УДК 511+519.719.2

О.А. Финько

Многоканальные модулярные системы, устойчивые к искажениям криптограмм

(*Краснодарское высшее военное училище (военный институт)*)

Предложен принцип построения многоканальных систем защиты информации, устойчивых к искажениям криптограмм. Криптограммы, передаваемые по каналам шифрования, сопоставлены символам модулярного кода. Вычисляются дополнительные криптограммы, которые соответствуют избыточным символам модулярного кода. Таким образом передаваемая система криптограмм является избыточным модулярным кодом. Это обеспечивает обнаружение и/или исправление ошибок различного происхождения (помехи, имитация злоумышленника). В отличие от известных методов индивидуального (одноканального) контроля в масштабе одной криптограммы обеспечивается коррекция ошибки любой кратности. Указано на возможность построения системы групповой цифровой подписи, обладающей новыми полезными свойствами.

Лавинный характер увеличения объемов передаваемой по каналам связи информации и переход к коллективным методам обработки информации на базе локальных вычислительных сетей обуславли-

вает необходимость перехода к многоканальным методам и средствам криптографической защиты информации. Известно сколь негативны последствия, вызываемые ошибками при передаче криптограмм. Поэтому все большее внимание уделяется изучению криптосистем, устойчивых к ошибкам. Если заранее известно, что система является многоканальной, то в ней могут быть использованы особые (групповые) методы контроля ошибок, позволяющие получить преимущества, недоступные обычным методам индивидуального контроля [4].

Будем рассматривать *n*-канальную систему шифрования (например, RSA), правила зашифрования и расшифрования в которой определены формулами:

$$\begin{cases} C^{(1)} = \mathrm{E}_{k^{(1)}}\left(M^{(1)}\right) \pmod{m^{(1)}}, \\ C^{(2)} = \mathrm{E}_{k^{(2)}}\left(M^{(2)}\right) \pmod{m^{(2)}}, \\ \mathbf{K}, \\ C^{(n)} = \mathrm{E}_{k^{(1)}}\left(M^{(n)}\right) \pmod{m^{(n)}}; \end{cases} \tag{1}$$

$$\begin{cases} M^{(1)} = \mathrm{D}_{k^{(1)}}\left(C^{(1)}\right) \pmod{m^{(1)}}, \\ M^{(2)} = \mathrm{D}_{k^{(2)}}\left(C^{(2)}\right) \pmod{m^{(2)}}, \\ \mathbf{K}, \\ M^{(n)} = \mathrm{D}_{k^{(n)}}\left(C^{(n)}\right) \pmod{m^{(n)}}; \end{cases} \tag{2}$$

где

$M^{(1)}, M^{(2)}, \mathbf{K}, M^{(n)}$ — открытые тексты,

$C^{(1)}, C^{(2)}, \mathbf{K}, C^{(n)}$ — криптограммы,

$k^{(1)}, k^{(2)}, \mathbf{K}, k^{(n)}$ — ключи (системы ключей).

Передача криптограмм $C^{(1)}, C^{(2)}, \mathbf{K}, C^{(n)}$ по каналу связи приведет к появлению в ней искажений, в результате которых процедуре расшифрования подвергнутся криптограммы $C^{*(1)}, C^{*(2)}, \mathbf{K}, C^{*(n)}$. Искажения могут возникнуть в результате как непреднамеренных (помехи, сбои, дефекты), так и преднамеренных воздействий.

Таким образом, процедура расшифрования (2) примет вид:

$$\begin{cases} M^{*(1)} = \mathrm{D}_{k^{(1)}}\left(C^{*(1)}\right) \pmod{m^{(1)}}, \\ M^{*(2)} = \mathrm{D}_{k^{(2)}}\left(C^{*(2)}\right) \pmod{m^{(2)}}, \\ \mathbf{K}, \\ M^{*(n)} = \mathrm{D}_{k^{(n)}}\left(C^{*(n)}\right) \pmod{m^{(n)}}; \end{cases} \tag{3}$$

где $M^{*(1)}, M^{*(2)}, \mathbf{K}, M^{*(n)}$ — открытые тексты, которые могут содержать ошибки в результате расшифрования искаженной криптограммы.

Введем требование: $\gcd(m_i, m_j) = 1$, где $\gcd(a, b)$ — наибольший общий делитель a и b; $i, j = 1, 2, \mathbf{K}, n$. Тогда системе уравнений (3) в соответствии с Китайской теоремой об остатках можно сопоставить единственное решение:

$$C = \underset{i=1}{\overset{n}{\mathrm{CRT}}} C_i \pmod{m^{(i)}},$$

где CRT — групповой оператор решения системы уравнений по Китайской теореме об остатках (Chinese remainder theorem) [1, 3].

Дополним систему модулей $m^{(1)}, m^{(2)}, \mathbf{K}, m^{(n)}$ еще r модулями $m^{(n+1)}, \mathbf{K}, m^{(n+r)}$ такими, что $\gcd(m_i, m_j) = 1$, где $i, j = 1, 2, \mathbf{K}, n+r$. Потребуем также, чтобы выполнялось условие: $m^{(1)}, m^{(2)}, \mathbf{K}, m^{(n)} < m^{(n+1)} < \mathbf{K} < m^{(n+r)}$. Тогда можем получить *расширенную* систему криптограмм:

$$C^{(1)}, C^{(2)}, \mathbf{K}, C^{(n)}, \mathbf{K}, C^{(n+r)},$$

где

$$C^{(n+1)} = C \pmod{m^{(n+1)}}, \mathbf{K}, C^{(n+r)} = C \pmod{m^{(n+r)}}.$$

Таким образом, систему уравнений (3) расшифрования перепишем в виде следующей расширенной системы:

$$\begin{cases} M^{*(1)} = \mathrm{D}_{k^{(1)}}\left(C^{*(1)}\right) \pmod{m^{(1)}}, \\ M^{*(2)} = \mathrm{D}_{k^{(2)}}\left(C^{*(2)}\right) \pmod{m^{(2)}}, \\ \mathbf{K}, \\ M^{*(n)} = \mathrm{D}_{k^{(n)}}\left(C^{*(n)}\right) \pmod{m^{(n)}}, \\ \mathbf{K}, \\ M^{*(n+r)} = \mathrm{D}_{k^{(n+r)}}(C^{*(n+r)}) \pmod{m^{(n+r)}}. \end{cases}$$

В соответствии с положениями модулярной арифметики расширенная система криптограмм представляет расширенный модулярный код (R-код), обладающий свойствами обнаружения и исправления ошибок [1, 2].

Под одиночной ошибкой будем понимать произвольное искажение одной из криптограмм. t - кратная ошибка — произвольное искажение t криптограмм. Известны следующие положения модулярной арифметики [1, 2]:

1) R-код обнаруживает все одиночные ошибки, если $r \geq 1$;

2) R-код исправляет t или менее ошибок, если $2t \leq r$.

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

$$C^* \geq \prod_{i=1}^{n} m^{(i)},$$

где $C^* = \mathrm{CRT}_{i=1}^{n} C_i^* \pmod{m^{(i)}}$.

Исследованиям методов коррекции модулярных кодов посвящено большое количество зарубежной и отечественной литературы, например [1, 2, 5, 6, 7]. Пример структурной схемы n-канальной криптосистемы с одним избыточным каналом и возможностью обнаружения однократных ошибок представлен на рис. 1. В литературе по модулярной арифметике процедура получения избыточных элементов R-кода называется расширением кода. Для обнаружения ошибок на приемной стороне используется устройство, обеспечивающее преобразование кода в соответствии с Китайской теоремой об остатках (CRT) и сравнение полученного результата с по-

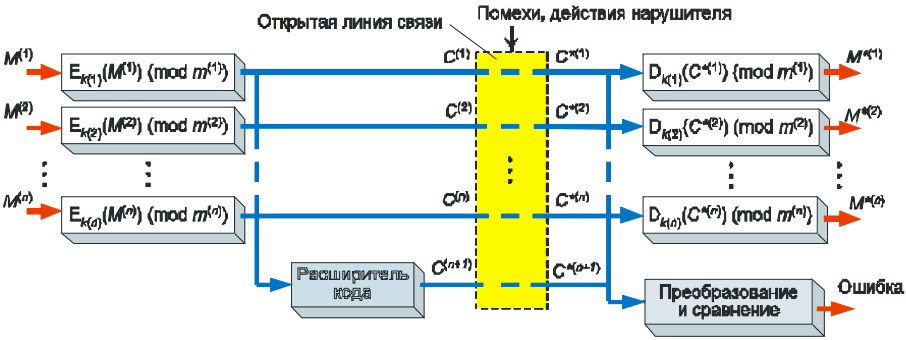

Рис. 1. Структурная схема n-канальной криптосистемы с одним избыточным каналом и возможностью обнаружения однократных ошибок

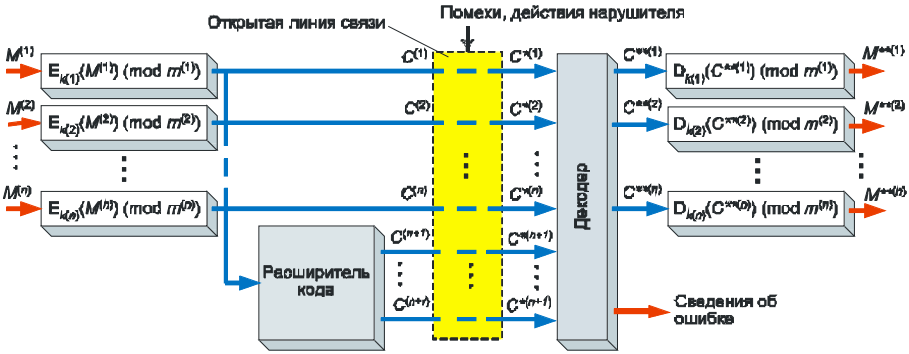

Рис. 2. n-канальная криптосистема с r избыточными каналами и возможностью исправления ошибок

роговым значением, равным произведению рабочих (не избыточных) модулей. Могут быть использованы и другие методы обнаружения ошибок R-кода.

Пример n-канальной криптосистемы с r избыточными каналами и возможностью исправления ошибок представлен на рис. 2. Здесь для исправления ошибок использован декодер, алгоритмы функционирования которого хорошо изучены. Отметим, что после выполнения процедуры исправления ошибок над кодовым словом $C^{*(1)}, C^{*(2)}, \mathbf{K}, C^{*(n+r)}$ мы получим криптограммы: $C^{**(1)}, C^{**(2)}, \mathbf{K}, C^{**(n)}$ и исправленные открытые тексты $M^{**(1)}, M^{**(2)}, \mathbf{K}, M^{**(n)}$. Здесь две звездочки ** указывают на ве-

роятностный характер исправления ошибки. Учитывая большую величину числового диапазона, с которым приходится оперировать, процедуры расширения и декодирования кода будут иметь максимальную эффективность, если они поддержаны аппаратно.

К достоинствам рассмотренного метода контроля ошибок отнесем возможность обнаружения (исправления) искажений в передаваемых криптограммах при *любой* (!) величине ошибки (в масштабе отдельной криптограммы), то есть и в случае стирания криптограмм или обрыве линии, если количество искаженных криптограмм не превышает обнаруживающих (исправляющих) возможностей R-кода.

Для осуществления навязывания ложной информации (имитации криптограммы или цифровой подписи) злоумышленнику придется иметь дело со всей совокупностью информационных криптограмм (для того чтобы получить избыточные криптограммы). При этом для получения гарантированного результата необходимо применить шифрование избыточных криптограмм (избыточных цифровых подписей).

Выбранный вариант помехоустойчивого группового контроля ошибок на основе расширенного модулярного кода основывается на *естественных* свойствах исходных криптосистем (модулярность), что в свою очередь обеспечивает необходимую *совместимость* построенной криптосистемы с другими абонентами, которые не используют рассмотренный метод.

Интересные возможности появляются при использовании данного метода контроля при формировании цифровых подписей для групп документов. В этом случае арбитр сможет восстанавливать любую утраченную (искаженную) цифровую подпись, даже если он хранит только избыточные подписи (избыточные криптограммы), но имеет юридическую возможность доступа к остальным (не утраченным) подписям (например, подписи хранятся у самих пользователей). Для обеспечения этих возможностей необходимо предусмотреть единый центр генерации ключей или обеспечить взаимодействие пользователей.

Устойчивость к криптоанализу обеспечивается правильным выбором точки расширения кода в системе. В данном случае расширению (введению избыточности) подвергаются не открытые тексты, а криптограммы. Решение, основанное на расширении множества

открытых текстов и, как следствие, расширение количества процедур зашифрования привлекательно с позиции открывающихся возможностей контроля ошибок процедур зашифрования-расшифрования. Однако оно не выдерживает атаки, основанной на Китайской теореме об остатках.

Ужесточение требований к модулям может быть компенсировано адекватным расширением множества модулей.

Литература

1. *Амербаев В.М.* Теоретические основы машинной арифметики. — Алма-Ата: Наука, 1976. — 324 с.

2. *Бояринов И.М.* Помехоустойчивое кодирование числовой информации. — М.: Наука, 1983. — 196 с.

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.