UDC 003.26

The necessary security requirements for the values used by the AJPS cryptosystem

A. Fesenko[1, a], D. Yadukha[1, b]

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

Abstract

D. Aggarwal and others have recently proposed a new quantum-resistant asymmetric cryptosystem AJPS [1] which uses operations modulo a Mersenne number. This paper imposes the restrictions on the public key of this cryptosystem and ciphertext requirements, and presents the active attack on AJPS and the AJPS cryptosystem usage recommendations.

Keywords: Mersenne numbers, asymmetric cryptosystem, quantum-resistant crypto primitives, the AJPS cryptosystem, Hamming weight

Introduction

Asymmetric cryptosystems or public-key cryptosystems are efficient cryptographic data protection systems, the main advantage of which is the ability for users to exchange messages without prior agreement on a shared secret. The security of most asymmetric cryptosystems is based on the complexity of chosen mathematical problems. For example, the security of RSA is based on computational complexity of the integer factorization problem, and the security of ElGamal encryption system is based on the discrete logarithm problem.

In the classical computational model it is considered that these problems are hard and at the moment there exist no effective algorithms, which are able to solve them. But in quantum computation model it is not so, since there exist algorithms for integer factorization and calculation of the discrete logarithm [2, 3]. In the past, these results were not considered as a real danger for practical cryptosystems, since quantum computers were not expected to be implement in a foreseeable future. Considering a significant amount of research on scalable quantum computers and its influence in recent years, the need of development of new systems of information security development becomes apparent. Such systems have to be able to resist attacks conducted by means of quantum computing devices.

In 2017, the National Institute of Standards and Technology (NIST) announced the competition of quantum-resistant cryptographic primitives [4]. One of the participants is the AJPS cryptosystem [1], based on arithmetic modulo a Mersenne number.

The purpose of this work is to analyze the features of the AJPS cryptosystem, which uses the operations modulo a Mersenne number and to search possible vulnerabilities of this cryptosystem.

[a] andrey.fesenko@gmail.com
[b] dariya.yadukha@gmail.com

1. Mersenne numbers and their properties

Integers of a special form often allow to perform arithmetic modulo operations faster [5, 6]. This property is widely used in practice and explains the large amount of research of special quick arithmetic.

The Mersenne numbers M_n of the form $2^n - 1$ is one of the most known types of integers, which was studied by the mathematicians since the 17th century [7].

These numbers have many advantages for use in practice. For example, the Mersenne numbers have properties that allow to simplify the calculations of module operations. There are algorithms for fast computation of reduction modulo a Mersenne number, and methods for fast multiplication and bitwise addition modulo a Mersenne number [6]. Also, there are some relations for Hamming weight of numbers modulo a Mersenne number [1]. Using these relations, we can avoid some cumbersome calculations in practice. All these facts explain the popularity of using Mersenne numbers in some applications.

The Hamming weight of an n-bit integer s is a total amount of 1's in binary representation of s and is denoted by $Ham(s)$. Obviously, in this case $0 \leq Ham(s) \leq n$.

Lemma 1. For integers $A, B \in \{0,1\}^n$ and module $M_n = 2^n - 1$ the following properties hold:

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

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

3) If $A \neq 0^n$, then
$$Ham(-A \bmod M_n) = n - Ham(A).$$

Using operations modulo a Mersenne number and relations for Hamming weight modulo a Mersenne number, a search problem was constructed, which is called *Mersenne Low Hamming Ratio Search Problem*

(MLHRSP) [1]. It is based on the following claim.

Claim 1. Let F and G be such integers, that the binary representations of $(F \bmod M_n)$ and $(G \bmod M_n)$ both have low Hamming weight h. Then, when we consider H as $\frac{F}{G} \bmod M_n$, H looks pseudorandom, i.e., it will be hard to distinguish H from a random integer modulo M_n.

Definition 1. (Mersenne Low Hamming Ratio Search Problem). Given an n-bit Mersenne number $M_n = 2^n - 1$, an n-bit integer H and an integer h, find two n-bit integers F and G, each of Hamming weight equal to h, such that:

$$H = \frac{F}{G} \bmod M_n.$$

It is considered that this problem is hard for solving. MLHRSP is resistant to many known attacks, namely *Meet-in-the-middle attacks, Guess and Win, Lattice-based attacks* etc [8, 9, 10]. Therefore, it is possible to build a cryptosystem, the security of which will be based on complexity of MLHRSP. One of such cryptosystems is AJPS from [1].

2. Description of the AJPS cryptosystem

Next, we describe the basic scheme of encryption for a single bit $b \in \{0, 1\}$.

Let public parameters of cryptosystem be:

- $M_n = 2^n - 1$ – Mersenne number;
- α – the security parameter;
- h – fixed integer, such that

$$\binom{n}{h} \geq 2^\alpha \text{ and } 4h^2 < n \leq 16h^2.$$

For convenience, we define the set of numbers which have Hamming weight h modulo a Mersenne number M_n as:

$$HM_{n,h} = \{x : \ Ham(x \bmod M_n) = h\}.$$

Key Generation. Let F and G be n-bit random integers, chosen independently and uniformly from all n-bit numbers of Hamming weight h:

$$F, G \in HM_{n,h}.$$

The integer F is secret parameter of the cryptosystem and G is private (secret) key. Public key H is calculated as

$$H = \frac{F}{G} \bmod M_n.$$

As mentioned earlier, the AJPS cryptosystem allows to encrypt one bit message. So, the plaintext for encrypting is a value $b \in \{0, 1\}$.

Encryption. The encryption algorithm chooses two random independent integers A and B uniformly from the set $HM_{n,h}$. Bit b is encrypted as:

$$C = (-1)^b (A \cdot H + B) \bmod M_n.$$

Decryption. The decryption algorithm computes

$$d = Ham(C \cdot G \bmod M_n).$$

Then it returns the value of b, depending on value of d:

$$b = \begin{cases} 0, & \text{if } d \leq 2h^2 \\ 1, & \text{if } d \geq n - 2h^2 \\ \perp \text{ (error)}, & \text{else} \end{cases}.$$

The correctness of the decryption follows from Lemma 1. To see this, note that

$$C \cdot G \bmod M_n = (-1)^b \cdot (A \cdot F + B \cdot G) \bmod M_n,$$

which by Lemma 1 has Hamming weight at most $2h^2$ if $b = 0$, and at least $n - 2h^2$ if $b = 1$.

3. Restrictions on the public key of the AJPS cryptosystem

Even relatively secure cryptosystems, that are used in practice, often appear to have vulnerabilities for some parameter values. This problem can be solved by imposing certain restrictions on the choice of public and/or secret parameters. It is clear that the number of such vulnerable values should be small, in order not to accelerate the brute force.

Let's describe the restriction on the choice of the public key H. These are the values of H, that if values of H and C are known, then plaintext (value b) could be calculated without knowledge of private key (value G). It should be noted that values of H and C are always known for everyone, since H is a public key, and C is a ciphertext, which is transmitted by open communication channel.

Claim 2. In the AJPS cryptosystem, if the public key H is such that

$$Ham(H) \leq 1,$$

then everyone can deduce the message without knowing the private key.

Proof. Consider cases where decryption is unambiguous without knowing secret key. To decrypt, find the value d:

$$d = Ham(C \cdot G \bmod M_n) =$$
$$= Ham((-1)^b (A \cdot H + B) \cdot G \bmod M_n).$$

Let's consider two cases, according to the value of b:

1) If $b = 0$, then

$$d = Ham((A \cdot H + B) \cdot G \bmod M_n).$$

Using Lemma 1, we have:

$$d = Ham((A \cdot H + B) \cdot G \bmod M_n) \overset{2}{\leq}$$
$$\overset{2}{\leq} Ham(A \cdot H + B) \cdot Ham(G) \overset{1}{\leq}$$
$$\overset{1}{\leq} (Ham(A \cdot H) + Ham(B)) \cdot Ham(G) \overset{2}{\leq}$$
$$\overset{2}{\leq} (Ham(A) \cdot Ham(H) + Ham(B)) \cdot Ham(G).$$

Note: The digit above the sign of inequality shows which inequality from Lemma 1 was used.

Since on the condition of a cryptosystem the number A, B and G have Hamming weight h, we get

the following relation:

$$d \le (h \cdot Ham(H) + h) \cdot h = h^2 \cdot Ham(H) + h^2 = \\ = h^2(Ham(H) + 1).$$

Recall that in order to get the decrypted bit 0, the value of d must be such that: $d \le 2h^2$. Thereby, we have

$$h^2(Ham(H) + 1) \le 2h^2.$$

Consequently, unambiguous decrypted bit $b = 0$ with the unknown secret key is possible with the condition that

$$Ham(H) \le 1.$$

2) If $b = 1$, then

$$d = Ham(-(A \cdot H + B) \cdot G \bmod M_n).$$

Using the third condition of Lemma 1, we have:

$$d = n - Ham((A \cdot H + B) \cdot G \bmod M_n).$$

Similarly, using conditions 1 and 2 of Lemma 1, we obtain:

$$d = n - Ham((A \cdot H + B) \cdot G \bmod M_n) \overset{2}{\ge} \\ \overset{2}{\ge} n - (Ham(A \cdot H + B) \cdot Ham(G)) \overset{1}{\ge} \\ \overset{1}{\ge} n - ((Ham(A \cdot H) + Ham(B)) \cdot Ham(G)) \overset{2}{\ge} \\ \overset{2}{\ge} n - ((Ham(A) \cdot Ham(H) + Ham(B)) \times \\ \times Ham(G)).$$

Given that

$$Ham(A) = Ham(B) = Ham(G) = h,$$

we have the following relation for d:

$$d \ge n - h^2(Ham(H) + 1).$$

Since for an unambiguous decryption of the bit $b = 1$ value of d must satisfy the inequality

$$d \ge n - 2h^2,$$

then we get inequality

$$n - h^2(Ham(H) + 1) \ge n - 2h^2.$$

Thus, an unambiguous decryption of bit 1 with an unknown secret key is possible under the condition

$$Ham(H) \le 1.$$

So, when $Ham(H) \le 1$, then anyone can determine the value of bit b without the knowledge of the private key.

Corollary 1. To prevent attacks that use the vulnerability described in Claim 2, the public key H of the AJPS cryptosystem must be such that:

$$Ham(H) \ge 1.$$

Obviously $Ham(H) \ne 0$, consequently the restriction on the public key of the AJPS cryptosystem H is:

$$Ham(H) \ne 1.$$

Also, there is a similar restriction on the multiplicative inverse of H modulo a Mersenne number. This restriction is based on the following vulnerability.

Claim 3. If public key of the AJPS cryptosystem H is such that

$$Ham(H^{-1} \bmod M_n) \le 1,$$

then everyone can define the message without knowledge of the private key.

Proof. To prove this restriction, it is necessary to express the private key through a public one. Because of

$$H = \frac{F}{G} \bmod M_n,$$

we get:

$$H \cdot G = F \bmod M_n;$$
$$G = H^{-1} \cdot F \bmod M_n.$$

We use the relation obtained for G in the formula for d:

$$d = Ham(C \cdot G \bmod M_n) = \\ = Ham((-1)^b(A \cdot H + B) \cdot G \bmod M_n) = \\ = Ham((-1)^b(A \cdot H + B) \cdot H^{-1} \cdot F \bmod M_n) = \\ = Ham((-1)^b(A \cdot H \cdot H^{-1} + B \cdot H^{-1}) \cdot F \bmod M_n) = \\ = Ham((-1)^b(A + B \cdot H^{-1}) \cdot F \bmod M_n).$$

Similarly to the proof of Claim 1, we consider two cases, use lemma 1 and take into account the fact that

$$Ham(A) = Ham(B) = Ham(F) = h.$$

1) Case $b = 0$:

$$d = Ham((A + B \cdot H^{-1}) \cdot F \bmod M_n) \overset{2}{\le} \\ \overset{2}{\le} Ham(A + B \cdot H^{-1} \bmod M_n) \cdot Ham(F) \overset{1}{\le} \\ \overset{1}{\le} (Ham(A) + Ham(B \cdot H^{-1} \bmod M_n)) \times \\ \times Ham(F) \overset{2}{\le} \\ \overset{2}{\le} (Ham(A) + Ham(B) \times Ham(H^{-1} \bmod M_n)) \times \\ \times Ham(F) = \\ = (h + h \cdot Ham(H^{-1} \bmod M_n)) \cdot h = \\ = h^2(1 + Ham(H^{-1} \bmod M_n)).$$

Thus, for the unambiguous decryption it is necessary that

$$h^2(1 + Ham(H^{-1} \bmod M_n)) \le 2h^2,$$

that means

$$h^2(1 + Ham(H^{-1} \bmod M_n) - 2) \le 0.$$

And, consequently, we get the constraint

$$Ham(H^{-1} \bmod M_n) \le 1.$$

2) Case $b = 1$:

$$d = Ham(-(A + B \cdot H^{-1}) \cdot F \bmod M_n) \overset{3}{=} \\ \overset{3}{=} n - Ham((A + B \cdot H^{-1}) \cdot F \bmod M_n) \overset{2}{\ge} \\ \overset{2}{\ge} n - (Ham(A + B \cdot H^{-1} \bmod M_n) \cdot Ham(F)) \overset{1}{\ge} \\ \overset{1}{\ge} n - ((Ham(A) + Ham(B \cdot H^{-1} \bmod M_n)) \times \\ \times Ham(F)) \overset{2}{\ge}$$

$$\overset{2}{\geq} n - ((Ham(A) + Ham(B)\times$$
$$\times Ham(H^{-1} \bmod M_n)) \cdot Ham(F)) =$$
$$= n - ((h + h \cdot Ham(H^{-1} \bmod M_n)) \cdot h) =$$
$$= n - h^2(1 + Ham(H^{-1} \bmod M_n)).$$

For unambiguous decryption we need:

$$n - h^2(1 + Ham(H^{-1} \bmod M_n)) \geq n - 2h^2.$$

Again we get the constraint

$$Ham(H^{-1} \bmod M_n) \leq 1.$$

Consequently, in case when $Ham(H^{-1} \bmod M_n) \leq 1$, everyone can decrypt the message without knowledge of the private key.

Corollary 2. To prevent attacks that use the vulnerability described in Claim 3, the public key H of the AJPS cryptosystem must be such that:

$$Ham(H^{-1} \bmod M_n) \geq 1.$$

Obviously $Ham(H^{-1} \bmod M_n) \neq 0$, consequently the restriction on the public key of the AJPS cryptosystem H is:

$$Ham(H^{-1} \bmod M_n) \neq 1.$$

Thus, the public key of the cryptosystem can't be whatever value. This value must satisfy certain conditions. Therefore, after the key generation procedure, it is necessary to check the public key for secure cryptosystem usage.

The complexity of attacks, based on Claim 2, is $O(n)$. And the complexity of attacks, based on Claim 3, is $O(n^2)$.

4. Requirements for the ciphertext of the AJPS cryptosystem

Many cryptosystems have weak ciphertext values that must be avoided for security reasons. The AJPS cryptosystem isn't the exception. If there is a certain dependence between the Hamming weight of ciphertext and the Hamming weight of the public key in AJPS, then AJPS is not secured. One of such vulnerabilities is described below.

Claim 4. Let C be ciphertext obtained by encryption in the AJPS cryptosystem with the public key H and the private key G. If at least one of the following conditions is satisfied:

- $Ham(C \cdot H^{-1} \bmod M_n) \leq 2h$;
- $Ham(-C \cdot H^{-1} \bmod M_n) \leq 2h$,

where $H^{-1} \bmod M_n$ is a multiplicative inverse of H modulo a Mersenne number; $(-C \bmod M_n)$ — additive inverse of C modulo a Mersenne number, then anyone can decrypt the message without knowledge of the private key.

Proof. Previously we obtained that:

$$d = Ham(C \cdot H^{-1} \cdot F \bmod M_n).$$

- Using Lemma 1 and the fact that $Ham(F) = h$, we obtain

$$d = Ham(C \cdot H^{-1} \cdot F \bmod M_n) \overset{2}{\leq}$$
$$\overset{2}{\leq} Ham(C \cdot H^{-1} \bmod M_n) \cdot Ham(F) =$$
$$= Ham(C \cdot H^{-1} \bmod M_n) \cdot h.$$

Thus, if

$$Ham(C \cdot H^{-1} \bmod M_n) \leq 2h,$$

then bit of the message will be decrypted and it will be equal to 0.

- Let's express d via the additive inverse of C modulo a Mersenne number:

$$d = Ham(C \cdot H^{-1} \cdot F \bmod M_n) =$$
$$= Ham(-(-C) \cdot H^{-1} \cdot F \bmod M_n) \overset{3}{=}$$
$$\overset{3}{=} n - Ham((-C) \cdot H^{-1} \cdot F \bmod M_n) \overset{2}{\geq}$$
$$\overset{2}{\geq} n - Ham(-C \cdot H^{-1} \bmod M_n) \cdot Ham\ F =$$
$$= n - Ham(-C \cdot H^{-1} \bmod M_n) \cdot h.$$

So, in case when

$$Ham(-C \cdot H^{-1} \bmod M_n) \leq 2h,$$

a bit of message will be decrypted and it will be equal to 1.

Corollary 3. To prevent attacks using the vulnerability described in Claim 4, we need to validate obtained ciphertext C after the encryption procedure. If at least one of the following conditions is satisfied:

- $Ham(C \cdot H^{-1} \bmod M_n) \leq 2h$;
- $Ham(-C \cdot H^{-1} \bmod M_n) \leq 2h$,

then the decryption of the message is possible without using the private key and the encryption procedure must be repeated again for the initial message value.

The decryption algorithm computes value

$$d = Ham(C \cdot G \bmod M_n),$$

and due to this fact vulnerabilities may occur at a certain value of Hamming weight of the ciphertext. These vulnerabilities allow the attacker to decrypt the message without the knowledge of the private key. Let's consider these vulnerabilities.

Claim 5. Let C be the ciphertext obtained by encryption using the AJPS cryptosystem with a public key H and private key G. If at least one of the following conditions is satisfied:

- $Ham(C \bmod M_n) \leq 2h$;
- $Ham(-C \bmod M_n) \leq 2h$,

where $(-C \bmod M_n)$ is an additive inverse of C modulo a Mersenne number, then anyone can decrypt the message without the knowledge of the private key.

Proof. During the decryption we calculate value of d:

$$d = Ham(C \cdot G \bmod M_n).$$

- Using Lemma 1 and taking into account that $Ham(G) = h$, we have

$$d = Ham(C \cdot G \bmod M_n) \overset{2}{\geq}$$
$$\overset{2}{\geq} Ham(C \bmod M_n) \cdot Ham(G) =$$
$$= Ham(C \bmod M_n) \cdot h.$$

  So, if

$$Ham(C \bmod M_n) \leq 2h,$$

  then value b is decrypted, and it equals 0.
- Lets represent value d via the additive inverse of C modulo a Mersenne number and apply Lemma 1:

$$d = Ham(-(-C) \cdot G \bmod M_n) \overset{3}{=}$$
$$n - Ham(-C \cdot G \bmod M_n) \overset{2}{\geq}$$
$$\overset{2}{\geq} n - Ham(-C \bmod M_n) \cdot Ham(G) =$$
$$= n - Ham(-C \bmod M_n) \cdot h.$$

  In this case, if

$$Ham(-C \bmod M_n) \leq 2h,$$

  then value b can be decrypted, and equals 1.

Corollary 4. To prevent attacks that use the vulnerability described in Claim 5, after the encryption procedure ciphertext C must be checked. Namely, it should be checked whether at least one of the following conditions is satisfied:

- $Ham(C \bmod M_n) \leq 2h$;
- $Ham(-C \bmod M_n) \leq 2h$.

If at least one of the conditions is satisfied, then the decryption of message is possible without the knowledge of the private key, and the encryption procedure must be repeated again for the initial message.

The complexity of attacks, based on Claim 4, is $O(n^2)$. And the complexity of attacks, based on Claim 5, is $O(n)$.

Using the results presented in Corollaries 1-4, we can formulate some general recommendations of the AJPS cryptosystem usage.

Claim 6. We should check the following conditions in order to avoid attacks on the AJPS cryptosystem.

1) Before encryption (conditions for the value of the public key):
   - $Ham(H) \neq 1$;
   - $Ham(H^{-1} \bmod M_n) \neq 1$;

   If at least one of the above conditions is not satisfied, we need to choose new values of F and G and calculate a new value of H. If all conditions are met, then the public key can be used to encrypt messages.
2) After encryption (conditions for the ciphertext, and for the relation with ciphertext and public key):
   - $Ham(C \bmod M_n) > 2h$;
   - $Ham(-C \bmod M_n) > 2h$;
   - $Ham(C \cdot H^{-1} \bmod M_n) > 2h$;
   - $Ham(-C \cdot H^{-1} \bmod M_n) > 2h$.

   If at least one of the above conditions is not satisfied, we need to repeat the encryption procedure again.

If all conditions are met, the ciphertext can be sent to the recipient.

The step-by-step implementation of key generation, encryption, decryption and necessary checks in the AJPS cryptosystem are schematically shown on the Figure 1.

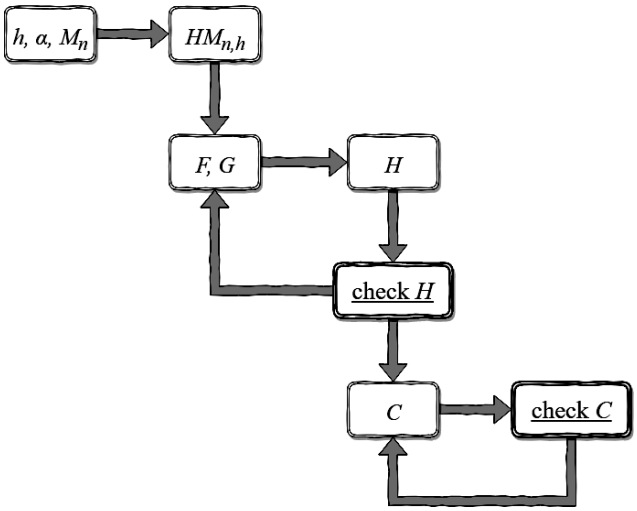

Fig. 1. Step-by-step applying procedures in AJPS

Remark. If conditions from 2) are not satisfied, we should not choose a new value of the public key. Since each procedure of the encryption uses new values A and B, then we get another value of C after next encryption.

The following recommendations for using the AJPS cryptosystem allow us to prevent the weak keys occurrence and to avoid some types of attacks, for example, an active attack.

Active attack is an attack in which an eavesdropper has the ability to modify transmitted messages and to insert its own messages instead.

One of the types of active attacks on the cryptosystem are forgery attacks.

Forgery attack is an active attack in which an eavesdropper does not expect true ciphertext from the sender, but immediately generates fake ciphertext and sends it to the recipient. The attack is considered successful if the recipient accepts a fake message as the sender's message. The attack is successful, even if the recip-

ient receives one more ciphertext later (true ciphertext).

Claim 7. Forgery attack is successful for the AJPS cryptosystem: regardless of the private key, if the eavesdropper sends a message C_1 such that

$$Ham(C_1 \bmod M_n) \leq 2h,$$

then the recipient decrypts it as a bit 0. And if the eavesdropper sends C_2 such that

$$C_2 = -C_1 \bmod M_n,$$

then the recipient decrypts it as a bit 1. The complexity of this attack is $O(n)$.

Proof. Obviously, we need to consider two cases: the case when the eavesdropper wants to send a ciphertext, which the recipient will decrypt as 0, and the case when the recipient will decrypt the ciphertext as 1.

1) If $b = 0$, then the eavesdropper chooses a ciphertext C_1, for which the following inequality holds true:

$$Ham(C_1 \bmod M_n) \leq 2h.$$

Then the eavesdropper sends this ciphertext to the recipient. And the recipient decrypts:

$$d = Ham(C_1 \cdot G \bmod M_n),$$

By the Lemma 1:

$$d = Ham(C_1 \cdot G \bmod M_n) \overset{2}{\leq}$$
$$\overset{2}{\leq} Ham(C_1 \bmod M_n) \cdot Ham(G) =$$
$$= Ham(C_1 \bmod M_n) \cdot h \leq 2h^2.$$

Since $d \leq 2h^2$, then $b = 0$.

2) If $b = 1$, then the eavesdropper chooses ciphertext

$$C_2 = -C_1 \bmod M_n,$$

where C_1 — ciphertext from 1), and sends it. Then

$$d = Ham(C_2 \cdot G \bmod M_n),$$

and by Lemma 1, we have:

$$d = Ham(C_2 \cdot G \bmod M_n) =$$
$$= Ham(-C_1 \cdot G \bmod M_n) \overset{3}{=}$$
$$\overset{3}{=} n - Ham(C_1 \cdot G \bmod M_n) \geq n - 2h^2.$$

Since $d \geq n - 2h^2$, that $b = 1$.

In this way, the eavesdropper without knowledge of the private key is able to send the ciphertext with the selected encrypted message, that will be properly decrypted by the recipient.

Conclusions

This paper analyzes the new public-key cryptosystem AJPS, which is one of the participants in the NIST quantum-resistant cryptography competition. The AJPS cryptosystem relies on the arithmetic modulo Mersenne numbers and uses operations in rings of integers modulo Mersenne number. This work introduces restrictions of cryptosystem public key, namely the restrictions of the Hamming weight of a public key and the restrictions of the Hamming weight of multiplicative inverse of a public key. Also ciphertext requirements were obtained in this work. If these requirements are not met, then a forgery attack will be successful for the cryptosystem. Aside from that, this paper illustrates the AJPS cryptosystem usage recommendations considering all found vulnerabilities about possibility of active attacks.

References

[1] D. Aggarwal, A. Joux, A. Prakash, M. Santha, "A New Public-Key Cryptosystem via Mersenne Numbers", Available: https://eprint.iacr.org/2017/481. Accessed on: 2017.

[2] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" / Peter W. Shor. Available: https://arxiv.org/abs/quant-ph/9508027. Accessed on: 1995.

[3] A. Kitaev, "Quantum measurements and the Abelian Stabilizer Problem" / Alexei Kitaev, Available: https://arxiv.org/abs/quant-ph/9511026. Accessed on: 1995.

[4] Post-Quantum cryptography standardization NIST, Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization. Accessed on: 2017.

[5] J. Bos, "Efficient SIMD arithmetic modulo a Mersenne number" / J. Bos, T. Kleinjung, A. Lenstra. Available: https://eprint.iacr.org/2010/338. Accessed on: 2010.

[6] M. Taschwer, "Modular Multiplication Using Special Prime Moduli" / Mario Taschwer. Available: http://www-itec.uni-klu.ac.at/bib/files/2001si_modmult.pdf. Accessed on: 2001.

[7] Encyclopedia Britannica. Mathematics. Mersenne prime. Available: https://www.britannica.com/science/Mersenne-prime.

[8] M. Beunardeau, F. Connolly, R. Géraud, D. Naccache, "On the Hardness of the Mersenne Low Hamming Ratio Assumption", Available: https://eprint.iacr.org/2017/522. Accessed on: 2017.

[9] K.de Boer, L. Ducas, S. Jeffery, R. de Wolf, "Attacks on the AJPS Mersenne-based cryptosystem", Available: https://eprint.iacr.org/2017/1171. Accessed on: 2018.

[10] H. Ferradi, "Integer Reconstruction Public-Key Encryption" / H. Ferradi, D. Naccache. Available: https://eprint.iacr.org/2017/1231. Accessed on: 2018.