number of unsuitable Boolean functions in $n$ variables for the combiner generator with LFSRs of lengths $n_1, \ldots, n_m$ all based on primitive polynomials is equal to

$$2^{2^{n_1+n_2+\cdots+n_m}-(2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_m}-1)} \sum_{\beta\in\mathbb{F}_2^s,\beta\neq 0} (-1)^{\beta_1+\cdots+\beta_s+1} 2^{p_1^{\alpha_1-\beta_1}\ldots p_s^{\alpha_s-\beta_s}},$$

where $\beta = (\beta_1, \ldots, \beta_s)$.

## 3. Functions for models with nonlinear registers

A *nonlinear feedback shift register* (*NFSR*) consists of two parts: a binary vector $x = (x_{n-1}, \ldots x_0)$ of length $n$ and a nonlinear state function $f : (x_{n-1}, \ldots, x_0) \to \{0, 1\}$ in $n$ variables.

Similarly to the linear case, consider the filter generator. We assume that NFSR passes over all $2^n$ states, i.e., it has maximal possible period.

**Theorem 3.** Let $n$ be an integer. Then the number of unsuitable Boolean functions in $n$ variables for the filter generator with NFSR of the maximal possible period is equal to $2^{2^{n-1}}$.

There is an another question related to NFSRs: how to determine for which nonlinear feedback functions NFSR of length $n$ has the maximal possible period $2^n$? This question is hard and still open.

We kindly thank the reviewer for careful reading of our paper and significant remarks.

REFERENCES

1. *Key E.* An analysis of the structure and complexity of nonlinear binary sequence generators. IEEE Trans. Inform Theory, 1976, no. 22, pp. 732–736.
2. *Gluhov M. M., Elizarov V. P., Nechaev A. A.* Algebra [Algebra]. Moscow, Gelios ARV Publ., 2003. (in Russian)
3. *Roman'kov V. A.* Vvedenie v kriptografiyu [Introduction to Cryptography]. Moscow, Forum Publ., 2012. (in Russian)
4. *Tokareva N. N.* Simmetrichnaya kriptografiya. Kratkiy kurs [Symmetric Cryptography. A Short Course]. Novosibirsk, NSU Publ., 2012.
5. *Carlet C.* Boolean functions for cryptography and error-correcting codes. Eds. P. Hammer and Y. Crama. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, Cambridge Univ. Press, 2010. Ch. 8, pp. 257–397. `www.math.univ-paris13.fr/~carlet/`.
6. *Hell M., Johansson T., and Meier W.* A stream cipher for constrained environments. Int. J. Wireless Mobile Comput., 2007, vol. 2, no. 1, pp. 86–93.
7. *Kumar N., Ojha S., Jain K., and Lal S.* BEAN: A lightweight stream cipher. Proc. 2nd Intern. Conf. SIN'2009, ACM, 2009, pp. 168–171.

UDC 621.391.7 DOI 10.17223/2226308X/13/24

# EFFICIENT $S$-REPETITION METHOD FOR CONSTRUCTING AN IND-CCA2 SECURE MCELIECE MODIFICATION IN THE STANDARD MODEL

Y. V. Kosolapov, O. Y. Turchenko

The paper is devoted to the construction of IND-CCA2-secure modification of the McEliece cryptosystem in the standard model. The modification uses $S$-repetition encryption of $S/2$ various messages with one common secret permutation, in contrast to other modifications that use $S$-repetition encryption of one message. Thus, this modification provides IND-CCA2-security with an efficient information transfer rate.

**Ключевые слова:** *post-quantum cryptography, McEliece-type cryptosystem,* IND-CCA2-*security,* $S$*-repetition encryption.*

## 1. Introduction

Currently, much effort is being devoted to the development of quantum computers. Therefore, the study of post-quantum cryptosystems is an important task. One suitable scheme in the post-quantum era is the McEliece cryptosystem [1]. Note that the McEliece cryptosystem does not use quantum mechanical properties. However, the original McEliece scheme is vulnerable to attacks on cyphertexts. To date, many approaches have been developed to modify the McEliece cryptosystem. One of the most successful approaches is based on the application of correlated products [2]. For instance, in [3, 4] authors presented IND-CCA2-secure modifications in the standard model. At the same time, the main idea of correlated products is not effective in practice, because it requires to transmit $S$ encrypted blocks for one information message. Based on the ideas from [3], we offer a new IND-CCA2-secure modification of the McEliece cryptosystem in the standard model, which requires to transmit $S$ encrypted blocks for $S/2$ information messages.

## 2. Preliminaries

Let $n$, $t$ be natural, $2t < n$, $[n] = \{1, \ldots, n\}$, $\beta \subseteq [n]$, $2^{[n]}$ is set of all subsets of $[n]$, $\mathbb{F}_2$ be a Galois field of cardinality 2. The support of the vector $\mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{F}_2^n$ is the set $\mathrm{supp}(\mathbf{m}) = \{i : m_i \neq 0\}$ and the Hamming weight of this vector is a number $\mathrm{wt}(\mathbf{m}) = |\mathrm{supp}(\mathbf{m})|$. A function $\gamma : \mathbb{N} \to [0, 1]$ is negligible of $k$, if

$$\forall c \in \mathbb{N}\ \exists k_c \in \mathbb{N}\ \forall k > k_c\,(\gamma(k) \leqslant k^{-c}).$$

We will use the notations similarly to the [3]. If $S$ is a finite set, then $s \in_R S$ denotes the operation of picking an element at random and uniformly from $S$. Denote by $\mathcal{E}_{n,t,\beta}$ the subset of $\mathbb{F}_2^n$ such that any vector $\mathbf{e} = (e_1, \ldots, e_n) \in \mathcal{E}_{n,t,\beta}$ has Hamming weight $t$ and $e_i = 0$ for any $i \in \beta$. We will write $\mathcal{E}_{n,t}$ when $\beta = \varnothing$. Let us define a cryptosystem as triplet of algorithms, i.e. $\Sigma = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, where:

1) $\mathcal{K}$ is a probabilistic polynomial-time key generation algorithm which takes as input a security parameter $N \in \mathbb{N}$ and outputs a pair of public-key and a secret-key $(pk, sk)$;
2) $\mathcal{E}$ is probabilistic polynomial-time encryption algorithm which takes as input a public-key $pk$ and a message $\mathbf{m}$ and outputs a ciphertext $\mathbf{c}$; we will write $\{\mathbf{m}\}_{pk}^{\Sigma}$ as encryption of the message $\mathbf{m}$ with the key $pk$;
3) $\mathcal{D}$ is deterministic polynomial-time decryption algorithm which takes as input a secret-key $sk$ and a ciphertext $\mathbf{c}$ and outputs either a message $\mathbf{m}$ or a symbol $\perp$ in the case, when the ciphertext is incorrect; decryption of the ciphertext $\mathbf{c}$ on the secret key $sk$ we will denote $\{\mathbf{c}\}_{sk}^{\Sigma}$.

Let us define signature scheme ($SS$) and one-time strongly unforgeable feature in the same way as [3]. A signature scheme is triplet of algorithms $\mathrm{SS} = (\mathcal{K}_{\mathrm{SS}}, Sign, Check)$, where $\mathcal{K}$ is key generation algorithm which takes as input a security parameter $N \in \mathbb{N}$ and outputs a signing-key $\mathbf{dsk}$ and a verification-key $\mathbf{vk}$, $Sign$ is signing algorithm which takes as input a signing-key $\mathbf{dsk}$ and a message $\mathbf{m}$ and outputs a signature $\sigma$, $Check$ is checking algorithm which takes as input a verification-key $\mathbf{vk}$ a message $\mathbf{m}$ and a signature $\sigma$ and outputs 1 if

$\sigma$ is valid for $\mathbf{m}$ and 0 otherwise. It is important to note, that one-time strongly unforgeable signature scheme can be constructed using one-way functions (see [5, 6]).

Consider the McEliece cryptosystem as a triplet of polynomial-time algorithms: $\mathrm{McE} = (\mathcal{K}_{\mathrm{McE}}, \mathcal{E}_{\mathrm{McE}}, \mathcal{D}_{\mathrm{McE}})$ on the linear $[n, k, d]$-code $C \subseteq \mathbb{F}_2^n$, where $n$ is the length, $k$ is the code dimension, and $d$ is the minimum code distance. Let $G$ be the generator matrix of the code $C$, $t = \lfloor (d-1)/2 \rfloor$. A secret key $sk$ is a pair $(S, P)$, where $S$ is a non-singular $(k \times k)$-matrix over the field $\mathbb{F}_2$ and $P$ is a permutation $(n \times n)$-matrix. A public key $pk$ is a pair $(\widetilde{G} = SGP, t)$. Encryption of a message $\mathbf{m} \in \mathbb{F}_2^k$ is performed according to the rule

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

To decrypt the ciphertext $\mathbf{c}$, one should use an effective decoder $\mathrm{Dec}_C : \mathbb{F}_2^n \to \mathbb{F}_2^k$ of the code $C$ and the secret key $sk$:

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

## 3. Efficient S-repetition construction

On the basis of the Randomized McEliece cryptosystem [7] we construct a new cryptosystem $\mathrm{bMcE}_l = (\mathcal{K}_{\mathrm{bMcE}_l}, \mathcal{E}_{\mathrm{bMcE}_l}, \mathcal{D}_{\mathrm{bMcE}_l})$ and call it the basic cryptosystem. For the vector $\mathbf{m}(\in \mathbb{F}_q^k)$ and the ordered set $\omega = \{\omega_1, \ldots, \omega_l\} \subseteq [k]$, where $\omega_1 < \ldots < \omega_l$, we consider the projection operator $\Pi_\omega : \mathbb{F}_q^k \to \mathbb{F}_q^{|\omega|}$ acting according to the rule: $\Pi_\omega(\mathbf{m}) = (m_{\omega_1}, \ldots, m_{i_{\omega_l}})$. For $\omega$ consider a subset $\mathcal{G}(\omega)$ of permutations group $\mathcal{S}_k$ acting on the elements of the set $[k]$:

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

With every permutation $\pi$ from $\mathcal{G}(\omega)$ we associate a permutation $(k \times k)$-matrix $R_\pi$. The encryption rule of basic McEliece $\mathrm{bMcE}_l$ has the form

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

where $\mathbf{m} \in \mathbb{F}_q^l$, $\omega \subset_R [k]$, $|\omega| = l$, $\mathbf{r}_1 \in_R \mathbb{F}_q^{k-l}$, $\mathbf{r}_2$ is formed in accordance with the restriction $\mathrm{supp}(\mathbf{r}_1 - \mathbf{r}_2) = [k] \setminus \omega$, $\pi \in_R \mathcal{G}(\omega)$. The error vectors $\mathbf{e}_1$ and $\mathbf{e}_2$, generated in McE-encryption, are chosen such that $\mathbf{e}_1 \in_R \mathcal{E}_{n,t}$, $\mathbf{e}_2 \in_R \mathcal{E}_{n,t,\mathrm{supp}(\mathbf{e}_1)}$. From here, it follows that

$$\mathrm{wt}(\mathbf{e}_1) + \mathrm{wt}(\mathbf{e}_2) = 2t.$$

To decrypt the ciphertext $\mathbf{c}$, one should calculate

$$\{\mathbf{c}\}_{sk}^{\mathrm{bMcE}_l} = \Pi_\eta(\{\mathbf{c}_1\}_{sk}^{\mathrm{McE}}),\ \eta = [k] \setminus \mathrm{supp}(\{\mathbf{c}_1\}_{sk}^{\mathrm{McE}} - \{\mathbf{c}_2\}_{sk}^{\mathrm{McE}}). \tag{1}$$

Using the one-time strongly unforgeable signature scheme $\mathrm{SS} = (\mathcal{K}_{\mathrm{SS}}, Sign, Check)$ we will construct a new S-repetition McEliece cryptosystem as a triplet of polynomial-time algorithms: $\mathrm{bMcE}_l^s = (\mathcal{K}_{\mathrm{bMcE}_l^s}, \mathcal{E}_{\mathrm{bMcE}_l^s}, \mathcal{D}_{\mathrm{bMcE}_l^s})$. Key generation algorithm $\mathcal{K}_{\mathrm{bMcE}_l^s}$ takes as input a security parameter $N \in \mathbb{N}$ and outputs a public-key $pk$ and a secret key $sk$ of the form

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

where $pk_i^b, sk_i^b \leftarrow \mathcal{K}_{\mathrm{McE}}(N)$, $b \in \{0, 1\}$, $i \in [s]$.

To define encryption algorithm, let us consider a message $\mathbf{m} = (\mathbf{m}_1 \parallel \ldots \parallel \mathbf{m}_s)$ where $\mathbf{m}_i \in \mathbb{F}_2^l$. Encryption algorithm $\mathcal{E}_{\mathrm{bMcE}_l^s}$ takes as input a public-key $pk$ and a message $\mathbf{m}$ and outputs a ciphertext $\mathbf{c}$:

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

where $(\mathbf{dsk}, \mathbf{vk}) \leftarrow \mathcal{K}_{\mathrm{SS}}(N)$, $\mathbf{vk} = (vk_1, \ldots, vk_s)$, $\sigma = Sign(\mathbf{dsk}, \mathbf{c}')$, $pk^{\mathbf{vk}} = (pk_1^{vk_1}, \ldots, pk_s^{vk_s})$, and $\mathbf{c}'$ calculated as follows:

$$\mathbf{c}' = \mathbf{c}'_1 \parallel \ldots \parallel \mathbf{c}'_s = [\mathbf{c}'_{1,1} \parallel \mathbf{c}'_{1,2}] \parallel \ldots \parallel [\mathbf{c}'_{s,1} \parallel \mathbf{c}'_{s,2}],$$

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

Decryption algorithm $\mathcal{D}_{\mathrm{bMcE}_l^s}$ takes as input a secret-key $sk$ and a ciphertext $\mathbf{c}$ and outputs either a message $\mathbf{m} \in \mathbb{F}_q^{sl}$ or a error symbol $\perp$. On the first step, $\mathcal{D}_{\mathrm{bMcE}_l^s}$ checks signature of the message. If $Check(\mathbf{c}', \mathbf{vk}, \sigma) = 0$, then $\mathcal{D}_{\mathrm{bMcE}_l^s}$ outputs $\perp$, otherwise it computes $\mathbf{m}$ as follows. For each $\mathbf{c}'_i$ from $\mathbf{c}' = \mathbf{c}'_1 \parallel \ldots \parallel \mathbf{c}'_s$ it finds $\mathbf{m}_i = \{\mathbf{c}'_i\}_{sk_i}^{\mathrm{bMcE}_l}$ and $\eta_i$ according to (1) and outputs

$$\mathbf{m} = \begin{cases} \mathbf{m}_1 \parallel \ldots \parallel \mathbf{m}_s, & \text{if } \eta_1 = \ldots = \eta_s, \\ \perp, & \text{otherwise.} \end{cases}$$

Let McE be the McEliece cryptosystem with security parameter $N$. The security of McE is based on two following standard assumptions.

**Assumption 1.** 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 2.** There is no polynomial algorithm that solves the problem of decoding a general linear code.

According to [8], the problem of decoding a general linear code is $NP$-hard. Since $P \neq NP$ has not been proved, we formulate this only as an assumption.

Note that, if these assumptions hold, then one can say that McE is one way trapdoor function (or OW-CPA secure) [9]. The hardness of most McE-type cryptosystems is based on the above assumptions (for example, [3, 4, 7]). To formulate the following theorem we should introduce auxiliary assumption.

**Assumption 3.** 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 $N$.

**Theorem 1.** Let SS be one-time strongly unforgeable signature scheme. Then $\mathrm{bMcE}_l^s$ with security parameter $N$ and fixed $s$ is IND-CCA2 secure if assumptions 1–3 hold.

REFERENCES

1. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. 1978. P. 42–44.
2. *Rosen A. and Segev G.* Chosen-ciphertext security via correlated products // LNCS. 2009. V. 5444. P. 419–436.

3. *Dottling N., Dowsley R., Quade J. M., and Nascimento A. C. A.* A CCA2 secure variant of the McEliece cryptosystem // IEEE Trans. Inform. Theory. 2012. V. 58(10). P. 6672–6680.
4. *Persichetti E.* On a CCA2-secure variant of McEliece in the standard model // Provable Security. 2018. V. 11192. P. 165–181.
5. *Lamport L.* Constructing Digital Signatures from One-Way Functions. SRI International, 1979. https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/
6. *Naor M. and Yung M.* Universal One-Way Hash Functions and their Cryptographic Applications // Proc. STOC'89. N.Y.: ACM, 1989. P. 33–43.
7. *Nojima R., Imai H., Kobara K., et al.* Semantic security for the McEliece cryptosystem without random oracles // Designs, Codes and Cryptography. 2008. V. 49. P. 289–305.
8. *Berlekamp E. R., McEliece R. J., and van Tilborg H. C.* On the inherent intractability of certain coding problems // IEEE Trans. Inform. Theory. 1978. V. 24. No. 3. P. 384–386.
9. *Kobara K. and Imai H.* On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC // IEEE Trans. Inform. Theory. 2003. V. 49. No. 12. P. 3160–3168.