UDC 003.26

The Modification of Post-Quantum AJPS-1 Cryptosystem by Changing the Metric

Dariya Yadukha[1]

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

Abstract

This paper considers the AJPS-1 post-quantum cryptosystem. A feature of this cryptosystem is the use of arithmetic modulo Mersenne number, in particular, the AJPS cryptosystem uses relations for the Hamming weight of integers modulo Mersenne number. To create a modification of this cryptosystem by changing the metric, relations of the OSD metric for integers modulo Mersenne number were obtained. The paper describes the constructed modification of the AJPS-1 cryptosystem with a changed metric and analyses its advantages compared to the AJPS-1 cryptosystem. This modification allows to increase the variance of the decryption parameter, which improves the resistance of the cryptosystem to ciphertext-only (known ciphertext) attacks aimed at determining the private key.

Keywords: post-quantum cryptography, the AJPS cryptosystem, the Mersenne-756839 cryptosystem, Hamming weight, Mersenne numbers

Introduction

In recent years, there has been rapid progress in post-quantum cryptography research. Post-quantum cryptography aims to create cryptographic primitives that can resist attacks from both quantum and classical computers.

Between 2017 and 2023, the National Institute of Standards and Technology (NIST) held a competition for quantum-resistant public-key cryptographic primitives [1]. As a result, the USA will soon 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 [1].

In August 2023, NIST published drafts of three future standards: FIPS 203 – Key-Encapsulation Mechanism Standard, and two Digital Signature Standards: FIPS 204 and FIPS 205 [2]. An ongoing open discussion is currently taking place regarding these draft standards.

Therefore, it is crucial to research various post-quantum cryptoprimitives to ensure information security and to resist future attacks by quantum computers, which pose a threat to the security of current cryptosystems.

One of the participants in the first round of the PQC-NIST competition is the Mersenne-756839 key encapsulation mechanism, which relies on the AJPS cryptosystem [3].

The AJPS cryptosystem utilises 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, 6]. AJPS has two versions – a bit-by-bit encryption scheme (AJPS-1) and a scheme for encrypting a message block (AJPS-2).

This paper presents the results of modifying the AJPS-1 cryptosystem by changing the metric used in the cryptosystem.

1. The AJPS-1 cryptosystem

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

The public parameters of the AJPS-1 cryptosystem are:

- Mersenne number $M_n = 2^n - 1$, $n \in \mathbb{N}$;
- 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 that have Hamming weight h modulo Mersenne number M_n as follows:

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

where $Ham(x)$ is the Hamming weight of x (total number of 1's in the binary representation of x). Due to the simplified notation, the set $HM_{n,h}$ can also be represented as the set of residues modulo the Mersenne number M_n, with Hamming weight h.

KeyGen. 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. The public key H is then calculated as follows:

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

Enc. 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:

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

Dec. 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:

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

The correctness of the decryption follows from Lemma 1.

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

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

To see the correctness of the decryption algorithm, note that:

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

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

The security of the AJPS-1 cryptosystem is based on the assumption that the Mersenne Low Hamming Ratio Search Problem (MLHRSP) is computationally infeasible. [3].

Definition 1. (MLHRSP) *Given a Mersenne number M_n, an n-bit integer H and an integer h, find F and G, where $F, G \in HM_{n,h}$, such that:*

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

The MLHRSP is based on the following claim.

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

It is considered that MLHRSP is hard to solve. This problem is resistant to many known attacks, including Meet-in-the-middle attacks, Guess and Win, Lattice-based attacks, etc [7, 8, 9, 10, 11].

The creators of AJPS recommended utilizing the following values for n and h (Table 1) [3].

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

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.

2. The Modification of AJPS-1 with OSD

The AJPS cryptosystem uses the Hamming weight calculation, in particular, the correctness of the AJPS-1 decryption is based on the relations for the Hamming weight of integers modulo the Mersenne number, which are described in Lemma 1.

The following modification illustrates and justifies the possibility of using metrics other than the Hamming weight in the AJPS-1 cryptosystem.

Let the metric OSD (*One-side disbalance*) be as follows:

$$OSD(X) = \#1(X) - \#0(X),$$

where $\#1(X)$ denotes the number of ones in the binary notation of the number X, and, accordingly, $\#0(X)$ – the number of zeros in X.

The relations for OSD of integers modulo Mersenne number described in the Lemma 2.

Lemma 2. *For integers $A, B \in \{0,1\}^n$ and Mersenne number $M_n = 2^n - 1$, where $n \in \mathbb{N}$, the following relations hold:*

1) $OSD(A + B \bmod M_n) \leq$
$$\leq OSD(A) + OSD(B) + n;$$
2) $OSD(A \cdot B \bmod M_n) \leq$
$$\leq \frac{OSD(A) \cdot OSD(B)}{2} + n \cdot \left(\frac{OSD(A) + OSD(B) + n}{2} - 1 \right);$$
3) $OSD(-A \bmod M_n) = -OSD(A)$.

Proof. It should be noted that the OSD metric can be represented in terms of the Ham metric as follows:

$$OSD(X) = Ham(X) - (n - Ham(X)) = 2 \cdot Ham(X) - n,$$

where X is an n-bit integer.

1) Using the described relation of the metrics OSD and Ham to the value $OSD(A + B \bmod M_n)$, we have:
$$OSD(A + B \bmod M_n) = 2 \cdot Ham(A + B \bmod M_n) - n.$$
Applying item 1 of Lemma 1, we have:
$$OSD(A + B \bmod M_n) \leq \leq 2 \cdot Ham(A) + 2 \cdot Ham(B) - n.$$
Again using the relation between Ham and OSD, we have:
$$OSD(A + B \bmod M_n) \leq \leq 2 \cdot Ham(A) + OSD(B) = = 2 \cdot Ham(A) - n + n + OSD(B) = = OSD(A) + OSD(B) + n.$$
2) Employing the relation of OSD and Ham alongside item 2 of Lemma 1, we obtain:
$$OSD(A \cdot B \bmod M_n) = = 2 \cdot Ham(A \cdot B \bmod M_n) - n \leq \leq 2 \cdot Ham(A) \cdot Ham(B) - n.$$
By replacing the metric according to this relation:
$$Ham(X) = \frac{OSD(X) + n}{2},$$
we get:
$$OSD(A \cdot B \bmod M_n) \leq \leq 2 \cdot \frac{OSD(A) + n}{2} \cdot \frac{OSD(B) + n}{2} = = \frac{OSD(A) \cdot OSD(B)}{2} + \frac{n \cdot (OSD(A) + OSD(B)) + n^2}{2} - n.$$
3) Applying item 3 of Lemma 1 and the dependence of OSD on Hamming weight, we obtain:
$$OSD(-A \bmod M_n) = = 2 \cdot Ham(-A \bmod M_n) - n = = 2 \cdot (n - Ham(A)) - n = = n - Ham(A) = -OSD(A).$$

■

Based on the results outlined in Lemma 2, it is possible to create a modification of the AJPS-1 cryptosystem, which will use the OSD metric instead of the Hamming weight. Let's consider such a modification further.

1) The ***KeyGen*** algorithm of the original AJPS-1 cryptosystem is used to generate the keys in this modification. It should be noted that
$$OSD(F) = OSD(G) = 2h - n,$$
because according to the AJPS-1 condition, Hamming weight of the numbers F and G is equal to h. For convenience, we denote $q = 2h - n$.
2) For encryption, this modification uses the ***Enc*** algorithm of the AJPS-1 cryptosystem. Note that for integers A and B used in encryption, similarly to the numbers F and G, we have:
$$OSD(A) = OSD(B) = q.$$
3) In the decryption algorithm ***Dec*** of this AJPS-1 modification, the value d is calculated as follows:
$$d = OSD(C \cdot G \bmod M_n).$$
Then the bit b is determined depending on d according to following relation:
$$b = \begin{cases} 0, & \text{if } s \leq (n+q)^2 - n; \\ 1, & \text{if } s \geq n - (n+q)^2; \\ \perp, & \text{else (decryption error).} \end{cases}$$

The correctness of the decryption follows from Lemma 2.

The security of the constructed modification of AJPS-1, as well as the original AJPS-1 cryptosystem, is based on the complexity of the Mersenne Low Hamming Ratio Search Problem. This is true because the OSD metric can be represented by the Ham metric, which allows reducing the problem of finding the secret key G (in the AJPS-1 modification with OSD) to the MLHRSP.

The advantage of the modification of AJPS-1 by changing the metric is increasing the set of values accepted by decryption parameter d according to which the message bit is determined in the decryption algorithm. This result was obtained experimentally through a series of 1,000,000 applications of encryption and decryption algorithms of the AJPS-1 cryptosystem and its modification with fixed key values.

Thus, the number of possible values of d in modification of AJPS-1 with OSD metric is greater than the number of possible values of d in the AJPS-1 cryptosystem. The obtained results are shown in Tables 2 and 3, as well as in Figures 1 and 2. Note that the interval length was calculated as the subtraction result between the maximum and minimum integers among the obtained results of d.

Table 2
The interval length to which d belong when $b = 0$ (in AJPS-1 and in the modification of AJPS-1 with OSD)

n	h	Metric	Interval length of d when $b = 0$
1279	17	Ham	105
		OSD	212
2203	23	Ham	147
		OSD	292
3217	28	Ham	171
		OSD	370
4253	32	Ham	201
		OSD	390
9689	49	Ham	294
		OSD	656

Table 3
The interval length to which d belong when $b = 1$ (in AJPS-1 and in the modification of AJPS-1 with OSD)

n	h	Metric	Interval length of d when $b = 1$
1279	17	Ham	112
		OSD	194
2203	23	Ham	141
		OSD	286
3217	28	Ham	170
		OSD	352
4253	32	Ham	204
		OSD	418
9689	49	Ham	319
		OSD	620

Figure 1 shows the distribution of d in the decryption algorithm of the AJPS-1 cryptosystem and of the modification of AJPS-1 using the OSD metric with the parameters $n = 1279$, $h = 17$ and the message bit $b = 0$.

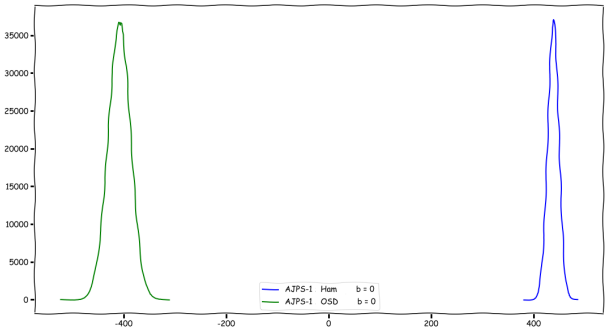

Figure 1: Distribution of d in AJPS-1 and in the modification of AJPS-1 by using the OSD metric, with the parameters $n = 1279$, $h = 17$ and the message bit $b = 0$

Figure 2 illustrates the distribution of d in both the decryption algorithm of the AJPS-1 cryptosystem and the modified AJPS-1 utilizing the OSD metric, with the parameters $n = 1279$, $h = 17$, and the message bit $b = 1$.

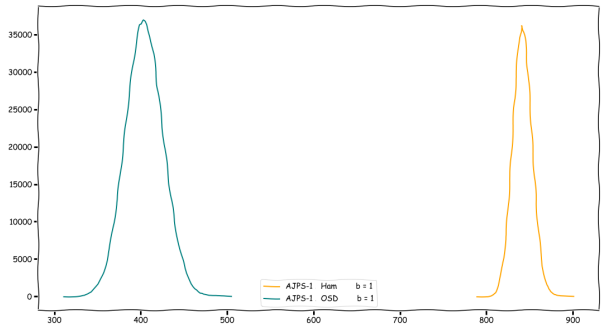

Figure 2: Distribution of d in AJPS-1 and in the modification of AJPS-1 by using the OSD metric, with the parameters $n = 1279$, $h = 17$ and the message bit $b = 1$

The d values in the AJPS-1 cryptosystem and the modification of the AJPS-1 cryptosystem using the OSD metric are random variables with a normal distribution. However, Figures 1 and 2 show that changing the metric in AJPS-1 increases the variance of the random variable. This means that the set of possible values of the parameter d in the modification of AJPS-1 with OSD is greater than the set of possible values of d in the classic version of AJPS-1.

Thus, the described modification of the AJPS-1 cryptosystem by changing the metric has an advantage compared to AJPS-1, because due to the small number of values of the d parameter in the AJPS-1 cryptosystem, ciphertext-only (known ciphertext) attacks aimed at determining the secret key G may be applied.

Conclusions

This paper presents the research results of the post-quantum AJPS-1 cryptosystem, which is one of the versions of the AJPS (Mersenne-756839) cryptosystem that participated in the first round of the NIST post-quantum cryptoprimitives competition. A feature of this cryptosystem is the use of arithmetic modulo Mersenne number, in particular, the cryptosystem uses relations for Hamming weight of integers modulo Mersenne number.

In this paper, we constructed a modification of the AJPS-1 cryptosystem by changing the metric – in our modification, we use the OSD (one-side disbalance) metric instead of Hamming weight. To construct such modification, relations of the OSD metric for integers modulo Mersenne number, which is also described in this paper, were obtained.

The advantage of this modification of AJPS-1 is to increase the set of values that the decryption parameter takes. This makes it possible to increase the resistance of the cryptosystem to ciphertext-only attacks, which are aimed at determining the secret key.

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] National Institute of Standards and Technology, "Three Draft Fips for Post-Quantum Cryptography." https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography, 2023.

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

[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] K. de Boer, L. Ducas, S. Jeffery, and R. de Wolf, "Attacks on the ajps mersenne-based cryptosystem," in Post-Quantum Cryptography (T. Lange and R. Steinwandt, eds.), (Cham), pp. 101–120, Springer International Publishing, 2018.