UDC 003.26.09

The Forgery Attack on the Post-Quantum AJPS-2 Cryptosystem and Modification of the AJPS-2 Cryptosystem by Changing the Class of Numbers Used as a Module

Dariya Yadukha[1,a]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology*

Abstract

In recent years, post-quantum (quantum-resistant) cryptography has been actively researched, in particular, due to the National Institute of Standards and Technology's (NIST) Post-Quantum Cryptography Competition (PQC), which has been running since 2017. One of the participants in the first round of the competition is the Mersenne-756839 key encapsulation mechanism based on the AJPS-2 encryption scheme. The arithmetic modulo Mersenne number is used to construct the cryptoprimitives of the AJPS family. In this paper, we propose a forgery attack on the AJPS-2 cryptosystem using an active eavesdropper, and two modifications of the post-quantum AJPS-2 cryptosystem, namely, the modification of AJPS-2 using the arithmetic modulo generalized Mersenne number and Crandall number. Moreover, new algebraic problems are defined, on the complexity of which the security of the created modifications is based. The advantages of these modifications are the extension of the number class used as a module in the cryptosystem and the security against the forgery attack with the active eavesdropper, which was successful in the original AJPS-2.

Keywords: the AJPS cryptosystem, Mersenne numbers, generalized Mersenne numbers, Crandall numbers, Hamming weight, forgery attack, post-quantum (quantum-resistant) cryptographic primitives

1. Introduction

The main goal of post-quantum cryptography is to develop cryptosystems that can be implemented on a classical computer, but at the same time, are secure even if an attacker uses a quantum computer to perform an attack. Since it is possible for most symmetric cryptosystems to develop analogs that have a higher level of security and are resistant to attacks using a quantum computer, researchers are focusing their efforts on developing asymmetric cryptoprimitives, particularly those that implement a digital signature scheme or key encapsulation mechanism.

Since 2017, the National Institute of Standards and Technology (NIST) has been hosting a competition for asymmetric post-quantum cryptoprimitives [1], after which the first versions of post-quantum cryptography standards will be published, that complement or replace the standards currently considered most vulnerable to quantum computer attacks, namely the FIPS 186-4 digital signature standard and the NIST SP 800-56A and NIST SP 800-56B standards describing key encapsulation mechanisms for asymmetric cryptosystems [1].

One of the participants in the first round of the NIST competition is the Mersenne-756839 key encapsulation mechanism based on the AJPS cryptosystem [2]. The structure of the cryptosystem uses arithmetic modulo Mersenne number, which can be effectively implemented using algorithms for fast computation of cumbersome operations modulo Mersenne number, such as reduction, multiplication, modular multiplicative inverse calculation, bitwise addition and multiplication, etc [3, 4, 5]. The AJPS cryptosystem has two versions: for encrypting one bit of a message (AJPS-1) and for encrypting a block of bits (AJPS-2).

In this paper, we continue the idea of constructing modifications of the cryptographic primitives of the AJPS family by changing the class of numbers used as a module, i.e. replacing the Mersenne numbers with other classes of numbers. In our previous paper [6], a modification of the AJPS-1

[a]dariya.yadukha@gmail.com

cryptosystem was constructed using generalized Mersenne numbers instead of Mersenne numbers, and a comparative analysis of the original AJPS-1 cryptosystem and the constructed modification using generalized Mersenne numbers was performed. In this work, two modifications of the AJPS-2 cryptosystem are developed: using generalized Mersenne numbers and Crandall numbers.

2. Description of the AJPS-2 cryptosystem

The AJPS-2 cryptosystem allows encrypting a block of bits with a length λ, where λ – the security parameter, which is specified during the construction of the cryptosystem, i.e. the plaintext is $M \in \{0,1\}^\lambda$. Public parameters of the cryptosystem are:

- Mersenne number $M_n = 2^n - 1$, $n \in \mathbb{N}$;
- integer $h \in \mathbb{N}$ that satisfies the conditions $h = \lambda$ and $10h^2 < n \leq 16h^2$;
- encryption and decryption functions of the error correction code:

$$\mathcal{E}: \{0,1\}^\lambda \to \{0,1\}^n;$$

$$\mathcal{D}: \{0,1\}^n \to \{0,1\}^\lambda,$$

which are chosen according to the following condition: in order for the cryptosystem to be $(1-\delta)$-correct, where δ is the decryption error probability, it is necessary that:

$$\forall M \in \{0,1\}^\lambda:$$
$$\Pr\{\mathcal{D}((F \cdot C_1) \oplus C_2) = M\} \geq 1 - \delta.$$

To simplify notation, we equate numbers modulo Mersenne number with binary strings from the set $\{0,1\}^n \setminus \{1^n\}$.

Let us describe the main algorithms of the AJPS-2 cryptosystem.

1) Key generation algorithm ***Gen***.
   a) Integers F and G are chosen randomly and independently from the set

$$HM_{n,h} = \{x \in \{0,1\}^n : \ Ham(x) = h\},$$

   where $Ham(x)$ denotes the Hamming weight of x (total amount of 1's in the binary representation of x).
   Note that the set $HM_{n,h}$ can also be represented as the set of residues modulo Mersenne number M_n, which have Hamming weight h.
   b) The number F is the secret key, and the value G is a secret parameter of the cryptosystem.
   c) The value R is chosen randomly from all n-bit integers.
   d) The number T is calculated according to the equation:

$$T = F \cdot R + G \bmod M_n.$$

   e) The public key is a pair of integers (R, T).
2) Algorithm ***Enc*** for encrypting the message M.
   a) Integers A, B_1 and B_2 are chosen randomly and independently from the set $HM_{n,h}$.
   b) The ciphertext of the message M is a pair of numbers (C_1, C_2), where C_1 and C_2 are calculated according to the equations:

$$C_1 = A \cdot R + B_1 \bmod M_n;$$

$$C_2 = (A \cdot T + B_2 \bmod M_n) \oplus \mathcal{E}(M).$$

   c) The decryption algorithm ***Dec*** consists in calculating the value

$$\mathcal{D}((C_1 \cdot F \bmod M_n) \oplus C_2),$$

   as a result, we get the value M.

The correctness of the cryptosystem is determined according to Definition 1.

Definition 1. An asymmetric encryption scheme (***Gen***, ***Enc***, ***Dec***) is called $(1-\delta)$-*correct* if for all valid messages M holds

$$Pr[\textbf{\textit{Dec}}(sk, \ \textbf{\textit{Enc}}(pk, m)) = M] \geq 1 - \delta.$$

Since the AJPS-2 cryptosystem uses an error correction code in its structure, the correctness of the cryptosystem depends on the specific values of the parameters of the error correction code, used in the AJPS-2 cryptosystem.

Claim 1 ([2])**.** *The AJPS-2 cryptosystem is $(1-\delta)$-correct if the error correction code $(\mathcal{E}, \mathcal{D})$ corrects to*

$$(4h^2 + 2h)(1 + \varepsilon)$$

errors for some value ε, $0 < \varepsilon < 1$, which satisfies the following condition:

$$2^{-\frac{(2h^2-1)\varepsilon^2}{6}} < \delta.$$

The proof of Claim 1 uses the relations for the Hamming weight of integers modulo Mersenne number, which are described in Lemma 1.

Lemma 1. *For integers $A, B \in \{0,1\}^n$ and a module M_n the following properties hold:*

1) $Ham(A + B \bmod M_n) \leq$
$\leq Ham(A) + Ham(B)$;

2) $Ham(A \cdot B \bmod M_n) \leq$
$\leq Ham(A) \cdot Ham(B)$;

3) *If $A \neq 0^n$, then*

$$Ham(-A \bmod M_n) = n - Ham(A).$$

Security of the AJPS-2 cryptosystem is based on the complexity of the Mersenne Low Hamming Combination Search Problem (MLHCSP).

Definition 2 (MLHCSP) ([2])**.** *Given a Mersenne number M_n, an integer h and a pair of integers (R, T), where R is a randomly chosen number from all n-bit integers, T is calculated according to the equation $T = F \cdot R + G \bmod M_n$, and F and G are chosen randomly and independently from the set $HM_{n,h}$, find the numbers F and G.*

It is considered that MLHCSP is hard to solve. This problem is resistant to many known attacks, namely Meet-in-the-middle attacks, Guess and Win, Lattice-based attacks, etc [7, 8, 9, 10].

3. Construction of a forgery attack on the AJPS-2 cryptosystem using an active eavesdropper

According to the G. Simmons theory, a forgery attack is an attack in which a cryptanalyst intercepts the true ciphertext from the sender, forms a false ciphertext, and sends it to the recipient [11]. The attack is considered successful if the recipient accepted the received message as veritable.

To construct a forgery attack on the AJPS-2 cryptosystem using the model of an active attacker, the property of arithmetic modulo Mersenne number is used, which is described in the following lemma.

Lemma 2. *For any numbers $A, B \in \{0,1\}^n$, the Mersenne number M_n and an natural number r such that $r < n$, the relation holds:*

$$\overleftarrow{A + B \bmod M_n} = \overleftarrow{A} + \overleftarrow{B} \bmod M_n,$$

where $\overleftarrow{X}$ is the operation of cyclic shift of X by r positions to the left.

Proof. Since the cyclic shift by r positions modulo Mersenne number is equivalent to the multiplication by 2^r [12], we have:

$$\overleftarrow{A + B \bmod M_n} = (A + B) \cdot 2^r \bmod M_n =$$

$$= (A \cdot 2^r) + (B \cdot 2^r) \bmod M_n = \overleftarrow{A} + \overleftarrow{B} \bmod M_n,$$

which had to be proved. □

Claim 2. *The forgery attack with modified plaintext is successful for the AJPS-2 cryptosystem: given the pair (C_1, C_2), the attacker can calculate the ciphertexts (C_1^*, C_2), where the value of $\overleftarrow{C_1}$ is the result of the cyclic shift of C_1 by r positions to the left, while the value of r is any natural number less than n.*

Proof. The result of the encryption algorithm of the AJPS-2 cryptosystem is a pair of numbers (C_1, C_2):

$$C_1 = A \cdot R + B_1 \bmod M_n;$$

$$C_2 = (A \cdot T + B_2 \bmod M_n) \oplus \mathcal{E}(M).$$

Performing a cyclic shift of the number C_1, according to Lemma 2, we have:

$$\overleftarrow{C_1} = \overleftarrow{A \cdot R} + \overleftarrow{B_1} \bmod M_n.$$

Since B_1 was chosen randomly from the set $HM_{n,h}$ during the encryption procedure and is used once when calculating the value of C_1, then using the value $\overleftarrow{B_1}$ instead of B_1 when calculating C_1 does not change the message m that will be received during decryption, because the Hamming weight does not change when the number is cyclically shifted, i.e. $\overleftarrow{B_1} \in HM_{n,h}$.

However, using $\overleftarrow{A \cdot R}$ instead of $A \cdot R$ affects the decrypted message, because R is a public key, that is, the value is known to the attacker, and the number A is chosen randomly from the set $HM_{n,h}$ at each encryption procedure. If we assume that the number R remains unchanged during the calculation of the cyclic shift operation to $A \cdot R$, then we have $\overleftarrow{A \cdot R} = Y \cdot R$, where Y is some n-bit number that satisfies the given condition.

If the number Y has the Hamming weight h (although the probability of this event is relatively small), then the value C_1^* will correspond to the correct message. But even in this case the forgery attack will be successful, because the integer A is used not only in the calculation of C_1, but also in

the calculation of C_2. Thus, we have:

$$(C_1^*, C_2) = (Y \cdot R + B_1, (A \cdot T + B_2) \oplus \mathcal{E}(M)),$$

that is, upon decryption of (C_1^*, C_2), the message M^*, $M^* \neq M$ will be received.

□

Therefore, the AJPS-2 cryptosystem is not resistant to a forgery attack using the active attacker model.

4. Modification of AJPS-2 by using other classes of numbers

As mentioned earlier, the arithmetic modulo Mersenne number has many advantages for use in cryptography, since there are efficient algorithms for calculating time-consuming operations. Such algorithms are often generalized to the case of larger classes of numbers, in particular to the generalized Mersenne numbers [4, 5].

Let us concentrate on two classes of numbers that are generalizations of Mersenne numbers:

- Crandall numbers $CR_{n,c} = 2^n - c$, where $n, c \in \mathbb{N}$ and $\log_2 c \leq \frac{n}{2}$;
- generalized Mersenne numbers of the type $GM_{n,m} = 2^n - 2^m - 1$, where $n, m \in \mathbb{N}$, $n > m$.

Let us consider modifications of the AJPS-2 cryptosystem using arithmetic modulo $GM_{n,m}$ and $CR_{n,c}$. Algorithms for key generation, encryption and decryption in the modifications are the same as in the AJPS-2 cryptosystem, except that all operations are performed modulo generalized Mersenne number or the Crandall number. Parameters F and G of the key generation algorithm ***Gen*** and parameters A, B_1 and B_2 of the encryption algorithm ***Enc*** are chosen from the set

$$HG_{n,m,h} = \{x \in \{0,1\}^n : \ x < GM_{n,m} \text{ and } Ham(x) = h\}$$

in a modification using arithmetic modulo generalized Mersenne number $GM_{n,m}$ and from the set

$$HC_{n,c,h} = \{x \in \{0,1\}^n : x < CR_{n,c} \text{ and } Ham(x) = h\}$$

in a modification using arithmetic modulo Crandall number $CR_{n,c}$.

In addition, in order to construct modifications of AJPS-2 by changing the class of numbers used as a module, it is necessary to define conditions on the characteristics of the error correction code used in the AJPS-2 encryption and decryption algorithms. The following theorems are used to determine the necessary conditions for error correction code parameters.

Theorem 1 ([2]). *Let X be any n-bit number, then for any n-bit number Y having Hamming weight k and any value ε, $\varepsilon > 0$ holds:*

$$\Pr\left\{Ham_{dist}(X, X+Y) \geq 2k(1+\varepsilon)\right\} \leq \leq 2^{-2k(\varepsilon - \ln(1+\varepsilon))},$$

where Ham_{dist} – a function for calculating the Hamming distance between two binary strings of the same length.

Theorem 2 ([13]). *Let $GM_{n,m,k}$ be a generalized Mersenne number of the form $GM_{n,m,k} = 2^n - 2^m - 1 - k$, where $n, m, k \in \mathbb{N}$, $n > m$ and $k < 2^n - 2^m - 1$, let there also be two n-bit numbers A, B such that $A < GM_{n,m,k}$ and $B < GM_{n,m,k}$. Then the following relations for the Hamming weight are fulfilled:*

$$1)\ Ham(A + B \bmod GM_{n,m,k}) \leq \leq Ham(A) + Ham(B) + k;$$

$$2)\ Ham(A \cdot B \bmod GM_{n,m,k}) \leq \leq (k+1) \cdot Ham(A) \cdot Ham(B) + +(m + k - 1) \cdot \min(Ham(A), Ham(B)).$$

Remark. It is obvious that the numbers $GM_{n,m,k}$ are a generalization of the numbers $GM_{n,m}$, because the numbers $GM_{n,m}$ – these are the numbers $GM_{n,m,k}$ when $k = 0$. In particular, the numbers $GM_{n,m,k}$ can be considered as Crandall numbers $CR_{n,c}$ for $c = 2^m + 1 + k$ for the parameters $k, m \in \mathbb{N}$, $k < 2^n - 2^m - 1$, $m < n$. Thus, the relations described in Theorem 2 can be generalized to the cases of the numbers $GM_{n,m}$ and $CR_{n,c}$.

Using Theorems 1 and 2, we determine the conditions for the error correction code for modifications of the AJPS-2 cryptosystem using arithmetic modulo generalized Mersenne numbers.

Claim 3. *A modification of the AJPS-2 cryptosystem using arithmetic modulo generalized Mersenne number $GM_{n,m}$ is $(1-\delta)$-correct if the error correction code $(\mathcal{E}, \mathcal{D})$ corrects to*

$$(4h^2 + 4mh - 2h)(1+\varepsilon)$$

errors for some value ε, $0 < \varepsilon < 1$, which satisfies the following condition:

$$2^{-2(h^2+(m-1)h)\frac{\varepsilon^2}{3}}\left(1+2^{-\frac{2h\varepsilon^2}{3}}\right) < \delta.$$

Proof. To decrypt the message, the following value is calculated:

$$\mathcal{D}((C_1 \cdot F \bmod GM_{n,m}) \oplus C_2),$$

where $(\mathcal{E}, \mathcal{D})$ is an error correction code, (C_1, C_2) is a pair of ciphertexts, F is a secret key. Herewith we have:

$$C_1 = A \cdot R + B_1 \bmod GM_{n,m};$$

$$C_2 = (A\cdot(F\cdot R+G)+B_2 \bmod GM_{n,m})\oplus\mathcal{E}(M).$$

For correct decryption, it is necessary that the values $C_1 \cdot F \bmod GM_{n,m}$ and C_2 have a small Hamming distance (the specific value of the Hamming distance depends on the determined value of the probability that the initial message M will be received as a result of decryption). Therefore, it is necessary to determine the dependence of the parameter δ and the Hamming distance of such values

$$C_1 \cdot F = A \cdot F \cdot R + B_1 \cdot F \bmod GM_{n,m};$$

$$C_2 = A \cdot F \cdot R + A \cdot G + B_2 \bmod GM_{n,m}.$$

1) Let us consider values $A \cdot F \cdot R + B_1 \cdot F$ and $A \cdot F \cdot R$. Given that all calculations are performed modulo $GM_{n,m}$, according to Theorem 2, the Hamming weight of the number $B_1 \cdot F$ can be estimated as follows:

$$Ham(B_1 \cdot F \bmod GM_{n,m}) \le h^2 + (m-1)h.$$

Let us denote the value $Ham_{dist}(AFR, AFR + +B_1F)$ as H_1. Then, applying Theorem 1, we have:

$$\Pr\left\{H_1 \ge 2(h^2+(m-1)h)(1+\varepsilon)\right\} \le$$

$$\le 2^{-2(h^2+(m-1)h)(\varepsilon-\ln(1+\varepsilon))}.$$

2) Now consider the values $A \cdot F \cdot R$ and $A \cdot F \cdot R + A \cdot G + B_2$. Similarly, using Theorem 2, we have:

$$Ham(A \cdot G + B_2 \bmod M_n) \le h^2 + m \cdot h.$$

Let us denote $Ham_{dist}(AFR, AFR + AG + B_2)$ as H_2. Then, applying Theorem 1, we have:

$$\Pr\left\{H_2 \ge 2(h^2+mh)(1+\varepsilon)\right\} \le$$

$$\le 2^{-2(h^2+mh)(\varepsilon-\ln(1+\varepsilon))}.$$

Then the combined probability of the considered events is as follows:

$$\Pr\big\{H_1 \ge 2(h^2+(m-1)h)(1+\varepsilon),$$
$$H_2 \ge 2(h^2+mh)(1+\varepsilon)\big\}.$$

Using the Boole's inequality, we have:

$$\Pr\big\{H_1 \ge 2(h^2+(m-1)h)(1+\varepsilon),$$
$$H_2 \ge 2(h^2+mh)(1+\varepsilon)\big\} \le$$
$$\le \Pr\left\{H_1 \ge 2(h^2+(m-1)h)(1+\varepsilon)\right\}+$$
$$+\Pr\left\{H_2 \ge 2(h^2+mh)(1+\varepsilon)\right\} \le$$
$$\le 2^{-2(h^2+(m-1)h)(\varepsilon-\ln(1+\varepsilon))}+$$
$$+2^{-2(h^2+mh)(\varepsilon-\ln(1+\varepsilon))} =$$
$$= 2^{-2(h^2+(m-1)h)(\varepsilon-\ln(1+\varepsilon))}\left(1+2^{-2h(\varepsilon-\ln(1+\varepsilon))}\right).$$

Let us consider the value $\varepsilon - \ln(1+\varepsilon)$. Using the expansion of $\ln(1+\varepsilon)$ into the Taylor series, we obtain:

$$\varepsilon - \left(\varepsilon - \frac{\varepsilon^2}{2} + \frac{\varepsilon^3}{6} - \dots\right) \ge \varepsilon - \varepsilon + \frac{\varepsilon^2}{2} - \frac{\varepsilon^3}{6} =$$
$$= \frac{\varepsilon^2}{2} - \frac{\varepsilon^3}{6} = \frac{3\cdot\varepsilon^2 - 2\cdot\varepsilon^3}{6}.$$

Since $0 < \varepsilon < 1$, then $\varepsilon^3 \le \varepsilon^2$, therefore, we have:

$$\varepsilon - \ln(1+\varepsilon) \ge \frac{3\cdot\varepsilon^2 - 2\cdot\varepsilon^2}{6} = \frac{\varepsilon^2}{6}.$$

According to the decryption algorithm of the AJPS-2 cryptosystem, it is necessary to obtain an estimate for the following value of the Hamming distance:

$$Ham_{dist}(AFR + B_1F,\ AFR + AG + B_2).$$

For this, we use the triangle inequality with the Ham_{dist} metric. Thus, we get the following:

$$Ham_{dist}\big(AFR+AG+B_2,\ AFR+B_1F\big) \ge$$
$$\ge Ham_{dist}(AFR, AF\cdot R + B_1F)+$$
$$+Ham_{dist}(AFR, AFR + AG + B_2) =$$
$$= H_1 + H_2 \ge$$
$$\ge 2(h^2+(m-1)h)(1+\varepsilon) + 2(h^2+mh)(1+\varepsilon) =$$
$$= (4h^2 + 4mh - 2h)(1+\varepsilon).$$

Then the probability of fulfilling this will be as follows:

$$\Pr\big\{Ham_{dist}(AFR+B_1F, AFR+AG+B_2) \ge$$
$$\ge (4h^2+4mh-2h)(1+\varepsilon)\big\} \le$$

$$\leq 2^{-2(h^2+(m-1)h)\frac{\varepsilon^2}{3}}\left(1+2^{-\frac{2h\varepsilon^2}{3}}\right).$$

Thus, to ensure the $(1-\delta)$-correctness of the modification of the AJPS-2 cryptosystem using arithmetic modulo generalized Mersenne number, it is necessary that the error correction code $(\mathcal{E},\mathcal{D})$ corrects to

$$(4h^2+4mh-2h)(1+\varepsilon)$$

errors for some ε, $0<\varepsilon<1$, which satisfying the condition:

$$2^{-2(h^2+(m-1)h)\frac{\varepsilon^2}{3}}\left(1+2^{-\frac{2h\varepsilon^2}{3}}\right)<\delta.$$

□

The security of the modification of the AJPS-2 cryptosystem using arithmetic modulo $GM_{n,m}$ is based on the complexity of *the Generalized Mersenne Low Hamming Combination Search Problem* (GMLHCSP).

Definition 3 (GMLHCSP)**.** *Given a generalized Mersenne number $GM_{n,m}$, an integer h and a pair of numbers (R,T), where R is a random n-bit number such that $R\leq GM_{n,m}$, and the integer T is calculated according to the relation*

$$T=F\cdot R+G \bmod GM_{n,m},$$

and F and G are chosen independently and randomly from the set $HG_{n,m,h}$, find F and G.

We also determine the conditions for the error correction code's parameters for the modification of the AJPS-2 cryptosystem using arithmetic modulo Crandall number $CR_{n,c}$.

Claim 4. *A modification of the* AJPS-2 *cryptosystem using arithmetic modulo Crandall number $CR_{n,c}$ is $(1-\delta)$-correct if the error correction code $(\mathcal{E},\mathcal{D})$ corrects to*

$$(4(c-2^m)h^2+2h(2m+2c+2^{m+1}-3)+$$

$$+2(c-2^m-1))(1+\varepsilon)$$

errors, where $c=2^m+1+k$, $m,k\in\mathbb{N}$, and ε, $0<\varepsilon<1$, which satisfies the following condition:

$$2^{-2\left((c-2^m)h^2+(m+c-2^m-2)h\right)\cdot\frac{\varepsilon^2}{3}}\times$$

$$\times\left(1+2^{-(h+c-2^m-1)\cdot\frac{\varepsilon^2}{3}}\right)<\delta.$$

Proof. The proof is similar to the proof of Claim 3.

Using Theorem 2, we have:

$$Ham(F\cdot B_1 \bmod CR_{n,c})\leq$$
$$\leq(c-2^m)h^2+(m+c-2^m-2)h;$$

$$Ham(A\cdot G+B_2 \bmod CR_{n,c})\leq$$
$$\leq(c-2^m)h^2+(m+c-2^m-1)h+c-2^m-1.$$

We obtain the following estimate of the combined probability:

$$2^{-2\left((c-2^m)h^2+(m+c-2^m-2)h\right)\frac{\varepsilon^2}{3}}+$$
$$+2^{-2\left((c-2^m)h^2+(m+c-2^m-1)h+c-2^m-1\right)\frac{\varepsilon^2}{3}}=$$
$$=2^{-2\left((c-2^m)h^2+(m+c-2^m-2)h\right)\cdot\frac{\varepsilon^2}{3}}\times$$
$$\times\left(1+2^{-2(h+c-2^m-1)\cdot\frac{\varepsilon^2}{3}}\right).$$

Applying the triangle inequality, we have:

$$2((c-2^m)h^2+(m+c-2^m-1)h+c-2^m-1)+$$
$$+2\left((c-2^m)h^2+(m+c-2^m-2)h\right)=$$
$$=4(c-2^m)h^2+2h(2m+2c-2^{m+1}-3)+$$
$$+2(c-2^m-1).$$

□

The security of the modification of AJPS-2, which uses operations modulo Crandall number $CR_{n,c}$, relies on the assumption that it is hard to solve the CRLHCSP (*Crandall Low Hamming Combination Search Problem*).

Definition 4 (CRLHCSP)**.** *Given a Crandall number $CR_{n,c}$, an integer h and a pair of numbers (R,T), where R is a random n-bit number such that $R\leq CR_{n,c}$, and T is calculated according to the relation*

$$T=F\cdot R+G \bmod CR_{n,c},$$

and F and G are chosen independently and randomly from the set $HC_{n,c,h}$, find the numbers F and G.

Thus, we have described two modifications of AJPS-2 that use classes of numbers other than the class of Mersenne numbers. The advantage of the constructed modifications of AJPS-2 using arithmetic modulo generalized Mersenne number and arithmetic modulo Crandall number is a significant increase in the class of numbers used as a module in the cryptosystem. Also, the forgery attack using the active attacker model, which is described in Claim 2 for the original AJPS-2 cryptosystem,

is unsuccessful for the constructed modifications of AJPS-2, since the attack is based on the property of the cyclic shift operation modulo Mersenne number described in Lemma 2, while for generalized Mersenne numbers and Crandall numbers this property is not fulfilled.

5. Conclusion

In this paper, we presented the results of the analysis of the post-quantum cryptosystem AJPS-2. We have constructed a forgery attack using the active attacker model for AJPS-2 and described two modifications of AJPS-2 by using number classes other than the class of Mersenne numbers. The class of generalized Mersenne numbers and the class of Crandall numbers were used to construct the modifications.

New algebraic problems are defined which are modifications of the MLHCSP problem: the GMLHCSP problem (using arithmetic modulo generalized Mersenne number) and the CRLHCSP (using arithmetic modulo Crandall number), where the security of the respective modifications is based on the complexity of these problems.

The advantage of created modifications of the AJPS-2 cryptosystem using arithmetic modulo generalized Mersenne number and arithmetic modulo Crandall number is a significant increase in the class of numbers used as a module in the cryptosystem, as well as security against a described forgery attack.

References

[1] National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization." https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization, 2017.

[2] D. Aggarwal, A. Joux, A. Prakash, and M. Santha, "New Public-Key Cryptosystem via Mersenne Numbers," *IACR Cryptology ePrint Archive*, no. 481, 2017.

[3] J. Bajard, "Modular Number Systems: Beyond the Mersenne Family," *Lecture Notes in Computer Science book series*, no. 3357, 2004.

[4] K. Nath and P. Sarkar, "Efficient Arithmetic in (Pseudo-) Mersenne Prime Order Fields," *IACR Cryptology ePrint Archive*, no. 985, 2018.

[5] M. Taschwer, *Modular Multiplication Using Special Prime Moduli*. Kommunikationssicherheit im Zeichen des Internet, 2001.

[6] D. Yadukha, "The Modification of the Quantum-Resistant AJPS-1 Cryptographic Primitive," *Theoretical and cryptographic problems of cybersecurity*, no. 4, 2022.

[7] M. Beunardeau, A. Connolly, R. Geraud, and D. Naccache, "On the Hardness of the Mersenne Low Hamming Ratio Assumption," *IACR Cryptology ePrint Archive*, no. 522, 2017.

[8] M. Tiepelt and A. Szepieniec, "Quantum LLL with an Application to Mersenne Number Cryptosystems," *Progress in Cryptology. LATINCRYPT*, 2019.

[9] J. Coron, "Improved Cryptanalysis of the ajps Mersenne Based Cryptosystem," *IACR Cryptology ePrint Archive*, no. 610, 2019.

[10] A. Budroni and A. Tenti, "The Mersenne Low Hamming Combination Search Problem can be reduced to an ILP Problem," *Lecture Notes in Computer Science. Progress in Cryptology – AFRICACRYPT 2019*, pp. 41–55, 2019.

[11] G. J. Simmons, "Authentication theory & coding theory," *Lecture Notes in Computer Science. CRYPTO 1984: Advances in Cryptology*, no. 184, pp. 411–431, 1985.

[12] S. Baktir and B. Sunar, "Optimal extension field inversion in the frequency domain," *Lecture Notes in Computer Science. Theoretical Computer Science and General Issues. Arithmetic of Finite Fields*, no. 5130, pp. 47–61, 2008.

[13] D. Yadukha and A. Fesenko, "Relations for the Hamming Weight of the Sum and Product of Two Numbers Modulo Generalized Mersenne Number," in *Theoretical and applied problems of physics, mathematics and informatics: materials of the XVIII Ukrainian scientific and practical conference of students, postgraduates and young scientists*, (Kyiv, Ukraine: National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"), pp. 252–254, Polytechnic, 2020.