ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

РАЗРАБОТКА ПОМЕХОУСТОЙЧИВОГО МЕТОДА РАЗДЕЛЕНИЯ СЕКРЕТА НА ОСНОВЕ ПРИМЕНЕНИЯ ДВУХСТУПЕНЧАТОЙ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Кочеров Ю.Н., Червяков Н.И.

В статье представлен групповой метод разделения секрета, базирующийся на системе остаточных классов. При использовании данного метода увеличивается обнаруживающая способность кода, то есть увеличивается количество обнаруживаемых ошибок.

Ключевые слова: система остаточных классов, обобщенная полиадическая система счисления, разделение секрета.

Введение

Схемы пространственного разделения секрета позволяют делить информацию на n частей и распространять ее среди территориально распределенных n участников, и при восстановлении информации необходимо соединять все части. Схемами разделения секрета, которым для восстановления необходимо k из n частей, называются пороговые схемы разделения секрета.

Изначально такие схемы применялись для хранения секретных ключей и распределенного доступа к стратегическим ресурсам. Такие схемы применяются, если нет доверия одному из участников обмена информации.

В работе проведено исследование метода разделения секрета на группы частей, показано, чем групповое разделение лучше линейного.

При работе схемы пространственного разделения секрета могут подвергается атакам, при которых если злоумышленник является одним из абонентов схемы разделения секрета, то он сможет получить тайную информацию или исказить ее таким образом, что она не сможет быть восстановлена.

Рассмотрим несколько видов таких атак:

- один из участников предоставляет ложную информацию, следовательно, секрет будет восстановлен неверно и определить, кто из участников предоставил неверную часть, невозможно;
- один из участников фальсифицирует запрос на восстановление секрета, когда остальные участники отправляют данные, он восстанавливает секрет;
- один из участников является злоумышленником, он предоставляет свою часть секрета, только узнав все остальные, он может вычислить и отправить свою долю информации, так что секрет восстановится верно и определить, кто «злоумышленник», невозможно.

Отсутствие возможности предупреждения участников разделения секрета о некорректном восстановлении информации может привести к достижению злоумышленником поставленных целей:

- легальные участники восстановили неверный секрет;
- злоумышленник получил правильный секрет.

Из рассмотренных видов атак следует, что для повышения достоверности восстановления информации следует использовать алгоритмы разделения информации с возможностью контроля ошибок. К таким алгоритмам можно отнести алгоритм разделения информации в обычных вычислениях, основанных на системе остаточных классов (СОК), которая глубоко изучена в теории чисел [7] и активно применяется в цифровой обработке сигналов, обработке изображений, кодах с обнаружением и коррекцией ошибок и криптографических системах [1-3].

Обзор методов преобразования СОК-ПСС

Для кодов, от которых требуется, чтобы они обладали возможностью обнаружения и коррекции ошибок, необходимо наличие двух групп чисел: информационных и контрольных. В информационную группу входят числа, составляющие значение закодированной величины, а в контрольную дополнительные числа, вводимые для обнаружения и исправления ошибок при передаче.

Система счисления в остаточных классах открывает возможность использования единого помехоустойчивого кода для борьбы с ошибками, возникающими при передаче информации по ка-

налам связи и при ее обработке в цифровых системах обработки данных.

Различают избыточную и неизбыточную СОК: последняя должна удовлетворять условию $\prod_{i=1}^{n-1} p_i < A \le \prod_{i=1}^{n} p_i$ где n – число оснований СОК; A – число, представляемое в СОК. Для получения избыточной СОК к числу рабочих оснований n добавляют k избыточных оснований $k \ge 1$, тогда $A < \prod_{i=1}^{n+k} p_i$. Используя избыточную СОК, можно обнаружить k ошибок.

Пример 1. Рассмотрим пример избыточной и неизбыточной СОК. Пусть дано число $A = 66$ и система оснований $p_1 = 2$, $p_2 = 5$, $p_3 = 7$, $p_4 = 13$. Так как неизбыточная СОК должна удовлетворять условию $\prod_{i=1}^{n-1} p_i < A \le \prod_{i=1}^{n} p_i$, то основания рабочего диапазона будут $p_1 = 2$, $p_2 = 5$, $p_3 = 7$, а избыточным $p_4 = 13$.

Представим это число в СОК $A = (0,1,3,1)$, для обратного преобразования из системы остаточных классов в позиционную систему счисления СОК → ПСС достаточно иметь три остатка из четырех. Также в данном примере можно обнаружить одну ошибку. Для этого необходимо найти проекции числа A по каждому модулю. Для восстановления числа из СОК в ПСС можно использовать метод, основанный на китайской теореме об остатках, метод Гарнера или метод совместного использования СОК и ОПСС.

Пример 2. Восстановление числа с использованием китайской теоремы об остатках. Восстановление числа из системы остаточных классов в позиционный код при использовании метода, основанного на китайской теореме об остатках [4], необходимо вычислить ортогональные базисы. Для этого рассчитываются величины P_i:

$$P_1 = \frac{P}{p_1} = \frac{910}{2} = 455;\ P_2 = \frac{P}{p_2} = \frac{910}{5} = 182;$$
$$P_3 = \frac{P}{p_3} = \frac{910}{7} = 130;\ P_4 = \frac{P}{p_4} = \frac{910}{13} = 70.$$

Ищем веса базисов:

- из $455 \cdot m_1 = 1 (\mathrm{mod} 2)$ вычисляем $m_1 \equiv 1$;
- из $182 \cdot m_2 = 1 (\mathrm{mod} 5)$ вычисляем $m_2 \equiv 3$;
- из $130 \cdot m_3 = 1 (\mathrm{mod} 7)$ вычисляем $m_3 \equiv 2$;
- из $70 \cdot m_4 = 1 (\mathrm{mod} 13)$ вычисляем $m_4 \equiv 8$.

Далее вычислим сами базисы:

$$B_1 = m_1 \cdot P_1 = 1 \cdot 455 = 455;$$
$$B_2 = m_2 \cdot P_2 = 3 \cdot 182 = 546;$$
$$B_3 = m_3 \cdot P_3 = 2 \cdot 130 = 260;$$
$$B_4 = m_4 \cdot P_4 = 8 \cdot 70 = 560.$$

Имея значения базисов, вычислим A:

$$A = \left|\alpha_1 \cdot B_1 + \alpha_2 \cdot B_2 + \alpha_3 \cdot B_3 + \alpha_4 \cdot B_4\right|_P$$
$$A = \left|0 \cdot 455 + 1 \cdot 546 + 3 \cdot 260 + 1 \cdot 560\right|_{910} =$$
$$= \left|1886\right|_{910} = 66.$$

Недостаток метода, основанного на китайской теореме об остатках заключается в том, что для обратного преобразования требуется умножение и сложение больших чисел, а также операция взятия остатка по модулю большого числа.

В методе Гарнера используется полиадическая система счисления, он основывается на идее, что любое число может быть представлено в системе взаимно простых чисел $p_1 \ \ldots \ p_n$ как [4]:

$$S = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + \ldots$$
$$+ a_{n-1} \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{n-2} + a_n \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1}.$$

Значения a_n вычисляются таким образом:

$$a_1 \equiv s_1 (\mathrm{mod}\, p_1);\ a_2 \equiv (s_2 - a_1)\ \tau_{12} (\mathrm{mod}\, p_2);$$
$$a_3 \equiv \left((s_3 - a_1)\ \tau_{13} - a_2\right)\tau_{23} (\mathrm{mod}\, p_3);$$
$$a_n \equiv \left(\left(\ldots(s_n - a_1)\ \tau_{1n} - a_2\right)\tau_{2n} - \ldots a_{n-1}\right)\tau_{n-1n} (\mathrm{mod}\, p_n).$$

Константы τ_{kj} можно записать как

$$\tau_{kj} = \left|\frac{1}{p_k}\right|_{p_j} \quad \text{где } 1 \le k < j \le n.$$

Подставив значения τ_{kj} в предыдущие выражения, получим:

$$a_1 \equiv \alpha_1 (\mathrm{mod}\, p_1);$$
$$a_2 = ((p_1^{-1}) \bmod p_2 \cdot (s_2 - a_1)) \bmod p_2;$$
$$a_3 = ((p_2^{-1}) \bmod p_3 \cdot ((p_1^{-1}) \bmod p3 \times$$
$$\times (s_3 - a_1) - a_2)) \bmod p_3;$$
$$a_4 = ((p_3^{-1}) \bmod p_4 \cdot ((p_2^{-1}) \bmod p_4 \times$$
$$\times ((p_1^{-1}) \bmod p_4 \cdot (s_4 - a_1) - a_2) - a_3)) \bmod p_3;$$

...

Пример 3. Восстановление числа с использованием метода Гарнера. Для восстановления числа необходимо найти константы τ_{kj}:

$$\tau_{12} = \left|\frac{1}{2}\right|_5 = 3;\ \tau_{13} = \left|\frac{1}{2}\right|_7 = 4;\ \tau_{14} = \left|\frac{1}{2}\right|_{13} = 7;$$

$$\tau_{23} = \left|\frac{1}{5}\right|_7 = 3;\ \tau_{24} = \left|\frac{1}{5}\right|_{13} = 8;\ \tau_{34} = \left|\frac{1}{7}\right|_{13} = 2.$$

Найдем значения a_n:

$$a_1 = s_1 = 0;$$

$$a_2 = ((p_1^{-1}) \bmod p_2 \cdot (s_2 - a_1)) \bmod p_2 =$$

$$= (3 \cdot (1-0)) \bmod 5 = 3;$$

$$a_3 = ((p_2^{-1}) \bmod p_3 \cdot ((p_1^{-1}) \bmod p_3 \times$$

$$\times (s_3 - a_1) - a_2)) \bmod p_3 =$$

$$= (3 \cdot (4 \cdot (3-0) - 3)) \bmod 7 = 6;$$

$$a_4 = ((p_3^{-1}) \bmod p_4 \cdot ((p_2^{-1}) \bmod p_4 \times$$

$$\times ((p_1^{-1}) \bmod p_4 \cdot (s_4 - a_1) - a_2) - a_3)) \bmod p_3 =$$

$$= (2 \cdot (8 \cdot (7 \cdot (1-0) - 3) - 6)) \bmod 13 = 0.$$

Тогда

$$S = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + a_3 \cdot p_1 \cdot p_2 \cdot p_3 =$$

$$= 0 + 3 \cdot 2 + 6 \cdot 2 \cdot 5 + 0 \cdot 2 \cdot 5 \cdot 7 = 66.$$

Рассмотрим метод совместного использования КТО и ОПСС[5]. Для этого представим ортогональные базисы в ОПСС

$$B_i = B_{i1} + B_{i2} \cdot p_1 + B_{i3} \cdot p_1 \cdot p_2 + \ldots$$

$$+ B_{in} \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1},$$

где B_{ij} коэффициенты ОПСС; $i, j = 1; 2 \ldots n$.

Тогда коэффициенты ОПС рассчитываются следующим образом

$$X_{ОПСС} = \alpha_1 (b_{11}, b_{12}, \ldots, b_{1n}) + \alpha_2 (b_{21}, b_{22}, \ldots, b_{2n}) +$$

$$\ldots + \alpha_n (b_{n1}, b_{n2}, \ldots, b_{nn}).$$

Секрет восстанавливается по формуле

$$S = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + \ldots$$

$$+ a_{n-1} \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{n-2} + a_n \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1}.$$

Так как $B_i \bmod p_i = 0, \forall j > i$, то перед первым значащим разрядом будет $i - 1$ нулей.

Для удобства вычислений базисы можно представить в виде матрицы

$$\begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ 0 & b_{22} & \ldots & b_{2n} \\ 0 & 0 & \ldots & b_{nn} \end{bmatrix}.$$

Тогда

$$X_{COK} \to \begin{bmatrix} |\alpha_1 b_{11}|_{p_1}^+ & |\alpha_1 b_{12}|_{p_2}^+ & \ldots & |\alpha_1 b_{1n}|_{p_n}^+ \\ 0 & |\alpha_2 b_{22}|_{p_2}^+ & \ldots & |\alpha_1 b_{2n}|_{p_n}^+ \\ 0 & 0 & \ldots & |\alpha_1 b_{nn}|_{p_n}^+ \end{bmatrix},$$

при этом $a_i = \left| \sum_{\substack{i=1 \\ j=1}}^{n} \alpha_i b_{ij} \right|_{\bmod p_i}$.

Пример 4. Восстановление числа с совместным использованием КТО и ОПСС. Представим базисы B_i в ОПСС, тогда b_{ij}:

$$b_{11} = 1; \quad b_{12} = 2; \quad b_{13} = 3; \quad b_{15} = 6;$$

$$b_{21} = 0; \quad b_{22} = 3; \quad b_{23} = 5; \quad b_{25} = 7;$$

$$b_{31} = 0; \quad b_{32} = 0; \quad b_{33} = 5; \quad b_{35} = 3;$$

$$b_{41} = 0; \quad b_{42} = 0; \quad b_{43} = 0; \quad b_{45} = 8.$$

Тогда

$$X_{COK} = \begin{bmatrix} |0 \cdot 1|_5^+ & |0 \cdot 2|_5^+ & |0 \cdot 3|_7^+ & |0 \cdot 6|_{13}^+ \\ 0 & |1 \cdot 3|_5^+ & |1 \cdot 5|_7^+ & |1 \cdot 7|_{13}^+ \\ 0 & 0 & |3 \cdot 5|_7^+ & |3 \cdot 3|_{13}^+ \\ 0 & 0 & 0 & |1 \cdot 8|_{13}^+ \end{bmatrix} =$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 3 & 5 & 7 \\ 0 & 0 & 1 & 11 \\ 0 & 0 & 0 & 8 \end{bmatrix};$$

$$a_1 = 0,\ a_2 = 3,\ a_3 = 6,\ a_4 = 0,$$

$$S = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + a_4 \cdot p_1 \cdot p_2 \cdot p_3 =$$

$$= 0 + 3 \cdot 2 + 6 \cdot 2 \cdot 5 + 0 \cdot 2 \cdot 5 \cdot 7 = 66.$$

Групповой метод разделения секрета

Для увеличения стойкости схемы разделения секрета на основе СОК можно использовать схему с групповым двухступенчатым разделением секрета, рис. 1.

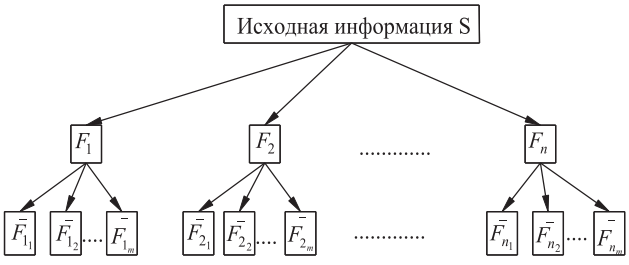

Рис. 1. Структурная схема группового разделения секрета

Работу схемы можно разделить на два этапа.

1. Исходная информация S делится на n частей и распределяется среди лидеров групп $F_1; F_2 \dots F_n$.

2. Информация, принадлежащая лидеру каждой группы $F_1; F_2 \dots F_n$, разделяется на m частей $\left(F_{1_1}; F_{1_2} \dots F_{1_m}\right)\left(F_{2_1}; F_{2_2} \dots F_{2_m}\right)..\left(F_{n_1}; F_{n_2} \dots F_{n_m}\right)$.

Далее эти части могут быть переданы либо по беспроводным сетям передачи данных либо храниться на удаленных серверах.

Исходную информацию предлагается хранить или передавать в виде набора частей, количество которых равно количеству оснований СОК. Введя избыточность среди лидеров групп и среди частей, принадлежащих им, получим пороговую схему, где для восстановления информации достаточно получить от k групп k частей. Уменьшение размера частей, а также их территориальное распределение приведет к снижению нагрузки на линии передачи данных, на серверы для хранения или на ретрансляторы для передачи данных по беспроводным сенсорным сетям. Также с помощью введенной избыточности мы можем локализовать места хранения ошибочных частей и не использовать их для восстановления информации.

Для того чтобы вывести из строя линейную одноуровневую схему, достаточно фальсифицировать k+1 абонентов, а для двухступенчатой необходимо фальсифицировать до $(k+1)K$, где K необходимое число групп для восстановления информации. Мера обнаруживающей способности линейной схемы может быть вычислена согласно [1] как $\frac{P_n - P_k}{P_n} = \frac{P_n - 1}{P_n}$.

Используя меру формулу для обнаруживающей способности линейной схемы, модернизируем ее для групповой схемы

$$\left(\frac{P_{n1} - P_{k1}}{P_{n1}} + \frac{P_{n2} - P_{k2}}{P_{n2}} + \dots + \frac{P_{nm} - P_{km}}{P_{nm}}\right) + \frac{P_n - P_k}{P_n},$$

где m – номер группы.

Таблица 1. Реализация схемы с групповым разделением секрета

Секрет $A = 12752322$		Группы				
		$p_1 = 229$ $F_1 = 228$	$p_2 = 233$ $F_1 = 232$	$p_3 = 239$ $F_3 = 238$	$p_4 = 241$ $F_4 = 48$	$p_5 = 251$ $F_5 = 16$
Части секрета	$p_{1\dots5_1} = 3$	0	1	1	0	1
	$p_{1\dots5_2} = 5$	3	2	3	3	3
	$p_{1\dots5_3} = 17$	7	11	0	14	13
	$p_{1\dots5_2} = 19$	0	4	10	10	13
	$p_{1\dots5_5} = 23$	21	2	8	2	13

В таблице 1 показан пример реализации схемы с групповым разделением секрета. Рассмотрим пример восстановления групповой схемы с применение метода совместного использования КТО и ОПСС для оснований $p_{1\dots5_1} = 3$, $p_{1\dots5_2} = 5$, $p_{1\dots5_3} = 17$, $p_{1\dots5_2} = 19$, $p_{1\dots5_5} = 23$, рассчитаем базисы, как показано в первом примере:

$$P = 3 \cdot 5 \cdot 17 \cdot 19 \cdot 23 = 111435;$$

$$P_1 = \frac{P}{p_1} = \frac{111435}{3} = 37145;$$

$$P_2 = \frac{P}{p_2} = \frac{111435}{5} = 22287;$$

$$P_3 = \frac{P}{p_3} = \frac{111435}{17} = 6555;$$

$$P_4 = \frac{P}{p_4} = \frac{111435}{19} = 5865;$$

$$P_5 = \frac{P}{p_5} = \frac{111435}{23} = 4845.$$

Затем ищем веса базисов:

- из $37145 \cdot m_1 = 1(\mathrm{mod}3)$ вычисляем $m_1 \equiv 2$;
- из $22287 \cdot m_2 = 1(\mathrm{mod}5)$ вычисляем $m_2 \equiv 3$;
- из $6555 \cdot m_3 = 1(\mathrm{mod}17)$ вычисляем $m_3 \equiv 12$;
- из $5865 \cdot m_4 = 1(\mathrm{mod}19)$ вычисляем $m_4 \equiv 3$;
- из $4845 \cdot m_5 = 1(\mathrm{mod}23)$ вычисляем $m_5 \equiv 20$.

Далее вычислим сами базисы:

$$B_1 = m_1 \cdot P_1 = 2 \cdot 37145 = 74290;$$

$$B_2 = m_2 \cdot P_2 = 3 \cdot 22287 = 66861;$$

$$B_3 = m_3 \cdot P_3 = 12 \cdot 6555 = 78660,$$

$$B_4 = m_4 \cdot P_4 = 3 \cdot 5865 = 17595,$$
$$B_5 = m_5 \cdot P_5 = 20 \cdot 4845 = 96900.$$

Найдем константы τ_{kj}:

$$\tau_{12} = \left|\frac{1}{3}\right|_5 = 2;\ \tau_{13} = \left|\frac{1}{3}\right|_{17} = 6;\ \tau_{14} = \left|\frac{1}{3}\right|_{19} = 13;$$
$$\tau_{15} = \left|\frac{1}{3}\right|_{23} = 8;\ \tau_{23} = \left|\frac{1}{5}\right|_{17} = 7;\ \tau_{24} = \left|\frac{1}{5}\right|_{19} = 4;$$
$$\tau_{25} = \left|\frac{1}{5}\right|_{23} = 14;\ \tau_{34} = \left|\frac{1}{17}\right|_{19} = 9;$$
$$\tau_{35} = \left|\frac{1}{17}\right|_{23} = 19;\ \tau_{45} = \left|\frac{1}{19}\right|_{23} = 17;$$

$$X1_{COK} = \begin{bmatrix} |0\cdot1|_3^+ & |0\cdot3|_5^+ & |0\cdot5|_{17}^+ & |0\cdot6|_{19}^+ & |0\cdot15|_{23}^+ \\ 0 & |3\cdot2|_5^+ & |3\cdot3|_{17}^+ & |3\cdot15|_{19}^+ & |3\cdot13|_{23}^+ \\ 0 & 0 & |7\cdot8|_{17}^+ & |7\cdot4|_{19}^+ & |7\cdot16|_{23}^+ \\ 0 & 0 & 0 & |0\cdot12|_{19}^+ & |0\cdot3|_{23}^+ \\ 0 & 0 & 0 & 0 & |21\cdot20|_{23}^+ \end{bmatrix} =$$
$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 10 & 7 & 18 \\ 0 & 0 & 5 & 12 & 21 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 \end{bmatrix};$$

$$a_1 = 0, a_2 = 1, a_3 = 15, a_4 = 0, a_5 = 0;$$
$$F_1 = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + a_3 \cdot p_1 + $$
$$+ a_4 \cdot p_1 \cdot p_2 \cdot p_3 + a_5 \cdot p_1 \cdot p_2 \cdot p_3 = 228;$$

$$X2_{COK} = \begin{bmatrix} |1\cdot1|_3^+ & |1\cdot3|_5^+ & |1\cdot5|_{17}^+ & |1\cdot6|_{19}^+ & |1\cdot15|_{23}^+ \\ 0 & |2\cdot2|_5^+ & |2\cdot3|_{17}^+ & |2\cdot15|_{19}^+ & |2\cdot13|_{23}^+ \\ 0 & 0 & |11\cdot8|_{17}^+ & |11\cdot4|_{19}^+ & |11\cdot16|_{23}^+ \\ 0 & 0 & 0 & |4\cdot12|_{19}^+ & |4\cdot3|_{23}^+ \\ 0 & 0 & 0 & 0 & |2\cdot20|_{23}^+ \end{bmatrix} =$$
$$= \begin{bmatrix} 1 & 3 & 5 & 6 & 15 \\ 0 & 4 & 6 & 11 & 4 \\ 0 & 0 & 3 & 11 & 17 \\ 0 & 0 & 0 & 10 & 14 \\ 0 & 0 & 0 & 0 & 17 \end{bmatrix};$$

$$a_1 = 1, a_2 = 2, a_3 = 15, a_4 = 0, a_5 = 0;$$
$$F_1 = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + a_3 \cdot p_1 + $$
$$+ a_4 \cdot p_1 \cdot p_2 \cdot p_3 + a_5 \cdot p_1 \cdot p_2 \cdot p_3 = 232;$$

$$X3_{COK} = \begin{bmatrix} |1\cdot1|_3^+ & |1\cdot3|_5^+ & |1\cdot5|_{17}^+ & |1\cdot6|_{19}^+ & |1\cdot15|_{23}^+ \\ 0 & |3\cdot2|_5^+ & |3\cdot3|_{17}^+ & |3\cdot15|_{19}^+ & |3\cdot13|_{23}^+ \\ 0 & 0 & |0\cdot8|_{17}^+ & |0\cdot4|_{19}^+ & |0\cdot16|_{23}^+ \\ 0 & 0 & 0 & |10\cdot12|_{19}^+ & |10\cdot3|_{23}^+ \\ 0 & 0 & 0 & 0 & |8\cdot20|_{23}^+ \end{bmatrix} =$$
$$= \begin{bmatrix} 1 & 3 & 5 & 6 & 15 \\ 0 & 1 & 10 & 7 & 18 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 13 \\ 0 & 0 & 0 & 0 & 22 \end{bmatrix};$$

$$a_1 = 1, a_2 = 4, a_3 = 15, a_4 = 0, a_5 = 0;$$
$$F_1 = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + a_3 \cdot p_1 + $$
$$+ a_4 \cdot p_1 \cdot p_2 \cdot p_3 + a_5 \cdot p_1 \cdot p_2 \cdot p_3 = 238;$$

$$X4_{COK} = \begin{bmatrix} |0\cdot1|_3^+ & |0\cdot3|_5^+ & |0\cdot5|_{17}^+ & |0\cdot6|_{19}^+ & |0\cdot15|_{23}^+ \\ 0 & |3\cdot2|_5^+ & |3\cdot3|_{17}^+ & |3\cdot15|_{19}^+ & |3\cdot13|_{23}^+ \\ 0 & 0 & |14\cdot8|_{17}^+ & |14\cdot4|_{19}^+ & |14\cdot16|_{23}^+ \\ 0 & 0 & 0 & |10\cdot12|_{19}^+ & |10\cdot3|_{23}^+ \\ 0 & 0 & 0 & 0 & |2\cdot20|_{23}^+ \end{bmatrix} =$$
$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 10 & 7 & 18 \\ 0 & 0 & 10 & 5 & 19 \\ 0 & 0 & 0 & 6 & 13 \\ 0 & 0 & 0 & 0 & 17 \end{bmatrix};$$

$$a_1 = 0, a_2 = 1, a_3 = 3, a_4 = 0, a_5 = 0;$$
$$F_1 = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + a_3 \cdot p_1 + a_4 \cdot p_1 \cdot p_2 \cdot p_3 + $$
$$+ a_5 \cdot p_1 \cdot p_2 \cdot p_3 = 48;$$

$$a_1 = 1, a_2 = 0, a_3 = 1, a_4 = 0, a_5 = 0$$
$$F_1 = a_1 + a_2 \cdot p_1 + a_3 \cdot p_1 \cdot p_2 + a_3 \cdot p_1 + $$
$$+ a_4 \cdot p_1 \cdot p_2 \cdot p_3 + a_5 \cdot p_1 \cdot p_2 \cdot p_3 = 48;$$

$$X4_{COK}=\begin{bmatrix}|1\cdot1|_3^+ & |1\cdot3|_5^+ & |1\cdot5|_{17}^+ & |1\cdot6|_{19}^+ & |1\cdot15|_{23}^+\\ 0 & |1\cdot2|_5^+ & |1\cdot3|_{17}^+ & |1\cdot15|_{19}^+ & |1\cdot13|_{23}^+\\ 0 & 0 & |16\cdot8|_{17}^+ & |16\cdot4|_{19}^+ & |16\cdot16|_{23}^+\\ 0 & 0 & 0 & |16\cdot12|_{19}^+ & |16\cdot3|_{23}^+\\ 0 & 0 & 0 & 0 & |16\cdot20|_{23}^+\end{bmatrix}=\begin{bmatrix}1 & 3 & 5 & 6 & 21\\ 0 & 2 & 3 & 15 & 13\\ 0 & 0 & 9 & 14 & 6\\ 0 & 0 & 0 & 2 & 11\\ 0 & 0 & 0 & 0 & 21\end{bmatrix}.$$

Далее таким же образом восстанавливаем и сам секрет из остатков принадлежащих лидерам групп:

$$\tau_{12}=\left|\frac{1}{229}\right|_{233}=291;\ \tau_{13}=\left|\frac{1}{229}\right|_{239}=454;$$

$$\tau_{14}=\left|\frac{1}{229}\right|_{241}=261;\ \tau_{15}=\left|\frac{1}{229}\right|_{251}=308;$$

$$\tau_{23}=\left|\frac{1}{233}\right|_{239}=438;\ \tau_{24}=\left|\frac{1}{233}\right|_{241}=271;$$

$$\tau_{25}=\left|\frac{1}{233}\right|_{251}=237;\ \tau_{34}=\left|\frac{1}{239}\right|_{241}=361;$$

$$\tau_{35}=\left|\frac{1}{251}\right|_{251}=230;\ \tau_{45}=\left|\frac{1}{241}\right|_{251}=276;$$

$$Xcco=\begin{bmatrix}|228\cdot1|_{229}^+ & |228\cdot175|_{233}^+ & |228\cdot65|_{239}^+ & |228\cdot186|_{241}^+ & |228\cdot202|_{251}^+\\ 0 & |57\cdot58|_{233}^+ & |57\cdot169|_{239}^+ & |57\cdot111|_{241}^+ & |57\cdot6|_{251}^+\\ 0 & 0 & |173\cdot4|_{239}^+ & |173\cdot2|_{241}^+ & |173\cdot42|_{251}^+\\ 0 & 0 & 0 & |54\cdot182|_{241}^+ & |54\cdot219|_{251}^+\\ 0 & 0 & 0 & 0 & |48\cdot31|_{251}^+\end{bmatrix}=$$

$$=\begin{bmatrix}228 & 57 & 173 & 54 & 47\\ 0 & 175 & 69 & 129 & 243\\ 0 & 0 & 235 & 238 & 208\\ 0 & 0 & 0 & 60 & 6\\ 0 & 0 & 0 & 0 & 245\end{bmatrix};$$

$$a_1=228, a_2=232, a_3=238, a_4=0, a_5=0.$$

Для обнаружения и коррекции ошибок необходимо иметь избыточные основания СОК. Выделим из таблицы 1 информационные и дополнительные основания, таблица 2.

Моделирование группового метода разделения секрета

Данная групповая схема реализована в среде разработки Borland C++ Builder. В качестве объекта разделения было принято 8-битное изображение с разрешением 220×220 точек. Каждый пиксель изображения последовательно переводился в СОК по основаниям

$$p_1=229,\ p_2=233,\ p_3=239,$$
$$p_4=241,\ p_5=251,$$

где p_1, p_2, p_3, p_4, p_5 – это основания лидеров групп. Основания p_1, p_2, p_3 являются рабочими, а p_4, p_5 – избыточными. Далее основание каждого лидера группы повторно преобразовывалось в СОК по основаниям $p_{n1}=3$, $p_{n2}=5$, $p_{n3}=17$, $p_{n4}=19$, $p_{n5}=23$, где n – это номер группы $n=1...5$. Основания СОК были подобраны таким образом, чтобы три основания были рабочими, а два избыточными. На избыточные основания частей каждой группы накладываем условие абсолютной надежности, что гарантирует достоверность избыточных оснований СОК.

На рис. 2 приведен пример программной реализации группового метода разделения секрета. На нем показано, как исходное изображение делится на пять частей для лидеров групп, и каждый лидер группы затем делится так же на пять частей, после чего изображение восстанавливается.

Система остаточных классов – это система счисления, которая имеет возможность обнару-

Таблица 2. Групповая СОК с избыточными основаниями частями и группами

Секрет $A=12752322$			Группы				
			$p_1=229$ $F_1=228$	$p_2=233$ $F_1=232$	$p_3=239$ $F_3=238$	$p_4=241$ $F_4=48$	$p_5=251$ $F_5=16$
			Информационные		Дополнительные		
Части секрета	$p_{1...5_1}=3$	Информационные	0	1	1	0	1
	$p_{1...5_2}=5$		3	2	3	3	1
	$p_{1...5_3}=17$		7	11	0	14	16
	$p_{1...5_2}=19$	Дополнительные	0	4	10	10	16
	$p_{1...5_5}=23$		21	2	8	2	16

жения и коррекции ошибок. При восстановлении изображения A из системы остаточных классов если $A > P^{/}$, то A является ошибочным.

Рассмотрим пример выполнения программы, когда часть информации потеряна. На рис. 3 показано, что часть информации потеряна, но для локализации достаточно оставшихся изображений.

Поиск локализация ошибок осуществляется путем вычисления проекций числа A по всем осно-

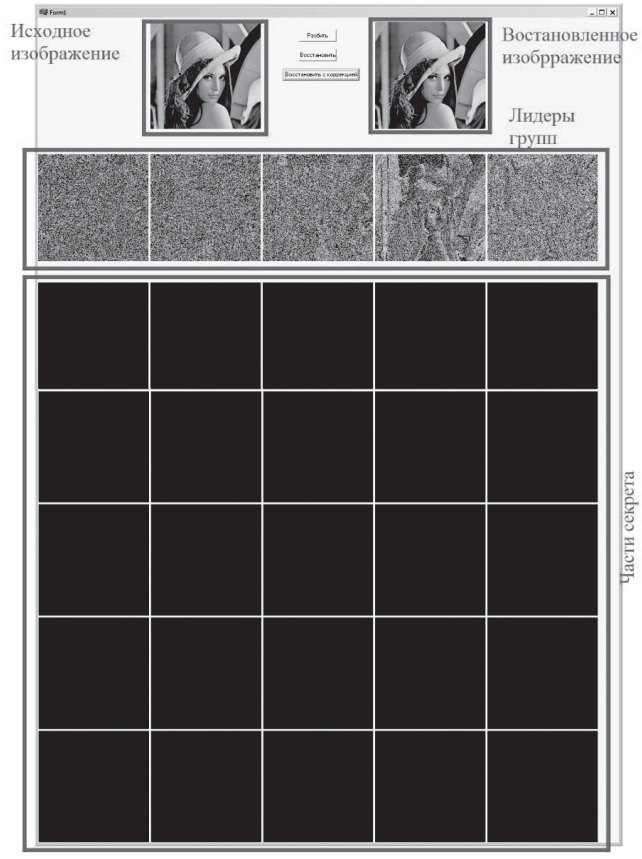

Рис. 2. Моделирование группового метода разделения секрета

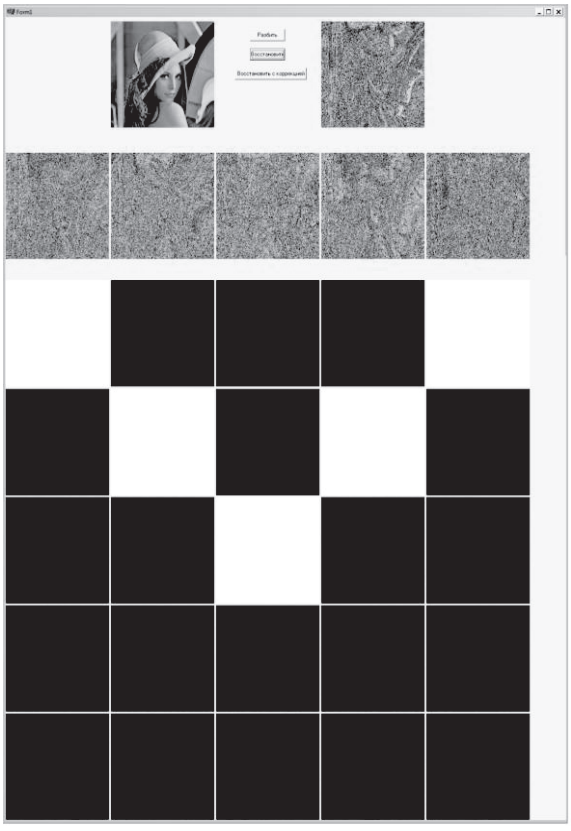

Рис. 3. Восстановление секрета без локализации ошибок

ваниям. Так как два основания являются избыточными, то можно найти две ошибки. Рассмотрим численный пример поиска восстановления секрета, если от лидеров групп придет две ошибки.

Пусть дан секрет $A=300$, $p_1=13$, $p_2=17$, $p_3=19$, $p_4=23$, $p_5=29$. Представим число A в СОК, тогда $A=(1,11,15,1,10)$. Введем ошибку в число, представленное в СОК $A=(0,2,15,1,10)$, тогда при восстановлении $\tilde{A}=1736501$, так как $A>P^{/}$, $P^{/}=2800733$, то можно сказать, что число $\tilde{A}$ ошибочно.

Найдем проекции числа A по двум основаниям:

- по основаниям $p_1=13$, $p_2=17$, $P^{/}=12673$, $\tilde{A}_{12}=300$;
- по основаниям $p_1=13$, $p_3=19$, $P^{/}=11339$, $\tilde{A}_{13}=6556$;
- по основаниям $p_2=17$, $p_3=19$, $P^{/}=8671$, $\tilde{A}_{23}=6970$.

Проекции по всем основаниям, кроме проекции по модулям $p_1=13$, $p_2=17$, больше рабочего диапазона секрета, следовательно, части по основаниям $p_1=13$, $p_2=17$ являются неверными, поэтому ошибку можно локализовать и восстановить секрет по основаниям $p_3=19$, $p_4=23$, $p_5=29$.

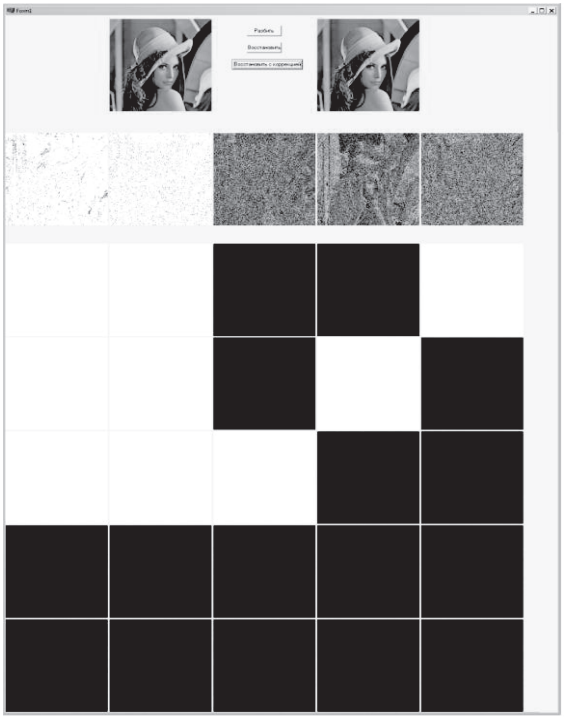

Рис. 4. Локализация ошибок в СОК

На рис. 4 показано, как при потери части информации, достаточной, для потери группы, секрет восстанавливается. Для восстановления секрета необходимо, чтобы в k группах были рабочими K частей, то есть для данного примера достаточно, чтобы в трех группах работало по три клиента. Необходимым условием является также то, чтобы СОК была упорядочена: при неупорядоченной СОК не все пиксели могут быть локализованы.

На рис. 5 показано, как при потере информации, большей, чем это достаточно для восстановления, выглядит восстановленный секрет.

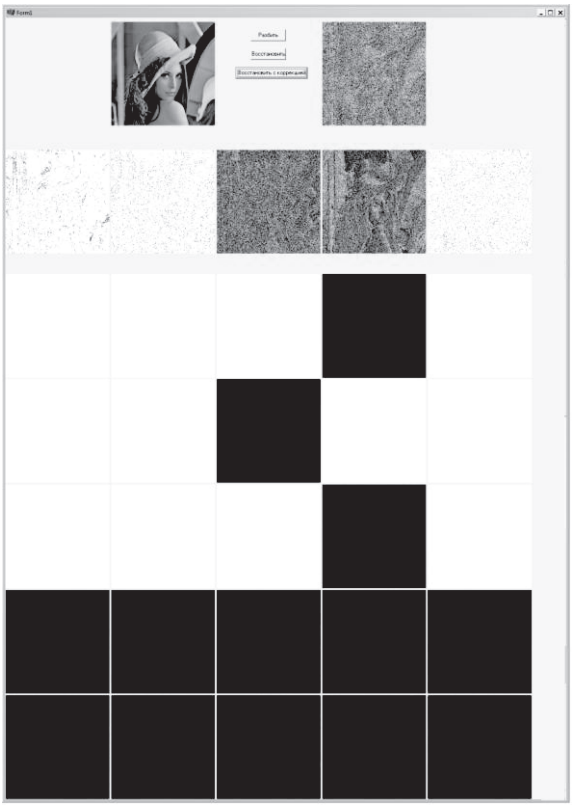

Рис. 5. Восстановление секрета при потере избыточной информации

Вывод

В статье представлен метод группового разделения секрета, основанный на системе остаточных классов. Показана его большая обнаруживающая способность в отличие от линейного метода ($\frac{P_n-P_k}{P_n}=\frac{P_n-1}{P_n}$ для линейного и $\left(\frac{P_{n1}-P_{k1}}{P_{n1}}+\frac{P_{n2}-P_{k2}}{P_{n2}}+\ldots+\frac{P_{nm}-P_{km}}{P_{nm}}\right)+\frac{P_n-P_k}{P_n}$ для группового), при этом уменьшение размерности частей приводит к снижению нагрузки на линии передачи данных либо на серверы их хранения. Приведены методы локализации оши-

бок в СОК, показан способ восстановления информации без коррекции ошибок. Разработано программное обеспечение для моделирования группового разделения секрета на примере разделения цветного изображения с локализацией ошибок. На программной модели показано, что для восстановления секрета групповым методом допустимо потерять больше частей информации, чем при использовании линейного метода. Показана возможность применения разработанной модели для криптографической и некриптографической защиты информации. Работа выполнена при поддержке РФФИ, проект № 13-07-00478-а.

Литература

1. Червяков Н.И., Сахнюк П.А., Шапошников А.В. и др. Нейрокомпьютеры в остаточных классах. Кн. 11. М.: Радиотехника, 2003. – 272 с.
2. Червяков Н.И., Евдокимов А.А. Галушкин А.И. и др. Применение искусственных нейронных сетей и систем остаточных классов в криптографии. М.: Физматлит, 2012. – 280 с.
3. Червяков Н.И., Сахнюк П.А., Шапошников А.В. и др. Модулярные параллельные вычислительные структуры нейропроцессорных систем. М.: Физматлит, 2003. – 288 с.
4. Soderstrand M.A., Jenkins W.K., Jullien G.A., Taylor F.J. Residue Number System Arithmetic: Modern Applications in Digital Signal Processing. IEEE Press, New York, 1986. – P. 15-19.
5. Патент RU № 2380751 от 30.05.2008. Нейронная сеть с пороговой (k,t) структурой для преобразования остаточного кода в двоичный позиционный код // Червяков Н.И., Головко А.Н., Лавриненко А.В. и др.
6. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах. М.: Сов. радио, 1968. – 440 с.
7. Нестеренко А. Введение в современную криптографию. Теоретико-числовые алгоритмы. Курс лекций для вузов. img0.liveinternet.ru, 2011. – 190 с.

METHOD DEVELOPMENT NOISEPROOF SECRET SHARING BASED ON THE APPLICATION OF TWO-STAGE SYSTEM, THE RESIDUAL CLASSES

Kocherov Y.N., Chervyakov N.I.

The article presents a group method of secret sharing, based on a residue number system. When using this method increases the ability to scan for code that is increasing the number of detected errors.

Keywords: *residue number system, generalized Polyadic number system, secret sharing.*

Кочеров Юрий Николаевич, аспирант Кафедры информационных систем, электропривода и автоматики Невинномысского технологического института – Филиала Северо-Кавказского федерального университета (СКФУ). Тел. 8-865-543-55-08; 8-918-866-91-93. E-mail: kocherov_yra@mail.ru

Червяков Николай Иванович, д.т.н., профессор, Заслуженный деятель науки и техники РФ, профессор Кафедры высшей алгебры и геометрии СКФУ. Тел.: (8-865) 275-35-64. E-mail: k-fmf-primath@stavsu.ru

УДК 621.391

МЕТОД ФОРМИРОВАНИЯ МЯГКИХ РЕШЕНИЙ В СИСТЕМЕ ШИРОКОПОЛОСНОГО КАНАЛА СВЯЗИ С НЕЗВЕСТНЫМИ ПАРАМЕТРАМИ ОСТАТОЧНЫХ КЛАССОВ

Баскакова Е.С., Гладких А.А.

Решается задача формирования индексов мягких решений (ИМР) символов применительно к технологии обработки сигналов в системе с ортогональным частотным мультиплексированием (OFDM), использующей каналы с неизвестными параметрами. Задачи подобного типа являются актуальными при обмене данными систем реального времени в ходе оперативного взаимодействия двух или нескольких подвижных объектов при применении в них широкополосных систем связи. Метод вычисления ИМР основан на критерии минимума евклидовой метрики.

Ключевые слова: мягкое декодирование, итеративный процесс, стирание, технология OFDM, логарифм отношения правдоподобия.