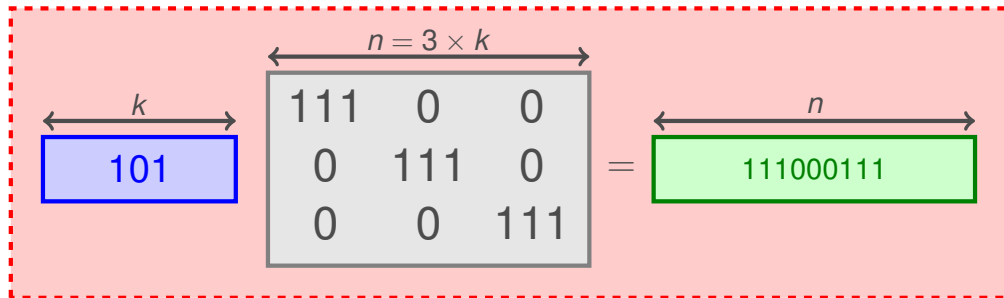
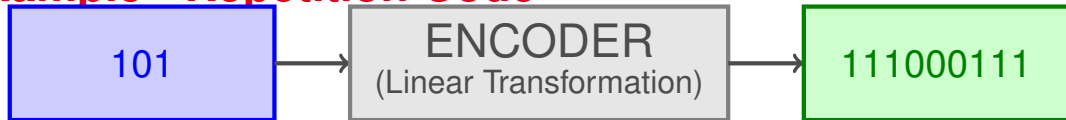
$\{\mathbf{m} = (m_1, \dots, m_k) \in \mathbb{F}_q^k\} \implies$ There are q^k possible messages
 \parallel



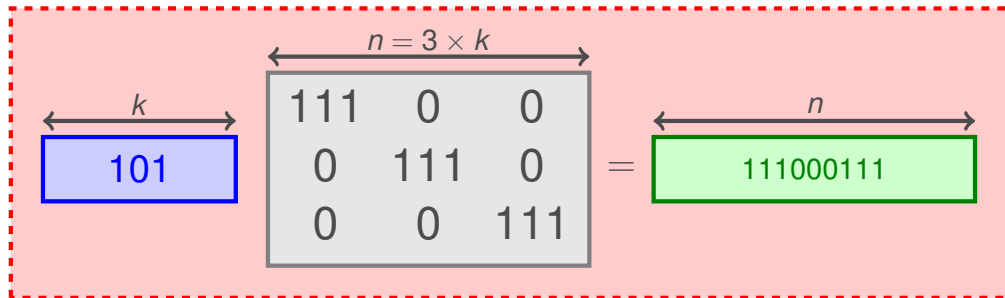
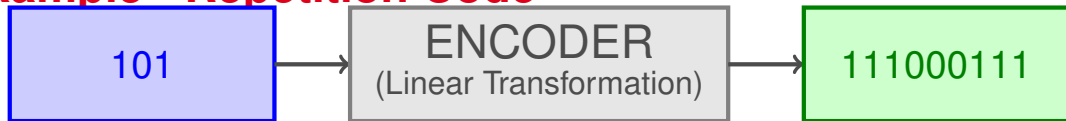
Example - Repetition Code



Example - Repetition Code

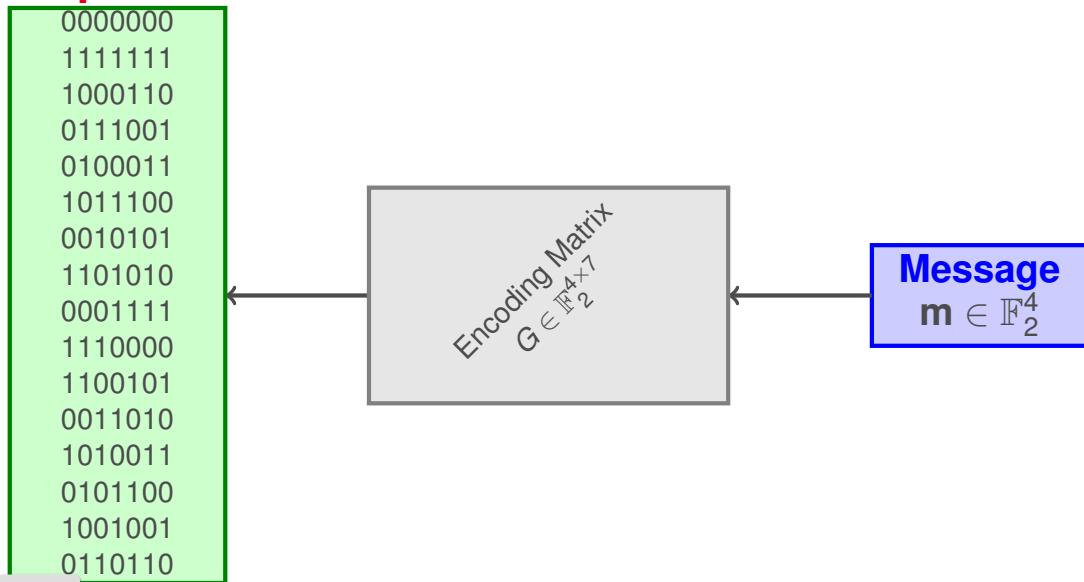


Example - Repetition Code

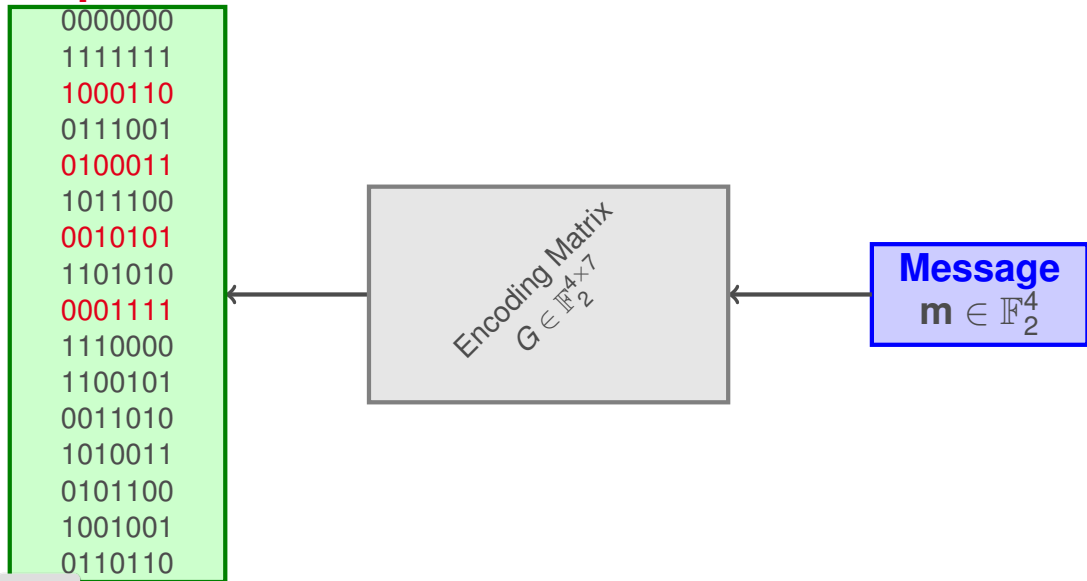


The 3-repetition code is an $[n, 1]_q$ code.

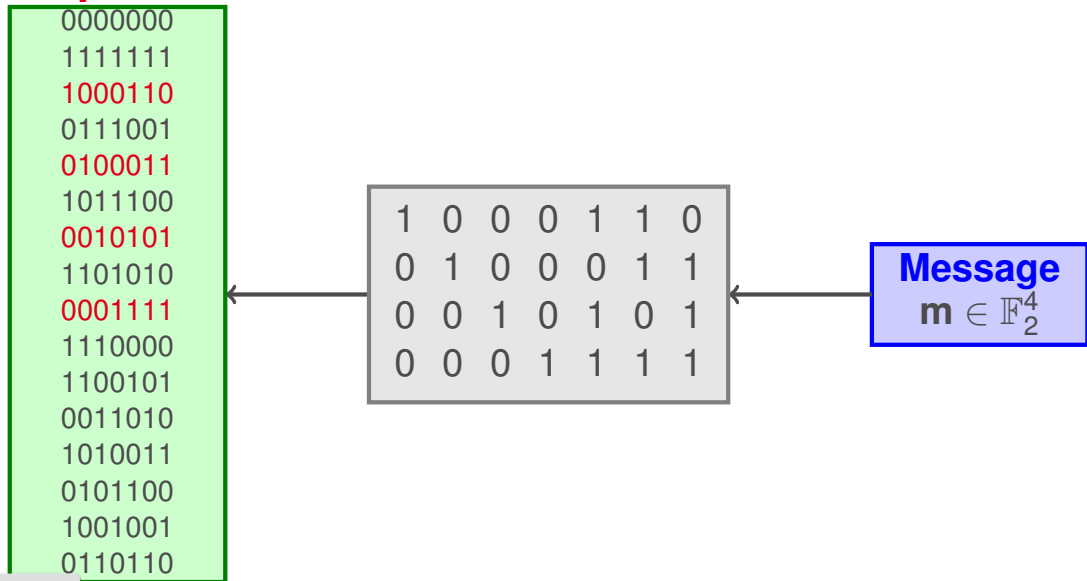
Example



Example



Example



Example

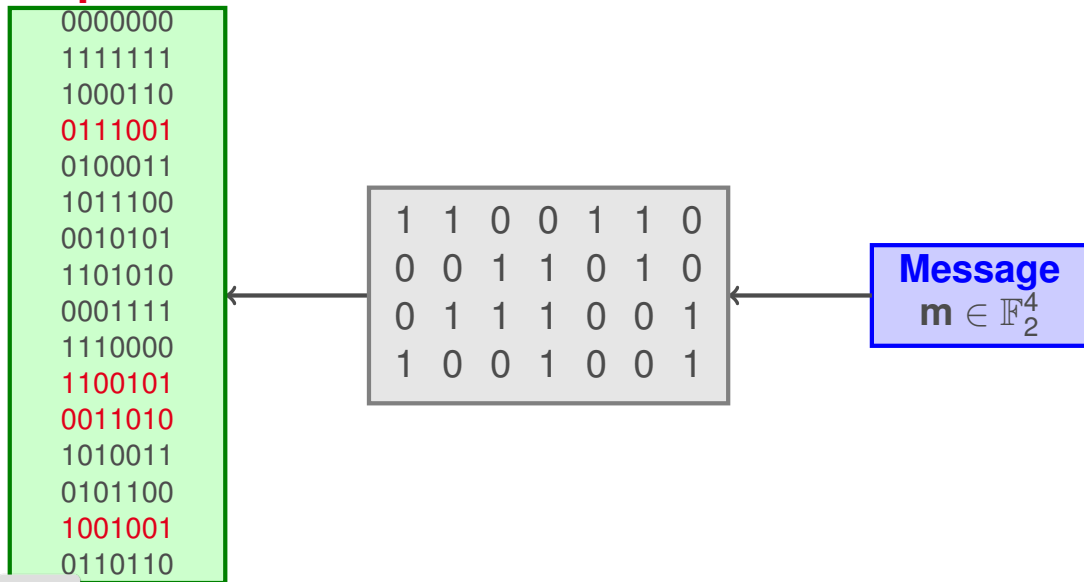
0000000
1111111
1000110
0111001
0100011
1011100
0010101
1101010
0001111
1110000
1100101
0011010
1010011
0101100
1001001
0110110

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

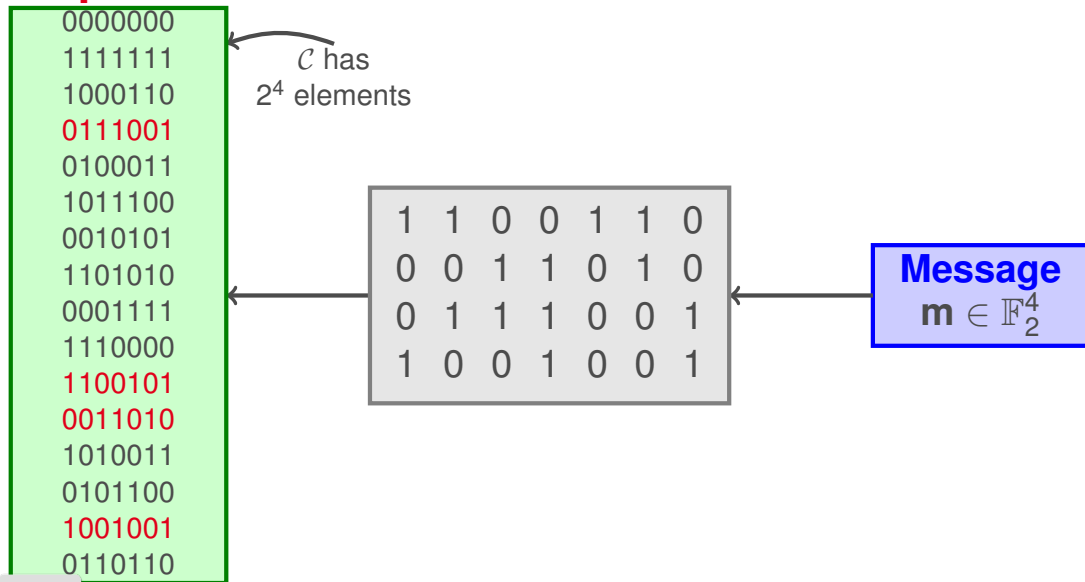
Message

$\mathbf{m} \in \mathbb{F}_2^4$

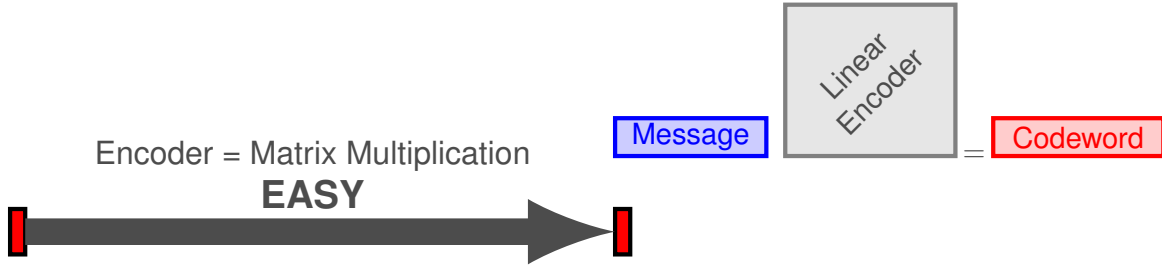
Example



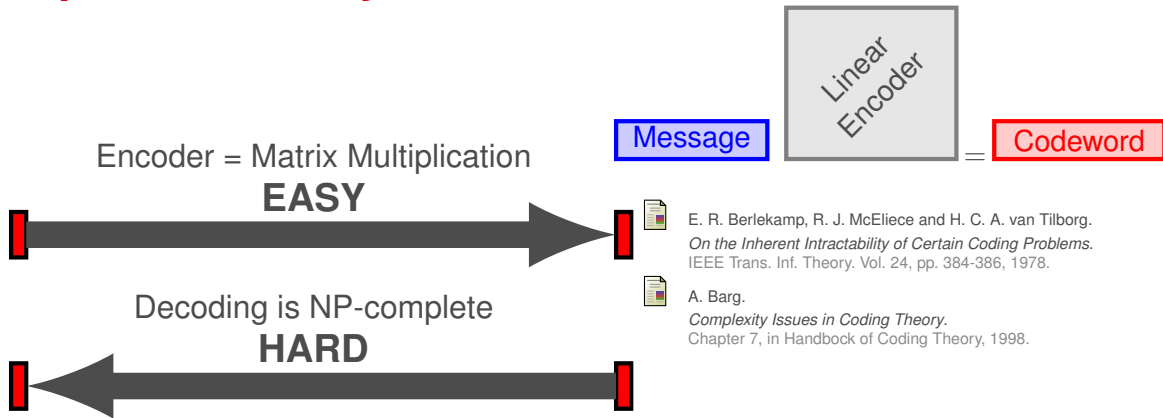
Example



Trapdoor one-way functions - Decoder



Trapdoor one-way functions - Decoder



Trapdoor one-way functions - Decoder

Encoder = Matrix Multiplication

EASY

Message

Linear
Encoder

Codeword

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 Handbook 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