UDC 003.26.09

The Modification of the Quantum-Resistant AJPS-1 Cryptographic Primitive

Dariya Yadukha[1, a]

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

Abstract

In recent years, quantum-resistant cryptography has been steadily developing, which is due, in particular, to the post-quantum cryptosystems competition of the National Institute of Standards and Technology (NIST), which has been ongoing since 2017. One of the participants in the first round of the competition is the AJPS cryptosystem. In this work, we propose the modification of the AJPS cryptosystem for bit-by-bit encryption by changing the numbers class used in the cryptosystem as a module. This modification increases the variability of the cryptosystem parameters.

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

1. Introduction

In recent years, a significant amount of research into technologies for creating scalable quantum computers has been conducted. In view of this, post-quantum cryptography has also begun to progress rapidly [1]. Its aim is to develop the cryptographic primitives that would be resistant to attacks using both quantum and classical computers.

In 2017, the National Institute of Standards and Technology (NIST) has launched the currently ongoing competition for quantum-resistant public-key cryptographic primitives [2]. According to the competition plan, it is going to be finished in 2024. As a result, USA will accept new post-quantum public-key cryptography standards, which will specify one or more additional digital signature, public key encryption, and key encapsulation algorithms to augment FIPS 186-4, Digital Signature Standard (DSS), as well as special publications SP 800-56A and SP 800-56B [2]. One of the participants of the first round of the competition is the Mersenne-756839 key encapsulation mechanism, which is based on the AJPS cryptosystem [3].

The AJPS cryptosystem was created by a group of famous cryptologists consisting of D. Aggarwal, A. Joux, A. Prakash and M. Santha. AJPS uses arithmetic modulo Mersenne number, which can be efficiently implemented using algorithms for fast computation of cumbersome modular operations, such as reduction, multiplication, modular multiplicative inverse calculation, bitwise addition and multiplication modulo Mersenne number [4, 5]. AJPS has two versions – bit-by-bit encryption scheme (AJPS-1) and scheme for encrypting a message block (AJPS-2).

This paper describes the results of the modification of the AJPS-1 cryptosystem by changing the class of numbers used in the cryptosystem as a module.

2. Description of the AJPS-1 cryptosystem

The AJPS-1 cryptosystem [3] allows encrypting one bit of a message, that is, the plaintext is the value $b \in \{0, 1\}$.

Let public parameters of cryptosystem be:

- Mersenne number $M_n = 2^n - 1$, where $n \in \mathbb{N}$;
- the security parameter λ;
- fixed integer h, such that:
  1) $C_n^h \geq 2^\lambda$;
  2) $4h^2 < n \leq 16h^2$.

To simplify notation, we equate numbers modulo Mersenne number with binary strings from the set $\{0,1\}^n \setminus \{1^n\}$. Also, we define the set of numbers which have Hamming weight h modulo Mersenne number M_n as:

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

where $Ham(x)$ is the Hamming weight of x (total amount of 1's in the binary representation of x).

[a] dariya.yadukha@gmail.com

Given the introduced simplification of the notation, the set $HM_{n,h}$ can also be represented as the set of residues modulo the Mersenne number M_n, which have Hamming weight 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:

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

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

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

Encryption. The encryption algorithm (for encrypting $b \in \{0,1\}$) chooses two random independent integers A and B uniformly from the set $HM_{n,h}$. Integers A and B are secret ephemeral parameters of the cryptosystem. A 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 the value of d:

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

The correctness of the decryption follows from Lemma 1.

Lemma 1. [3] *For integers $A, B \in \{0,1\}^n$ and a module M_n the following properties hold:*

1) $Ham(A+B \bmod M_n) \le Ham(A)+Ham(B)$;
2) $Ham(A \cdot B \bmod M_n) \le Ham(A) \cdot Ham(B)$;
3) *If $A \neq 0^n$, then*

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

To see the correctness of the decryption algorithm, 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 $b = 1$.

Security of the AJPS-1 cryptosystem rests upon the conjectured intractability of the Mersenne Low Hamming Ratio Search Problem (MLHRSP) [3].

Definition 1. (MLHRSP) *Given a Mersenne number M_n, 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:*

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

It is considered that MLHRSP 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. [6, 7, 8, 9] MLHRSP is based on the following claim.

Claim 1. [3] *Let F and G be such integers, that they both have low Hamming weight h. Then, when we consider H as $F \cdot G \bmod M_n$, H looks pseudorandom, i.e., it will be hard to distinguish H from a random integer modulo M_n.*

AJPS creators suggested using the following values for n and h (Table 1) [3]. Such parameters satisfy all the necessary requirements of the key generation algorithm, and in this case, it is considered that the value of h is low enough, compared to n, so that Claim 1 is fulfilled.

Table 1. Suggested values of n and h for AJPS-1

n	h	λ
1279	17	120
2203	23	174
3217	28	221
4253	32	260
9689	49	432

3. Modification of AJPS-1

As we said earlier, the arithmetic modulo Mersenne number has many advantages for using in cryptography due to the existence of efficient algorithms for calculating cumbersome modulo operations. Such algorithms are often generalized to the case of larger number classes, in particular *generalized Mersenne numbers* [4, 5, 10].

Let us consider generalized Mersenne numbers such that:

$$GM_{n,m} = 2^n - 2^m - 1,$$

where $n, m \in \mathbb{N}$, $n > m$. To create a modification of the AJPS-1 cryptosystem with this class of numbers as a module, first and foremost, it is necessary to determine the Hamming weight relations, similar to those in Lemma 1. Such relations for generalized Mersenne numbers are described in Theorems 1 and 2.

Theorem 1. [11] Let us have integers A and B such that $A \le GM_{n,m}$ and $B \le GM_{n,m}$. Then the following properties are fulfilled:

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

Theorem 2. [12] Let A is an n-bit integer such that $A \ne 0$ and $A \le GM_{n,m}$. Denote $A = a_{n-1}\, a_{n-2} \dots a_1\, a_0$, where $a_i \in \{0,1\}$, $i = \overline{0, n-1}$.

1) If $a_m = 0$, then:
$$Ham(-A \bmod GM_{n,m}) = n - 1 - Ham(A).$$
2) If $a_m = 1$, let us represent A in the form $A = h_1 \,||\, h_2 \,||\, h_3$, where:
   - $h_3 = a_{m-1}\, a_{m-2} \dots a_0$, so h_3 includes m lower bits of A;
   - $h_2 = a_{k-1}\, a_{k-2} \dots a_m$, where
   $$k = \min_i\{a_i = 0 \mid a_j = 1, m \le j < i\},$$
   so h_2 includes bits from a_m to the first zero after a_m;
   - $h_1 = a_{n-1}a_{n-2} \dots a_k$.

   Then we have:
$$Ham(-A \bmod GM_{n,m}) =$$
$$= n - k - Ham(h_1) + Ham(h_2) +$$
$$+m - Ham(h_3).$$

Using Theorems 1 and 2, we create a modification of the AJPS-1 cryptosystem using arithmetic modulo the generalized Mersenne number $GM_{n,m}$.

Let public parameters be:

- generalized Mersenne number
$$GM_{n,m} = 2^n - 2^m - 1,$$
where $n, m \in \mathbb{N}$, $n > m$;
- the security parameter λ;
- fixed integer h, such that:
  1) $C_n^h \ge 2^\lambda$;
  2) $4h^2 < n \le 16h^2$;
  3) $m < \frac{n-1}{2h} - h$.

For convenience, we define the set of numbers which have Hamming weight h modulo generalized Mersenne number $GM_{n,m}$ as:
$$HG_{n,m,h} = \{x < GM_{n,m} : Ham(x) = h\}.$$

Key Generation. Let F and G be random integers, chosen independently and uniformly from the set $HG_{n,m,h}$, and let the m-th bit of G equals 0. The integer F is a secret parameter of the cryptosystem and G is a private (secret) key. Public key H is calculated as
$$H = F \cdot G^{-1} \bmod GM_{n,m}.$$

Encryption. For encryption, we choose two random independent integers A, B from the set $HG_{n,m,h}$. Integers A and B are secret ephemeral parameters of the cryptosystem. Then we check such requirements:

1) $Ham(A + B \bmod GM_{n,m}) \ge$
$$\ge |Ham(A) - Ham(B)|;$$
2) $Ham(A \cdot B \bmod GM_{n,m}) \ge$
$$\ge |Ham(A) - Ham(B)|.$$

If at least one of the requirements is not fulfilled, then we need to choose another values of A and B.

The probability that randomly selected numbers A and B from the set $HG_{n,m,h}$ fulfil both requirements is 0.988 (experimentally established for 1000000 randomly selected numbers $A, B \in HG_{n,m,h}$ for values n and h from Table 1). Therefore, these requirements do not significantly limit the choice of parameters A and B.

Then, a bit b is encrypted as:
$$C = A \cdot H + (-1)^b \cdot B \bmod GM_{n,m}.$$

Note that changing of encryption formula compared to classic AJPS-1 is due to the fact that the secret parameters A, B and F should not be used during decryption, but only the secret key G and the ciphertext C should be used. Since the Hamming weight of the additive inverse modulo generalized Mersenne number depends on the m-th bit of this number, it is necessary to ensure that we will compute the additive inverse to the secret key G during decryption.

Decryption. The decryption algorithm computes
$$d = Ham(C \cdot G \bmod GM_{n,m}).$$
Then it returns the value of b, depending on the value of d:
$$b = \begin{cases} 0, & \text{if } d \le 2h^2 + h(2m-2); \\ 1, & \text{if } d \ge n - 2h^2 - 1; \\ \perp \text{ (error)}, & \text{else.} \end{cases}$$

Let us show that the algorithm is correct. To do this, consider two cases depending on the value of the bit b.

1) If $b = 0$, then ciphertext is as follows:
$$C = A \cdot H + B \bmod GM_{n,m}.$$

Then, when decrypting, we have:

$$d = Ham(C \cdot G \bmod GM_{n,m}) =$$
$$= Ham(A \cdot F + B \cdot G \bmod GM_{n,m}).$$

Using the item 1 of Theorem 1, we have:

$$d \leq Ham(A \cdot F \bmod GM_{n,m}) +$$
$$+Ham(B \cdot G \bmod GM_{n,m}).$$

After that, using twice the item 2 of Theorem 1, we have:

$$d \leq Ham(A) \cdot Ham(F) +$$
$$+(m-1) \cdot \min\{Ham(A), Ham(F)\} +$$
$$+Ham(B) \cdot Ham(G) +$$
$$+(m-1) \cdot \min\{Ham(B), Ham(G)\}.$$

Using the fact that $A, B, F, G \in HG_{n,m,h}$, we have:

$$d \leq 2h^2 + h(2m-2).$$

2) If $b = 1$, ciphertext is:

$$C = A \cdot H - B \bmod GM_{n,m}.$$

Then, using Theorem 1, we have:

$$d = Ham(A \cdot F - B \cdot G \bmod GM_{n,m}) =$$
$$= Ham(A \cdot F + B \cdot (-G) \bmod GM_{n,m}).$$

Using requirements from the encryption algorithm, we have:

$$d \geq \big|\, |Ham(A) - Ham(F)| -$$
$$-|Ham(B) - Ham(-G \bmod GM_{n,m})| \,\big| =$$
$$= \big||h-h| - |h - Ham(-G \bmod GM_{n,m})|\big| =$$
$$= |h - Ham(-G \bmod GM_{n,m})|.$$

Since $Ham(G) = h$ and, by the requirement of the cryptosystem, h is a small number compared to n, then the Hamming weight of additive inverse of G modulo $GM_{n,m}$ is greater than h. Then we have:

$$d \geq Ham(-G \bmod\ GM_{n,m}) - h.$$

Using Theorem 2, we get the desired result.

Note that such a modification of AJPS-1 is possible even without the restriction on the m-th bit of the secret key G. In this case, the decryption algorithm should be modified in accordance with both items of Theorem 2. However, then it is necessary to ensure that the condition

$$2h^2 + h(2m-2) < Ham(-G \bmod GM_{n,m}) - h$$

is also fulfilled for the case when the m-th bit of G is 1. For the case when the m-th bit of G is 0, this condition is satisfied by the requirement

$$m \leq \frac{n-1}{2h} - h,$$

however, it is not sufficient for the case when the m-th bit of G is 1.

The advantage of this modification is a significant increase in the number class which can be used as a module in the cryptosystem. In addition, the other advantage of the modification is an increase in the interval length of the decryption parameter d, in particular, the number of unique values that the parameter d takes.

The justification for this are the experimental results, which are described in Figures 1 and 2, and also in Tables 2 and 3.

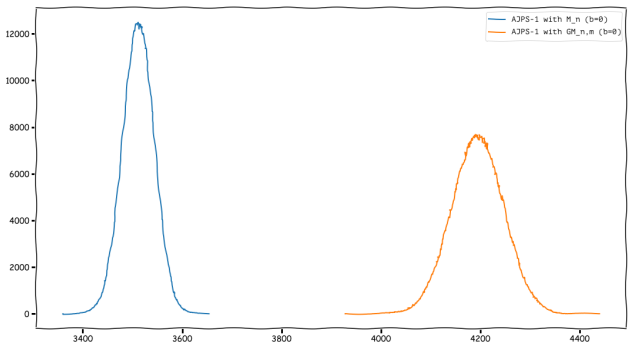

Fig. 1. Distribution of the decryption parameter d in AJPS-1 and in the modification of AJPS-1 using generalized Mersenne numbers as a module (when encryption of bit $b = 0$) for parameters $n = 9689$ and $h = 49$

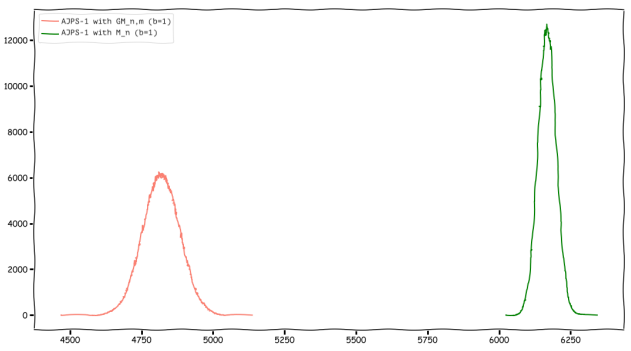

Fig. 2. Distribution of the decryption parameter d in AJPS-1 and in the modification of AJPS-1 using generalized Mersenne numbers as a module (when encryption of bit $b = 1$) for parameters $n = 9689$ and $h = 49$

Note. Distributions of the decryption parameter d for other values of n and h which are given in Table 1, can be found in [13].

Table 2. The interval length of the decryption parameter d in AJPS-1 and in the modification of AJPS-1 using generalized Mersenne number $GM_{n,m}$ as a module

n	h	Number class	Interval length of values d	
			$b = 0$	$b = 1$
1279	17	*Mersenne*	105	112
		Generalized Mersenne	173	256
2203	23	*Mersenne*	147	141
		Generalized Mersenne	233	295
3217	28	*Mersenne*	171	170
		Generalized Mersenne	279	367
4253	32	*Mersenne*	201	204
		Generalized Mersenne	331	415
9689	49	*Mersenne*	294	319
		Generalized Mersenne	512	668

Table 3. The count of unique values of the decryption parameter d in AJPS-1 and in the modification of AJPS-1 using generalized Mersenne number $GM_{n,m}$ as a module

n	h	Number class	Count of unique values d	
			$b = 0$	$b = 1$
1279	17	*Mersenne*	103	104
		Generalized Mersenne	150	224
2203	23	*Mersenne*	139	139
		Generalized Mersenne	208	280
3217	28	*Mersenne*	166	162
		Generalized Mersenne	256	325
4253	32	*Mersenne*	192	190
		Generalized Mersenne	299	386
9689	49	*Mersenne*	285	284
		Generalized Mersenne	457	553

To obtain these results a series of 1,000,000 applications of encryption and decryption algorithms of the AJPS-1 cryptosystem and its modification with fixed key values were performed. The public and secret keys are obtained as a result of key generation algorithms of the AJPS-1 cryptosystem and its modification. When applying key generation, encryption and decryption algorithms of the modification of the AJPS-1 cryptosystem using arithmetic modulo generalized Mersenne number, the parameter $m = 25$ was used for the generalized Mersenne number $GM_{n,m}$.

The interval length is calculated as the subtraction result between the maximum and minimum values of d among the obtained results. The count of unique values is the number of unique values of d among the obtained 1,000,000 values.

Thus, the number of different values of d in the modification increased by a factor of two, on average, compared to the AJPS-1 cryptosystem.

Therefore, such modification allows us to increase the resistance of the AJPS-1 cryptosystem to known-plaintext attacks, which are aimed at determining the secret key. Also, the constructed modification of AJPS-1 has a greater variability of parameters, in particular, it allows using different number classes as a module, which increases the flexibility of the practical application of this cryptosystem.

The security of this modification of the AJPS-1 cryptosystem relies on the assumption that it is hard to solve the *Generalized Mersenne Low Hamming Ratio Search Problem* (GMLHRSP).

Definition 2. (GMLHRSP) *Given a generalized Mersenne number $GM_{n,m}$, an n-bit integer H and an integer h, find two integers F and G, such that $F, G \in HG_{n,m,h}$ and*

$$H = F \cdot G^{-1} \bmod GM_{n,m}.$$

4. Conclusion

This paper analyses the quantum-resistant public-key cryptosystem AJPS, which is one of the participants in the NIST post-quantum cryptography competition. The AJPS cryptosystem relies on the arithmetic modulo Mersenne numbers.

In this work, we considered the bit-by-bit encryption scheme of the AJPS cryptosystem, which is called AJPS-1, and we constructed a modification of AJPS-1 by changing the number class used in the cryptosystem as a module. Instead of Mersenne numbers $M_n = 2^n - 1$, our modification uses generalized Mersenne numbers of the form $GM_{n,m} = 2^n - 2^m - 1$. To create such a

modification, we had to obtain the relations for the Hamming weight of the sum and product of the two numbers modulo generalized Mersenne number and relations for Hamming weight of additive inverse modulo generalized Mersenne number.

As a result of the statistical analysis of the modification of AJPS-1, we found that the advantage of these modifications is not only a significant increase in the class of modules used, but also an increase in the interval length and the number of unique values of the decryption parameter d.

Thus, the constructed modification of the AJPS-1 cryptosystem allows us to increase the resistance to known-plaintext attacks, which are aimed at determining the secret key.

References

[1] S. Antipolis, "Quantum Safe Cryptography and Security. an Introduction, Benefits, Enablers and Challenges," *European Telecommunications Standards Institute White Papers*, no. 8, 2015.

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

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

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

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

[6] 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.

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

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

[9] 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.

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

[11] 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.

[12] D. Yadukha, "Hamming Weight Bound for Additive Inverse Modulo Generalized Mersenne Number," in *Proceedings of the International Scientific Conference "Information Technologies and Computer Modelling"*, (Ivano-Frankivsk, Ukraine), pp. 165–168, 2018.

[13] D. Yadukha, "The Modification and Cryptanalysis of Quantum-Resistant AJPS Family Primitives." https://ela.kpi.ua/handle/123456789/34344, 2020.