УДК 004.056.55, 004.056.2; MSC2020 68P25, 94A60

CRYPTOSYSTEM WITH PUBLIC KEYS AND PUBLIC OPERATIONS

ALEXANDER N. ZHVANKO

Abstract. Based on the template implemented by the RSA algorithm, we have defined a cryptosystem with public keys and public operations, which complements the classical scheme with the property that encryption is performed by public keys and operations, and decryption by private keys and operations. By eliminating the use of public keys from our scheme, we get a cryptosystem with public operations. The sets of operations that we have in mind are non-classical arithmetics. This means, having got rid of the secrecy of operations, we will get a cryptosystem with public keys and non-classical arithmetics.

1. Introduction

The purpose of this note is to define a cryptosystem equipped with non-classical arithmetics (NCAs). The latter are described in three sentences: (1) well-known arithmetics of real, complex, quaternions, etc., as well as p-adic, modular, "+" operation on an elliptic curve, etc., based on the use of "school" arithmetic, are not NCAs; (2) non-classical arithmetics must be sets of efficient algebraic operations defined on infinite subsets of $\mathbb{R}^n$; (3) with these sets of operations, we can replace the operations of "school" arithmetic in well-known constructions — functions, equations, etc. The idea of using non-classical arithmetic was expressed in [1]. There you can also find DR_+ — an example of non-classical arithmetic of non-negative real numbers.

We assume that the use of non-classical arithmetic in general in cryptography can be useful in a situation where (1) replacing conventional operations with non-classical ones in known algorithms improves cryptographic strength or performance; (2) when the specified characteristics are equal for algorithm A_{CA} with classical arithmetic CA and algorithm A_{NCA} with non classical arithmetic NCA, then changing CA arithmetic to NCA arithmetic can make useless effort of an intruder who invented an attack against an algorithm with CA arithmetic. This principle can be generalized to all arithmetics as follows: if there is a successful attack on $A_{\mathfrak{A}}$, then replace $\mathfrak{A}$ with $\mathfrak{B}$.

It was said in the paper [1], section "Введение", that the RSA encryption algorithm could be a theoretical use case for NCAs. Indeed, if the factorization of a number with respect to classical multiplication gives some prime factors, then with respect to another multiplication the same number can be factorized by other prime factors. Since there are a lot of multiplications, there are a lot of factorizations. Hiding the multiplication from the attacker makes it harder for him to break the system.

Date: December 5, 2022.

Key words and phrases. public-key-operation cryptography (PKOC), public-operation cryptography (POC), public-key cryptography with non-classical arithmetics (PKCWNCAs), RSA.

Starting from all the considerations above, we arrive at the RSA template as the object of our efforts, resulting in a cryptosystem with public keys and public operations for encryption along with secret keys and secret operations for decryption — all based on non-classical arithmetics. The existence of such systems is assumed as well as the existence of cryptosystems with public operations, but without keys at all.

The claimed novelty refers to the reuse of known algorithms by providing them with non-classical arithmetics.

2. Cryptosystem with public keys and public operations

Since our system will include arithmetics, we need to define some class of them.

Definition 2.1. Let we have a set A of all words $a = a_0a_1 \dots a_{l_1}$ of length l_1, a set B of all words $b = b_0b_1 \dots b_{l_2}$ of length l_2, and an arbitrary subset C of words $c = c_0c_1 \dots c_{l_3}$ of the set C' of all words $c'_0c'_1 \dots c'_{l_3}$ of length l_3 — all of them in the alphabet $\mathscr{A}$, — then set $A \times B \times C$ is a *substitution table*, words a are rows, b are columns, c are cell values ab. ◁

Definition 2.2. A *substitution arithmetic* is a tuple

$$\mathfrak{A} = (X, Y, B, F_{\mathfrak{A}}) \tag{2.1}$$

composed by the arithmetic domain X, the arithmetic codomain Y, the set B of substitution tables of Definition 2.1, and the set of functions

$$F_{\mathfrak{A}} = \{f_i \mid f_i : S_i \times X \to Y\}, \quad i = 1, \dots, N \in \mathbb{N},$$

$S_i = \{(s^i_1, \dots, s^i_{q(i)}) \mid s^i_j \in A \subseteq B\}$, $q(i) = 1, \dots, Q \in \mathbb{N}$, $1 \le j \le q(i)$, each f_i takes an individual number $q(i)$ of tables and an element from X. ◁

The *substitution* in the definition indicates the substitution of the tables of operations in the function f_i. The introduction of $A \subseteq B$ into the definition of the set S_i is dictated by the selection in B of a subset of tables for inverse operations. This is a convenient element of the definition for the practice of arithmetic in general, but specifically in the text below this element is not important.

As an illustration of the arithmetic above, the reader can imagine the algorithms for ordinary addition and multiplication performed on other addition and multiplication tables. Another example is in [1].

Using the template set out in [2], sections II-IV[1], we define a cryptosystem with encryption performed by public operations and keys, and decryption performed by private operations and private keys.

Definition 2.3. A *cryptosystem with public keys and public operations* is a tuple

$$\mathfrak{S} = (\mathcal{U}, \mathcal{M}, \mathcal{C}, \mathcal{K}, \mathfrak{V}, \mathfrak{W}, \mathcal{E}, \mathcal{D}, \mathcal{F}),$$

where:

$\mathcal{U} = \{U_i \mid i \in I\}$ is the set of users;

$\mathcal{M} \subset \mathbb{Z}$ is the set of plaintexts represented as integers;

$\mathcal{C} \subset \mathbb{Z}$ is the set of ciphertexts;

$\mathcal{K} = \{e_i, d_i \mid i \in I\} \subset \mathbb{Z}$ is the set of public (e_i) and private (d_i) keys;

$\mathfrak{V}$ is public substitution arithmetic 2.1 with operations $F_{\mathfrak{V}}$; tables of operations of specific users are stored in their personal public files;

[1] The authors proposed encryption/decryption methods for the previously known scheme.

$\mathfrak{W}$ is (if possible) public substitution arithmetic 2.1 with operations $F_{\mathfrak{W}}$; (if possible) everyone knows the algorithms of the operations, but the operation tables of specific users are secret;

$\mathcal{E} = \{E_i \mid E_i : \mathcal{M} \to \mathcal{C}, i \in I\}$ is a set of encryption functions equipped with arithmetic $\mathfrak{V}$, each E_i produces a $C \in \mathcal{C}$ from $M \in \mathcal{M}$ using an individual key e_i and operations $F_{\mathfrak{V}}$ (see note 2.4); E_i function algorithm is public;

$\mathcal{D} = \{D_i \mid D_i : \mathcal{C} \to \mathcal{M}, i \in I\}$ is a set of decryption functions equipped with arithmetic $\mathfrak{W}$, each D_i produces $M \in \mathcal{M}$ from $C \in \mathcal{C}$ using individual key d_i and operations $F_{\mathfrak{W}}$ (see note 2.4); the algorithm of the D_i function (if possible) is publicly available;

$\mathcal{F} = \big\{F_i \mid F_i = \big\{e_i, B_i, E_i\big\}, i \in I\big\}$ is the set of public files of users U_i, where $B_i \subset B_{\mathfrak{V}}$ are tables of public operations (the actual definitions of $\mathfrak{V}$ and (perhaps) $\mathfrak{W}$ are stored somewhere in another public place).

Associated with each user U_i are individual keys, tables of public operations, tables of private operations, encryption functions, decryption functions and a public file, respectively —

$$U_i \Longrightarrow \big(e_i, d_i, B_i^{\mathfrak{V}}, B_i^{\mathfrak{W}}, E_i, D_i, F_i\big).$$

Taking into account $M, M' \in \mathcal{M}$, $C, S, T \in \mathcal{C}$, $i, j, k \in I$ a number of conditions are fulfilled in $\mathfrak{S}$:

(1) Condition

$$\forall M \forall i \big(M = D_i[E_i(M)] \wedge M = E_i[D_i(M)]\big)$$

is true for any messages and encryption/decryption functions.

(2) Both E_i and D_i are easy to calculate.

(3) Neither the discovery of the key e_i nor the discovery of the tables $B_i^{\mathfrak{V}}$ of operations provide a practical way to decrypt M.

(4) Sender U_j encrypts message M to recipient U_i with key e_i and function E_i of recipient U_i —

$$C = E_i(M).$$

(5) The receiver U_i decrypts C with his private key and function D_i, and he is the only one who can decrypt —

$$(\forall M, C, i)(\exists! k)(C = E_i(M) \wedge M = D_k(C) \Rightarrow k = i\big).$$

(6) The signature S of the sender U_j of the message M for the recipient U_i is performed by its own function D_j and the signature is non-repudiable (no one but U_j can calculate S) —

$$(\forall M, S, j)(\exists! k)\big(S = D_j(M) \wedge S = D_k(M) \Rightarrow j = k\big).$$

(7) The sender U_j encrypts his S with the function E_i of the receiver U_i —

$$T = E_i(S).$$

(8) The receiver U_i extracts S from T with its function D_i —

$$S = D_i(T).$$

(9) Finally, the receiver U_i extracts M from S by the E_j function of the sender U_j —

$$M = E_j(S).$$

(10) The recipient U_i cannot violate the integrity of the message M sent to him, i.e. cannot change it to M', since his signature will not be equal to the signature of the sender U_j —
$$(\forall M', M, i, j)(i \neq j \wedge M' \neq M \Rightarrow D_i(M') \neq D_j(M')).$$

The cryptosystem $\mathfrak{S}$ with an empty set of keys is called a *public operations cryptosystem*; if $\mathfrak{S}$ has no secret operations, then $\mathfrak{S}$ is a *public-key cryptosystem with non-classical arithmetics.* ◁

Remark 2.4. Like [2], p. 2, we say that any two $E_i, E_k \in \mathcal{E}$ are *usually* combined by one procedure E, i.e. $E_i(M_j) = E(e_i, B_i^{\mathfrak{V}}, M_j)$ — for the user, U_i and $E_k(M_j) = E(e_k, B_k^{\mathfrak{V}}, M_j)$ — for the user U_k, with fixed i, k and $j = 1, 2, \ldots, |\mathcal{M}|$. The same is true for any $D_i, D_k \in \mathcal{D}$ and D. However, our definition of system $\mathfrak{S}$ leaves room for the functions E_i, E_k (D_i, D_k) to differ in procedures. ◁

Now let's implement the definition above in RSA. Let E_x, D_x be the procedures for encrypting and decrypting user x, respectively, and, for definiteness, $\underset{x}{*}, +_x$ are the public operations of user x, $\otimes_x, \oplus_x$ are his private operations[2]. The corresponding user designations for Alice and Bob are A, B.

$$C \equiv E_A(M) \equiv M^{e_A} \pmod n \quad \Longrightarrow \quad \overbrace{M \underset{A}{*} \cdots \underset{A}{*} M}^{e_A} = c \underset{A}{*} n +_A C$$

is the procedure for Bob to encrypt message M to Alice with Alice's public key and operations. To the right of the symbol $\Longrightarrow$ there is an expanded record of the remainder C from dividing M^{e_A} by n, expressed in terms of multiplication and addition — an explanation equally applicable to the procedures below and omitted there.

$$M \equiv D_A(C) \equiv C^{d_A} \pmod n \quad \Longrightarrow \quad \overbrace{C \otimes_A \cdots \otimes_A C}^{d_A} = m \otimes_A n \oplus_A M$$

is the procedure for Alice to decrypt the ciphertext C with her secret key and operations.

$$S \equiv D_B(M) \equiv M^{d_B} \pmod n \quad \Longrightarrow \quad \overbrace{M \otimes_B \cdots \otimes_B M}^{d_B} = s \otimes_B n \oplus_B S$$

is the procedure for Bob to sign the message M for Alice using his private key and operations.

$$T \equiv E_A(S) \equiv S^{e_A} \pmod n \quad \Longrightarrow \quad \overbrace{S \underset{A}{*} \cdots \underset{A}{*} S}^{e_A} = t \underset{A}{*} n +_A T$$

is the procedure for Bob to encrypt the signed message S with Alice's public key and operations.

$$S \equiv D_A(T) \equiv T^{d_A} \pmod n \quad \Longrightarrow \quad \overbrace{T \otimes_A \cdots \otimes_A T}^{d_A} = s' \otimes_A n \oplus_A S$$

is procedure for decrypting S by Alice with her secret key and operations.

$$M \equiv E_B(S) \equiv S^{e_B} \pmod n \quad \Longrightarrow \quad \overbrace{S \underset{B}{*} \cdots \underset{B}{*} S}^{e_B} = m \underset{B}{*} n +_B M$$

[2] No connection to the established use of these symbols is implied here–only the convenient association of multiplication and addition with the secrecy indicated by the circle.

is the procedure for Alice to retrieve the original M using the public key and Bob's operations.

3. Conclusion

The cryptosystem defined above has many conditions. Usually, an increase in the restrictions on the desired object entails a complication of the search. We don't know if systems with open operations exist at all. The next reasonable question is the performance of the cryptosystem. At the moment, the author can only refer to a huge number of arithmetics, among which, perhaps, there is more than one that satisfies an acceptable calculation speed. To date, the only motivation for further research is the lack of refutation of the potential benefits.

In our note, we took one well-known scheme and proposed to supply it with non-classical arithmetics. The researcher can repeat our trick for other cryptosystems.

References

[1] Жванько А. Н. 2022. Арифметика DR+. PREPRINTS.RU. https://doi.org/10.24108/preprints-3112222

[2] R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb. 1978), 120–126. https://doi.org/10.1145/359340.359342 (Дата обращения: 23 ноября 2022 г.)

Email address: a.n.zhvanko@gmail.com