ПОВЫШЕНИЕ ПОМЕХОУСТОЙЧИВОСТИ МНОГОКАНАЛЬНЫХ RSA-СИСТЕМ

Черненко Ю.В.

Краснодарское высшее военное училище
Россия, 350035, Краснодар, Красина ул., 4
E-mail: *ofinko@yandex.ru*

Рассмотрена помехоустойчивая многоканальная ассиметричная криптосистема на базе одноканальной системы RSA. Для получения нового свойства помехоустойчивости использованы свойства избыточного модулярного кода, основанного на Китайской теореме об остатках.

Систему передачи конфиденциальной информации можно представить в следующем виде (рис. 1).

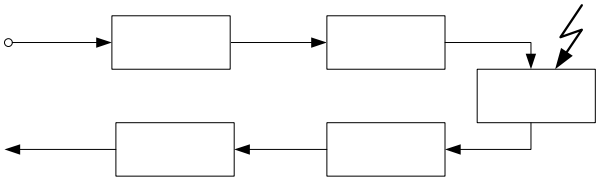

Рис. 1. Одноканальная система передачи конфиденциальной информации

Представленная система предполагает возможность искажения криптограммы C передаваемой от источника к получателю сообщения. В результате шифратор получателя сообщения обрабатывает искаженную криптограмму C^*. Следовательно, существует вероятность получения ложного сообщения M^*, отличного от переданного M. Получатель сообщения при этом может принять M^* за истинное или ложное. В случае определения M^* как ложного он может составить запрос на повтор переданного сообщения (при использовании решающей обратной связи), что снижает оперативность обмена информацией между источником и получателем.

При использовании алгоритма RSA правила зашифрования и расшифрования описываются выражениями:

$$C = M^e \pmod{m}, \quad (1)$$

$$M = C^d \pmod{m}. \quad (2)$$

Рассмотрим ситуацию, когда в роли источника и получателя сообщений выступают пользователи, объединенные в локальные сети ***A*** и ***B***. В этом случае можно говорить о многоканальной системе передачи конфиденциальной информации. Устройство, которое назовем сервером связи, будет формировать n виртуальных каналов для передачи криптограмм $C_1, C_2, \ldots, C_n$, формируемых пользователями одной из сетей (рис. 2). Повышение помехоустойчивости в многоканальной системе на базе алгоритма RSA возможно за счет применения методов избыточного кодирования.

Рассмотрим многоканальную систему на базе алгоритма RSA с одним избыточным каналом и возможностью обнаружения однократных ошибок (рис. 3).

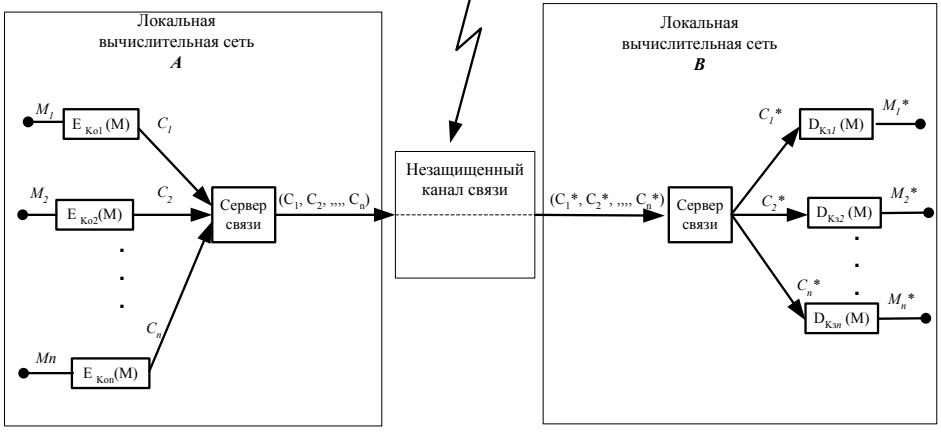

Рис. 2. Многоканальная система передачи конфиденциальной информации

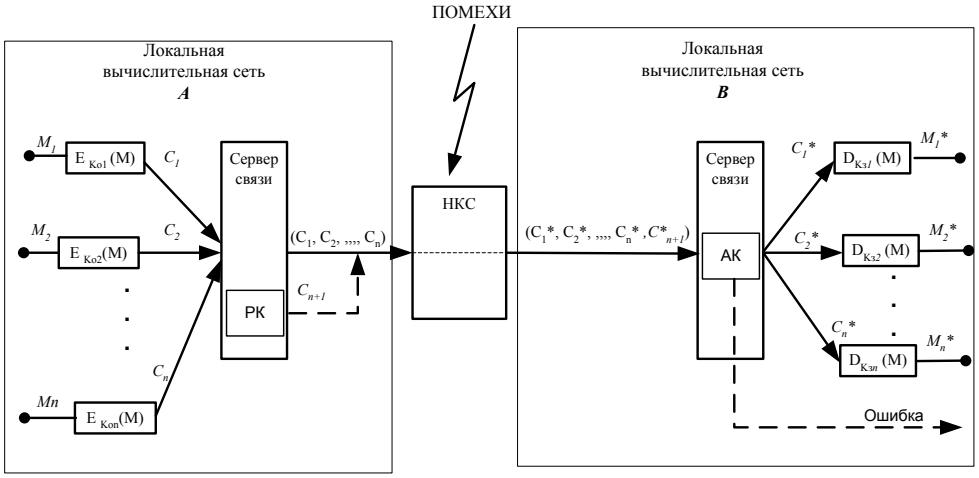

Рис. 3. Многоканальная криптосистема на базе алгоритма RSA с одним избыточным каналом и возможностью обнаружения однократных ошибок (РК — расширитель кода, АК — анализатор кода)

Правила зашифрования и расшифрования (1) и (2) для случая многоканальной системы примут следующий вид:

$$\begin{cases} C_1 = M_1^{e_1} \pmod{m_1}, \\ C_2 = M_2^{e_2} \pmod{m_2}, \\ \ldots, \\ C_n = M_n^{e_n} \pmod{m_n}. \end{cases} \tag{3}$$

$$\begin{cases} M_1 = C_1^{d_1} \pmod{m_1}, \\ M_2 = C_2^{d_2} \pmod{m_2}, \\ \ldots, \\ M_n = C_n^{d_n} \pmod{m_n}. \end{cases} \tag{4}$$

где $M_1, M_2, \ldots, M_n$ — открытые тексты; $C_1, C_2, \ldots, C_n$ — криптограммы; $m_1, m_2, \ldots, m_n$ — модули шифрования; $e_1, e_2, \ldots, e_n$ — открытые ключи зашифрования криптосистемы на базе алгоритма RSA; $d_1, d_2, \ldots, d_n$ — закрытый ключ расшифрования криптосистемы на базе алгоритма RSA.

При передаче криптограмм $C_1, C_2, \ldots, C_n$ по незащищенному каналу связи, также как и в одноканальной криптосистеме могут произойти искажения и принимающий корреспондент (в рассматриваемом случае — корреспонденты) локальной вычислительной сети ***B*** получат криптограммы $C_1^*, C_2^*, \ldots, C_n^*$. Таким образом, процедура расшифрования (2) примет вид:

$$\begin{cases} M_1^* = C_1^{*d_1} \pmod{m_1}, \\ M_2^* = C_2^{*d_2} \pmod{m_2}, \\ \ldots, \\ M_n^* = C_n^{*d_n} \pmod{m_n}, \end{cases} \tag{5}$$

где $M_1^*, M_2^*, \ldots, M_n^*$ — открытые тексты, которые могут содержать ошибки в результате расшифрования искаженных криптограмм.

Введем новые условия к выбору модулей шифрования: $\gcd(m_i, m_j) = 1$, где $\gcd(a, b)$ — наибольший общий делитель a и b $(i, j = 1, 2, \ldots, n)$. Тогда системе уравнений (3) в соответствии с Китайской теоремой об остатках можно сопоставить единственное решение:

$C = \mathrm{CRT}_{i=1}^{n} C_i \pmod{m_i}$, где CRT — групповой оператор решения системы уравнений по Китайской теореме об остатках (Chinese remainder theorem) [1, 3].

Если рассматривать криптограммы $C_1, C_2, \ldots, C_n$ как элементы кода, передаваемого от одного корреспондента сети другому в n-канальной криптосистеме, то добавление избыточной криптограммы C_{n+1} можно назвать расширением кода, а устройство выполняющее этот процесс — расширителем кода. На приемном конце должно осуществляться сравнение и выработка сигнала «ОШИБКА» анализатором кода, обеспечивающим преобразование кода в соответствии с Китайской теоремой об остатках и сравнение полученного результата с пороговым значением, равным произведению модулей $m_1, m_2, \ldots, m_n$. Учитывая, рассмотренное выше многоканальная криптосистема представленная на рисунке 2 примет следующий вид, представленный на рис. 3.

Для получения расширенной системы криптограмм дополним систему модулей $m_1, m_2, \ldots, m_n$ еще одним модулем: m_{n+1} таким, что $\gcd(m_i, m_j) = 1$, где $i, j = 1, 2, \ldots, n+1$. Потребуем, чтобы выполнялось условие: $m_1, m_2, \ldots, m_n < m_{n+1}$. Тогда можем получить *расширенную* систему криптограмм:

$C_1, C_2, \ldots, C_n, C_{n+1}$, где $C_n = C \pmod{m_n}$, $C_{n+1} = C \pmod{m_{n+1}}$.

В соответствии с положениями модулярной арифметики расширенная система криптограмм представляет расширенный модулярный R-код, обладающий свойствами обнаружения и исправления ошибок [1, 2, 5–7]. Представленная на рис. 3 n-канальная криптосистема позволяет обнаруживать однократные ошибки.

Таким образом, систему уравнений (5) расшифрования перепишем в виде следующей расширенной системы:

$$\begin{cases} M_1^* = C_1^{*d_1} \pmod{m_1}, \\ M_2^* = C_2^{*d_2} \pmod{m_2}, \\ \ldots, \\ M_n^* = C_n^{*d_n} \pmod{m_n}, \\ M_{n+1}^* = C_{n+1}^{*d_{n+1}} \pmod{m_{n+1}}. \end{cases} \qquad (6)$$

Простейшим признаком обнаруживаемой ошибки является выполнение неравенства [1, 2]:

$C^* \geq \prod_{i=1}^{n} m_i$, где $C^* = \mathrm{CRT}_{i=1}^{n} C_i^* \pmod{m_i}$.

Применение данного метода повышения помехоустойчивости многоканальных криптосистем на базе алгоритма RSA, позволяет обеспечить возможность обнаружения искажений в передаваемых криптограммах при любой величине ошибки (в масштабе одной криптограммы), то есть и в случае стирания криптограмм или обрыве линии, если количество искаженных криптограмм не превышает обнаруживающих возможностей *R*-кода. В дальнейших исследованиях предполагается рассмотреть вопросы: 1) обеспечения помехоустойчивой передачи ключей; 2) возможности исправления ошибок при передаче криптограмм; 3) обеспечения имитостойкости многоканальных криптосистем на базе алгоритма RSA.

Литература

1. Амербаев В.М. Теоретические основы машинной арифметики. — Алма-Ата: Наука, 1976.

2. Бояринов И.М. Помехоустойчивое кодирование числовой информации. — М.: Наука, 1983.

3. Финько О.А. Восстановление числа в системе остаточных классов с минимальным количеством оснований // Электронное моделирование. — 1998. — Т. 20, № 3. — С. 56–61.

4. Финько О.А. Групповой контроль ассиметричных криптосистем методами модулярной арифметики // XIV Междунар. школа-семинар «Синтез и сложность управляющих систем». Н. Новгород, 27 окт. — 2 нояб. 2003. Сб. тр. / Под ред. акад. РАН О.Б. Лупанова. — Н. Новгород: Изд-во Нижегород. пед. ун-та, 2003. — С. 85–86.

5. Mandelbaum D.M. Error correction in residue arithmetic // IEEE Trans. Comput. — 1972. — Vol. 21, № 6. — P. 538–545.

6. Mandelbaum D.M. On a class of arithmetic codes and decoding algorithm // IEEE Trans. On Information Theory. — 1976. — № 21. — P. 85–88.

7. Mandelbaum D.M. Further results on decoding arithmetic residue codes // IEEE Trans. On Information Theory. — 1978. — № 24. — P. 643–644.

MULTICHANNEL RSA-SYSTEMS BOOSTING OF NOISE STABILITY

Chernenko J.

Krasnodar higher military school
Russia, 350035, Krasnodar, street Krasina, 4
E-mail: ofinko@yandex.ru

The noise-resistant multichannel dissymetric cryptosystem is considered on the basis of one-channel system RSA. For deriving new property of noise stability properties of the surplus modular code based on the Chinese remainder theorem are used.

At usage of algorithm RSA of a code rule and decoding action are described by expressions:

$$C = M^e \pmod{m};\ M = C^d \pmod{m}. \quad (1)$$

Code rules and decoding actions (1) for a case of a multichannel system will receive the following aspect:

$$\begin{cases} C_1 = M_1^{e_1} \pmod{m_1}, \\ C_2 = M_2^{e_2} \pmod{m_2}, \\ \ldots, \\ C_n = M_n^{e_n} \pmod{m_n}. \end{cases}, \quad \begin{cases} M_1 = C_1^{d_1} \pmod{m_1}, \\ M_2 = C_2^{d_2} \pmod{m_2}, \\ \ldots, \\ M_n = C_n^{d_n} \pmod{m_n}. \end{cases}$$

Where $M_1, M_2, \ldots, M_n$ —- clear texts; $C_1, C_2, \ldots, C_n$ — cryptograms; $m_1, m_2, \ldots, m_n$ — modules of a ciphering; $e_1, e_2, \ldots, e_n$ — open keys of encoding; $d_1, d_2, \ldots, d_n$ — the closed key of decoding action.

Let's enter new conditions to choice of modules of a ciphering: $\gcd(m_i, m_j) = 1$. Then according to the Chinese remainder theorem it is possible to receive the unique decision: $C = \mathop{\mathrm{CRT}}_{i=1}^{n} C_i \pmod{\mathrm{m_i}}$, where CRT — a group operator of the decision of a set of equations under the Chinese remainder theorem. If to consider cryptograms $C_1, C_2, \ldots, C_n$ as the code units, transmitted from one correspondent of a network to another in *a n-channel* cryptosystem adding of an excessive cryptogram C_{n+1} can be named code extension.

For deriving the extended system of cryptograms we shall add a system of modules $m_1, m_2, \ldots, m_n$ one more module: m_{n+1} such, that $\gcd(m_i, m_j) = 1$, where $i,\ j = 1, 2, \ldots, n+1$. We shall demand, that the condition satisfied: $m_1, m_2, \ldots, m_n < m_{n+1}$. Then we can receive *the extended* (excessive) system of cryptograms:

$C_1, C_2, \ldots, C_n, C_{n+1}$, where $C_n = C \pmod{m_n},\ C_{n+1} = C \pmod{m_{n+1}}$.

According to positions of modular arithmetics the extended system of cryptograms represents the extended modular R-code possessing properties of detection and an error-checking. The elementary indication of a discovered error is realization of an inequality:

$$C^* \geq \prod_{i=1}^{n} m_i, \text{ where } C^* = \mathop{\mathrm{CRT}}_{i=1}^{n} C_i^* \pmod{m_i}.$$

Application of the given method of boosting of noise stability allows to provide a possibility of detection of distortions in transmitted cryptograms at any error figure (in plotting scale of one cryptogram).