IND-CCA2 secure McEliece-type modification in the standard model

Turchenko O., Kosolapov Y.

Southern federal university, Russia

17.09.2020

McEliece cryptosystem (over $\mathbb{F}_q^n$)

G is a generator matrix of $[n, k, d]$ Goppa code, S is a non-singular $(k \times k)$-matrix and P is a permutation $(n \times n)$-matrix.

$sk = (S, G, P)$, $pk = (\widetilde{G} = SGP, t)$

Encryption:

$$\{\mathbf{m}\}_{pk}^{\mathrm{McE}} = \mathbf{m}\widetilde{G} + \mathbf{e} = \mathbf{c}, \text{where } \mathbf{e} \in_R \mathcal{E}_{n,t}$$

Decryption:

$$\{\mathbf{c}\}_{sk}^{\mathrm{McE}} = \mathrm{Decoder}_C(\mathbf{c}P^{-1})S^{-1}.$$

McEliece cryptosystem

Key features of original McEliece cryptosystem:

- \+ there are no structural attacks so far (with Goppa code)
- \+ resistance to quantum computer attacks
- \+ fast encryption and decryption operations
- – large public and secret keys
- – not secure against ciphertext attacks

Way of constructing IND-CCA2 modification

Based on ideas of Dottling et al.[1] we construct the following nested encryption schemes:

- Basic cryptosystem
- Verifiable auxiliary cryptosystem
- S-concatenation cryptosystem with one time strong signature

[1] Dottling N., Dowsley R., Muller-Quade J. and Nascimento A. C. A. // A CCA2 Secure Variant of the McEliece Cryptosystem

Basic McEliece modification bMcE$_l$

Necessary notions:

- For $\omega = \{\omega_1, ..., \omega_l\} \subset [k] = \{1, ..., k\}$ consider a subset $\mathcal{G}(\omega)$ of permutations group $\mathcal{S}_l$:

$$\mathcal{G}(\omega) = \{\pi \in \mathcal{S}_l : \pi(1) = \omega_1, ..., \pi(l) = \omega_l\}.$$

- For every π from $\mathcal{G}(\omega)$ associate $(l \times l)$-matrix R_π.
- $\mathcal{E}_{n,t,\beta}$ is subset of $\mathbb{F}_2^n$ such that any vector $\mathbf{e} = (e_1, ..., e_n)(\in \mathcal{E}_{n,t,\beta})$ has Hamming weight t and $e_i = 0$ for any $i \in \beta$.

Basic McEliece modification bMcE$_l$

Encryption:

$$\{\mathbf{m}\}^{\mathrm{bMcE}_l}_{pk,\omega} = \{(\mathbf{m} \parallel \mathbf{r}_1)R_\pi\}^{\mathrm{McE}}_{pk} \parallel \{(\mathbf{m} \parallel \mathbf{r}_2)R_\pi\}^{\mathrm{McE}}_{pk} = \mathbf{c}_1 \parallel \mathbf{c}_2 = \mathbf{c},$$

where

- $\mathbf{m} \in \mathbb{F}_2^l$,
- $\omega \subset_R [k]$, $|\omega| = l$, $\pi \in_R \mathcal{G}(\omega)$,
- $\mathbf{r}_1 \in_R \mathbb{F}_2^{k-l}$, $\mathbf{r}_2 : \mathrm{supp}(\mathbf{r}_1 - \mathbf{r}_2) = [k] \setminus \omega$
- $\mathbf{e}_1$ and $\mathbf{e}_2$ in McE-encryption are chosen such that $\mathbf{e}_1 \in_R \mathcal{E}_{n,t}$, $\mathbf{e}_2 \in_R \mathcal{E}_{n,t,\mathrm{supp}(\mathbf{e}_1)}$.

Basic McEliece modification bMcE$_I$

Decryption:

1. Decrypt $\{\mathbf{c}_1\}_{sk}^{\mathrm{McE}} = (\mathbf{m} \parallel \mathbf{r}_1)R_\pi$ and $\{\mathbf{c}_2\}_{sk}^{\mathrm{McE}} = (\mathbf{m} \parallel \mathbf{r}_2)R_\pi$
2. Calculate $(\mathbf{m} \parallel \mathbf{r}_1)R_\pi \oplus (\mathbf{m} \parallel \mathbf{r}_2)R_\pi = (\mathbf{0} \parallel \mathbf{1})R_\pi$
3. Find $\omega = [k] \setminus \mathrm{supp}((\mathbf{0} \parallel \mathbf{1})R_\pi)$
4. Return $\mathbf{m} = \Pi_\omega((\mathbf{m} \parallel \mathbf{r}_1)R_\pi)$

Auxilary McEliece modification $\widehat{\text{bMcE}}_l^s$

$$pk = (pk_1, ..., pk_s), sk = (sk_1, ..., sk_s),$$
$$\mathbf{m} = (\mathbf{m}_1 \parallel ... \parallel \mathbf{m}_s)$$

Encryption:

$$\{\mathbf{m}\}_{pk}^{\widehat{\text{bMcE}}_l^s} = \mathbf{c}' = \overbrace{[\mathbf{c}'_{1,1} \parallel \mathbf{c}'_{1,2}]}^{\mathbf{c}'_1} \parallel ... \parallel \overbrace{[\mathbf{c}'_{s,1} \parallel \mathbf{c}'_{s,2}]}^{\mathbf{c}'_s},$$

where $\mathbf{c}'_j = [\mathbf{c}'_{j,1} \parallel \mathbf{c}'_{j,2}] = \{\mathbf{m}_j\}_{pk_j,\omega}^{\text{bMcE}_l}$ for $j \in [s]$ and ω is chosen randomly once for all $j = 1, ..., s$.

Auxilary McEliece modification $\widehat{\text{bMcE}}_l^s$

Decryption:

1. For each $\mathbf{c}'_i$ from $\mathbf{c}' = \mathbf{c}'_1 \parallel ... \parallel \mathbf{c}'_s$ find $\mathbf{m}_i = \{\mathbf{c}'_i\}_{sk_i}^{\text{bMcE}_l}$ and set ω^i
2. if $\omega^1 = ... = \omega^s$ return $\mathbf{m}_1 \parallel ... \parallel \mathbf{m}_s$, otherwise return $\perp$

Verifiability property

Auxiliary McEliece modification is $(1-\varepsilon)$-verifiable if there is such polynomial time algorithm *Verify* that:

- if $\mathit{Verify}(\mathbf{c}', pk, sk_i) = 1$ than $\{\mathbf{c}'\}_{sk}^{\widehat{\mathrm{bMcE}_l^s}} = \mathbf{m}$ with probability $1-\varepsilon$
- if $\mathit{Verify}(\mathbf{c}', pk, sk_i) = 0$ than $\{\mathbf{c}'\}_{sk}^{\widehat{\mathrm{bMcE}_l^s}} = \perp$ with probability $1-\varepsilon$

where ε is negligible function

Constructing a Verify algorithm

1. find ω^i from $\mathbf{c}'_i$ using sk_i
2. for each $j \neq i$ find $\mathbf{x}_j = \mathbf{c}'_{j,1} \oplus \mathbf{c}'_{j,2} = (\mathbf{0} \parallel \mathbf{1}) R_{\pi_j} \widetilde{G}_j \oplus \mathbf{e}'_{j,1} \oplus \mathbf{e}'_{j,2}$
3. for each $j \neq i$ find $\mathbf{z}_j = \mathbf{x}_j \oplus (\mathbf{0} \parallel \mathbf{1}) R_{\pi_i} \widetilde{G}_j$
4. for each $j \neq i$ check $\mathrm{wt}(\mathbf{z}_j) = 2t$. If at least one of $s - 1$ check fails then return 0.
5. for each $j \neq i$ execute the information set decoding algorithm (in polynomial time) to decrypt every $\mathbf{x}_j$ with probability $(1 - \varepsilon)$
6. check that $\omega^j = \omega^i$ for each $j \neq i$. If it's satisfied return 1, otherwise return 0.

S-concateniation McEliece modification

$$pk = ((pk_i^0, pk_i^1))_{i=1}^s, sk = ((sk_i^0, sk_i^1))_{i=1}^s,$$

Encryption:

$$\mathbf{c} = \{\mathbf{m}\}_{pk}^{\mathrm{bMcE}_l^s} = \mathbf{c}' \parallel \mathbf{vk} \parallel \sigma,$$

where

- $(\mathbf{dsk}, \mathbf{vk}) = \mathcal{K}_{\mathrm{SS}}(N)$, $\mathbf{vk} = (vk_1, ..., vk_s) \in \{0,1\}^s$
- $pk^{\mathbf{vk}} = (pk_1^{vk_1}, ..., pk_s^{vk_s})$
- $\mathbf{c}' = \{\mathbf{m}\}_{pk^{\mathbf{vk}}}^{\widehat{\mathrm{bMcE}_l^s}}$
- $\sigma = Sign(\mathbf{dsk}, \mathbf{c}')$

S-concateniation McEliece modification

Decryption:

1. check signature of the message $\mathbf{c}'$. If $Check(\mathbf{c}', \mathbf{vk}, \sigma) = 0$ then return $\perp$
2. return $\mathbf{m}' = \{\mathbf{c}'\}_{sk^{\mathbf{vk}}}^{\widehat{\mathrm{bMcE}_l^s}}$ where $sk^{\mathbf{vk}} = (sk_1^{vk_1}, ..., sk_s^{vk_s})$.

Standard security assumptions

Assumption

There is no polynomial algorithm capable of distinguishing the $(k \times n)$-matrix of the public key of the McE cryptosystem from a random $(k \times n)$-matrix with non-negligible probability in N.

Assumption

There is no polynomial algorithm that solves the problem of decoding a general linear code.

Additional assumption

Assumption

There is no polynomial algorithm that takes as input ciphertext $\mathbf{c}$ of the McE and the number $L \in \mathbb{N}$, and outputs 0 if $\mathbf{c}$ corresponds to an information message of a weight less than L and outputs 1 if $\mathbf{c}$ corresponds to an information message of weight L with non-negligible distinguishing advantage in the N.

Results

Theorem

bMcE_l is IND-CPA secure if assumptions 1-3 hold.

Theorem

$\widehat{\text{bMcE}_l^s}$ is IND-CPA secure if assumptions 1-3 hold.

Theorem

bMcE_l^s is IND-CCA2 secure if assumptions 1-3 hold.

Practical recommendations

- Goppa code parameters[2]:
  $[4096, 3604, 83]$
- The length of information message $s \cdot l$ where:
  $l = k/2$ ($C_k^{\frac{k}{2}}$ variants to brute force)
- One-time strong signature scheme:
  Stern signature (public key size - 347 bits)

[2]Bernstein D.J., Chou T. and Schwabe P. // McBits: Fast Constant-Time Code-Based Cryptography

Comparison

IND-CCA2 secure schemes based on McEliece cryptosystem

Scheme	Public key	Secret key
Persichetti	$2 \cdot k \cdot \lvert pk_{\mathrm{McE}} \rvert$	$2 \cdot k \cdot \lvert sk_{\mathrm{McE}} \rvert$
Dottling et al.	$2 \cdot \lvert vk \rvert \cdot \lvert pk_{\mathrm{McE}} \rvert$	$2 \cdot \lvert vk \rvert \cdot \lvert sk_{\mathrm{McE}} \rvert$
Proposed	$2 \cdot \lvert vk \rvert \cdot \lvert pk_{\mathrm{McE}} \rvert$	$2 \cdot \lvert vk \rvert \cdot \lvert sk_{\mathrm{McE}} \rvert$

- k – code dimension
- $|vk|$ – verification key size,
- $|pk_{\mathrm{McE}}|$ – McE public key size,
- $|sk_{\mathrm{McE}}|$ – McE private key size.

Comparison

IND-CCA2 secure schemes based on McEliece cryptosystem

Scheme	Plaintext	Cyphertext
Persichetti	$*$	$n \cdot k + \|vk\| + \|\sigma\|$
Dottling et al.	l	$n \cdot \|vk\| + \|vk\| + \|\sigma\|$
Proposed	$l \cdot \|vk\|$	$2 \cdot n \cdot \|vk\| + \|vk\| + \|\sigma\|$

- $*$ – from 1 to cyphertext size
- k – code dimension
- $|vk|$ – verification key size,
- $|\sigma|$ – signature size.

Comparison

Cyphertext sizes for suggested parameters.

Scheme	Plaintext size	Cyphertext size
Dottling et al.	1.802	1.541.659
Proposed	625.294	2.962.971

Thank you for your attention!