УДК 004.056.55, 004.056.2; MSC2020 68P25, 94A60

КРИПТОСИСТЕМА С ОТКРЫТЫМИ ОПЕРАЦИЯМИ И КЛЮЧАМИ

АЛЕКСАНДР Н. ЖВАНЬКО

Аннотация. На основе шаблона, в котором реализован алгоритм RSA, мы определили криптосистему с открытыми ключами и открытыми операциями, дополняющую классическую схему свойством, при котором шифрование производится открытыми ключами и операциями, а расшифровывание — закрытыми ключами и операциями. Исключив из нашей схемы использование открытых ключей, мы получим криптосистему с открытыми операциями.

1. Введение

В работе [1] было предложено использование неклассических арифметик и функций/уравнений разнообразия, было сказано (еще в версии 3 препринта от 25.02.2022), что теоретическим примером их использования может быть алгоритм шифрования RSA. В самом деле, если разложение числа относительно классического умножения дает одни простые множители, то относительно другого умножения это же число может быть разложено на другие простые множители. Поскольку умножений очень много, то и факторизаций имеется большое множество. Скрыв от взломщика умножение, мы усложняем ему задачу взлома.

Использование неклассических арифметик в целом в криптографии может быть полезным в ситуации, когда замена обычных операций на неклассические в известных алгоритмах повышает криптостойкость или производительность; когда же указанные показатели равны, то смена арифметики A на арифметику B может сделать бесполезной усилия атакующего, изобретшего взлом против алгоритма с арифметикой A. Впрочем, это ничем не подкрепленные рассуждения неспециалиста, не работавшего над реализацией идеи и не предлагающего ничего на момент написания, кроме определения криптосистемы.

2. Криптосистема с открытыми ключами и открытыми операциями

Поскольку наша система будет включать арифметики, нам нужно определить их некоторый класс.

Определение 2.1. Пусть имеем множество A всех слов $a = a_0a_1 \dots a_{l_1}$ длины l_1, множество B всех слов $b = b_0b_1 \dots b_{l_2}$ длины l_2 и произвольное подмножество C слов $c = c_0c_1 \dots c_{l_3}$ множества C' всех слов $c'_0c'_1 \dots c'_{l_3}$ длины l_3 — все они в алфавите $\mathscr{A}$, — тогда множество $A \times B \times C$ есть *таблица подстановок*, слова a — строки, b — столбцы, c — значения ячеек ab. ◁

Date: 5 декабря 2022 года.

Key words and phrases. public-key-operation cryptosystem, public-operation cryptosystem, RSA, криптосистема с открытыми ключами и операциями, криптосистема с открытыми операциями.

Определение 2.2. *Подстановочная арифметика* — это кортеж

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

из X — области определения арифметики, Y — области значений арифметики B — множества таблиц подстановок определения 2.1 и множества функций

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

$S_i = \{(s^i_1, \ldots, s^i_{q(i)}) \mid s^i_j \in A \subseteq B\}$, $q(i) = 1, \ldots, Q \in \mathbb{N}$, $1 \leq j \leq q(i)$, каждая из которых принимает индивидуальное число $q(i)$ таблиц и элемент из X. ◁

Подстановочная в определении сообщает о подстановке таблиц операций в функцию f_i. Введение $A \subseteq B$ в определение множества S_i продиктовано выделением в B подмножества таблиц для обратных операций. Это удобный элемент определения для практики работы с арифметиками в целом, но конкретно в тексте ниже этот элемент не важен.

По шаблону, изложенному [2], разделы II–IV[1], определим криптосистему с шифрованием, производимым открытыми операциями и ключами, и расшифровыванием, выполняемым закрытыми операциями и закрытыми ключами.

Определение 2.3. *Криптосистемой с открытыми ключами и открытыми операциями* (public-key-operation cryptography) является кортеж

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

где:

$\mathcal{U} = \{U_i \mid i \in I\}$ — множество пользователей;

$\mathcal{M} \subset \mathbb{Z}_+$ — множество открытых текстов, представленных как целые числа;

$\mathcal{C} \subset \mathbb{Z}_+$ — множество зашифрованных текстов;

$\mathcal{K} = \{e_i, d_i \mid i \in I\} \subset \mathbb{Z}_+$ — множество открытых (e_i) и закрытых (d_i) ключей;

$\mathfrak{V}$ — общедоступная подстановочная арифметика 2.1 с операциями $F_{\mathfrak{V}}$; таблицы операций конкретных пользователей хранятся в их личных публичных файлах;

$\mathfrak{W}$ — (возможно) общедоступная подстановочная арифметика 2.1 с операциями $F_{\mathfrak{W}}$; (возможно) все знают алгоритмы операций, но таблицы операций конкретных пользователей секретны;

$\mathcal{E} = \{E_i \mid E_i : \mathcal{M} \to \mathcal{C}, i \in I\}$ — множество шифрующих функций, снабженных арифметикой $\mathfrak{V}$, каждая из которых производит $C \in \mathcal{C}$ из $M \in \mathcal{M}$ с помощью индивидуальных ключа e_i и операций $F_{\mathfrak{V}}$ (см. примечание 2.4); алгоритм функции E_i общедоступен;

$\mathcal{D} = \{D_i \mid D_i : \mathcal{C} \to \mathcal{M}, i \in I\}$ — множество расшифровывающих функций, снабженных арифметикой $\mathfrak{W}$, каждая из которых производит $M \in \mathcal{M}$ из $C \in \mathcal{C}$ с помощью индивидуальных ключа d_i и операций $F_{\mathfrak{W}}$ (см. примечание 2.4); алгоритм функции D_i (возможно) общедоступен;

$\mathcal{F} = \{F_i \mid F_i = \{e_i, B_i, E_i\}, i \in I\}$, с таблицами $B_i \subset B_{\mathfrak{V}}$ открытых операций, — множество публичных файлов пользователей U_i (собственно определения $\mathfrak{V}$ и (возможно) $\mathfrak{W}$ хранятся где-то в другом публично доступном месте).

---

[1] Авторы предложили методы шифрования для известной до них схемы.

С каждым пользователем U_i связаны индивидуальные ключи, таблицы открытых операций, таблицы закрытых операций, шифрующие функции, расшифровывающие функции и публичный файл соответственно —

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

С учетом $M, M' \in \mathcal{M}$, $C, S, T \in \mathcal{C}$, $i, j, k \in I$ в $\mathfrak{S}$ выполняется ряд условий:

(1) Для любых сообщений и функций шифрования/расшифровывания верно

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

(2) И E_i, и D_i легко вычисляются.

(3) Ни открытие ключа e_i, ни открытие таблиц операций $B_i^{\mathfrak{V}}$ не дают практически пригодного способа расшифровать M.

(4) Отправитель U_j шифрует сообщение M получателю U_i ключом e_i и функцией E_i получателя U_i —

$$C = E_i(M).$$

(5) Получатель U_i расшифровывает C своими приватными ключом и функциями D_i, и он единственный, кто может расшифровать —

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

(6) Подпись S отправителя U_j сообщения M для получателя U_i осуществляется собственной функцией D_j и подпись не отказуема (никто кроме U_j не может вычислить S) —

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

(7) Отправитель U_j шифрует свое S функцией E_i получателя U_i —

$$T = E_i(S).$$

(8) Получатель U_i извлекает S из T своей функцией D_i —

$$S = D_i(T).$$

(9) Наконец, получатель U_i извлекает M из S функцией E_j отправителя U_j —

$$M = E_j(S).$$

(10) Получатель U_i не может нарушить целостность посланного ему сообщения M, т. е. не может изменить его на M', поскольку его подпись не будет равна подписи отправителя U_j —

$$(\forall M', M, i, j)(i \neq j \wedge M' \neq M \Rightarrow D_i(M') \neq D_j(M')).$$

Криптосистема выше с пустым множеством ключей называется *криптосистемой с открытыми операциями.* ◁

Примечание 2.4. Как и [2], с. 2, мы говорим, что любые два $E_i, E_k \in \mathcal{E}$ *обычно*, объединены одной процедурой E, т. е. $E_i(M_j) = E(e_i, B_i^{\mathfrak{V}}, M_j)$ — для пользователя, U_i и $E_k(M_j) = E(e_k, B_k^{\mathfrak{V}}, M_j)$ — для пользователя U_k, при фиксированных i, k и $j = 1, 2, \ldots, \mathcal{M}$. Аналогично для любых $D_i, D_k \in \mathcal{D}$ и D. Тем не менее, наше определение системы $\mathfrak{S}$ оставляет место различаться процедурами функциям E_i, E_k (D_i, D_k). ◁

Теперь воплотим определение выше в RSA. Пусть E_x, D_x — процедуры шифрования и расшифровки пользователя x соответственно, и, для определенности, $\underset{x}{*}, +_x$ — открытые операции пользователя x, $\otimes_x, \oplus_x$ — его закрытые операции[2]. Соответственные обозначения пользователей Алисы и Боба: A, B.

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

— процедура шифрования Бобом сообщения M Алисе открытыми ключом и операциями Алисы. Справа от $\Longrightarrow$ находится развернутая запись остатка C от деления M^{e_A} на n, выраженная через умножение и сложение — пояснение, аналогично применимое к процедурам ниже и опускаемое там.

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

— процедура расшифровывания Алисой зашифрованного текста C своими секретными ключом и операциями.

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

— процедура подписи Бобом сообщения M для Алисы посредством своих секретных ключа и операций.

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

— процедура шифровки Бобом подписанного сообщения S открытыми ключом и операциями Алисы.

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

— процедура расшифровки S Алисой ее секретными ключом и операциями.

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

— процедура извлечения Алисой исходного M посредством открытых ключа и операций Боба.

(Осуществимость реализации RSA с простотой чисел относительно секретного умножения могла бы повысить криптостойкость алгоритма при прочих условиях, поскольку лишает взломщика знания критериев факторизуемости.)

3. Заключение

Определенная выше криптосистема имеет много условий. Обычно увеличение ограничений на искомый объект влечет за собой усложнение отыскания. С другой стороны, RSA нам дает готовый рецепт. Следующий резонный вопрос — производительность криптосистемы. На данный момент автор может только сослаться на громадное число арифметик, среди которых, быть может, найдется неединственная, удовлетворяющая приемлемой скорости вычислений.

[2]Никакой связи с установившимся использованием этих символов здесь не предполагается — только удобная ассоциация умножения и сложения с обозначенной взятием в кружок закрытостью.

В нашей заметке мы взяли одну известную схему и предложили ее снабжать неклассическими арифметиками. Исследователь может повторить наш прием для других криптосистем.

Список литературы

[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