5. Жданов А.А. О методе автономного адаптивного управления. Научная сессия МИФИ – 2004. VI Всероссийская научно-техническая конференция «Нейроинформатика - 2004»: Лекции по нейроинформатике. Часть 2. – М.: МИФИ, 2004. – 200 с.
6. Осовецкий Л.Г., Нестерук Г.Ф., Бормотов В.М. К вопросу иммунологии сложных информационных систем // Изв.вузов. Приборостроение. – 2003. - Т.46, №7. - С.34-40.
7. Кобозева А.А., Хорошко В.А. Модель системы защиты информации, основанная на принципах естественной системы управления // «Захист інформації». – 2007. - Спецвипуск, с.56-62.
8. Кобозева А.А., Хорошко В.А. Методика оценки адекватности системы защиты информации // Вісник ДУІКТ. – 2007. – т.5, №3. – С. 328-334.
9. Каханер Д., Моулер К., Нэш С. Численные методы и программное обеспечение. – М.: Мир, 2001. – 575 с.
10. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы.- М.: БИНОМ. Лаборатория знаний, 2006 г.-636 с.
11. Кобозева А.А. Sign-чувствительность и ее использование в стеганографических алгоритмах // Вестник Херсонского национального технического университета. - 2007. - №2(28). - С. 142-146.
12. Кобозева А.А., Борисенко И.И. Практическая реализация стеганографического метода, основанного на решении системы линейных алгебраических уравнений // «Праці УНДІРТ». – 2006. - №3(47). - С. 78-83.
13. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. - 430 с.
14. Г.М. Фихтенгольц. Курс дифференциального и интегрального исчисления. – М.: Наука, 1969.

Поступила 20.03.2008г.

УДК 621.391:519.7:510.5

А. Л. Волошин

МЕТОДИКА ФОРМИРОВАНИЯ МАТРИЦ НАД КОЛЬЦАМИ ВЫЧЕТОВ ДЛЯ ПОСТРОЕНИЯ ЛИНЕЙНЫХ ПРОТОКОЛОВ МНОЖЕСТВЕННОГО РАЗДЕЛЕНИЯ СЕКРЕТА С МНОГОАДРЕСНЫМ СООБЩЕНИЕМ ДЛЯ ЗАДАННОЙ ИЕРАРХИИ ДОСТУПА

Введение

Протокол разделения секрета (ПРС) представляет собой криптографический протокол, позволяющий “разделить” некоторый секретный параметр (секрет) среди множества участников протокола таким образом, чтобы только некоторые, заранее определенные (разрешенные) коалиции участников могли восстановить его значение при объединении хранящейся у них индивидуальной секретной информации (проекций секрета). Протокол разделения секрета называется совершенным, если участники запрещенных коалиций не могут получить никакой апостериорной информации о значении секрета из имеющихся у них проекций [1].

Свойства и способы построения протоколов разделения единственного секрета интенсивно изучались, начиная с 1979 года, в [2 – 9] и ряде других работ. В силу простоты схемно-технической реализации и вычислительной эффективности особый интерес исследователей вызвали конструкции линейных ПРС, основанных на линейных (над конечными полями, кольцами вычетов и т.д.) математических преобразованиях (см., например, работы [4 – 9]).

Естественным обобщением ПРС на случай нескольких секретов являются протоколы множественного разделения секрета (ПМРС), впервые введенные в статье [10] и формально

описанные в работе [11]. Данный вид протоколов позволяет решать более разнообразный, по сравнению с ПРС, спектр задач, связанных с разграничением доступа к ресурсам информационно-телекоммуникационных систем (ИТС), и имеет более широкую сферу практического применения [10].

Дальнейшим развитием ПРС стали протоколы разделения секрета с многоадресным сообщением, которые, наряду с традиционными свойствами ПМРС, осуществляют заблаговременное распределение секретной информации участникам без риска несанкционированного восстановления секретов и при этом допускают изменение (в определенных пределах) состава разрешенных коалиций участников [12 – 14]. Известно, что применение протоколов разделения секрета, обладающих всеми приведенными выше свойствами (совершенных линейных протоколов множественного разделения секрета с многоадресным сообщением), при построении подсистем управления доступом современных ИТС позволяет, как правило, существенно повысить уровень защищенности их информационных ресурсов [15, 16]. В то же время, задача построения таких протоколов разделения секрета для заданной иерархии доступа на сегодняшний день, судя по известным публикациям [11 – 15], не решена.

В [17, 18] предложен метод построения совершенных линейных ПМРС над кольцами вычетов целых чисел. Показано также (см. [17]), что матрица, задающая ПМРС над произвольным кольцом вычетов, может быть построена из матриц, задающих протоколы множественного разделения секрета над кольцами примарного порядка, входящими в разложение исходного кольца в прямое произведение колец. Позднее в статье [19] предложена конструкция совершенных линейных ПМРС с многоадресным сообщением, а в [20] получено аналитическое описание указанных протоколов разделения секрета, реализующих заданную иерархию доступа, и установлена связь между этими протоколами и ПМРС, описанными в [17]. Наконец, в работе [21] предложен алгоритм формирования матриц над примарными кольцами вычетов, используемых для построения протоколов множественного разделения секрета, реализующих заданную иерархию доступа.

Данная статья имеет целью разработку методики формирования матриц над кольцами вычетов целых чисел, необходимых для построения совершенных линейных ПМРС с многоадресным сообщением, реализующих заданную иерархию доступа, и оценку эффективности этой методики. Первая задача решается на основе синтеза результатов, полученных в статьях [17 – 21], вторая – путем сравнения вычислительных сложностей предложенной и тривиальной (переборной) методик; обе эти задачи, по сути, завершают начатые в статьях [17 – 21] исследования.

1. Основные понятия, обозначения и вспомогательные результаты

Пусть даны различные простые числа $p_1, \ldots, p_w$ и натуральные числа $d_1, \ldots, d_w$. Положим $m = p_1^{d_1} \cdots p_w^{d_w}$, $R = \mathbf{Z}/(m)$, $R_j = \mathbf{Z}/(p_j^{d_j})$, $j \in \overline{1,w}$,

$$S_0 = \{(s_{ij}): s_{ij} \in \{0, 1, \ldots, p_j - 1\}, i \in \overline{0,d_j - 1}, j \in \overline{1,w}\}. \quad (1)$$

Обозначим R^* и $D(R) = R \setminus R^*$ соответственно множество обратимых элементов и множество делителей нуля кольца R.

Для любого $A \subseteq P \cup \{0\}$ обозначим символом G_A подматрицу матрицы G, состоящую из ее столбцов с номерами из множества A. Для любой матрицы U над кольцом R обозначим $M(U)$ R-модуль, порожденный строками матрицы U, $\langle U \rangle_R$ – R-модуль, порожденный столбцами матрицы U. Символом $\#M$ обозначим мощность произвольного конечного множества M, а символом $\mathfrak{I}^0$ – совокупность минимальных элементов конечного частично упорядоченного множества $\mathfrak{I}$.

Зафиксируем матрицу

$$G = \left(\begin{array}{c|ccc|c} 1 & 0 & \Lambda & 0 & g_{0,n+1} \\ \hline 0 & & & & \\ \mathrm{M} & & G' & & g_{n+1}^{\downarrow} \\ 0 & & & & \end{array}\right), \qquad (2)$$

размера $(k+1)\times(n+2)$ над кольцом R ($k, n \geq 2$), где $g_{0,n+1} \in R^*$, $g_{n+1}^{\downarrow} \notin D(R)^{(k)}$. Согласно [19], матрице G вида (2) ставится в соответствие ПМРС с многоадресным сообщением $\rho(G)$, реализующий распределение наборов секретов $(s_{ij}) \in S_0$, $i \in \overline{0, d_j - 1}$, $j \in \overline{1, w}$, участникам, принадлежащим множеству $P = \{1, 2, \ldots, n\}$. Иерархией доступа протокола $\rho(G)$ называется совокупность множеств $\widetilde{\Psi} = \{\widetilde{\Psi}_t : t \mid m\}$ таких, что для любого делителя $t = p_1^{l_1} \cdots p_w^{l_w}$ числа m ($0 \leq l_j \leq d_j$, $j \in \overline{1, w}$) любая коалиция участников $A \in \widetilde{\Psi}_t$ не получит никакой апостериорной информации о секретах s_{ij} с номерами $d_j - l_j < i \leq d_j - 1$, $j \in \overline{1, w}$ и полностью восстановит секреты s_{ij} с номерами $0 \leq i \leq d_j - l_j$, $j \in \overline{1, w}$. В [19] показано, что для любого делителя t числа m справедливо равенство

$$\widetilde{\Psi}_t = \{A \subseteq P : tR = I_G(A)\}, \qquad (3)$$

где

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

Пусть теперь задана совокупность $\Psi = \{\Psi_t : t \mid m\}$ попарно непересекающихся подмножеств Ψ_t множества 2^P (случай $\Psi_t = \varnothing$ не исключается) таких, что $\bigcup_{t \mid m} \Psi_t = 2^P$. Необходимо разработать методику формирования матрицы G вида (2), удовлетворяющей условию $\widetilde{\Psi}_t = \Psi_t$ для всех $t \mid m$, где множество $\widetilde{\Psi}_t$ определяется по формуле (3). Другими словами, указанная методика должна позволять выяснять, существует ли матрица G, задающая ПМРС с многоадресным сообщением для данной совокупности множеств Ψ, и, в случае положительного ответа, строить эту матрицу в явном виде.

Заметим, что для решения поставленной задачи можно предложить тривиальную (переборную) методику, которая состоит в опробовании всех матриц вида (2) над кольцом R и проверке для каждой из них выполнения указанного условия для всех $A \in \Psi_t^0$, $t \mid m$. Оценка трудоемкости алгоритма реализации этой методики приведена в п. 3.

Приведем ряд вспомогательных обозначений. Для любых $j \in \overline{1, w}$, $l \in \overline{0, d_j}$ обозначим $D_{lj}(m)$ множество делителей t числа m, представимых в виде $t = p_j^{\,l}\tau$, где τ не делится на p_j. Введем в рассмотрение множества

$$\Psi_l^{(j)} = \bigcup_{t \in D_{lj}(m)} \Psi_t, \; j \in \overline{1, w}, \; l \in \overline{0, d_j}. \qquad (4)$$

Положим $\Psi^{(j)} = \{\Psi_l^{(j)} : l \in \overline{0, d_j}\}$, $j \in \overline{1, w}$. Для удобства обозначим $\mu_l^{(j)} = \left(\bigcup_{i=0}^{l} \Psi_i^{(j)}\right)^0 = \left(\bigcup_{i=0}^{l} \bigcup_{t \in D_{ij}(m)} \Psi_t\right)^0$ и пусть $\mu^{(j)} = \{\mu_l^{(j)} : l \in \overline{0, d_j}\}$, $j \in \overline{1, w}$.

Отметим, что, согласно введенным выше обозначениям, условие $A \in \mu_l^{(j)}$ означает, что множество A является минимальным (относительно включения) элементом совокупности всех коалиций участников, которые при объединении своих проекций и получении многоадресного сообщения могут восстановить секреты s_{ij} с номерами $0 \leq i \leq d_j - l - 1$ и, возможно, некоторые другие секреты из набора $(s_{ij}) \in S_0$, где множество S_0 имеет вид (1), $l \in \overline{0, d_j - 1}$, $j \in \overline{1, w}$.

регламентується і досягається наданням та дотриманням комплексу послуг фізичної безпеки за рекомендаціями і вимогами наступних міжнародних і вітчизняних документів з метою попередження професійних захворювань та підвищення рівня фізичної безпеки при використанні персональних комп'ютерів [8-14].

1. Міжнародні рекомендації і довідкові дані щодо відомих основних факторів впливу роботи за комп'ютером на фізичний стан здоров'я людини (монітор, клавіатура, види полів випромінювання комп'ютера від електростатичних до таємних торсіонних, які поки що залишаються мало вивченими, але дуже загрозливими, безпечні рівні випромінювання, огляд стану фізичної безпеки в різних країнах тощо).

2. Вимоги і рекомендації щодо рівнів електромагнітних випромінювань моніторів, що вважаються безпечними для здоров'я, які регламентуються нормами MPR II 1990:10 Шведського національного комітету з вимірами і випробуванням. Вони вважаються базовими і більш жорсткими нормами, чим TCO 92, 95 Шведської конфедерації профспілок [10].

3. Російський нормативний документ Держкомсанепідемнадзора "Гигиенические требования к видеодисплейным терминалам и ВЭВМ и организация работ. Санитарные нормы и правила". Санітарні правила й норми, що вступили в силу із січня 1997 р., повністю збігаються в частині рівнів ПЕМВН з вимогами MPR II. У Росії донедавна існував ряд документів, що містили норми побічних електромагнітних випромінювань і наведень (ПЕМВН).

4. Правила охорони праці під час експлуатації електронно-обчислювальних машин, затверджені наказом Міністерства праці та соціальної політики України від 10.02.99р. № 21. З метою впровадження вимог цих Правил охорони праці у кожному Міністерстві розроблюється та затверджується Типова інструкція з охорони праці для працюючих з персональними комп'ютерами. Дія такої інструкції поширюється на користувачів персональних комп'ютерів (ПК), які за умовами їх праці зчитують текстову або іншу інформацію з екрана відеодисплея (ВД) на підприємствах, установах, в організаціях, закладах освіти, військових частинах (далі – підрозділи міністерств). Списки користувачів ПК повинні бути затверджені керівником підрозділу.

Коротко прокоментуємо найбільш суттєві рекомендації цих документів. Російський Науково-дослідний інститут охорони праці провів медико-біологічні дослідження впливу ПК на операторів. Дані таблиці 1 ілюструють результати цих досліджень [10].

Справедливості заради, слід зазначити, що існує думка й про відсутність впливу комп'ютерів на здоров'я. Але все вищесказане переконливо підтверджує існування так званого феномена комп'ютерного стресу. Цієї ж думки дотримується й А.В. Бобров і В.П. Скарбников, які затверджують, що торсіонні поля - основа інформаційних взаємодій у біології [10] .

Таблиця 1

Припустимі рівні випромінювань моніторів ПК

Види поля	TCO	MPR	Нормативи Росії
Електричне поле	(+ -) 500	(+ -) 500	1500-2000 В/м на робочому місці
Змінне електричне поле 5 Гц-2 кгц 2-400 кгц	10 В/м, на відстані 0,3 м від центра екрана й 0,5 м навколо монітора	25 В/м, 2,5 В/м на відстані 0,5 м навколо монітора	500 В/м, 50 В/м на робочому місці
Змінне магнітне поле 5 Гц-2 кгц 2-400 кгц	250 нТл, 200 мА/м, 25 нТл, 20 ма/м на відстані 0,3 м від центра екрана і 0,5 м навколо монітора	250 нТл, 200 ма/м, 25 нТл, 20 ма/м на відстані 0,5 м навколо монітора	1,4 кА/м, 5000 мА/м на робочому місці

В [20] доказана следующая теорема, позволяющая свести проверку существования матрицы G вида (2), удовлетворяющей условию $\widetilde{\Psi}_t = \Psi_t$ для всех $t \mid m$, где множество $\widetilde{\Psi}_t$ определяется по формуле (3), к проверке существования некоторой другой матрицы H над кольцом R и указать способ построения искомой матрицы G по матрице H.

Теорема 1 [20]. Пусть существует $k\times(n+1)$-матрица

$$H = \left(h^{\downarrow}, H'\right) \tag{5}$$

над кольцом R такая, что

$$h^{\downarrow} \notin D(R)^{(k)}, \tag{6}$$

и для любых $t \mid m$, $A \in \Psi_t$ выполняется равенство

$$\#M(H_{A\cup\{0\}}) = \#M(H_A)t. \tag{7}$$

Тогда существует ПМРС с многоадресным сообщением $\rho(G)$, реализующий совокупность Ψ в качестве иерархии доступа, где матрица G имеет вид

$$G = \left(\begin{array}{c|ccc|c} 1 & 0 & \Lambda & 0 & 1 \\ \hline 0^{\downarrow} & & H' & & h^{\downarrow} \end{array}\right). \tag{8}$$

Справедливо также обратное утверждение.

Следующая теорема, доказанная в [17], устанавливает необходимые и достаточные условия существования матрицы H вида (5), удовлетворяющей условиям (6), (7) для всех $t \mid m$, $A \in \Psi_t$. С целью дальнейшего применения, сформулируем ее ниже в следующем, эквивалентном по отношению к исходному, виде.

Теорема 2 [17]. Матрица H вида (5) над кольцом R, удовлетворяющая условиям (6), (7) для всех $A \in \Psi_t$, $t \mid m = p_1^{d_1} \cdots p_w^{d_w}$, существует тогда и только тогда, когда для любого $j \in \overline{1,w}$ существует $k\times(n+1)$-матрица $H^{(j)}$ над кольцом $R_j = \boldsymbol{Z}/(p_j^{d_j})$ такая, что для любых $l \in \overline{0,d_j}$, $A \in \Psi_l^{(j)}$ выполняется равенство

$$\Psi_l^{(j)} = \{A \subseteq P:\ p_j^l R_j = I_{H^{(j)}}(A)\}, \tag{9}$$

где

$$I_{H^{(j)}}(A) = \{r \in R_j :\ rH_0^{(j)} \in \left\langle H_A^{(j)} \right\rangle_{R_j}\},\ A \subseteq P.$$

При этом матрицы $H^{(j)}$, $j \in \overline{1,w}$, связаны с матрицей H соотношениями

$$H^{(j)} \equiv H \pmod{p_j^{d_j}},\ j \in \overline{1,w}. \tag{10}$$

Задача формирования матриц $H^{(j)}$, $j \in \overline{1,w}$, по совокупности множеств $\mu^{(j)}$, $j \in \overline{1,w}$, решена в [21], где описан алгоритм, позволяющий для любого $j \in \overline{1,w}$ проверять существование матрицы $H^{(j)}$ над кольцом R_j, удовлетворяющей условию (9) для всех $l \in \overline{0,d_j}$, $A \in \Psi_l^{(j)}$, и, в случае существования, строить эту матрицу в явном виде. Отметим также, что связь между совокупностями множеств $\mu^{(j)}$, $j \in \overline{1,w}$, и $\Psi = \{\Psi_t : t \mid m\}$ описывается соотношением (4).

Далее в статье излагается и обосновывается методика, позволяющая по заданной совокупности множеств $\mu^{(j)}$, $j \in \overline{1,w}$, строить в явном виде (при условии существования) искомую матрицу G, а также проводится оценка ее эффективности. Описанию самой методики посвящен п. 2, в п. 3 приведены аналитические выражения оценок временной сложности алгоритма ее реализации и результаты оценки эффективности предложенной методики по сравнению с тривиальной (переборной).

2. Формальное описание предлагаемой методики

Методика предназначена для формирования по заданной совокупности множеств $\mu^{(j)}$, $j \in \overline{1,w}$, матрицы G вида (2), удовлетворяющей условию $\widetilde{\Psi}_t = \Psi_t$ для всех $t \mid m$, где множество $\widetilde{\Psi}_t$ определяется по формуле (3), то есть задающей протокол множественного разделения секрета с многоадресным сообщением, который реализует совокупность Ψ в качестве иерархии доступа.

Исходными данными для применения методики являются следующие объекты:

1) множество $P = \{1, 2, \ldots, n\}$ участников протокола разделения секрета;
2) наборы простых чисел $p_1, \ldots, p_w$ и натуральных чисел $d_1, \ldots, d_w$;
3) совокупности $\mu^{(j)}$, $j \in \overline{1,w}$, подмножеств множества P.

Сущность методики заключается в последовательном решении трех вычислительных задач с использованием алгоритмов, разработанных на основе результатов, которые изложены в п. 1. Эти задачи состоят в следующем:

1) формирование для каждого $j \in \overline{1,w}$ матрицы $H^{(j)}$ над кольцом R_j, удовлетворяющей условию (9) для всех $l \in \overline{0,d_j}$, $A \in \Psi_l^{(j)}$, в соответствии с алгоритмом, описанным в [21];

2) нахождение по матрицам $H^{(j)}$, $j \in \overline{1,w}$, матрицы H над кольцом R, удовлетворяющей соотношениям (10);

3) построение матрицы G по матрице H с использованием формул (5), (8).

Алгоритм реализации предлагаемой методики состоит из следующих этапов.

1. С использованием алгоритма, описанного в [21], проверяется существование матриц $H^{(j)}$, $j \in \overline{1,w}$, и проводится их построение (при условии существования). Исходными данными для выполнения этого этапа являются числа n, p_j, d_j и множества $\mu^{(j)}$, $j \in \overline{1,w}$. В результате выполнения будет получен искомый набор матриц $H^{(j)}$, $j \in \overline{1,w}$, либо сделан вывод о том, что для указанных входных данных такого набора не существует. В этом случае не существует и искомой матрицы G, задающей ПМРС для иерархии доступа Ψ.

2. Формируется матрица H вида (5) над кольцом R, удовлетворяющая соотношениям (11). Исходными данными для этого этапа являются полученные выше матрицы $H^{(j)}$, $j \in \overline{1,w}$. Для построения матрицы H можно использовать известный алгоритм решения систем линейных сравнений вида (10) (см., например, [23], стр. 100).

3. По формуле (8) вычисляется искомая матрица G. Исходными данными для этого этапа является матрица H, полученная на предыдущем этапе.

Таким образом, в результате выполнения изложенного алгоритма либо будет построена матрица G, задающая ПМРС с многоадресным сообщением $\rho(G)$, реализующий данную иерархию доступа Ψ, либо будет установлено, что такой матрицы не существует.

3. Оценка эффективности предложенной методики

Оценим временную сложность алгоритма реализации методики – число элементарных операций (ЭО) (сложения, вычитания, умножения, обращения) в кольце R, которые выполняются в наихудшем случае при построении искомой матрицы G вида (2). В качестве модели вычислительного устройства, используемого для реализации этого алгоритма, примем равнодоступную адресную машину [22].

Введем следующие обозначения [21]. Пусть множество $\mu_l^{(j)}$, $l \in \overline{0,d_j}$, $j \in \overline{1,w}$, имеет вид $\mu_l^{(j)} = \{A_{l,1}^{(j)}, \text{K}, A_{l,r_l}^{(j)}\}$. Обозначим через $M_l^{(j)}$ множество максимальных (относительно включения) элементов дополнения в 2^P к множеству $\mu_l^{(j)}$, $l \in \overline{0,d_j}$,

$j \in \overline{1,w}$; для любого $j \in \overline{1,w}$ положим $\alpha_j = \sum_{l=0}^{d_j-1} \sum_{i=1}^{r_l} \# A_{l,i}^{(j)}$.

Согласно [21], на первом этапе методики для проверки существования и формирования матрицы $H^{(j)}$ для любого $j \in \overline{1,w}$ достаточно выполнить не более

$$\left(6n^2+5n-1\right)\left(p_j^{d_j}-1\right)^{(\alpha_j-n)}\left(d_j\right)^n \sum_{l=0}^{d_j-1} \# M_l^{(j)} + \frac{10n^3-6n^2-n}{3}$$

ЭО. Всего же на первом этапе потребуется выполнить не более

$$\left(6n^2+5n-1\right)\sum_{j=1}^{w}\left(\left(p_j^{d_j}-1\right)^{(\alpha_j-n)}\left(d_j\right)^n \sum_{l=0}^{d_j-1} \# M_l^{(j)}\right) + \frac{w\left(10n^3-6n^2-n\right)}{3}$$

элементарных операций. На втором этапе методики для построения матрицы H (в наихудшем случае размера $n\times(n+1)$) необходимо решить не более n^2+n систем линейных сравнений специального вида над кольцом R (см. формулу (10)). Используя метод, описанный в [23, стр. 100] для решения этой задачи потребуется выполнить не более $n(n+1)w(w+1)(2w+10)/12$ ЭО. Наконец, формирование матрицы G на третьем этапе не требует выполнения арифметических операций. Таким образом, временная сложность алгоритма реализации предложенной методики составляет

$$T = \left(6n^2+5n-1\right)\sum_{j=1}^{w}\left(\left(p_j^{d_j}-1\right)^{(\alpha_j-n)}\left(d_j\right)^n \sum_{l=0}^{d_j-1} \# M_l^{j}\right) + \varphi(n,w) \qquad (11)$$

ЭО, где

$$\varphi(n,w) = \frac{w\left(10n^3-6n^2-n\right)}{3} + \frac{n(n+1)w(w+1)(2w+10)}{12}.$$

Оценим временную сложность алгоритма реализации тривиальной (переборной) методики, упомянутой в п. 1. Отметим, что для его выполнения необходимо в наихудшем случае перебрать все матрицы вида (2) над кольцом R (то есть, в силу неравенства $k \le n$, не более $(m)^{n^2+n+1}$ матриц), для каждой из которых $\sum_{t|m} \# \Psi_t^0$ раз проверить выполнение условия $\widetilde{\Psi}_t = \Psi_t$, где множество $\widetilde{\Psi}_t$ определяется по формуле (3). Проверка указанного условия заключается в решении системы линейных уравнений $G_{A\cup\{n+1\}} x^{\downarrow} = rG_0$, $r \in R$, $x^{\downarrow} \in R^{(\#A+1)}$, $A \subseteq P \cup \{0\}$, над кольцом R, для чего требуется не более $\left(10n^3-6n^2-n\right)/3$ ЭО [23]. Далее, помимо указанных действий необходимо выполнить построение совокупности множеств Ψ_t, $t \mid m$, по совокупности множеств $\mu^{(j)}$, $j \in \overline{1,w}$. Такое построение осуществляется с использованием соотношения (4), при этом арифметические операции в кольце R не выполняются. Таким образом, временная сложность алгоритма выполнения тривиальной (переборной) методики составляет

$$T_{\text{ПЕР}} = (m)^{n(n+1)+1}\left(\frac{10}{3}n^3-2n^2-\frac{1}{3}n\right)\sum_{t|m} \# \Psi_t^0 \qquad (12)$$

ЭО.

Получим нижнюю оценку параметра $\nu = T_{\text{ПЕР}}/T$, характеризующего выигрыш в трудоемкости предложенной методики по сравнению с переборной. На основании равенств (11), (12), а также оценок

$$\sum_{t|m} \# \Psi_t^0 \ge \prod_{j=1}^{w}\left(d_j+1\right) = \left(d_{\text{MIN}}+1\right)^w,$$

$$\sum_{l=0}^{d_j-1} \#M_l^j \le 2^n,\ m \le (p_{\mathrm{MAX}})^{wd_{\mathrm{MAX}}},\ m \ge (p_{\mathrm{MIN}})^{wd_{\mathrm{MIN}}},$$

где $d_{\mathrm{MAX}} = \max_{j\in 1,w}(d_j)$, $d_{\mathrm{MIN}} = \min_{j\in 1,w}(d_j)$ $p_{\mathrm{MAX}} = \max_{j\in 1,w}(p_j)$, $p_{\mathrm{MIN}} = \min_{j\in 1,w}(p_j)$, $\alpha_{\mathrm{MAX}} = \max_{j\in 1,w}(\alpha_j)$, справедливо следующее соотношение

$$v \ge \frac{(p_{\mathrm{MIN}})^{wd_{\mathrm{MIN}}(n^2+n+1)}\left(\frac{10}{3}n^3 - 2n^2 - \frac{1}{3}n\right)(d_{\mathrm{MIN}}+1)^w}{2^n w(6n^2+5n-1)(d_{\mathrm{MAX}})^n\left(p_{\mathrm{MAX}}^{d_{\mathrm{MAX}}}\right)^{(\alpha_{\mathrm{MAX}}-n)} + \varphi(n,w)}. \qquad (13)$$

Ниже, в табл. 1 – 6 приведены результаты численных расчетов десятичного логарифма нижней границы параметра v, полученные с использованием формулы (13) при различных значениях параметров α_{MAX}, p_{MAX}, d_{MAX}, p_{MIN}, d_{MIN}, w, n. При этом в каждой таблице приведены данные, отдельно рассчитанные для $w = 1, 2, 3$.

Таблица 1

Результаты численных расчетов v при $p_{\mathrm{MAX}} = 17$, $p_{\mathrm{MIN}} = 11$, $d_{\mathrm{MAX}} = d_{\mathrm{MIN}} = 2$, $n = 10$

α_{MAX}	4	8	12	16	20	24	28	32
lg$v$ ($w = 1$)	149,63	139,79	129,94	120,10	110,26	100,41	90,57	80,73
lg$v$ ($w = 2$)	151,04	141,19	131,35	121,51	111,66	101,82	91,98	82,13
lg$v$ ($w = 3$)	152,57	142,72	132,88	123,04	113,19	103,35	93,51	83,66
α_{MAX}	36	40	44	48	52	56	60	64
lg$v$ ($w = 1$)	70,88	61,04	51,19	41,35	31,51	21,66	11,82	1,98
lg$v$ ($w = 2$)	72,29	62,44	52,60	42,76	32,91	23,07	13,23	3,38
lg$v$ ($w = 3$)	73,82	63,98	54,13	44,29	34,45	24,60	14,76	4,91

Таблица 2

Результаты численных расчетов v при $p_{\mathrm{MIN}} = 2$, $\alpha_{\mathrm{MAX}} = 15$, $d_{\mathrm{MAX}} = 3$, $d_{\mathrm{MIN}} = 1$, $n = 10$

p_{MAX}	3	5	7	11	13	17
lg$v$ ($w = 1$)	19,52	16,19	14,00	11,05	9,96	8,22
lg$v$ ($w = 2$)	19,82	16,49	14,30	11,35	10,26	8,52
lg$v$ ($w = 3$)	20,24	16,92	14,72	11,78	10,69	8,94
p_{MAX}	19	23	29	31	33	37
lg$v$ ($w = 1$)	7,49	6,25	4,74	4,30	3,90	3,15
lg$v$ ($w = 2$)	7,79	6,55	5,04	4,60	4,20	3,45
lg$v$ ($w = 3$)	8,22	6,97	5,46	5,03	4,62	3,88

Таблица 3

Результаты численных расчетов v при $p_{\mathrm{MAX}} = 17$, $p_{\mathrm{MIN}} = 11$, $\alpha_{\mathrm{MAX}} = 15$, $d_{\mathrm{MIN}} = 1$, $n = 10$

d_{MAX}	2	4	6	8	10
lg$v$ ($w = 1$)	121,15	105,84	91,77	78,22	64,95
lg$v$ ($w = 2$)	122,38	107,07	93,00	79,45	66,18
lg$v$ ($w = 3$)	123,74	108,42	94,36	80,81	67,53
d_{MAX}	12	14	16	18	20

Продолжение таблицы3

lgv ($w = 1$)	51,85	38,88	25,99	13,18	0,41
lgv ($w = 2$)	53,08	40,11	27,22	14,41	1,64
lgv ($w = 3$)	54,44	41,46	28,58	15,76	3,00

Таблица 4

Результаты численных расчетов v при $p_{MAX} = 29$, $\alpha_{MAX} = 15$, $d_{MAX} = 3$, $d_{MIN} = 1$, $n = 10$

p_{MIN}	3	5	7	11
lgv ($w = 1$)	24,41	49,48	66,00	88,18
lgv ($w = 2$)	24,89	50,18	66,84	89,22
lgv ($w = 3$)	25,49	51,01	67,81	90,38
p_{MIN}	13	17	19	23
lgv ($w = 1$)	96,38	109,54	115,00	124,38
lgv ($w = 2$)	97,49	110,77	116,28	125,74
lgv ($w = 3$)	98,73	112,13	117,68	127,22

Таблица 5

Результаты численных расчетов v при $p_{MAX} = 17$, $p_{MIN} = 11$, $\alpha_{MAX} = 15$, $d_{MAX} = 20$, $n = 10$

d_{MIN}	2	4	6	8	10
lgv ($w = 1$)	1,82	4,50	7,11	9,68	12,23
lgv ($w = 2$)	3,23	6,13	8,88	11,56	14,20
lgv ($w = 3$)	4,76	7,88	10,78	13,57	16,29
d_{MIN}	12	14	16	18	20
lgv ($w = 1$)	14,76	17,28	19,80	22,31	24,81
lgv ($w = 2$)	16,80	19,39	21,96	24,52	27,06
lgv ($w = 3$)	18,97	21,62	24,24	26,85	29,44

Таблица 6

Результаты численных расчетов v при $p_{MAX} = 17$, $p_{MIN} = 11$, $d_{MAX} = d_{MIN} = 2$, $\alpha_{MAX} = 15$

n	4	5	6	7	8	9
lgv ($w = 1$)	0,11	14,43	31,17	50,34	71,97	96,04
lgv ($w = 2$)	1,52	15,84	32,58	51,75	73,37	97,44
lgv ($w = 3$)	3,05	17,37	34,11	53,28	74,90	98,97
n	10	11	12	13	14	15
lgv ($w = 1$)	122,56	151,54	182,97	216,86	253,21	292,02
lgv ($w = 2$)	123,97	152,95	184,38	218,27	254,62	293,43
lgv ($w = 3$)	125,50	154,48	185,91	219,80	256,15	294,96

Анализируя данные табл. 1 – 6, можно сделать следующие выводы.

1. С уменьшением любого из параметров α_{MAX} (общее количество участников во всех разрешенных коалициях), p_{MAX} (мощность самого большого множества секретов), d_{MAX} (максимальное количество секретов в наборе) или с увеличением любого из параметров p_{MIN} (мощность самого малого множества секретов), d_{MIN} (минимальное количество секретов в

наборе), n (количество участников протокола), w (количество наборов секретов) при фиксированных остальных параметрах выигрыш от применения предложенной методики растет. При этом выигрыш изменяется от нескольких раз ($10^{0,11}$ для $w = 1$, $d_{MAX} = 2$, $d_{MIN} = 2$, $p_{MAX} = 17$, $p_{MIN} = 11$, $\alpha_{MAX} = 15$, $n = 4$) до нескольких сотен порядков ($10^{294,96}$ для $w = 3$, $p_{MAX} = 17$, $p_{MIN} = 11$, $\alpha_{MAX} = 15$, $d_{MAX} = d_{MIN} = 2$, $n = 15$).

2. Наибольший выигрыш достигается в том случае, когда $p_{MAX} \approx p_{MIN}$ или $d_{MAX} = d_{MIN}$ (при фиксированных значениях остальных параметров). Например, при $w = 1$, $p_{MIN} = 2$, $\alpha_{MAX} = 15$, $d_{MAX} = 3$, $d_{MIN} = 1$, $n = 10$, если $p_{MAX} = 37$ ($p_{MAX} >> p_{MIN}$), то выигрыш составляет только $10^{3,15}$ раз, а если $p_{MAX} = 3$ ($p_{MAX} \approx p_{MIN}$), то – $10^{19,52}$ раз. Также, при $w = 1$, $p_{MAX} = 17$, $p_{MIN} = 11$, $\alpha_{MAX} = 15$, $d_{MIN} = 1$, $n = 10$, если $d_{MAX} = 20$ ($d_{MAX} >> d_{MIN}$), то выигрыш составляет $10^{0,41}$ раз, а если $d_{MAX} = 2$ ($d_{MAX} \approx d_{MIN}$), то – $10^{121,15}$ раз.

Заключение

В статье предложена методика проверки существования и формирования (в случае существования) матрицы над кольцом вычетов, используемой для построения ПМРС с многоадресным сообщением, реализующего заданную иерархию доступа. Сущность методики заключается в последовательном применении алгоритмов, разработанных на основе результатов работ [17 – 21].

Разработанная методика позволяет осуществлять проверку существования для заданной совокупности множеств Ψ матрицы G вида (2), задающей протокол множественного разделения секрета с многоадресным сообщением, который реализует совокупность Ψ в качестве иерархии доступа. В случае существования методика позволяет построить эту матрицу в явном виде.

Для предложенной методики получены аналитическая оценка временной сложности (см. формулу (11)), а также нижняя граница выигрыша при ее применении по сравнению с тривиальной переборной методикой (см. формулу (13)) по каждому из следующих параметров (при фиксированных остальных): количество наборов секретов, минимальное и максимальное количество секретов в наборе, мощности самого большого и самого малого множеств секретов, число участников протокола, общее количество участников во всех разрешенных коалициях. Показано, что выигрыш от применения предложенной методики увеличивается с ростом количества наборов секретов, минимальным количеством секретов в наборе, мощностью самого малого множества секретов и числа участников протокола и уменьшается с ростом общего количества участников во всех разрешенных коалициях, мощностью самого большого множества секретов и максимальным количеством секретов в наборе. При этом наибольший выигрыш достигается в том случае, когда $p_{MIN} \approx p_{MAX}$ или $d_{MIN} = d_{MAX}$.

Список литературы

1. Введение в криптографию / Под общ. ред. В. В. Ященко. – М.: МЦНМО: "ЧеРо", 1999. – 272 с.

2. *Blakley G.R.* Safeguarding cryptographic keys // Proc. AFIPS 1979 National Computer Conference. – N-Y.:1979. – V. 48. – P. 313 – 317.

3. *Shamir A.* How to share a secret // Comm. ACM. – 1979. – V. 22. – № 1. – P. 612 – 613.

4. *Bertilsson M.* Linear codes and secret sharing. – PhD Thesis. – Linkoping University. – 1993.

5. *Brickell E.F.* Some ideal secret sharing schemes // J. Combin. Math. and Combin. Comput. – 1989. – № 9. – P. 105 – 113.

6. *Blakley G.R., Kabatianski G.A.* Linear algebra approach to secret sharing schemes // Preproc. of Workshop on Information Protection.: Moscow, 1993.

7. *Massey J.L.* Minimal codewords and secret sharing // Proc. 6th Joint Swedish-Russian Int. Workshop on Information Protection. – 1993. – P. 276 – 279.

8. *Ashikhmin A., Barg A.* Minimal vectors in linear codes and sharing of secrets // Univ. Bielefeld, SFB 343 Diskrete Strukturen in der Mathematik. – 1994. – Preprint 94 – 113, available from ftp.uni-bielefeld.de.

9. *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.

10. *Simmons G.J.* How to (really) share a secret // Advances in Cryptology – CRYPTO'88, Lecture Notes in Computer Science. – 1989. – Vol. 403. – P. 390 – 448.

11. *Blundo C., de Santis A., di Crescenzo D., Gaggia A. G., Vaccaro U.* Multi-secret sharing schemes // Advances in Cryptology – CRYPTO'94, Lecture Notes in Computer Science. – 1994. – Vol. 839. – P. 150 – 163.

12. *Simmons G.J.* Prepositioned shared secret and/or shared control schemes // Advances in Cryptology – EUROCRYPT'89, Lecture Notes in Computer Science. – 1990. – Vol. 434. – P. 436 – 467.

13. *Harn L., Hwang T., Laih C., Lee J.* Dynamic threshold scheme based on the definition of cross- product in a N-dimensional linear space // Advances in Cryptology – EUROCRYPT'89. – Lecture Notes in Comput. Science. – V. 435. – P. 286 – 298.

14. *Blundo C., Cresti A., de Santis A., Vaccaro U.* Fully dynamic secret sharing schemes // Theoretical Computer Science. – 1996. – Vol. 155. – P. 407 – 410.

15. *Seberry J., Charnes C., Pieprzyk J., Safavi-Naini R.* 41 Crypto topics and applications II. Handbook on Algorithms and Theory of Computation, 1998. – P. 1 – 22.

16. *McLean J.* Reasoning about security models // Proceeding IEEE Symposium on privacy and security. – IEEE Computer Society Press. – 1987. – P. 123-131.

17. *Алексейчук А.Н., Волошин А.Л.* Совершенная схема множественного разделения секрета над кольцом вычетов по модулю *m* // Реєстрація, зберігання і обробка даних. – 2005. – Т. 7. – № 4. – С. 44 – 53.

18. *Алексейчук А.Н., Волошин А.Л., Скрыпник Л.В.* Совершенная схема множественного разделения секрета на основе линейных преобразований над конечным цепным коммутативным кольцом // Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2 – 3 ноября 2005 г. – М.: МЦНМО, 2006. – С. 149 – 154.

19. *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.

20. *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.

21. *Волошин А.Л.* Алгоритм формирования матрицы над примарным кольцом вычетов для построения протокола множественного разделения секрета, реализующего заданную иерархию доступа // Захист інформації. – 2007. – № 3 (34). – С. 88 – 94.

22. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. – Пер. с англ. – М.: Мир, 1979. – 536 с.

23. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра. Учебник. В 2-х т. Т. 1. – М.: Гелиос АРВ, 2003. – 336 с.

Поступила 14.03.2008г.