

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**

Public Key Cryptography

644

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

I. INTRODUCTION

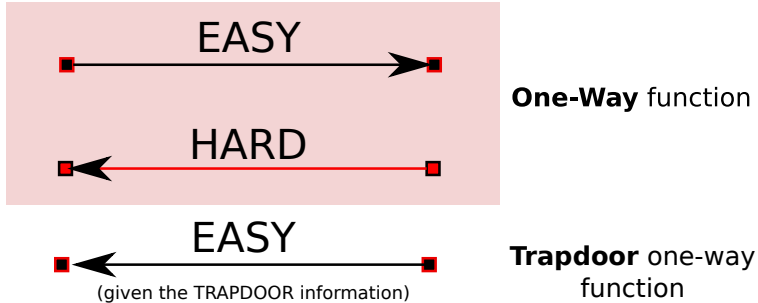
WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory

The best known cryptographic vacy: preventing the unauthorized from communications over order to use cryptography to insure currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

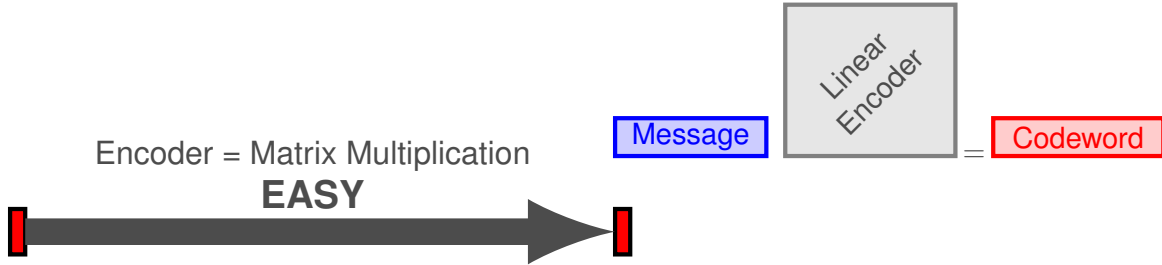
Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a public key cryptosystem enciphering and deciphering are governed by distinct keys, E and D , such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering



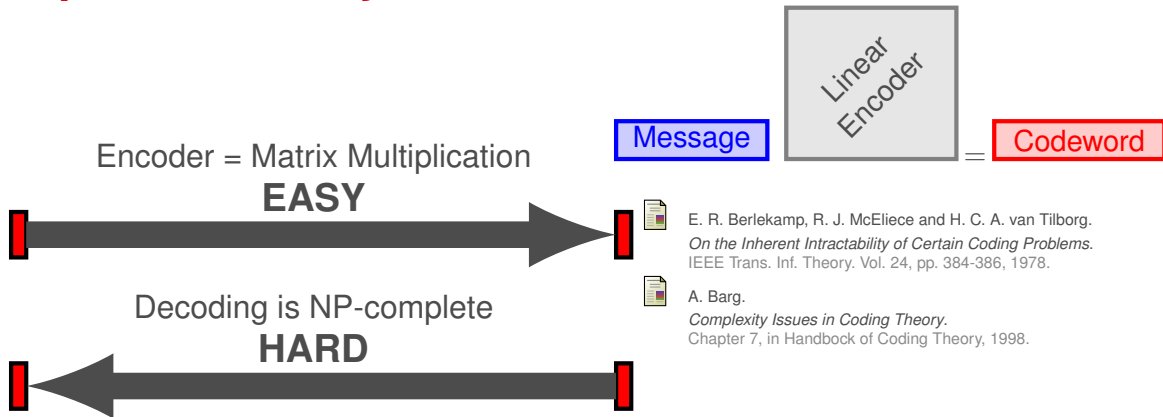
Public Key Cryptography



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.

The McEliece Cryptosystem

McEliece introduced the first PKC based on **Error-Correcting Codes** in **1978**.



R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.



The McEliece Cryptosystem

Security of the McEliece scheme is based on:

1. Hardness of decoding random linear codes
2. Distinguishing Goppa codes

McEliece introduced the first PKC based on **Error-Correcting Codes** in **1978**.



R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.



The McEliece Cryptosystem

Advantages:

1. **Fast** ENCRYPT and DECRYPT.
2. **Post-quantum cryptosystem.**

Security of the McEliece scheme is based on:

1. Hardness of decoding random linear codes
2. Distinguishing Goppa codes

McEliece introduced the first PKC based on **Error-Correcting Codes** in **1978**.



R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.



The McEliece Cryptosystem

Advantages:

1. **Fast** ENCRYPT and DECRYPT.
2. **Post-quantum cryptosystem.**

Drawback:

- Large key size.

Security of the McEliece scheme is based on:

1. Hardness of decoding random linear codes
2. Distinguishing Goppa codes

McEliece introduced the first PKC based on **Error-Correcting Codes** in **1978**.



R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.



The McEliece Cryptosystem

Consider (\mathcal{F}) family of codes

The McEliece Cryptosystem

Consider (\mathcal{F}) family of codes

with an **efficient**
decoding algorithm

The McEliece Cryptosystem

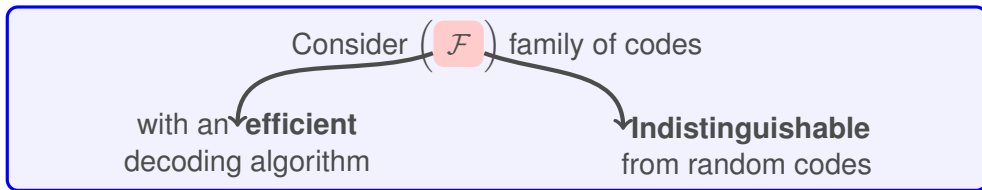
Consider (\mathcal{F}) family of codes

with an **efficient** decoding algorithm

Indistinguishable from random codes

```
graph TD; A["Consider (F) family of codes"] --> B["with an efficient decoding algorithm"]; A --> C["Indistinguishable from random codes"];
```

The McEliece Cryptosystem



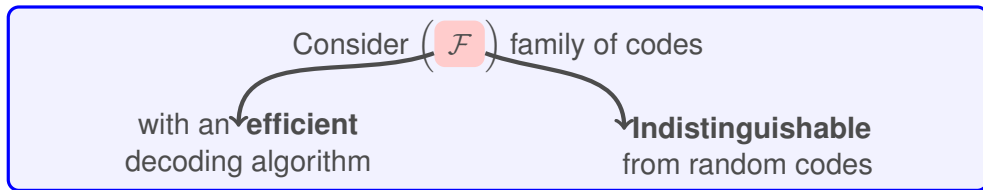
Key Generation Algorithm:

1. $G \in \mathbb{F}_q^{k \times n}$ a **generator matrix** for $\mathcal{C} \in \mathcal{F}$
2. $\mathcal{A}_{\mathcal{C}}$ an **“Efficient” decoding algorithm** for \mathcal{C} which corrects up to t **errors**.

Public Key: $\mathcal{K}_{\text{pub}} = (G, t)$

Private Key: $\mathcal{K}_{\text{secret}} = (\mathcal{A}_{\mathcal{C}})$

The McEliece Cryptosystem



Key Generation Algorithm:

1. $G \in \mathbb{F}_q^{k \times n}$ a **generator matrix** for $\mathcal{C} \in \mathcal{F}$
2. $\mathcal{A}_{\mathcal{C}}$ an **“Efficient” decoding algorithm** for \mathcal{C} which corrects up to t **errors**.

Public Key: $\mathcal{K}_{\text{pub}} = (G, t)$

Private Key: $\mathcal{K}_{\text{secret}} = (\mathcal{A}_{\mathcal{C}})$

Parameters	Key size	Security level
$[1024, 524, 101]_2$	67 ko	2^{62}
$[2048, 1608, 48]_2$	412 ko	2^{96}

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\text{ENCRYPT}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

where \mathbf{e} is a random error vector of weight at most t .

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\text{ENCRYPT}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

where \mathbf{e} is a random error vector of weight at most t .

Decryption Algorithm:

Using $\mathcal{K}_{\text{secret}}$, the receiver obtain \mathbf{m} .

$$\text{DECRYPT}(\mathbf{y}) = \mathcal{A}_{\mathcal{C}}(\mathbf{y}) = \mathbf{m}$$

Which code Family? - GRS codes



Generalized Reed-Solomon codes



H. Niederreiter.

Knapsack-type cryptosystems and algebraic coding theory.

Problems of Control and Information Theory, 15(2):159-166, 1986.

Parameters	Key size	Security level
$[256, 128, 129]_{256}$	67 ko	2^{95}

Which code Family? - GRS codes



Generalized Reed-Solomon codes



H. Niederreiter.

Knapsack-type cryptosystems and algebraic coding theory.

Problems of Control and Information Theory, 15(2):159-166, 1986.

Parameters	Key size	Security level
$[256, 128, 129]_{256}$	67 ko	2^{95}



Attack against this proposal:



V. M. Sidelnikov and S. O. Shestakov.

On the insecurity of cryptosystems based on generalized Reed-Solomon codes.

Discrete Math. Appl., 2:439-444, 1992.

Which code Family? - Subcodes of GRS codes



Subcodes of GRS codes



T. Berger and P. Loidreau.

How to mask the structure of codes for a cryptographic use.

Des. Codes Cryptogr., 35:63-79, 2005.

Which code Family? - Subcodes of GRS codes



Subcodes of GRS codes



T. Berger and P. Loidreau.

How to mask the structure of codes for a cryptographic use.

Des. Codes Cryptogr., 35:63-79, 2005.



Attack against this proposal:



C. Wieschebrink.

Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes.

In Post-Quantum Cryptography, volume 6061 of Lecture Notes in Comput. Sci., pages 61-72, 2010.

Which code Family? - Reed-Muller codes



Reed-Muller codes



V. Sidelnikov.

A public-key cryptosystem based on Reed-Muller codes.
Discrete Math. Appl., 4(3):191-207, 1994.

Parameters	Key size	Security level
$[1024, 176, 128]_2$	22.5 ko	2^{72}
$[2048, 232, 256]_2$	59, 4 ko	2^{93}

Which code Family? - Reed-Muller codes



Reed-Muller codes



V. Sidelnikov.

A public-key cryptosystem based on Reed-Muller codes.

Discrete Math. Appl., 4(3):191-207, 1994.

Parameters	Key size	Security level
$[1024, 176, 128]_2$	22.5 ko	2^{72}
$[2048, 232, 256]_2$	59, 4 ko	2^{93}



Attacks against this proposal:



L. Minder and A. Shokrollahi.

Cryptanalysis of the Sidelnikov cryptosystem.

In EUROCRYPT 2007, pages 347-360, 2007.



I. V. Chizhov, and M. A. Borodin.

The failure of McEliece PKC based on Reed-Muller codes.

IACR Cryptology ePrint Archive, 287, 2013.

Which code Family? - AG codes

Algebraic Geometry codes



H. Janwa and O. Moreno.

McEliece public crypto system using algebraic-geometric codes.
Designs, Codes and Cryptography, 1996.

Parameters	Key size	Security level
$[171, 109, 61]_{128}$	16 ko	2^{66}

Which code Family? - AG codes

➤ Algebraic Geometry codes



H. Janwa and O. Moreno.

McEliece public crypto system using algebraic-geometric codes.
Designs, Codes and Cryptography, 1996.

Parameters	Key size	Security level
$[171, 109, 61]_{128}$	16 ko	2^{66}



Attacks against this proposal:



C. Faure and L. Minder.

Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes.

Proceedings 11th Int. Workshop on Algebraic and Combinatorial Coding Theory, 2008.



A. Couvreur, I. Márquez-Corbella and R. Pellikaan.

A polynomial time attack against Algebraic Geometry code based Public-Key Cryptosystems.

ISIT 2014, 1446-1450, 2014.

Which code Family? - Concatenated codes



Concatenated codes



H. Niederreiter.

Knapsack-type cryptosystems and algebraic coding theory.

Problems of Control and Information Theory, 15(2):159-166, 1986.

Which code Family? - Concatenated codes



Concatenated codes



H. Niederreiter.

Knapsack-type cryptosystems and algebraic coding theory.

Problems of Control and Information Theory, 15(2):159-166, 1986.



Attack against this proposal:



N. Sendrier.

On the concatenated structure of a linear code.

AAECC, 9(3):221-242, 1998

Which code Family? - Binary Goppa codes

➤ Binary Goppa codes



R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.

DSN Progress Report, 42-44:114-116, 1978.

Parameters	Key size	Security level
$[1024, 524, 101]_2$	67 ko	2^{62}
$[2048, 1608, 48]_2$	412 ko	2^{96}

Which code Family? - Binary Goppa codes

➤ Binary Goppa codes



R. J. McEliece.

A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

Parameters	Key size	Security level
$[1024, 524, 101]_2$	67 ko	2^{62}
$[2048, 1608, 48]_2$	412 ko	2^{96}



**McEliece scheme with Goppa codes
has resisted cryptanalysis so far!**

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**

Code-Based Cryptography

1. Error-Correcting Codes and Cryptography
2. **McEliece Cryptosystem**
3. Message Attacks (ISD)
4. Key Attacks
5. Other Cryptographic Constructions Relying on Coding Theory