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

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

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 $f : (x_{n-1}, \ldots, x_0) \rightarrow \{0, 1\}$ 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 $2^{2n-1}$.

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

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.

**Key words:** 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, $2t < n$, $[n] = \{1, \ldots, n\}$, $\beta \subseteq [n]$, $2^{|\beta|}$ is set of all subsets of $[n]$,

$\mathbb{F}_2$ be a Galois field of cardinality 2. The support of the vector $m = (m_1, \ldots, m_n) \in \mathbb{F}_2^n$
is the set $\text{supp}(m) = \{i : m_i \neq 0\}$ and the Hamming weight of this vector is a number

$\text{wt}(m) = |\text{supp}(m)|$. A function $\gamma : \mathbb{N} \to [0, 1]$ is negligible of $k$, if

$$\forall c \in \mathbb{N} \exists k_c \in \mathbb{N} \forall k > k_c \left(\gamma(k) \leq k^{-c}\right).$$

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 $e = (e_1, \ldots, e_n) \in \mathcal{E}_{n,t,\beta}$ has Hamming weight $t$
and $e_i = 0$ for any $i \in \beta$. We will write $\mathcal{E}_{n,t}$ when $\beta = \emptyset$. 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 $m$ and outputs a ciphertext $c$; we will write $\{m\}^\Sigma_{pk}$
as encryption of the message $m$ with the key $pk$;

3) $\mathcal{D}$ is deterministic polynomial-time decryption algorithm which takes as input a
secret-key $sk$ and a ciphertext $c$ and outputs either a message $m$ or a symbol $\perp$ in the case, when the ciphertext
is incorrect; decryption of the ciphertext $c$ on the secret key $sk$ we will denote $\{c\}^\Sigma_{sk}$.

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 $SS = (\mathcal{K}_{SS}, \text{Sign}, \text{Check})$, where

$\mathcal{K}$ is key generation algorithm which takes as input a security parameter $N \in \mathbb{N}$ and outputs

a signing-key $dsk$ and a verification-key $vk$, $\text{Sign}$ is signing algorithm which takes as input a
signing-key $dsk$ and a message $m$ and outputs a signature $\sigma$, $\text{Check}$ is checking algorithm

which takes as input a verification-key $vk$ a message $m$ and a signature $\sigma$ and outputs 1 if
σ is valid for 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: McE = (K_{McE}, E_{McE}, D_{McE}) on the linear [n, k, d]-code C ⊆ F_q^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 = [(d − 1)/2]. A secret key sk is a pair (S, P), where S is a non-singular (k × k)-matrix over the field F_q and P is a permutation (n × n)-matrix. A public key pk is a pair (G = SGP, t). Encryption of a message m ∈ F_q^n is performed according to the rule

\[ \{m\}_{pk}^{McE} = mG + e = c, \quad e ∈_R E_{n,t}. \]

To decrypt the ciphertext c, one should use an effective decoder Dec_C : F_q^n → F_q^k of the code C and the secret key sk:

\[ \{c\}_{sk}^{McE} = Dec_C(cP^{-1})S^{-1}. \]

3. Efficient S-repetition construction

On the basis of the Randomized McEliece cryptosystem [7] we construct a new cryptosystem bMcE_l = (K_{bMcE_l}, E_{bMcE_l}, D_{bMcE_l}) and call it the basic cryptosystem. For the vector m(∈ F_q^k) and the ordered set ω = \{ω_1, ..., ω_l\} ⊆ [k], where ω_1 < ... < ω_l, we consider the projection operator Π_ω : F_q^k → F_q^{|ω|} acting according to the rule: Π_ω(m) = (m_{ω_1}, ..., m_{ω_l}). For ω consider a subset G(ω) of permutations group S_k acting on the elements of the set [k]:

\[ G(ω) = \{π ∈ S_k : π(1) = ω_1, ..., π(l) = ω_l\}. \]

With every permutation π from G(ω) we associate a permutation (k × k)-matrix R_π. The encryption rule of basic McEliece bMcE_l has the form

\[ \{m\}_{pk,ω}^{bMcE_l} = \{(m || r_1)R_π\}_{pk}^{McE} || \{(m || r_2)R_π\}_{pk}^{McE} = c_1 || c_2 = c, \]

where m ∈ F_q^l, ω ⊆_R [k], |ω| = l, r_1 ∈_R F_q^{k-l}, r_2 is formed in accordance with the restriction supp(r_1 − r_2) = [k] \ ω, π ∈_R G(ω). The error vectors e_1 and e_2, generated in McE-encryption, are chosen such that e_1 ∈_R E_{n,t}, e_2 ∈_R E_{n,t,supp(e_1)}. From here, it follows that

\[ wt(e_1) + wt(e_2) = 2t. \]

To decrypt the ciphertext c, one should calculate

\[ \{c\}_{sk}^{bMcE_l} = Π_ω(\{c_1\}_{sk}^{McE}), \quad η = [k] \ \\supp(\{c_1\}_{sk}^{McE} - \{c_2\}_{sk}^{McE}). \]  

Using the one-time strongly unforgeable signature scheme SS = (K_{SS}, Sign, Check) we will construct a new S-repetition McEliece cryptosystem as a triplet of polynomial-time algorithms: bMcE'_l = (K_{bMcE'_l}, E_{bMcE'_l}, D_{bMcE'_l}). Key generation algorithm K_{bMcE'_l} takes as input a security parameter N ∈ N and outputs a public-key pk and a secret key sk of the form

\[ pk = ((pk^0_i, pk^1_i))_{i=1}^s, \quad sk = ((sk^0_i, sk^1_i))_{i=1}^s. \]

where \( pk_i^b, sk_i^b \leftarrow K_{McE}(N), \) \( b \in \{0, 1\}, i \in [s]. \)
To define encryption algorithm, let us consider a message $m = (m_1 \parallel \ldots \parallel m_i)$ where $m_i \in \mathbb{F}_2^n$. Encryption algorithm $E_{\text{bMcE}}^*$ takes as input a public-key $pk$ and a message $m$ and outputs a ciphertext $c$:

$$c = \{m\}_{pk^{vk}} = c' \parallel vk \parallel \sigma,$$

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

$$c' = c_1' \parallel \ldots \parallel c_s' = [c'_{1,1} \parallel c'_{1,2}] \parallel \ldots \parallel [c'_{s,1} \parallel c'_{s,2}],$$

where $c_j' = [c_{j,1} \parallel c_{j,2}] = \{m_j\}_{pk_j^{vk_j}}$ for $j \in [s]$ and $\omega$ is chosen randomly once for all $j = 1, \ldots, s$.

Decryption algorithm $D_{\text{bMcE}}^*$ takes as input a secret-key $sk$ and a ciphertext $c$ and outputs either a message $m \in \mathbb{F}_q^n$ or a error symbol $\bot$. On the first step, $D_{\text{bMcE}}^*$ checks signature of the message. If $\text{Check}(c', vk, \sigma) = 0$, then $D_{\text{bMcE}}^*$ outputs $\bot$, otherwise it computes $m$ as follows. For each $c'_i$ from $c' = c_1' \parallel \ldots \parallel c_s'$ it finds $m_i = \{c'_i\}_{sk_i}$ and $\eta_i$ according to (1) and outputs

$$m = \begin{cases} m_1 \parallel \ldots \parallel m_s, & \text{if } \eta_1 = \ldots = \eta_s, \\ \bot, & \text{otherwise}. \end{cases}$$

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 $c$ of the McE and the number $l \in \mathbb{N}$, and outputs 0 if $c$ corresponds to an information message of a weight less than $l$ and outputs 1 if $c$ 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 $bMcE_{\ell}^*$ with security parameter $N$ and fixed $s$ is IND-CCA2 secure if assumptions 1–3 hold.

REFERENCES


