Code-Based Cryptography

McEliece Cryptosystem

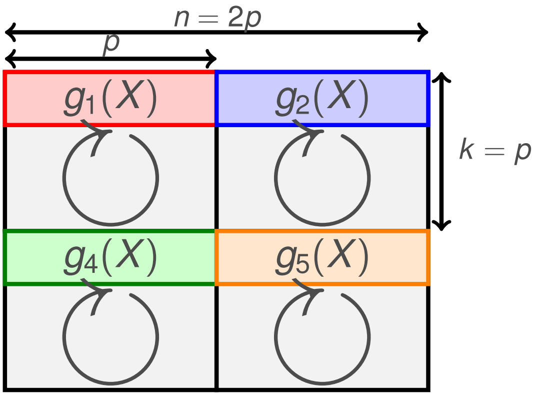
I. Márquez-Corbella

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

MDPC - Introduction

Moderate Density Parity Check (MDPC)



R. Misoczki, J.P. Tillich, N. Sendrier, P. Barreto.
New McEliece variants from moderate density parity-check codes.
IACR Cryptology ePrint Archive, Report 2012/409, 2012.

R. Misoczki, J.P. Tillich, N. Sendrier, P. Barreto.
MDPC-McEliece: New McEliece variants from moderate density parity-check codes.
ISIT 2013, pp. 2069-2073.

QC-MDPC McEliece scheme

Key Generation Algorithm:

- Pick a (sparse) vector $(h_0, h_1) \in \{0,1\}^p \times \{0,1\}^p$ of weight w

  Repeat until $h_0(X)$ is invertible in $\mathbb{F}_2[X]/X^p - 1$ (The weight of h_0 has to be odd)

QC-MDPC McEliece scheme

Key Generation Algorithm:

➜ Pick a (sparse) vector $(h_0, h_1) \in \{0,1\}^p \times \{0,1\}^p$ of weight w

Repeat until $h_0(X)$ is invertible in $\mathbb{F}_2[X]/X^p - 1$ (The weight of h_0 has to be odd)

$$H_{\text{secret}} = \begin{array}{|c|c|} \hline h_0 & h_1 \\ \hline \circlearrowright & \circlearrowright \\ \hline \end{array}$$

QC-MDPC McEliece scheme

Key Generation Algorithm:

- Pick a (sparse) vector $(h_0, h_1) \in \{0,1\}^p \times \{0,1\}^p$ of weight w

  Repeat until $h_0(X)$ is invertible in $\mathbb{F}_2[X]/X^p - 1$ (The weight of h_0 has to be odd)

$$H_{\text{secret}} = \left[\begin{array}{c|c} h_0 & h_1 \\ \hline & \end{array}\right]$$

$$G_{\text{public}} = \left[\begin{array}{c|ccc} g & 1 & & 0 \\ \hline & & \ddots & \\ & 0 & & 1 \end{array}\right] \quad \text{or} \quad H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ \hline & \ddots & & \\ 0 & & 1 & \end{array}\right]$$

with $h(X) = \frac{h_1(X)}{h_0(X)}$ and $g(X) = x\overline{h(x)}$

$$h(X) = h_0 + h_1 X + \ldots + h_{p-1} X^{p-1} \implies \overline{h(X)} = h_{p-1} + \ldots + h_1 X^{p-2} + h_0 X^{p-1}$$

QC-MDPC McEliece scheme

Encryption Algorithm:

Encrypt a message $m(X) \in \frac{\mathbb{F}_2[X]}{\langle X^p - 1 \rangle}$ as

$$\textsc{Encrypt}(m(X)) = \left(\; m(X)g(X) + e_0(X), \quad m(X) + e_1(X) \; \right)$$

where $\mathbf{e}(X) = (e_0(X), e_1(X))$ is a random error vector of weight at most t.

QC-MDPC McEliece scheme

Encryption Algorithm:

Encrypt a message $m(X) \in \frac{\mathbb{F}_2[X]}{\langle X^p - 1 \rangle}$ as

$$\textsc{Encrypt}(m(X)) = \left(\ m(X)g(X) + e_0(X), \quad m(X) + e_1(X) \ \right)$$

where $\mathbf{e}(X) = (e_0(X), e_1(X))$ is a random error vector of weight at most t.

Decryption Algorithm:

The secret key will be any LDPC-like iterative decoding algorithm.

(Gallager's bit-flipping algorithm)

Security Reduction

$$H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ & \ddots & & \circlearrowright \\ 0 & & 1 & \end{array}\right] \quad \text{with } h(X) = \frac{h_1(X)}{h_0(X)} \mod X^p - 1$$

Security Reduction

$$H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ & \ddots & & \circlearrowright \\ 0 & & 1 & \end{array}\right] \quad \text{with } h(X) = \frac{h_1(X)}{h_0(X)} \mod X^p - 1$$

The QC-MDPC is secure under two assumptions:

Security Reduction

$$H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ & \ddots & & \circlearrowright \\ 0 & & 1 & \end{array}\right] \quad \text{with } h(X) = \frac{h_1(X)}{h_0(X)} \mod X^p - 1$$

The QC-MDPC is secure under two assumptions:

1. **QC - MDPC indistinguishability:**
   Pseudorandomness of the public key

   Hard to find sparse vector in the code spanned by H
   (dual of the MDPC code).

Security Reduction

$$H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ & \ddots & & \\ 0 & & 1 & \end{array}\right] \quad \text{with } h(X) = \frac{h_1(X)}{h_0(X)} \mod X^p - 1$$

The QC-MDPC is secure under two assumptions:

1. **QC - MDPC indistinguishability:**
   Pseudorandomness of the public key

   Hard to find sparse vector in the code spanned by H (dual of the MDPC code).

2. **QC Syndrome Decoding:** Hardness of generic decoding of QC codes

Security Reduction - in terms of polynomials

$$H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ & \ddots & & \circlearrowright \\ 0 & & 1 & \end{array}\right] \quad \text{with } h(X) = \frac{h_1(X)}{h_0(X)} \mod X^p - 1$$

Security Reduction - in terms of polynomials

$$H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ & \ddots & & \circlearrowleft \\ 0 & & 1 & \end{array}\right] \quad \text{with } h(X) = \frac{h_1(X)}{h_0(X)} \mod X^p - 1$$

1. **QC - MDPC indistinguishability:**
   Given $h(X)$, find non-zero $(h_0(X), h_1(X))$ such that:

$$\begin{cases} h_0(X) + h(X)h_1(X) = 0 \mod X^p - 1 \\ w_{\mathrm{H}}(h_0) + w_{\mathrm{H}}(h_1) \leq w \end{cases}$$

Security Reduction - in terms of polynomials

$$H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ & \ddots & & \\ 0 & & 1 & \end{array}\right] \quad \text{with } h(X) = \frac{h_1(X)}{h_0(X)} \mod X^p - 1$$

1. **QC - MDPC indistinguishability:**
   Given $h(X)$, find non-zero $(h_0(X), h_1(X))$ such that:

$$\begin{cases} h_0(X) + h(X)h_1(X) = 0 \mod X^p - 1 \\ w_{\mathrm{H}}(h_0) + w_{\mathrm{H}}(h_1) \leq w \end{cases}$$

2. **QC Syndrome Decoding:**
   Given $h(X)$, $S(X)$. Find $e(X) = (e_0(X), e_1(X))$ such that

$$\begin{cases} e_0(X) + h(X)e_1(X) = S(X) \mod X^p - 1 \\ w_{\mathrm{H}}(e_0) + w_{\mathrm{H}}(e_1) \leq t \end{cases}$$

Security Reduction - in terms of polynomials

$$H_{\text{public}} = \left[\begin{array}{ccc|c} 1 & & 0 & h \\ & \ddots & & \circlearrowright \\ 0 & & 1 & \end{array}\right] \quad \text{with } h(X) = \frac{h_1(X)}{h_0(X)} \mod X^p - 1$$

1. **QC - MDPC indistinguishability:**
   Given $h(X)$, find non-zero $(h_0(X), h_1(X))$ such that:
   $$\begin{cases} h_0(X) + h(X)h_1(X) = 0 \mod X^p - 1 \\ w_{\mathrm{H}}(h_0) + w_{\mathrm{H}}(h_1) \leq w \end{cases}$$

2. **QC Syndrome Decoding:**
   Given $h(X)$, $S(X)$. Find $e(X) = (e_0(X), e_1(X))$ such that
   $$\begin{cases} e_0(X) + h(X)e_1(X) = S(X) \mod X^p - 1 \\ w_{\mathrm{H}}(e_0) + w_{\mathrm{H}}(e_1) \leq t \end{cases}$$

In both cases, best known solutions use generic decoding algorithms

Practical Security - Best known attacks

$W_{\mathrm{SD}}(n, k, t)$ = cost for the generic decoding of t errors in a binary $[n, k]$ code

Parameters:

n k w and p

Practical Security - Best known attacks

$W_{\mathrm{SD}}(n, k, t)$ = cost for the generic decoding of t errors in a binary $[n, k]$ code

Parameters:

$n \rightarrow$ length k w and p

Practical Security - Best known attacks

$W_{\mathrm{SD}}(n, k, t)$ = cost for the generic decoding of t errors in a binary $[n, k]$ code

Parameters:

n $k \rightarrow$ dimension w and p

Practical Security - Best known attacks

$W_{\mathrm{SD}}(n, k, t)$ = cost for the generic decoding of t errors in a binary $[n, k]$ code

Parameters:

n k $w \to$ weight of the parity check equations and p

Practical Security - Best known attacks

$W_{\mathrm{SD}}(n, k, t)$ = cost for the generic decoding of t errors in a binary $[n, k]$ code

Parameters:

n k w and $p \rightarrow$ circulant blocks of size p

Practical Security - Best known attacks

$W_{\mathrm{SD}}(n,k,t)$ = cost for the generic decoding of t errors in a binary $[n,k]$ code

Parameters:

n k w and p

1. **QC-MDPC Indistinguishability:** Find a word of weight w in a quasi-cyclic binary $[n, n-k]$ code

$$W_K(n,k,w) \geq \frac{W_{\mathrm{SD}}(n,n-k,w)}{n-k}$$

(there are $n-k$ words of weight w)

Practical Security - Best known attacks

$W_{\mathrm{SD}}(n, k, t)$ = cost for the generic decoding of t errors in a binary $[n, k]$ code

Parameters:

n k w and p

1. **QC-MDPC Indistinguishability:** Find a word of weight w in a quasi-cyclic binary $[n, n-k]$ code

$$W_K(n, k, w) \geq \frac{W_{\mathrm{SD}}(n, n-k, w)}{n-k}$$

(there are $n-k$ words of weight w)

2. **QC Syndrome Decoding:** Decode t errors in a quasi-cyclic binary $[n, k]$ code

$$W_M(n, k, t, p) \geq \frac{W_{\mathrm{SD}}(n, k, t)}{\sqrt{p}}$$

(Decoding One Out of Many $\rightarrow$ factor $\sqrt{p}$)

N. Sendrier
Decoding one out of many.
Post-Quantum Cryptography, 2011, 51-67, 2011.

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

p w and t

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

$p \rightarrow$ block size $\quad w \quad$ and $\quad t$

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

p $\quad$ $w \rightarrow$ weight of the parity check equations $\quad$ and $\quad$ t

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

p w and $t \longrightarrow$ error weight

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

p w and t

Thus parameters will be such that:

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

$$p \quad w \quad \text{and} \quad t$$

Thus parameters will be such that:

- Find w the smallest integer such that $W_K(n, k, w) \geq 2^S$

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

$$p \quad w \quad \text{and} \quad t$$

Thus parameters will be such that:

- Find w the smallest integer such that $W_K(n, k, w) \geq 2^S$
- Find t the error correcting capability of the corresponding MDPC code

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

p w and t

Thus parameters will be such that:

- Find w the smallest integer such that $W_K(n, k, w) \geq 2^S$
- Find t the error correcting capability of the corresponding MDPC code
- Check that $W_M(n, k, t, p) \geq 2^S$

Parameter Selection

To reach a given security level S (for instance 80 or 128) we need to select the parameters

$$p \quad w \quad \text{and} \quad t$$

Thus parameters will be such that:

- Find w the smallest integer such that $W_K(n, k, w) \geq 2^S$
- Find t the error correcting capability of the corresponding MDPC code
- Check that $W_M(n, k, t, p) \geq 2^S$

80 bits of security		128 bits of security
$n = 9602$ $k = 4801$ $p = 4801$ $w = 90$ $t = 84$		$n = 19714$ $k = 9857$ $p = 9857$ $w = 142$ $t = 134$

Conclusion

QC-MDPC-McEliece is a **promising** variant which enjoys

- ➜ a reasonable key size
- ➜ good security arguments (very little structure)
- ➜ secure against quantum computers
- ➜ easy implementation

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**