Література ***1.*** *Дмитриев А. С., Клецов А. В., Лактюшкин А. М., Панас А. И., Старков С. О. "Сверхширокополосные коммуникационные системы на основе динамического хаоса", Успехи современной радиоэлектроники, 2008, №1, С. 4–18.* ***2.*** *Дмитриев А. С., Ефремова Е. В., Максимов Н. А., Григорьев Е. В. "Генератор хаотических колебаний сверхвысокочастотного диапазона на основе автоколебательной системы с 2,5 степенями свободы", Радиотехника и электроника, 2007, Т. 52. № 10, С. 1232-1240.* ***3.*** *Кальянов Г. Н., Кальянов Э. В. // Письма в ЖТФ. 2005. Т. 31. В. 24. С. 45-50.*

УДК 621.391:519.7:510.5

ОПТИМАЛЬНЫЕ ПРОТОКОЛЫ МНОЖЕСТВЕННОГО РАЗДЕЛЕНИЯ СЕКРЕТА С МНОГОАДРЕСНЫМ СООБЩЕНИЕМ, ОСНОВАННЫЕ НА ЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЯХ НАД КОЛЬЦАМИ ВЫЧЕТОВ

Антон Алексейчук, Андрей Волошин
Институт специальной связи и защиты информации НТУУ «КПИ»

Анотація: **Отримані достатні умови оптимальності (за критерієм максимуму інформаційних відношень) протоколів множинного розподілу секрету з багатоадресним повідомленням, що реалізують певні ієрархії доступу. Наведено низку конструкцій зазначених протоколів, які задовольняють отриманим умовам оптимальності.**
Summary: **The sufficient conditions of optimality (i. e. of information rates maximality) of multi-secret sharing schemes with broadcast message for certain access hierarchies are obtained. Some constructions of such schemes satisfied the described conditions are presented.**
Ключевые слова: **криптографическая защита информации, протокол множественного разделения секрета с многоадресным сообщением, иерархия доступа, кольцо вычетов.**

Введение

Как известно, при разработке современных информационно-телекоммуникационных систем (ИТС) особое внимание уделяется вопросам разграничения доступа к их ресурсам [1]. Согласно принятой мировой и отечественной практике [2, 3], решение задач разграничение доступа к ресурсам таких систем возлагают на подсистему управления доступом. При этом расширение функциональных возможностей ИТС, как правило, приводит к необходимости значительного повышения гибкости и надежности используемых подсистем управления доступом [4]. Для решения последней задачи, наряду с другими методами, применяют так называемые протоколы разделения секрета (ПРС), позволяющие получать приемлемые решения, как с точки зрения надежности, так и с точки зрения гибкости подсистемы управления доступом [5, 6].

Из анализа результатов статей [5 – 7] и ряда других публикаций следует, что повышение надежности и гибкости подсистем управления доступом современных ИТС может быть достигнуто при применении ПРС, обладающих следующими свойствами:

1) возможность одновременного разделения нескольких секретных ключей (секретов);
2) безусловная (совершенная) стойкость ПРС;
3) возможность реализации процедур восстановления секретов с использованием многоадресных сообщений, в том числе, для семейств иерархий доступа на множестве участников протокола;
4) вычислительная эффективность процедур формирования секретной информации, передаваемой участникам протокола, и восстановления секретов соответствующими коалициями участников.

В [8 – 10] предложены и исследованы протоколы разделения секрета, обладающие перечисленными свойствами. Указанные ПРС, названные линейными протоколами множественного разделения секрета с многоадресным сообщением (ПМРС с МС), строятся на основе линейных преобразований над кольцами вычетов целых чисел и обобщают классические векторные схемы разделения секрета над конечными полями [11, 12] и линейные ПРС над кольцами вычетов примарного порядка [13].

Для оценки эффективности ПМРС с МС, как правило, используют два показателя: информационное отношение и многоадресное информационное отношение. Первый из них определяется как отношение суммарной длины разделяемых секретных ключей к максимуму длин сообщений, передаваемых участникам протокола на первом этапе, а второй – как отношение суммарной длины секретов к длине многоадресного сообщения, необходимого для восстановления секретных ключей соответствующими коалициями участников [14]. Протокол множественного разделения секрета с многоадресным сообщением называется оптимальным в заданном классе ПМРС с МС, если он имеет наибольшее информационное отношение и

(одновременно) наибольшее многоадресное информационное отношение среди всех ПМРС с МС в этом классе.

Настоящая статья посвящена исследованию условий оптимальности ПМРС с МС, описанных в [8]. Получены достаточные условия оптимальности указанных протоколов в классе всех ПМРС с МС, реализующих данную иерархию доступа. Предложены также конструкции оптимальных линейных ПМРС с МС над примарными кольцами вычетов. По мнению авторов статьи, применение указанных протоколов разделения секрета при проектировании подсистем управления доступом современных информационно-телекоммуникационных систем позволит повысить их надежностные и эксплуатационные характеристики, а, значит, и уровень защищенности информации в таких системах в целом.

I Основные понятия, обозначения и вспомогательные результаты

Напомним определение ПМРС с МС, введенных в статье [8].

Пусть даны различные простые числа $p_1, \dots, p_w$ и натуральные числа $d_1, \dots, d_w$. Обозначим $R = \mathbf{Z}/(m)$ кольцо вычетов по модулю $m = p_1^{d_1} \cdots p_w^{d_w}$, R^* – множество обратимых элементов кольца R, $D(R) = R \setminus R^*$. Для любой матрицы H и произвольного множества A номеров ее столбцов обозначим H_A подматрицу матрицы H, содержащуюся в ее столбцах с номерами из A, $\| H_A \|$ – число различных строк матрицы H_A. В случае, когда H является матрицей над кольцом R обозначим символом $\langle H \rangle_R$ R-модуль, порожденный ее столбцами.

Рассмотрим матрицу

$$G = \left(\begin{array}{c|ccc|c} 1 & 0 & \cdots & 0 & g_{0,n+1} \\ \hline 0 & & & & \\ \vdots & & G' & & g_{n+1}^{\downarrow} \\ 0 & & & & \end{array}\right) \tag{1}$$

размера $(k+1)\times(n+2)$ над кольцом R, где $k, n \geq 2$, $g_{0,n+1} \in R^*$, $g_{n+1}^{\downarrow} \notin D(R)^{(k)}$. Обозначим $G_0, G_1, \dots, G_{n+1}$ столбцы матрицы G. Согласно [8], этой матрице соответствует протокол $\rho(G)$ множественного разделения секрета с многоадресным сообщением, реализующий распределение наборов секретных ключей, принадлежащих множеству

$$S_0 = \{(s_{lj}) : s_{lj} \in \mathbf{GF}(p_j), l \in \overline{0, d_j - 1},\ j \in \overline{1, w}\}, \tag{2}$$

между участниками из множества $P = \{1, 2, \dots, n\}$. Указанный протокол состоит из двух этапов, на первом из которых дилер ПРС выбирает независимо, случайно и равновероятно элементы $a_1, \dots, a_k \in R$, вычисляет вектор $(s_1, \dots, s_n, b(a_1, \dots, a_k)) = (a_1, \dots, a_k)(G', g_{n+1}^{\downarrow})$ и передает сообщение s_i i-му участнику протокола, $i \in P$, по защищенному каналу связи. На втором этапе для распределения набора ключей $(s_{lj}) \in S_0$ дилер находит элемент $s \in R$ такой, что $s \equiv \sum_{l=0}^{d_j - 1} p_j^{\,l} s_{lj} (\mathrm{mod}\, p_j^{d_j})$ для любого $j \in \overline{1, w}$, вычисляет многоадресное сообщение $\hat{A} = g_{0,n+1} s + b(a_1, \dots, a_k) \in R$ и направляет его по широковещательному каналу связи всем участникам протокола. В [8] показано, что описанный протокол разделения секрета обладает следующим свойством: для любой коалиции $A \subseteq P$ существует единственный делитель $t = p_1^{l_1} \cdots p_w^{l_w}$ числа m такой, что после получения сообщения B участники коалиции A могут однозначно восстановить ключи s_{lj} с номерами из множества

$$M(t) = \{(l, j) : 0 \leq l \leq d_j - l_j - 1,\ j \in \overline{1, w}\} \tag{3}$$

и не имеют никакой апостериорной информации об остальных ключах из набора (s_{lj}).

Обозначим $\widetilde{\Psi}_t$ множество всех коалиций $A \subseteq P$, удовлетворяющих указанному выше условию. Семейство множеств $\widetilde{\Psi} = (\widetilde{\Psi}_t : t \mid m)$ называется иерархией доступа ПМРС с МС $\rho(G)$, а сами множества $\widetilde{\Psi}_t$ – уровнями иерархии доступа. Согласно [8], для любого $t \mid m$ выполняется равенство

$$\widetilde{\Psi}_t = \{A \subseteq P : tR = I_G(A)\}, \tag{4}$$

где $I_G(A) = \{r \in R : rG_0 \in \langle G_{A \cup \{n+1\}} \rangle_R\}$, $A \subseteq P$.

Обозначим S_i множество всех секретных сообщений s_i, передаваемых i-му участнику на первом этапе ПМРС с МС $\rho(G)$, S_{n+1} – множество многоадресных сообщений B, передаваемых участникам на втором этапе этого протокола. На основании вышеизложенного справедливо неравенство

$$\log |S_i| \le \log |S_0|, \ i \in P,$$

которое обращается в равенство, если i-й столбец матрицы G содержит обратимые элементы кольца R. Аналогично, в силу обратимости элемента $g_{0,n+1}$ матрицы G выполняется равенство

$$\log |S_{n+1}| = \log |S_0|.$$

Таким образом, при выполнении условия $\exists\, i \in P : G_i \notin D(R)^{(k+1)}$ информационное отношение $\rho^{\rho(G)}$ и многоадресное информационное отношение $\rho_{\mathrm{M}}^{\rho(G)}$ ПМРС с МС $\rho(G)$ имеют следующий вид:

$$\rho^{\rho(G)} \stackrel{\text{def}}{=} \frac{\log |S_0|}{\max\limits_{i \in P} \{\log |S_i|\}} = 1, \ \rho_{\mathrm{M}}^{\rho(G)} \stackrel{\text{def}}{=} \frac{\log |S_0|}{\log |S_{n+1}|} = 1. \tag{5}$$

Равенства (5) приводят к естественному вопросу о том, существуют ли более эффективные по сравнению с $\rho(G)$ протоколы множественного разделения секрета с многоадресным сообщением, реализующие распределение секретных ключей из множества (2) для иерархии доступа, состоящей из множеств (4). Другими словами: существуют ли для данных S_0 и $\widetilde{\Psi}$ такие ПМРС с МС, для которых максимальная длина сообщений s_i ($i \in P$) или B меньше, чем $\log |S_0|$? Ниже показано, что при достаточно общих ограничениях на матрицу (1) ответ на поставленный вопрос является отрицательным. Для того, что привести точные формулировки полученных результатов, уточним определение произвольного протокола множественного разделения секрета с многоадресным сообщением.

Опишем комбинаторную модель ПМРС с МС, реализующего распределение секретных ключей из множества (2) для иерархии доступа (4). Отметим, что эта модель аналогична известной комбинаторной модели совершенной схемы разделения (единственного) секрета [15, 16] и описывает, в том числе, традиционные (“вероятностные”) протоколы разделения секрета с многоадресным сообщением, задаваемые с помощью равномерных распределений вероятностей на конечных множествах [14].

Итак, пусть $S_1, \ldots, S_{n+1}$ – конечные множества, $|S_i| \ge 2$, $i \in \overline{1, n+1}$. Рассмотрим множество L, состоящее из слов $(s_0, s_1, \ldots, s_{n+1})$, где $s_0 = (s_{lj}) \in S_0$, $s_i \in S_i$, $i \in \overline{1, n+1}$, которое удовлетворяет следующему условию: для любых $i \in \overline{0, n+1}$, $r \in S_i$ существует слово $s = (s_0, s_1, \ldots, s_{n+1}) \in L$ такое, что $s_i = r$. Отождествим наборы $s_0 = (s_{lj}) \in S_0$ с векторами длины $d = d_1 + \ldots + d_w$, координаты которых занумерованы определенным образом элементами множества $M = \{(l, j) : l \in \overline{0, d_j - 1}, \ j \in \overline{1, w}\}$. Запишем слова, принадлежащие множеству L, в виде таблицы (матрицы) размера $|L| \times (d + n + 1)$, которую будем отождествлять с этим множеством и обозначать тем же символом. Отметим, что в силу принятых соглашений первые d столбцов таблицы L занумерованы элементами множества M, а оставшиеся $n+1$ столбцов – элементами множества $P \cup \{n+1\}$. Напомним также, что символ L_A обозначает таблицу (подматрицу), содержащуюся в столбцах таблицы L с номерами из множества $A \subseteq M \cup P \cup \{n+1\}$.

Будем говорить, что таблица L задает совершенный ПМРС с МС, реализующий иерархию доступа вида

(4), если выполняются следующие условия:

(а) $\left\|L_{P\cup M}\right\| = \left\|L_P\right\| m$;

(б) для любых $t \mid m$, $A \in \widetilde{\Psi}_t$ справедливы равенства

$$\left\|L_{M(t)\cup A\cup\{n+1\}}\right\| = \left\|L_{A\cup\{n+1\}}\right\|, \tag{6}$$

$$\left\|L_{\overline{M(t)}\cup A\cup\{n+1\}}\right\| = \left\|L_{A\cup\{n+1\}}\right\| t, \tag{7}$$

где множество $M(t)$ определяется по формуле (3), $\overline{M(t)} = M \setminus M(t)$.

Протокол разделения секрета, соответствующий таблице L, описывается следующим образом. Пусть $s_0 = (s_{ij}) \in S_0$ – набор ключей, подлежащих распределению между участниками из множества P. Тогда на первом этапе дилер выбирает произвольное слово $s = (s_0, s_1, \ldots, s_{n+1}) \in L$ и передает сообщение s_i по защищенному каналу связи i-му участнику ПМРС с МС, $i \in \overline{1, n}$. Затем, на втором этапе дилер передает сообщение s_{n+1} всем участникам протокола по широковещательному каналу связи. На основании формул (6), (7) участники произвольной коалиции $A \in \widetilde{\Psi}_t$ смогут однозначно восстановить секретные ключи с номерами из множества $M(t)$ по имеющимся у них сообщениям s_i, s_{n+1} и не получат никакой информации об остальных ключах (в том смысле, что ни один из этих ключей не может быть отбракован как ложный по известным сообщениям s_i, $i \in A$, и s_{n+1}; см. формулу (7)). Кроме того, согласно условию (а), до получения многоадресного сообщения все участники протокола не имеют апостериорной информации о наборе ключей s_0 (в том же смысле, что и выше).

Отметим, что линейный ПМРС с МС $\rho(G)$ может быть задан с помощью таблицы L, строками которой являются всевозможные линейные комбинации строк матрицы G с коэффициентами из кольца R.

Информационное отношение ρ^{Σ} и многоадресное информационное отношение $\rho_{\mathrm{M}}^{\Sigma}$ произвольного ПМРС с МС Σ, заданного таблицей L, удовлетворяющей условиям (а), (б), определяются по формулам

$$\rho^{\Sigma} = \frac{\log |S_0|}{\max\limits_{i\in P} \log |S_i|},\ \rho_{\mathrm{M}}^{\Sigma} = \frac{\log |S_0|}{\log |S_{n+1}|}.$$

Обозначим $\Omega(S_0, \widetilde{\Psi})$ класс всех ПМРС с МС, реализующих распределение секретных ключей из множества S_0 вида (2) для иерархии доступа $\widetilde{\Psi}$, состоящей из множеств (4). Назовем протокол $\Sigma_0 \in \Omega(S_0, \widetilde{\Psi})$ оптимальным, если для любого $\Sigma \in \Omega(S_0, \widetilde{\Psi})$ выполняются следующие неравенства:

$$\rho^{\Sigma} \le \rho^{\Sigma_0},\ \rho_{\mathrm{M}}^{\Sigma} \le \rho_{\mathrm{M}}^{\Sigma_0}.$$

Отметим, что сам факт существования оптимальных протоколов разделения секрета для конкретных множеств S_0 и $\widetilde{\Psi}$ не очевиден и требует обоснования. Ниже показано, что при определенных условиях линейный ПМРС с МС $\rho(G)$ является оптимальным в соответствующем классе $\Omega(S_0, \widetilde{\Psi})$ и описаны конструкции протоколов, удовлетворяющих указанным условиям оптимальности.

II Достаточные условия оптимальности линейных протоколов множественного разделения секрета с многоадресным сообщением

Зафиксируем матрицу G вида (1), удовлетворяющую условию

$$G_0 \in \left\langle G_{P\cup\{n+1\}} \right\rangle_R. \tag{8}$$

Как и выше, обозначим S_0 множество вида (2), $\widetilde{\Psi}$ – семейство множеств (4), соответствующее матрице G.

Получим нижние границы длин сообщений, передаваемых участникам произвольного протокола разделения секрета, принадлежащего классу $\Omega(S_0, \widetilde{\Psi})$.

Лемма. Пусть $L \subseteq S_0 \times S_1 \times \ldots \times S_{n+1}$ – множество, задающее произвольный ПМРС с МС $\Sigma \in \Omega(S_0, \widetilde{\Psi})$. Тогда при выполнении условия (8) справедливы следующие неравенства:

$$\log |S_i| \geq \max_{(A, t_1, t_2)} \{\log(t_1/t_2)\}, \; i \in P, \tag{9}$$

где максимум берется по всем упорядоченным наборам (A, t_1, t_2) таким, что $A \subseteq P$, $t_1, t_2 \mid m$ и

$$A \in \widetilde{\Psi}_{t_1}, \; A \cup \{i\} \in \widetilde{\Psi}_{t_2}; \tag{10}$$

$$\log |S_{n+1}| \geq \log m. \tag{11}$$

Доказательство. Для любого $A \subseteq M \cup P \cup \{n+1\}$ обозначим $h(A) = \log \|L_A\|$. Непосредственно из определения множества L (см. п. I) вытекают следующие свойства функции h:

1) $h(\{i\}) = \log |S_i|$ для любого $i \in P \cup \{n+1\}$;

2) $h(A \cup B) \leq h(A) + h(B)$ для любых $A, B \subseteq M \cup P \cup \{n+1\}$;

3) $A \subseteq B \subseteq M \cup P \cup \{n+1\} \;\Rightarrow\; h(A) \leq h(B)$.

Докажем неравенство (9). Рассмотрим произвольный набор (A, t_1, t_2), удовлетворяющий условию (10). Обозначим $A' = A \cup \{n+1\}$. На основании формул (7), (10) выполняются равенства

$$\left\| L_{\overline{M(t_1)} \cup A'} \right\| = \|L_{A'}\| t_1, \;\; \left\| L_{\overline{M(t_2)} \cup A' \cup \{i\}} \right\| = \|L_{A' \cup \{i\}}\| t_2. \tag{12}$$

Кроме того, в силу соотношений (4) и (10) $t_2 \mid t_1$, откуда на основании формулы (3) вытекает включение

$$\overline{M(t_1)} \subseteq \overline{M(t_2)}. \tag{13}$$

Используя формулы (12), (13) и перечисленные выше свойства функции h, получим следующую цепочку соотношений:

$$h(A') + \log |S_i| = h(A') + h(\{i\}) \geq h(A' \cup \{i\}) = h(\overline{M(t_2)} \cup A' \cup \{i\}) - \log t_2 \geq$$
$$\geq h(\overline{M(t_1)} \cup A') - \log t_2 = h(A') + \log t_1 - \log t_2 = h(A') + \log(t_1/t_2).$$

Итак, $\log |S_i| \geq \log(t_1/t_2)$, следовательно, выполняется неравенство (9).

Убедимся теперь в справедливости неравенства (11). Заметим, что в силу соотношений (4), (8) $P \in \widetilde{\Psi}_1$; следовательно, на основании формулы (6)

$$h(P \cup \{n+1\}) = h(P \cup M(1) \cup \{n+1\}) = h(P \cup M \cup \{n+1\}). \tag{14}$$

Кроме того, согласно условию (а) определения ПМРС с МС, выполняется равенство

$$h(P \cup M) = h(P) + \log m. \tag{15}$$

Используя формулы (14), (15) и свойства 1) – 3) функции h, получим, что

$$h(P) + \log |S_{n+1}| = h(P) + h(\{n+1\}) \geq h(P \cup \{n+1\}) =$$
$$= h(P \cup M \cup \{n+1\}) \geq h(P \cup M) = h(P) + \log m.$$

Итак, $\log |S_{n+1}| \geq \log m$, что и требовалось доказать.

Лемма доказана.

Следующая теорема устанавливает достаточные условия оптимальности линейных протоколов множественного разделения секрета с многоадресным сообщением.

Теорема. Пусть G – матрица вида (1) над кольцом R, удовлетворяющая следующим условиям:

а) $G_i \notin D(R)^{(k+1)}$, $i \in P$;

б) для любого $i \in P$ существует множество $A \subseteq P$ такое, что

$$G_0 \in \left\langle G_{A \cup \{i, n+1\}} \right\rangle_R, \; \left\langle G_0 \right\rangle_R \cap \left\langle G_{A \cup \{n+1\}} \right\rangle_R = \{0\}. \tag{16}$$

Тогда ПМРС с МС $\rho(G)$ является оптимальным в классе $\Omega(S_0, \widetilde{\Psi})$.

Доказательство. Заметим, что из условия б) теоремы следует справедливость формулы (8). Кроме того, в силу равенства (4) соотношения (16) равносильны соотношениям $A \cup \{i\} \in \widetilde{\Psi}_1$, $A \in \widetilde{\Psi}_m$. Отсюда на основании утверждения леммы вытекает, что для любого ПМРС с МС $\Sigma \in \Omega(S_0, \widetilde{\Psi})$, заданного множеством $L \subseteq S_0 \times S_1 \times \ldots \times S_{n+1}$, справедливы неравенства

$$\log |S_i| \geq \log m\,,\ i \in P \cup \{n+1\}\,.$$

Следовательно,

$$\rho^{\Sigma} = \frac{\log |S_0|}{\max\limits_{i \in P} \log |S_i|} \leq 1\,,\ \rho_{\mathrm{M}}^{\Sigma} = \frac{\log |S_0|}{\log |S_{n+1}|} \leq 1\,,$$

и для завершения доказательства остается воспользоваться равенствами (5), справедливыми в силу условия а).

Теорема доказана.

Отметим, что условия а) и б) теоремы гарантируют более сильное по сравнению с оптимальностью свойство ПМРС с МС $\rho(G)$. Действительно, как показано выше, при выполнении этих условий длина каждого из сообщений B, s_i ($i \in P$), передаваемых участникам протокола $\rho(G)$, принимает наименьшее возможное значение $\log m$ (в классе всех ПМРС с МС $\Sigma \in \Omega(S_0, \widetilde{\Psi})$). При этом оптимальность протокола $\rho(G)$ равновильна лишь условию минимальности длины сообщения B и наибольшей из длин сообщений s_i, $i \in P$ (в том же классе ПМРС с МС).

III Конструкции оптимальных протоколов множественного разделения секрета с многоадресным сообщением

Приведем примеры матриц, удовлетворяющих условиям а), б) теоремы. Для простоты изложения ограничимся случаем примарного кольца вычетов $R = \mathbf{Z}/(p^d)$, где p – простое чило, $d \geq 1$. Обобщение описанных ниже конструкций ПМРС с МС на произвольные кольца вычетов не представляет затруднений.

Утверждение 1. Пусть $k \geq 2$, Q – $(k-1) \times n'$-матрица над кольцом R, каждый столбец которой отличен от нуля по модулю p, $n = 2n'$. Тогда $(k+1) \times (n+2)$-матрица

$$G = \left(\begin{array}{c|ccc|ccc|c} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 \\ \hline 0 & 1 & \cdots & 1 & 0 & \cdots & 0 & -1 \\ \hline 0 & & & & & & & 0 \\ \vdots & & Q & & & Q & & \vdots \\ 0 & & & & & & & 0 \end{array}\right) \qquad (17)$$

удовлетворяет условиям а) и б) теоремы.

Доказательство. Ясно, что матрица (17) удовлетворяет условию а), поэтому остается проверить выполнение условия б).

Пусть, как и выше, G_i обозначает i-й столбец матрицы G, $i \in \overline{0, n+1}$. Заметим, что

$$G_0 = G_i - G_{i+n'} + G_{n+1}\,,\ i \in \overline{1, n'}\,.$$

Далее, из условия утверждения следует, что для любого $i \in \overline{1, n'}$ системы векторов (G_0, G_i, G_{n+1}) и $(G_0, G_{i+n'}, G_{n+1})$ линейно независимы над кольцом R.

Пусть теперь $i \in \overline{1, n}$. Положим

$$A = \begin{cases} \{i + n'\}, \text{ åñëè } & i \in \overline{1, n'}; \\ \{i - n'\}, \text{ åñëè } & i \in \overline{n'+1, n}. \end{cases}$$

Тогда на основании вышеизложенного для указанных i и A выполняются соотношения (16).

Утверждение доказано.

Утверждение 2. Пусть $H = \left(h_{i,j}\right)_{i \in \overline{1,k},\, j \in \overline{k,n}}$ – матрица размера $k \times (n+1-k)$ над кольцом R, удовлетворяющая следующим условиям:

1) $h_{1,j} \in R^*$ для любого $j \in \overline{k,n}$;

2) для любого $l \in \overline{2,k}$ существует $j \in \overline{k,n}$ такое, что $h_{l,j} \in R^*$.

Обозначим I_{k-1} единичную матрицу порядка $k-1$ над кольцом R. Тогда $(k+1)\times(n+2)$-матрица

$$G = \left(\begin{array}{c|ccccc|ccc|c} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 \\ \hline 0 & 0 & \cdots & 0 & 0 & & & & -1 \\ \vdots & & & & & & H & & 0 \\ \vdots & & & I_{k-1} & & & & & \vdots \\ 0 & & & & & & & & 0 \end{array}\right) \tag{18}$$

удовлетворяет условиям а) и б) теоремы.

Доказательство. По условию утверждения каждый столбец матрицы (18) содержит обратимые элементы кольца R. Следовательно, выполняется условие а) теоремы. Убедимся в справедливости условия б).

Пусть $i \in \overline{k,n}$. Из формулы (18) следует равенство

$$G_i = \sum_{s=1}^{k-1} G_s h_{s+1,i} + (G_0 - G_{n+1}) h_{1,i},$$

которое в силу обратимости элемента $h_{1,i}$ может быть записано в виде

$$G_0 = -\sum_{s=1}^{k-1} G_s h_{s+1,i} h_{1,i}^{-1} + G_i h_{1,i}^{-1} + G_{n+1} h_{1,i}^{-1}. \tag{19}$$

Положим $A = \{1, 2, \ldots, k-1\}$. На основании формулы (19) для указанных i и A выполняется первое из соотношений (16). С другой стороны, поскольку векторы $G_0, G_1, \ldots, G_{k-1}, G_{n+1}$ линейно независимы над кольцом R, то справедливо второе из этих соотношений.

Рассмотрим теперь случай, в котором $i \in \overline{1,k-1}$. По условию утверждения существует $j \in \overline{k,n}$ такое, что $h_{i+1,j} \in R^*$. Положим $A = (\{1, 2, \ldots, k-1\} \setminus \{i\}) \cup \{j\}$. На основании формулы (18) выполняется равенство $G_j = \sum_{s=1}^{k-1} G_s h_{s+1,j} + (G_0 - G_{n+1}) h_{1,j}$, где $h_{1,j} \in R^*$. Отсюда непосредственно следует справедливость для данных i и A первого из соотношений (16).

Докажем второе из этих соотношений. Предположим противное: пусть существуют элементы $u_0 \in R \setminus \{0\}$, $u_\nu \in R$, где $\nu \in A \cup \{n+1\}$, такие, что

$$u_0 G_0 = \sum_{\nu \in A \cup \{n+1\}} u_\nu G_\nu. \tag{20}$$

Из формул (18) и (20) вытекает равенство

$$\left(u_0, 0, \ldots, 0\right) = \left(0, u_1, \ldots, u_{i-1}, 0, u_{i+1}, \ldots, u_{k-1}\right) + u_j \left(h_{1,j}, \ldots, h_{i+1,j}, \ldots, h_{k,j}\right), \tag{21}$$

из которого следует, что $u_j h_{i+1,j} = 0$. В силу обратимости элемента $h_{i+1,j}$ в кольце R имеем $u_j = 0$. Но тогда в силу равенства (21) $u_0 = 0$. Итак, для данных i, A выполняется второе из соотношений (16), что и требовалось доказать.

Утверждение 3. Пусть G – матрица вида (1), где $g_{0,n+1}=1$, а столбцы $G'_1,\ldots,G'_n$ матрицы G' и вектор $g^{\downarrow}_{n+1}$ удовлетворяют следующему условию: для любого $i\in\overline{1,n}$ существует множество $A=\{i_1,\ldots,i_{k-1}\}\subseteq P$ такое, что системы векторов

$$\left(g^{\downarrow}_{n+1},G'_{i_1},\ldots,G'_{i_{k-1}}\right), \tag{22}$$

$$\left(G'_{i_1},\ldots,G'_{i_{k-1}},G'_i\right) \tag{23}$$

являются линейно независимыми над кольцом R. Тогда для матрицы G выполняются условия а) и б) теоремы.

Доказательство. В силу линейной независимости системы (22) $g^{\downarrow}_{n+1}\notin\left\langle G'_{i_1},\ldots,G'_{i_{k-1}}\right\rangle_R$, откуда следует справедливость второго соотношения (16) для данных i и A. Далее, в силу линейной независимости системы (23) ее элементы образуют базис модуля $R^{(k)}$. Следовательно, $g^{\downarrow}_{n+1}\in\left\langle G'_{i_1},\ldots,G'_{i_{k-1}},G'_i\right\rangle_R$ и, значит, выполняется первое соотношение (16).

Утверждение доказано.

Отметим, что последнее утверждение позволяет проверять выполнение условий а) и б) теоремы для данной матрицы G непосредственно по ее гомоморфному образу $\overline{G}=G\,(\mathrm{mod}\,p)$ над полем вычетов $\overline{R}=\mathbf{GF}(p)$ кольца $R=\mathbf{Z}/(p^d)$. Действительно, нетрудно убедиться в том, что произвольные векторы $A_1,\ldots,A_l\in R^{(k)}$ линейно независимы тогда и только тогда, когда линейно независимы их образы $\overline{A_1},\ldots,\overline{A_l}$ при отображении, индуцированном естественным гомоморфизмом кольца R в поле $\overline{R}$. Следовательно, линейная независимость каждой из систем (22), (23) равносильна условию

$$\left\langle\overline{g}^{\downarrow}_{n+1},\overline{G'}_{i_1},\ldots,\overline{G'}_{i_{k-1}}\right\rangle_{\overline{R}}=\left\langle\overline{G'}_{i_1},\ldots,\overline{G'}_{i_{k-1}},\overline{G'}_i\right\rangle_{\overline{R}}=\overline{R}^{(k)}. \tag{24}$$

В качестве примера, иллюстрирующего применение утверждения 3, рассмотрим матрицу G вида (1) такую, что $g_{0,n+1}=1$, а $(\overline{G'},\overline{g}^{\downarrow}_{n+1})$ – проверочная матрица кода Хэмминга с числом проверочных символов k над полем $\overline{R}=\mathbf{GF}(p)$. Напомним (см., например, [17], с. 596), что в этом случае столбцами матрицы $(\overline{G'},\overline{g}^{\downarrow}_{n+1})$ являются все ненулевые попарно непропорциональные k-мерные векторы над данным полем, число которых равно $n+1=(p^k-1)/(p-1)$. Покажем, что рассматриваемая матрица G удовлетворяет условиям а) и б) теоремы.

Действительно, пусть $i\in\overline{1,n}$. Тогда существует $(k-1)$-мерное подпространство W_{k-1} векторного пространства $\overline{R}^{(k)}$, не содержащее векторов $\overline{g}^{\downarrow}_{n+1}$, $\overline{G'}_i$. Поскольку столбцами матрицы $(\overline{G'},\overline{g}^{\downarrow}_{n+1})$ являются все попарно непропорциональные k-мерные векторы над полем $\overline{R}$, то существует множество $A=\{i_1,\ldots,i_{k-1}\}\subseteq P$ такое, что векторы $\overline{G'}_{i_1},\ldots,\overline{G'}_{i_{k-1}}$ образуют базис пространства W_{k-1}. Отсюда на основании соотношений $\overline{g}^{\downarrow}_{n+1}\notin W_{k-1}$, $\overline{G'}_i\notin W_{k-1}$ следует справедливость равенств (24).

Итак, согласно утверждению 3 и теореме из п. II, матрица G вида (1), построенная по коду Хэмминга над полем $\mathbf{GF}(p)$, задает оптимальный протокол множественного разделения секрета с многоадресным сообщением.

Заключение

В настоящей статье получены достаточные условия оптимальности ПМРС с МС (см. теорему в п. 2) в классе всех протоколов множественного разделения секрета с многоадресным сообщением, реализующих данную

иерархию доступа. Предложены также конструкции линейных ПМРС с МС над примарными кольцами вычетов, для которых выполняются полученные условия (утверждения 1 – 3).

Применение оптимальных протоколов разделения секрета при построении подсистем управления доступом современных информационно-телекоммуникационных систем позволит повысить надежностные и эксплуатационные характеристики данных систем, а, значит, и уровень защищенности информации в таких системах в целом [5, 6].

Литература: ***1.*** *НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***2.*** *ISO/IEC 15408:2000 – Information technologies – Security techniques – Evaluation criteria for IT security.* ***3.*** *НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***4.*** *McLean J. Reasoning about security models // Proceeding IEEE Symposium on privacy and security. – IEEE Computer Society Press. – 1987. – P. 123-131.* ***5.*** *Zhu B. B., Feng M., Li S. An efficient key scheme for layered access control of MPEG-4 FGS Video // ICME. – 2004. – P. 443 – 446.* ***6.*** *Wu J., Wei R. An access control scheme for partially ordered set hierarchy with probable security // Cryptology ePrint Archive. – Report. – 2004/295.* ***7.*** *Sklavos N., Koufopavlou O. Access control in network hierarchy: implementation of key management protocol // International Journal of Network Security. – 2005. – Vol.1. – № 2. – P.103 – 109.* ***8.*** *Алексейчук А. Н., Волошин А. Л. Схема разделения нескольких секретов с многоадресным сообщением на основе линейных преобразований над кольцом вычетов по модулю m // Реєстрація, зберігання і обробка даних. – 2006. – Т. 8. – № 1. – С. 92 – 102.* ***9.*** *Алексейчук А. Н., Волошин А. Л. Аналитическое описание конструкций протоколов множественного разделения секрета с многоадресным сообщением, реализующих заданную иерархию доступа // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 3. – С. 391 – 396.* ***10.*** *Волошин А. Л. Метод построения совершенных протоколов множественного разделения секрета с многоадресным сообщением, реализующих семейства иерархий доступа, для подсистем управления доступом информационно-телекоммуникационных систем // Захист інформації. – 2007. – № 3. – С.88 – 94.* ***11.*** *Brickell E. F. Some ideal secret sharing schemes // J. Combin. Math. and Combin. Comput. – 1989. – № 9. – P. 105 – 113.* ***12.*** *Van Dijk M. A linear construction of perfect secret sharing schemes // Advances in Cryptology – EUROCRYPT'94. – Lecture Notes in Comput. Science. – V. 950. – P. 23 – 34.* ***13.*** *Ashikhmin A., Barg A. Minimal vectors in linear codes // IEEE Trans. on Inform. Theory. – 1998. – V. 5. – P. 2010 – 2018.* ***14.*** *Blundo C., Cresti A., de Santis A., Vaccaro U. Fully dynamic secret sharing schemes // Advances in Cryptology – CRYPTO'93. – Proceedings. – Springer Verlag, 1994. – P. 110 –125.* ***15.*** *Brickell E. F., Davenport D. M. On the classification of ideal secret sharing schemes // J. Cryptology. – 1991. – № 4. – P. 123 – 134.* ***16.*** *Блейкли Р. Г., Кабатянский Г. А. Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. – 1997. – Т. 33. – Вып. 3. – С. 102 – 110.* ***17.*** *Лидл Р., Нидеррайтер Г. Конечные поля: В 2 т. / Пер. с англ. – М.: Мир, 1988. – 818 с.*

УДК 621.391:519.2

КАСКАДНА СХЕМА ФЕЙСТЕЛЯ ТА ЇЇ СТІЙКІСТЬ ДО ДИФЕРЕНЦІАЛЬНОГО ТА ЛІНІЙНОГО КРИПТОАНАЛІЗУ

Сергій Яковлєв
Фізико-технічний інститут НТУУ "КПІ"

Анотація: **Запропоновано та проаналізовано нову конструкцію блочних шифрів – каскадну схему Фейстеля, виведені оцінки її стійкості до диференціального та лінійного криптоаналізу.**

Summary: **New construction of block ciphers' design, a cascade Feistel network, is proposed and analysed, its resistance to differential and linear cryptanalysis is evaluated.**

Ключові слова: **Блочний шифр, схема Фейстеля, диференціальний криптоаналіз, лінійний криптоаналіз.**

І Вступ

Запропонована ще у 1971 році схема Фейстеля [1] – один з найпоширеніших в наш час варіантів побудови блочних шифрів. Проста для криптоаналізу та зручна в реалізації схема Фейстеля лягла в основу таких відомих алгоритмів, як DES, Blowfish та ГОСТ 28147-89.

Однією з властивостей схеми є те, що за один раунд обробляється лише половина блоку даних; наприклад, для 64-бітового блоку за раунд обробляється тільки 32 біти. Це дозволяло ефективно