Innovative: International Multi-disciplinary Journal of Applied Technology
(ISSN 2995-486X) VOLUME 04 ISSUE 06, 2026

Mathematical Analysis of the R-Parametric Operation Presented in the O'zmst 286:2024 Standard

N. R. Zaynalov
Head of the Department of "Cybersecurity and Cryptology", TUIT Samarkand branch
E-mail: bekibrohimov2522@gmail.com

U. B. Sharipova
Teacher of the Department of "Cybersecurity and Cryptology", TUIT Samarkand branch
E-mail: bekibrohimov2522@gmail.com

B. Sh. Ibrohimov
Student of "Information Security", TUIT Samarkand branch
E-mail: bekibrohimov2522@gmail.com

O. A. Oydinov
Student of "Information Security", TUIT Samarkand branch
E-mail: bekibrohimov2522@gmail.com

Abstract:

This article mathematically analyzes the R parametric multiplication operation introduced in the national standard of the Republic of Uzbekistan O'zMSt 286:2024 "Processes of generating and verifying electronic digital signatures". The theoretical foundations of the parametric multiplication and exponentiation operations presented in the standard are considered, and the computational processes generated on the basis of these operations are analyzed using examples. In particular, the commutativity of the parametric multiplication operation, the determination of the inverse element, and the exponentiation processes are mathematically considered. Additionally, the computational efficiency of the method recommended in the standard is analyzed during the calculation of large powers, and the possibility of optimizing this calculation is demonstrated. The research results determine that certain computational processes related to the R-parametric operation can be simplified.

Keywords: Electronic Digital Signature, Cryptography, Parametric Multiplication, Modular Arithmetic, Discrete Logarithm, Cryptographic Algorithms.

Introduction

The integration of advanced cryptographic mechanisms is crucial for ensuring message integrity, user authentication, and data non-repudiation within modern information security systems. In the Republic of Uzbekistan, the newly introduced national standard **O'zMSt 286:2024** regulates electronic digital signature (EDS) processes by introducing two distinct cryptographic algorithms. A pivotal mathematical concept introduced in this standard is the **R-parametric multiplication operation**, defined over a prime modulo p with an arbitrary residue parameter R. This framework transitions classical cryptographic calculations into a specialized parametric group structure [1]. While the standard establishes foundational definitions for parametric systems, a deeper algebraic exploration of its core properties remains a crucial knowledge gap. Previous studies and regulatory documents outline the practical generation of digital signatures, but they lack comprehensive optimization strategies for the accompanying multi-stage computational workflows [2].

To address this gap, this research employs a strict methodological approach utilizing **algebraic methods, congruent arithmetic formulas, and a process-oriented analysis**. The primary objective is to evaluate the fundamental properties of the parametric operation—specifically its **commutativity and inversion operations**—while testing its performance during large-scale calculations [3]. It is hypothesized that mapping the non-standard operation to classic isomorphic functions can bypass the demanding linear steps typical of large power computations.

The structural findings of this mathematical analysis successfully prove the **commutative property** of the R-parametric operation. Furthermore, the study re-evaluates the standard's inversion formula, distinguishing its behavioral mechanics from classical multiplicative inverses and formalizing a streamlined **parametric exponentiation algorithm**. By applying a fast exponentiation framework and the extended Euclidean algorithm, the general expression is heavily optimized [4]. The practical implication of these results is a significantly simplified computational blueprint that enhances execution efficiency, offering a vital optimization that should be integrated directly into national cryptographic implementations.

Materials and Methods

Analysis methods, a process approach, algebraic methods, and congruent arithmetic formulas were used during the research.

Literature Review

One of the main normative documents regulating EDS algorithms in the Republic of Uzbekistan is the national standard O'zMSt 286:2024 "Processes of generating and verifying electronic digital signatures" [5]. This standard describes two different cryptographic algorithms for generating and verifying electronic digital signatures. As one of the important aspects of the standard, a special multiplication operation defined modulo p with the parameter R is introduced.

This operation is defined as follows:

$$x \circledR y = x + (1 + xR)y \pmod{p} \qquad (1)$$

Here p is a prime number, and R is any residue of modulo p (natural number $R < p$). This operation is used to organize cryptographic calculations in a parametric group. However, it is necessary to analyze in detail some mathematical properties and computational processes associated with this operation [6].

Results and Discussion

It is required to practically prove the properties of the R parametric multiplication operation. The special operation given in the standard is defined as follows:

$$\boldsymbol{x \circledR y = x + (1 + xR)y \pmod{p}}$$

Some algebraic properties of this operation are determined as follows.

1.*Commutativity property.* The following equality is considered:

$$\boldsymbol{x \circledR y = x + (1 + xR)y}$$
$$\boldsymbol{y \circledR x = y + (1 + yR)x}$$

The difference is calculated:

$$\boldsymbol{x \circledR y - y \circledR x}$$

$$= x + (1 + xR)y - y - (1 + yR)x$$

$$= x + y + xRy - y - x - yRx$$

$$= 0 \pmod{p}$$

Thus

$$x \circledR y = y \circledR x$$

the equality is determined to be fulfilled. Therefore, the R-parametric operation is a commutative operation.

2. *R parametric inversion operation.* In the standard, the parametric inversion operation is determined by the following formula:

$$x^{/-1} \equiv -x(1 + xR)^{-1} \pmod{p} \qquad (2)$$

In this part, we consider the existence of an inverse element with respect to the parametric operation. If

$$x^{/-1} \equiv -x(1 + xR)^{-1} \pmod{p}$$

then

$$x \circledR x^{-1} \equiv 1 \pmod{p}$$

the equality is fulfilled. According to the definition of the parametric operation

$$x \circledR y = x + (1 + xR)y \pmod{p}$$

Here, *y* is replaced by x^{-1} :

$$x \circledR x^{-1} = x + (1 + xR)x^{-1} \pmod{p}$$

Now the value of x^{-1} is substituted:

$$x^{/-1} = -x(1 + xR)^{-1}$$

As a result

$$x \circledR x^{-1} = x + (1 + xR)(-x(1 + xR)^{-1}) \pmod{p}$$

the expression is generated. If we simplify the product:

$$(1 + xR)(1 + xR)^{-1} = 1$$

since

$$x \circledR x^{/-1} = x - x \pmod{p}$$

it will be equal to

$$x \circledR x^{/-1} = 0 \neq 1 \pmod{p}$$

From this the result is obtained. Therefore, the *R* parametric inversion operation (2) is considered based on the addition operation [7], [8]. For this reason, when designating this formula, it is advisable to introduce the "+" sign as an index as follows:

$$x^{/-1}{}_{(+)} \equiv -x(1 + xR)^{-1} \pmod{p}$$

Above, the existence of the defined inverse element for the parametric operation was shown. This theoretical result can also be seen in a concrete example. For example, when *p*=31 and *R*=13, the parametric inverse element for *x*=12 is determined using the following formula:

$$x^{/-1} \equiv -x(1 + xR)^{-1} \pmod{p}$$

As a result of the calculation

$$12^{/-1} = 25 \pmod{31}$$

is determined. This result shows that the inverse element obtained by the parametric operation satisfies the theoretical equality presented above [9].

In classical modular arithmetic, the inverse element with respect to the multiplication operation is determined by the following condition:

$$x \circledR x^{-1} \equiv 1 \pmod{p}$$

where the inversion is calculated according to the multiplication operation.

$$x \circledR y \equiv 1 \pmod{p}.$$

This equation represents the condition that the result of the parametric operation is equal to 1 [10], [11]. According to the definition of the parametric operation (1), the equation is brought to the following form:

$$x + (1 + xR)y \equiv 1 \pmod{p}.$$

Now, considering y as an unknown in this equation, the equation is solved in accordance with the rules of modular arithmetic. First, the term x is moved to the right side:

$$(\mathbf{1}+\boldsymbol{xR})\boldsymbol{y}\equiv\mathbf{1}-\boldsymbol{x}\ (\mathbf{mod}\ \boldsymbol{p}).$$

As a result, the solution of the equation is determined in the following form:

$$\boldsymbol{y}\equiv(\mathbf{1}-\boldsymbol{x})(\mathbf{1}+\boldsymbol{xR})^{-\mathbf{1}}\ (\mathbf{mod}\ \boldsymbol{p}).$$

Therefore, the inverse element with respect to the multiplication operation is determined by the following expression.

$$\boldsymbol{x}^{/-\mathbf{1}}\equiv(\mathbf{1}-\boldsymbol{x})(\mathbf{1}+\boldsymbol{xR})^{-\mathbf{1}}\ (\mathbf{mod}\ \boldsymbol{p}).$$

Thus, it is observed that the concept of an "inverse element" within the framework of a parametric operation has a different algebraic interpretation than the inverse element in the classical multiplication operation [12]. This situation is of great importance in the mathematical analysis of cryptographic algorithms built on the basis of a parametric operation.

3. *Parametric exponentiation operation.* The exponentiation operation is also defined in a parametric form in the standard. For example:

$$\boldsymbol{X}^{/37}$$

the process of calculating the power is expressed in the following form:

$$\boldsymbol{X}^{/37}=\boldsymbol{X}^{/32+4+1}$$

which is calculated sequentially through parametric multiplication operations [13], [14]. However, since this method requires multi-stage calculations during the computation of large powers, a method for optimizing the calculation process was proposed.

We define the following function:

$$\boldsymbol{\varphi}(\boldsymbol{x})=\boldsymbol{xR}+\mathbf{1} \qquad (3)$$

And the inverse function is:

$$\boldsymbol{\varphi}^{-\mathbf{1}}(\boldsymbol{z})=(\boldsymbol{z}-\mathbf{1})\boldsymbol{R}^{-\mathbf{1}}$$

Then we change the special parametric multiplication operation (1) into the following form:

$$\boldsymbol{x}\circledR\boldsymbol{y}=\boldsymbol{\varphi}^{-\mathbf{1}}\big(\boldsymbol{\varphi}(\boldsymbol{x})\boldsymbol{\varphi}(\boldsymbol{y})\big)$$

Using these formulas, the following calculations are performed:

$$\boldsymbol{x}\circledR\boldsymbol{x}=\boldsymbol{\varphi}^{-\mathbf{1}}((\mathbf{1}+\boldsymbol{xR})^{\mathbf{2}})$$

$$\boldsymbol{x}\circledR\boldsymbol{x}\circledR\boldsymbol{x}=\boldsymbol{\varphi}^{-\mathbf{1}}((\mathbf{1}+\boldsymbol{xR})^{\mathbf{3}})$$

$$\boldsymbol{x}^{/N}=((\boldsymbol{xR}+\mathbf{1})^{N}-\mathbf{1})\boldsymbol{R}^{-\mathbf{1}}\ (\mathbf{mod}\ \boldsymbol{p})$$

The value of $(\boldsymbol{xR}+\mathbf{1})^{N}$ is calculated via the fast exponentiation algorithm. $\boldsymbol{R}^{-\mathbf{1}}$ is determined using the extended Euclidean algorithm.

As a result, the general formula is written as follows:

$$\boldsymbol{x}^{N}=((\boldsymbol{xR}+\mathbf{1})^{N}-\mathbf{1})\boldsymbol{R}^{-\mathbf{1}}\ (\mathbf{mod}\ \boldsymbol{p}) \qquad (4)$$

Through this expression, the exponentiation process can be significantly simplified. In this regard, it is considered appropriate to introduce the application of this simplified approach in calculating parametric exponentiation as a recommendation in the relevant part of the standard [15].

Conclusion

In this article, the R-parametric multiplication operation introduced in the O'zMSt 286:2024 standard was mathematically analyzed.

As a result of the research, it was shown that the parametric multiplication operation has a commutative property, the method of determining the inverse element within the special R-parametric operation was analyzed, and an effective calculation algorithm based on the method proposed in the standard for calculating the parametric exponentiation operation was described. As a result, it was determined that certain computational processes performed on the basis of the *R* parametric operation can be simplified using mathematical calculations.

References

[1] O'zMSt 286:2024. Information technology. Cryptographic protection of information. Processes of generating and verifying electronic digital signatures. Standards Institute of Uzbekistan, Tashkent, 2024.

[2] N. R. Zaynalov, Collection of examples and problems in cryptography. Part I. Study guide. Tashkent, Uzbekistan: Science and Technologies Publishing and Printing House, 2023.

[3] D. Y. Akbarov, P. F. Khasanov, K. P. Khasanov, O. P. Akhmedova, and I. U. Kholimtayeva, Mathematical foundations of cryptography. Textbook. Tashkent, Uzbekistan: TATU, 2018.
[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.
[5] D. E. Knuth, The Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd ed. Reading, MA, USA: Addison-Wesley, 1997.
[6] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY, USA: John Wiley & Sons, 1996.
[7] N. Koblitz, A Course in Number Theory and Cryptography, 2nd ed. New York, NY, USA: Springer-Verlag, 1994.
[8] O. N. Vasilenko, Number-Theoretic Algorithms in Cryptography. Moscow, Russia: MCNMO, 2003.
[9] L. K. Babenko and E. A. Ishchukova, Modern Cryptography Algorithms and Their Application in Information Security Systems. Moscow, Russia: Goryachaya Liniya-Telekom, 2006.
[10] National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)," FIPS PUB 186-5, Gaithersburg, MD, USA, 2023.
[11] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586-615, 2003.
[12] Neal Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987.
[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
[14] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, Jul. 1985.
[15] C. Pomerance, "A tale of two sieves," Notices of the AMS, vol. 43, no. 12, pp. 1473-1485, Dec. 1996.