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

Circulant matrix

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{r-1} \\ a_{r-1} & a_0 & a_1 & \cdots & a_{r-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

Circulant matrix

$$\boxed{a(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_{r-1} X^{r-1}}$$

Polynomial Representation

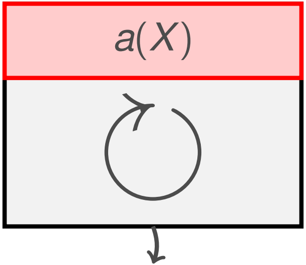
$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{r-1} \\ a_{r-1} & a_0 & a_1 & \cdots & a_{r-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

Circulant matrix

$$a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_{r-1}X^{r-1}$$

Polynomial Representation

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{r-1} \\ a_{r-1} & a_0 & a_1 & \cdots & a_{r-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} =$$



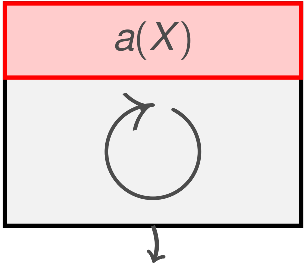
i-th row: $X^i a(X) \mod (X^r - 1)$

Circulant matrix

$$a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_{r-1}X^{r-1}$$

Polynomial Representation

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{r-1} \\ a_{r-1} & a_0 & a_1 & \cdots & a_{r-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} =$$



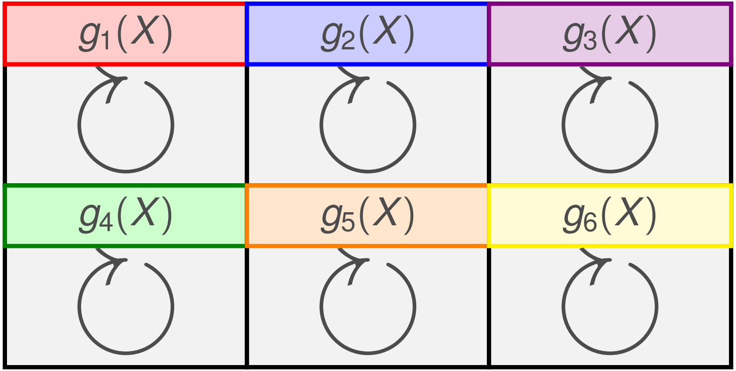
i-th row: $X^i a(X) \mod (X^r - 1)$

Proposition:

Circulant matrices of size $r \times r$ $\simeq$ Polynomials in $\mathbb{F}_q[X]/X^r - 1$

Quasi-cyclic codes

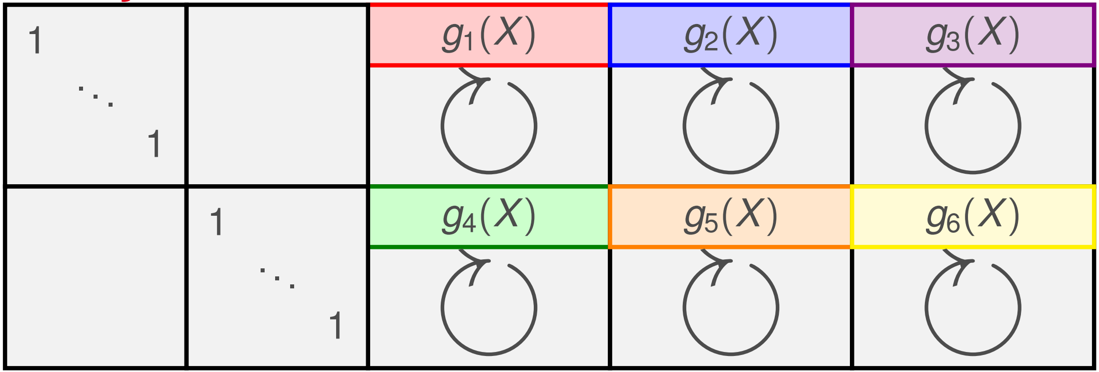
Block-Circulant Matrix



Quasi-Cyclic codes

A Linear code that admit a block-circulant parity check matrix.

Quasi-cyclic codes



Quasi-Cyclic codes

A Linear code that admit a block-circulant parity check matrix.

Variants based on Algebraic codes with symmetry

Using subcodes of BCH codes

P. Gaborit.
Shorter keys for code based cryptography.
In International Workshop on Coding and Cryptography (WCC 2005), pp. 81-91.

n	t	Claimed security	Public-Key sizes
2047	31	2^{80}	40505 bits
4095	26	2^{90}	12302 bits

Variants based on Algebraic codes with symmetry

Using subcodes of BCH codes

P. Gaborit.
Shorter keys for code based cryptography.
In International Workshop on Coding and Cryptography (WCC 2005), pp. 81-91.

n	t	Claimed security	Public-Key sizes
2047	31	2^{80}	40505 bits
4095	26	2^{90}	12302 bits

✗ Attack against this proposal:

A. Otmani, J.P. Tillich and L. Dallot.
Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes.
Special Issues of Mathematics in Computer Science, 3(2), pp. 129-140. 2010.

Variants based on Algebraic codes with symmetry

➢ Using subcodes of BCH codes

P. Gaborit.
Shorter keys for code based cryptography.
In International Workshop on Coding and Cryptography (WCC 2005), pp. 81-91.

n	t	Claimed security	Public-Key sizes
2047	31	2^{80}	40505 bits
4095	26	2^{90}	12302 bits

✗ Attack against this proposal:

A. Otmani, J.P. Tillich and L. Dallot.
Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes.
Special Issues of Mathematics in Computer Science, 3(2), pp. 129-140. 2010.

Weakness of the proposal:

1. The public code comes from a primitive BCH code

Variants based on Algebraic codes with symmetry

Using subcodes of BCH codes

P. Gaborit.
Shorter keys for code based cryptography.
In International Workshop on Coding and Cryptography (WCC 2005), pp. 81-91.

n	t	Claimed security	Public-Key sizes
2047	31	2^{80}	40505 bits
4095	26	2^{90}	12302 bits

Attack against this proposal:

A. Otmani, J.P. Tillich and L. Dallot.
Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes.
Special Issues of Mathematics in Computer Science, 3(2), pp. 129-140. 2010.

Weakness of the proposal:

1. The public code comes from a primitive BCH code
2. The permutation (used to hide the secret code) is too restrictive

Variants based on Algebraic codes with symmetry

➢ Using subcodes of QC-Alternant codes

T.P. Berger, P.L. Cayrel, P. Gaborit and A. Otmani.
Reducing key length of the McEliece cryptosystem.
In AFRICACRYPT 2009, pp. 77-97.

q	n	k	t	Security	Public-Key sizes
2^8	663	561	25	2^{80}	8980 bits
2^8	663	510	37	2^{95}	12240 bits
2^8	1020	867	37	2^{116}	20800 bits

✗ Attack against this proposal:

J.C. Faugère, A. Otmani, L. Perret and J.P. Tillich.
Algebraic cryptanalysis of McEliece variants with compact keys.
In EUROCRYPT 2010, pp. 279-298.

Variants based on Algebraic codes with symmetry

Idea of the attack:

Solve the system

$$G \, H^T = 0$$

Variants based on Algebraic codes with symmetry

Idea of the attack:

Solve the system

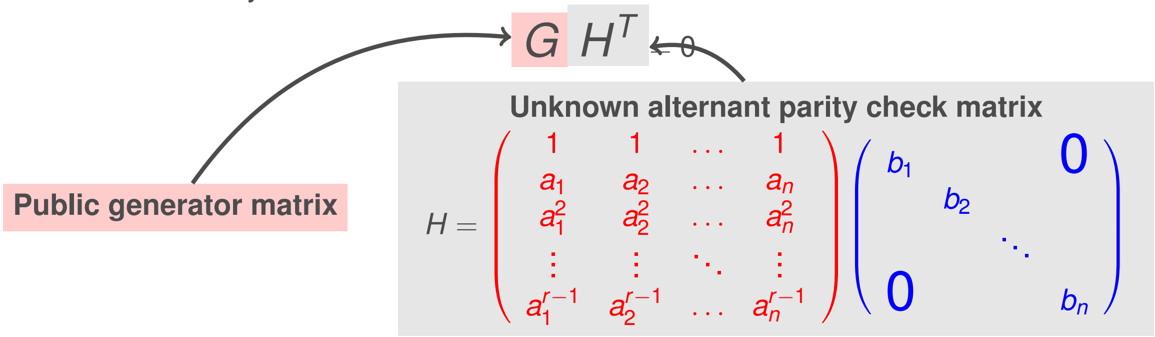
$$G \, H^T = 0$$

Public generator matrix

Variants based on Algebraic codes with symmetry

Idea of the attack:

Solve the system



$$G\,H^T = 0$$

Public generator matrix

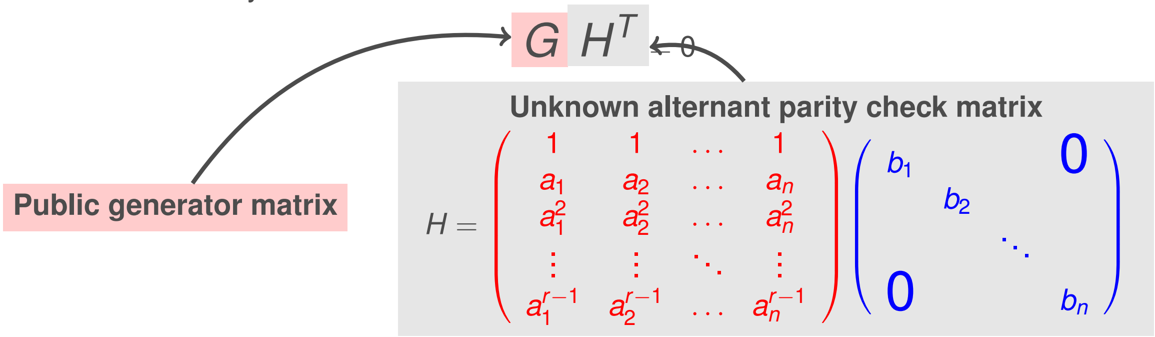
Unknown alternant parity check matrix

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{r-1} & a_2^{r-1} & \cdots & a_n^{r-1} \end{pmatrix} \begin{pmatrix} b_1 & & & \mathbf{0} \\ & b_2 & & \\ & & \ddots & \\ \mathbf{0} & & & b_n \end{pmatrix}$$

Variants based on Algebraic codes with symmetry

Idea of the attack:

Solve the system



$$G\,H^T = 0$$

Public generator matrix

Unknown alternant parity check matrix

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{r-1} & a_2^{r-1} & \cdots & a_n^{r-1} \end{pmatrix} \begin{pmatrix} b_1 & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix}$$

The quasi-cyclic structure allows a drastic reduction of the number of unknowns

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