McEliece asymmetric encryption algorithm

Vojtěch Myslivec, Róbert Lórencz

Faculty of information technology
Czech Technical University in Prague

November 24, 2020

Introduction

- The McEliece cryptosystem is an asymmetric encryption algorithm (1978 Robert McEliece [1])
- First scheme that used ranomization in the encryption process
- Never was popular in the cryptographic community
- A candidate for *post-quantum cryptography* because it is resistant against attack using quantum computers (Shor algorithm)
- Uses a linear code for error correction
  - Random error vector as a part of the cipher
  - Decoding a general linear code is an NP-hard problem [2]
- Large key size (hundreds of kilobits to megabits)

McEliece Cryptosystem

Key generation

1. *Linear code* $\mathcal{K}$ (n, k) correcting t errors, with $k \times n$ generator matrix G
2. Random $k \times k$ non-singular matrix S
3. Random $n \times n$ permutation matrix P
4. Compute $k \times n$ matrix $\hat{G} = SGP$

Generated keys

Public parameters

Numbers k, n, t

Public key

Matrix $\hat{G}$ $(\hat{G} = SGP)$

Private key

Matrices S, P and code $\mathcal{K}$ generated by G

McEliece Cryptosystem

Example

Code Γ with parameters $(n, k, t) = (8, 2, 2)$:

$$G = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Random matrices S and P:

$$S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$SG = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Public key – matrix $\hat{G}$:

$$\hat{G} = SGP = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

McEliece cryptosystem

Encryption

Algorithm E**:**

Let us have a message m of length k, public key $\hat{G}$ and parameter t

1. Generate an error vector z of length n with *Hamming weight* t
2. Ciphertext $c = m\hat{G} + z$

Decryption

Algorithm D**:**

1. Compute $\hat{c} = cP^{-1}$
2. Decode $\hat{m}$ z $\hat{c}$ using the chosen code
   $Dec(\hat{c}) = \hat{m}$
3. Compute the original plaintext $m = \hat{m}S^{-1}$

Example encryption

Plaintext $m = (\ 1\ 1\ )$, random error vector z *of weight* $t = 2$:

$$c = m\hat{G} + z = (\,1\ 1\,)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} + (\,1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\,)$$

$$c = (\,1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\,)$$

Example decryption

Multiply c with inverse permutation:

$$\hat{c} = cP^{-1} = (\,0\ 1\ 1\ 0\ 1\ 1\ 1\ 0\,)$$

Decode with the Γ code – error correction:

$$\hat{m} = Dec_{\Gamma}(\hat{c}) = (\,0\ 1\,)$$

Multiply by inverse S:

$$m = \hat{m}S^{-1} = (\,0\ 1\,)\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} = (\,1\ 1\,)$$

McEliece cryptanalysis

Secure parameters

Cryptosystem	Parameters	Security strength	Key size	Complexity encr.	Complexity decr.
RSA	1024b modulus	~ 80 b	1 kb	2^{30}	2^{30}
	2048b modulus	~ 112 b	2 kb	2^{33}	2^{33}
	4096b modulus	~ 145 b	4 kb	2^{36}	2^{36}
McEliece	$(2048, 1608, 40)$	~ 98 b	691 kb	2^{20}	2^{23}
	$(2048, 1278, 70)$	~ 110 b	961 kb	2^{20}	2^{24}
	$(4096, 2056, 170)$	~ 184 b	4096 kb	2^{22}	2^{26}

Table: Comparison of *McEliece* and *RSA* according to [4, 6]

Binary Goppa codes

- Can correct arbitrary number of errors
- Basis for *code-based* cryptography
- No attacks on the code structure known

Binary Goppa codes

Creation of a binary (irreducible) Goppa code

Code Γ with parameters $(n, k) = (2^m, 2^m - tm)$ correcting t errors

- **Goppa polynomial** g
  Irreducible of degree t, from the ring of polynomials $GF(2^m)[x]$
  $\Rightarrow$ field *extension* $GF((2^m)^t)$
- **Support** L
  Random permutation of all elements from the field $GF(2^m)$
- **Parity-check matrix** H (over $GF(2^m)$)

$$H = VD$$

Binary Goppa codes

Example

Irreducible *Goppa* polynomial $g(x) = (001)x^2 + (100)x + (001)$ over the field $GF(2^3)$ with irreducible polynomial 1011.
Generate the support L:

$$L = (100, 001, 111, 011, 010, 000, 101, 110)$$

Vandermond matrix V and *diagonal* matrix D:

$$V = \begin{pmatrix} 001 & 001 & 001 & \dots & 001 \\ 100 & 001 & 111 & \dots & 110 \end{pmatrix} \quad D = \begin{pmatrix} 001 & & & \\ & 111 & & \\ & & \ddots & \\ & & & 011 \end{pmatrix}$$

By multiplying the matrices, we get the *parity-check* matrix H (over $GF(2^m)$):

$$H = VD = \begin{pmatrix} 001 & 111 & 110 & 110 & 011 & 001 & 111 & 011 \\ 100 & 111 & 100 & 001 & 110 & 000 & 110 & 001 \end{pmatrix}$$

Binary Goppa codes

Decoding

Patterson Algorithm [7]

- Corrects up to t errors
- Computation in the field $GF((2^m)^t)$
- Individual steps:
  - Square root computation
  - Modified *EEA* Algorithm
  - Error locator polynomial construction
  - Search for roots of the error locator polynomial

Finite field extensions

- Necessary for working with *Goppa codes*
- Implemented operations
  - Addition
  - Multiplication
  - Exponentiation
  - Inverse
  - ...

Finite field extensions

Example

Extended Euclidean Algorithm for computing the *inverse* of polynomial $(101)x^3 + (010)x^2 + (110)x + (111)$ *modulo* $(001)x^4 + (011)x^3 + (011)x^2 + (001)x + (011)$ (over the field $GF(2^3)$ with irreducible polynomial 1101):

Quotient	Remainder	Coefficient
	(001)(011)(011)(001)(011)	(000)
	(101)(010)(110)(111)	(001)
(111)(000)	(110)(011)(011)	(111)(000)
(111)(001)	(001)(100)	(010)(111)(001)
(110)(001)	(111)	(001)(111)(110)(001)

$\Rightarrow ((101)(010)(110)(111))^{-1} = (101)(001)(100)(101)$

Measurement results

- Measurement performed in the *GPU lab* (T9:350) (2016)
  - 4-core CPU Intel i5-6500, *3.2 GHz*
  - *16 GB RAM* DDR3
- For several m and t
  - Key generation
  - Encryption
  - Decryption

Measurement results

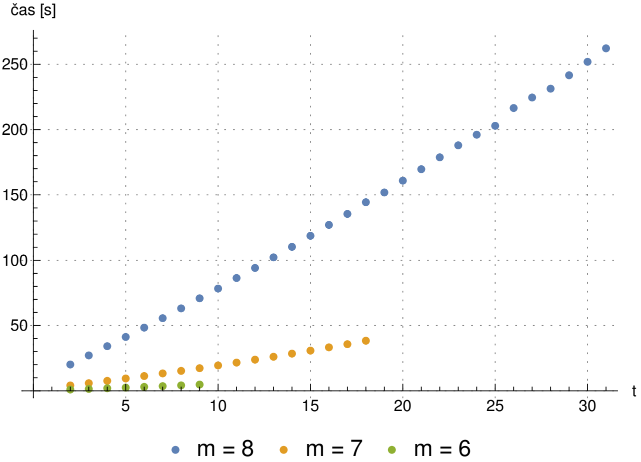

Figure: Time of key generation depending on t

Measurement results

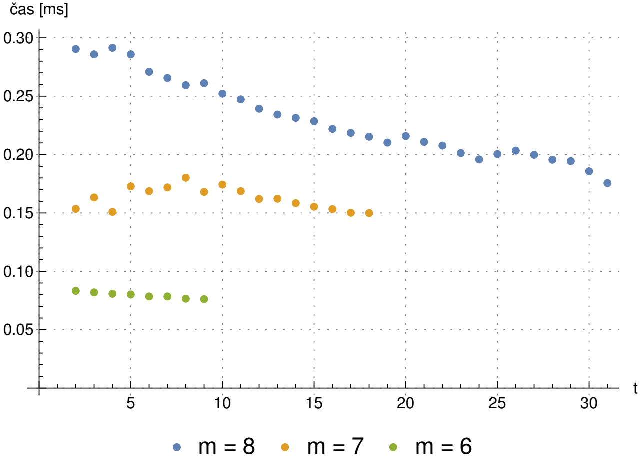

Figure: Time of message encryption depending on t

Measurement results

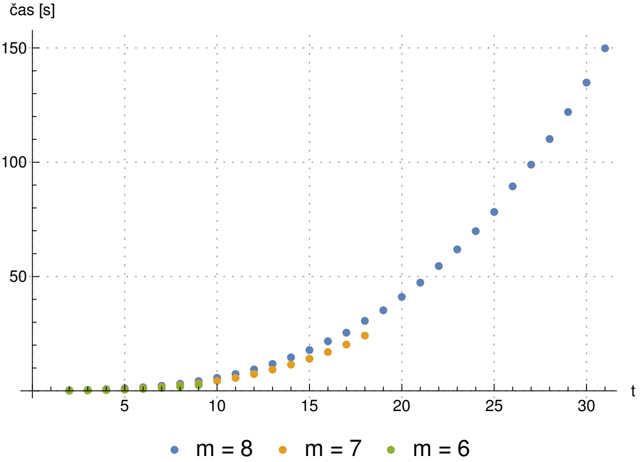

Figure: Závislost doby deEncryption zprávy na parametru t

Measurement results

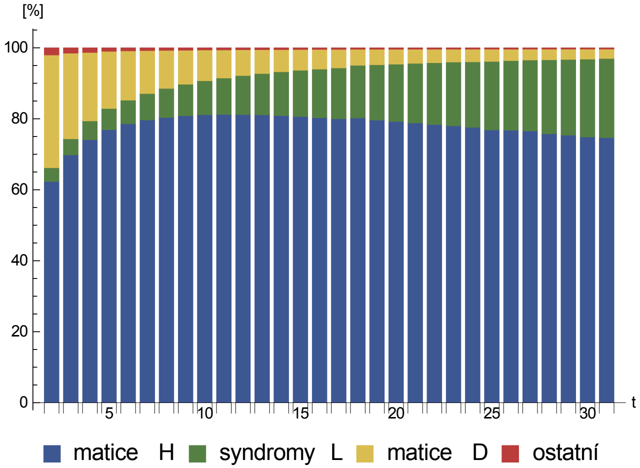

Figure: Ratio of important parts of key generation depending on the parameter t (with $m = 8$)

Measurement results

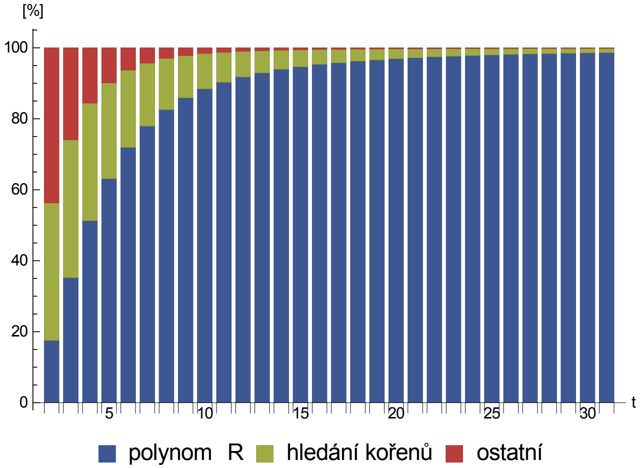

Figure: Ratio of important parts of message decryption depending on the parameter t (with $m = 8$)

Cryptanalysis of McEliece

Known attacks on McEliece

- Attacks on the public key
  - Attacks on the structure of the code used
  - *Support Spliting Algorithm*
- Attacks on the ciphertext
  - *Information set* decoding
  - Finding a *low Hamming weight codeword*
    - Algorithm Canteaut and Chabaud [**?**]

Conclusion

- Algorithm description
  - Basic variant and a digital signature scheme
  - Cryptanalysis
  - Methods of key size reduction and moder variants
- Demonstration implementation
  - Reusable packages
- Experimentally confirmed complexity
  - Isolated critical parts of computation

References I

[1] Robert J. McEliece. A Public-Key Cryptosystem Based on Algebraic Coding Theory v *JPL Deep Space Network Progress Report*, strany 114-116. 1978. Dostupné online http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF

[2] Elwyn R. Berlekamp, Robert J. McEliece, Henk C. A. van Tilborg. On the Inherent Intractibility v *IEEE Transactions of Information Theory*, vol. IT-24, No. 3, strany 384-386. IEEE, květen 1978.

[3] Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen. *Post-Quantum Cryptography*. ISBN 978-3-540-88701-0. Springer Berlin Heidelberg, 2009.

References II

[4] Daniela Engelbert, Raphael Overbeck, Arthur Schmidt. A Summary of McEliece-Type Cryptosystems and their Security v *Journal of Mathematical Cryptology*. IACR 2006. Dostupné online http://eprint.iacr.org/2006/162

[5] Valery D. Goppa. A New Class of Linear Correcting Codes v *Problemy Peredachi Informatsii*, vol. 6, strany 24-30. 1970.

[6] Christof Paar, Jan Pelzl. *Understanding Cryptography*: A Textbook for Students and Practitioners. Springer-Verlag Berlin Heidelberg, 2010. Dostupné online: https://www.springer.com/us/book/9783642041006

[7] Nicholas J. Patterson, The algebraic decoding of Goppa codes v *IEEE Transactions on Information Theory*, vol. 21, strany 203-207. IEEE 1975. Dostupné online http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1055350

References III

[8] J. M. Schanck, W. Whyte, Z. Zhang. Criteria for selection of public-key cryptographic algorithms for quantum-safe hybrid cryptography (Internet-draft). IETF, 2016. Dostupné online https://datatracker.ietf.org/doc/draft-whyte-select-pkc-qsh/