УДК 621.391:519.7:510.5

А. Н. Алексейчук[1], А. Л. Волошин[2]
[1]Специальный факультет СБ Украины в составе Военного института телекоммуникаций и информатизации НТУУ «КПИ»
[2]ДСТСЗИ СБ Украины

Схема разделения нескольких секретов с многоадресным сообщением на основе линейных преобразований над кольцом вычетов по модулю m

Введено понятие схемы разделения $d \geq 2$ секретов с многоадресным сообщением (d-СРСМС). Предложена конструкция совершенной d-СРСМС, основанная на линейных преобразованиях над кольцом вычетов целых чисел. Установлены необходимые и достаточные условия существования и предложен алгоритм построения указанной d-СРСМС для произвольной заранее определенной иерархии доступа.

Ключевые слова: *криптографическая защита информации, схема разделения секрета, иерархия доступа, кольцо вычетов.*

Введение

Среди разнообразных конструкций схем разделения секрета (СРС) представляют практический интерес так называемые схемы разделения секрета с многоадресным сообщением (СРСМС — secret sharing schemes with broadcast message) [1–4]. В этих схемах необходимым условием восстановления секретного ключа каждой разрешенной коалицией участников является предварительное получение всеми участниками некоторого открытого сообщения, передаваемого дилером по широковещательному каналу связи.

Впервые СРСМС выделены в отдельный класс схем разделения секрета в их общей классификации, приведенной в работе [1]. В [2] описан алгоритм построения пороговой СРСМС (структура доступа которой состоит из всех коалиций мощности не меньшей заданного числа участников). В [3] предложена СРСМС, реализующая структуру доступа общего вида с изменяющимся в дискретные моменты времени составом разрешенных коалиций участников. Наконец, в [4] построена общая теоретико-информационная модель СРСМС, и получены нижние границы количества информации, хранящейся у участников произвольной схемы разделения секрета с многоадресным сообщением.

Естественным обобщением СРСМС являются криптографические протоколы, позволяющие «разделять» одновременно $d \geq 2$ секретных ключей таким образом, чтобы участники каждой коалиции после получения некоторого открытого сообщения, передаваемого дилером по широковещательному каналу связи, могли однозначно восстановить определенные («назначенные» им, согласно протоколу) секретные ключи. Более формальное определение указанных СРС, названных в настоящей статье *схемами разделения d секретов с многоадресным сообщением* (*d-СРСМС*), приведено ниже.

Следует отметить, что в силу разнообразия иерархий доступа, реализуемых *d*-СРСМС (см. ниже п. 2), спектр возможных применений этих криптографических протоколов может быть весьма широким, начиная от систем разделенной электронной цифровой подписи и, заканчивая протоколами управления доступом к ресурсам информационных и телекоммуникационных систем. Таким образом, задача разработки методов построения *d*-СРСМС является актуальной и практически важной.

В настоящей статье предлагается конструкция совершенных *d*-СРСМС, основанная на линейных преобразованиях над кольцом вычетов по модулю *m*. Охарактеризованы иерархии доступа предложенных *d*-СРСМС. На основе результатов, полученных ранее в [5], установлены необходимые и достаточные условия существования и предложен алгоритм построения *d*-СРСМС, реализующей заранее определенную иерархию доступа. Наконец, представлены две модификации исходной схемы разделения *d* секретов с многоадресным сообщением, каждая из которых позволяет активизировать любую (заранее определенную) иерархию доступа из некоторого семейства таких иерархий на множестве участников *d*-СРСМС.

1. Математическая модель схемы разделения нескольких секретов с многоадресным сообщением

Следуя основной идее определения схемы разделения (одного) секрета с многоадресным сообщением [4], определим *d*-СРСМС как криптографический протокол, состоящий из следующих двух этапов.

На первом этапе (*предварительного распределения секретной информации*) дилер передает по защищенному каналу связи индивидуальную секретную информацию каждому участнику *d*-СРСМС.

На втором этапе (*разделения и восстановления секретных ключей*) дилер выбирает набор, состоящий из *d* секретных ключей, принадлежащих некоторому множеству *S*. Затем он вычисляет по этому набору некоторое сообщение *B*, которое передает всем участникам *d*-СРСМС по широковещательному каналу связи. Предполагается, что после получения сообщения *B* каждая коалиция участников может однозначно восстановить «назначенное» ей, согласно протоколу, (возможно пустое) множество секретных ключей из исходного набора.

Назовем схему разделения нескольких секретов с многоадресным сообщением *совершенной*, если:

1) до получения сообщения *B* каждая коалиция участников не имеет никакой информации о значениях секретных ключей;

2) после получения сообщения B каждая коалиция участников может восстановить «назначенные» ей, согласно протоколу, секретные ключи, в то время как об остальных ключах она не имеет никакой апостериорной информации.

Отметим, что в частном случае $d = 1$ понятие совершенной d-СРСМС совпадает с известным понятием совершенной схемы разделения (одного) секрета с многоадресным сообщением, реализующей единственную структуру доступа [4].

Опишем предлагаемую конструкцию d-СРСМС, основанную на линейных преобразованиях над кольцом вычетов по модулю m.

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

$$S = \{(s_{ij}): s_{ij} \in \mathbf{GF}(p_j),\ i \in \overline{0,d_j - 1},\ j \in \overline{1,w}\}.$$

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

Зафиксируем $(k + 1)\times(n + 2)$-матрицу G над кольцом R с элементами g_{ij}, ($i \in \overline{0,k}$, $j \in \overline{0,n+1}$, $k, n \geq 2$) следующего вида:

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

где $g_{0,n+1} \in R^*$, $g_{n+1}^{\downarrow} \notin D(R)^{(k)}$. Занумеруем столбцы этой матрицы слева направо числами от 0 до $n + 1$, а строки — сверху вниз числами от 0 до k.

Матрице G вида (1) поставим в соответствие d-СРСМС $\rho(G)$, реализующую распределение наборов секретных ключей $(s_{ij}) \in S$, $i \in \overline{0,d_j - 1}$, $j \in \overline{1,w}$, между участниками, принадлежащими множеству $P = \{1, 2, \ldots, n\}$. Отметим, что в предлагаемой ниже конструкции d-СРСМС матрица G известна всем участникам схемы разделения секрета.

На этапе предварительного распределения секретной информации дилер независимо, случайно и равновероятно выбирает элементы $a_1, \ldots, a_k \in R$ и вычисляет вектор

$$(\pi_1, \ldots, \pi_n, b(a_1, \ldots, a_k)) = (a_1, \ldots, a_k)(G', g_{n+1}^{\downarrow}), \qquad (2)$$

первые n координат которого составляют секретную информацию участников. При этом элемент $\pi_i \in R$ доставляется i-му участнику d-СРСМС $\rho(G)$ по защищенному каналу связи, $i \in \overline{1,n}$, а элемент $b(a_1, \ldots, a_k)$ хранится в секрете у дилера.

На этапе разделения и восстановления секретных ключей $(s_{ij}) \in S$, $i \in \overline{0, d_j - 1}$, $j \in \overline{1, w}$, дилер применяет следующий алгоритм.

1. Вычисляет элементы:

$$s_j = \sum_{i=0}^{d_j - 1} p_j^{\,i} s_{ij}\,,\ j \in \overline{1, w}. \tag{3}$$

2. Находит единственный элемент $s \in R$ такой, что $s \equiv s_j \pmod{p_j^{d_j}}$, $j \in \overline{1, w}$.

3. Вычисляет многоадресное сообщение

$$B = g_{0,n+1} s + b(a_1, \ldots, a_k) \in R \tag{4}$$

и направляет его по широковещательному каналу связи всем участникам d-СРСМС $\rho(G)$.

Назовем описанную d-СРСМС *линейной над кольцом R схемой разделения d секретов с многоадресным сообщением*.

Для любого делителя $t = p_1^{l_1} \cdots p_w^{l_w}$ числа m ($0 \le l_j \le d_j$, $j \in \overline{1, w}$) обозначим $\widetilde{\Psi}_t$ совокупность всех множеств A участников d-СРСМС $\rho(G)$, которые при объединении своих секретных значений и получении многоадресного сообщения B могут восстановить ровно $d_j - l_j$ младших p_j-х разрядов числа s_j вида (3), $j \in \overline{1, w}$. Следуя терминологии, принятой в [5], назовем семейство множеств $\widetilde{\Psi} = (\widetilde{\Psi}_t : t \mid m)$ *иерархией доступа d-СРСМС* $\rho(G)$.

Ниже приведено полное описание иерархии доступа d-СРСМС $\rho(G)$ и показано, что $\rho(G)$ является совершенной схемой разделения нескольких секретов с многоадресным сообщением.

2. Характеризация иерархии доступа *d*-СРСМС $\rho(G)$

Введем ряд вспомогательных обозначений.

Для любой матрицы H над кольцом R, имеющей n столбцов, и произвольного множества $A \subseteq P$ обозначим H_A подматрицу матрицы H, содержащуюся в ее столбцах с номерами из A.

Для любой матрицы H над кольцом R обозначим $M(H)$ и $\langle H \rangle_R$ R-модули, порожденные строками и столбцами матрицы H соответственно. Для любого $U \subseteq P \cup \{0, n+1\}$ обозначим $\|M(G_U)\|$ число различных векторов, содержащихся в столбцах с номерами из множества U таблицы размера $|M(G)| \times (n + 2)$, составленной из элементов модуля $M(G)$.

Следующая теорема устанавливает свойство совершенности d-СРСМС $\rho(G)$ и описывает строение ее иерархии доступа.

Теорема 1. Для любого делителя t числа m справедливо равенство:

$$\widetilde{\Psi}_t = \{A \subseteq P: tR = I_G(A)\}, \tag{5}$$

где

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

При этом до получения многоадресного сообщения B участники d-СРСМС $\rho(G)$ не имеют никакой информации о секретных ключах s_{ij}, $i \in \overline{0, d_j - 1}$, $j \in \overline{1, w}$:

$$||G_{P\cup 0}|| = ||G_P||m. \tag{6}$$

Кроме того, если $\widetilde{\Psi}_t \neq \varnothing$, $t = p_1^{l_1} \cdots p_w^{l_w} \mid m$, то после получения сообщения B участники, входящие в произвольную коалицию $A \in \widetilde{\Psi}_t$, не имеют никакой информации о ключах s_{ij} с номерами $i \in \overline{d_j - l_j, d_j - 1}$, $j \in \overline{1, w}$:

$$||G_{A\cup 0\cup\{n+1\}}|| = ||G_{A\cup\{n+1\}}||\, t.$$

Таким образом, $\rho(G)$ является совершенной d-СРСМС.

Доказательство. Равенство (6) следует непосредственно из формулы (1). Остальные утверждения теоремы доказываются аналогично теореме 1 в статье [5].

Заметим, что соотношения (1)–(5) позволяют построить алгоритм восстановления участниками произвольной коалиции $A \in \widetilde{\Psi}_t$ «назначенных» ей, согласно протоколу, секретных ключей s_{ij}, $i \in \overline{0, d_j - l_j - 1}$, $j \in \overline{1, w}$.

Пусть $t = p_1^{l_1} \cdots p_w^{l_w} \mid m$, $A \in \widetilde{\Psi}_t$, $\chi^{\downarrow} \in R^{|A|}$ — произвольное решение системы линейных уравнений $G_A x^{\downarrow} = t(G_0 - G_{n+1})$ над кольцом R (см. формулы (1), (5)). Обозначим $\pi_A = (\pi_i : i \in A)$ вектор-строку, составленную из секретных значений, полученных участниками коалиции A на первом этапе d-СРСМС $\rho(G)$. Для любого $j \in \overline{1, w}$ обозначим $\alpha_j(t)$ элемент кольца $R_j = \mathbf{Z}/(p_j^{d_j})$, обратный к произведению $\prod_{\nu \neq j} p_\nu^{l_\nu} (\mathrm{mod}\, p_j^{d_j})$.

Заметим, что на основании формул (2)–(4) справедливы следующие равенства:

$$p_j^{l_j} s_j \equiv \alpha_j(t)(g_{0,n+1})^{-1}(\overrightarrow{\pi_A}\chi^{\downarrow} + tB)(\mathrm{mod}\, p_j^{d_j}),\ j \in \overline{1, w}. \tag{7}$$

Таким образом, вычислив значения (7), участники коалиции A однозначно восстановят секретные ключи s_{ij} с номерами $i \in \overline{0, d_j - l_j - 1}$, $j \in \overline{1, w}$.

3. Критерий существования и алгоритм построения *d*-СРСМС $\rho(G)$ для заданной иерархии доступа

Пусть задано семейство $\Psi = (\Psi_t : t \mid m)$ попарно непересекающихся подмножеств Ψ_t множества 2^P (случай $\Psi_t = \varnothing$ не исключается) таких, что $\bigcup_{t|m} \Psi_t = 2^P$.

Требуется установить необходимые и достаточные условия, при которых семейство Ψ является иерархией доступа некоторой линейной над кольцом R d-СРСМС и (в случае существования) построить в явном виде матрицу G вида (1), задающую такую d-СРСМС.

Для решения поставленной задачи воспользуемся результатами, полученными ранее в [5]. Докажем следующую теорему.

Теорема 2. Пусть существует $k\times(n + 1)$-матрица

$$H = \left(h^{\downarrow}, H'\right) \tag{8}$$

над кольцом R такая, что

$$h^{\downarrow} \notin D(R)^{(k)}, \tag{9}$$

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

$$||M(H_{A\cup\{0\}})|| = ||M(H_A)||t. \tag{10}$$

Тогда существует d-СРСМС $\rho(G)$, реализующая семейство Ψ, в качестве иерархии доступа, где матрица G имеет вид:

$$G = \left(\begin{array}{c|ccc|c} 1 & 0 & \cdots & 0 & 1 \\ \hline 0^{\downarrow} & & H' & & h^{\downarrow} \end{array}\right). \tag{11}$$

Справедливо также обратное утверждение.

Доказательство. Согласно теореме 1 из [5], при выполнении соотношений (9), (10) для любого $t \mid m$ имеет место равенство:

$$\Psi_t = \{A \subseteq P: tR = I_H(A)\}, \tag{12}$$

где

$$I_H(A) = \{r \in R: rh^{\downarrow} \in \langle H_A \rangle_R\}, A \subseteq P.$$

Обозначим $\widetilde{\Psi} = \{\widetilde{\Psi}_t : t \mid m\}$ иерархию доступа d-СРСМС $\rho(G)$, где матрица G определяется по формуле (11). На основании соотношений (5), (12) для доказа-

тельства равенства $\widetilde{\Psi} = \Psi$ достаточно убедиться в справедливости следующего утверждения: для любых $t \mid m$, $A \in \Psi_t$, $r \in R$

$$rh^{\downarrow} \in \langle H_A \rangle_R \Leftrightarrow rG_0 \in \langle G_{A \cup \{n+1\}} \rangle_R . \tag{13}$$

Но формула (13) следует непосредственно из равенств (8), (11). Таким образом, существование матрицы H, удовлетворяющей условиям (9), (10), влечет существование d-СРСМС $\rho(G)$ с иерархией доступа Ψ, где матрица G определяется по формуле (11).

Обратное утверждение теоремы доказывается аналогично с использованием теоремы 1 из [5].

Отметим, что необходимые и достаточные условия существования матрицы H вида (8), удовлетворяющей соотношениям (9), (10), получены в той же статье [5] (теорема 2). Как показано в [5], эти условия могут быть положены в основу алгоритма построения искомой матрицы H, а, следовательно, и матрицы G вида (11), задающей d-СРСМС $\rho(G)$ с иерархией доступа Ψ. Описание этого алгоритма и оценка его временной сложности приведены в [5].

4. Обобщение конструкции d-СРСМС ρ(G) на схемы разделения нескольких секретов с многоадресным сообщением для семейств иерархий доступа

В [4] введено понятие совершенной СРСМС, реализующей произвольное конечное семейство структур доступа. В такой схеме на этапе разделения и восстановления секретного ключа дилер формирует многоадресное сообщение B таким образом, чтобы активизировать лишь одну (заранее определенную) структуру доступа из заданного семейства структур. При этом каждая коалиция участников, принадлежащая выбранной структуре доступа, может однозначно восстановить секрет по принятому сообщению B и секретной информации, полученной от дилера на первом этапе; все остальные коалиции участников не имеют никакой апостериорной информации о секретном ключе. Таким образом, различные способы формирования сообщения B позволяют задавать различные (простые) схемы разделения секрета на множестве участников при неизменной секретной информации, полученной ими на первом этапе СРСМС.

Ниже представлены две модификации d-СРСМС $\rho(G)$, описанной в п. 2, каждая из которых обобщает конструкцию $\rho(G)$ и является схемой разделения d секретов с многоадресным сообщением, реализующей некоторое семейство иерархий доступа. Обе модификации отличаются от исходной d-СРСМС $\rho(G)$ исключительно способом формирования сообщения B (см. формулу (4)).

В первой модификации на шаге 3 алгоритма, описанного в п. 2, дилер фиксирует число τ такое, что $\tau \mid m$, генерирует случайный равновероятный и не зависящий от s элемент $r \in R$ и вычисляет сообщение B по формуле:

$$B = g_{0,n+1}s + b(a_1,...,a_k) + \frac{m}{\tau}r . \tag{14}$$

Во второй модификации *d*-СРСМС $\rho(G)$ для выбранного $\tau \mid m$ дилер вычисляет сообщение *B*, полагая:

$$B = g_{0,n+1}s + \tau b(a_1,...,a_k)\,. \tag{15}$$

Ясно, что при $\tau = 1$ каждое из соотношений (14), (15) совпадает с равенством (4).

С целью описания семейств иерархий доступа, реализуемых предложенными *d*-СРСМС, введем следующие обозначения.

Для любых $u, v \in R$ обозначим (u,v) и $[u,v]$ соответственно наибольший общий делитель и наименьшее общее кратное чисел *u* и *v*.

Для любых натуральных делителей t, τ числа *m* обозначим символом $\Psi_t^{(1)}(\tau)$ (символом $\Psi_{t'}^{(2)}(\tau)$) совокупность всех коалиций $A \in 2^P$ таких, что *t* является наименьшим натуральным числом, для которого участники, входящие в *A*, могут однозначно восстановить элемент *ts* по секретным значениям π_l, $l \in A$ и многоадресному сообщению *B* вида (14) (вида (15)).

Отметим, что на основании соотношений $s \equiv s_j \pmod{p_j^{d_j}}$, $j \in \overline{1,w}$, и формулы (3) для любых $t = p_1^{l_1} \cdots p_w^{l_w} \mid m$, $\tau \mid m$, $q = 1, 2$ участники произвольной коалиции $A \in \Psi_t^{(q)}(\tau)$ могут однозначно восстановить секретные ключи s_{ij} с номерами $i \in \overline{0, d_j - l_j - 1}$, $j \in \overline{1,w}$ и только их.

Положим $\Psi^{(q)}(\tau) = (\Psi_t^{(q)}(\tau) : t \mid m)$, $\Psi^{(q)} = (\Psi^{(q)}(\tau) : \tau \mid m)$, $q = 1, 2$. Как показывает следующая теорема, семейство $\Psi^{(q)}$ состоит из всех различных иерархий доступа, реализуемых *q*-й модификацией *d*-СРСМС $\rho(G)$. При этом множества $\Psi_t^{(q)}(\tau)$, $t \mid m$, $\tau \mid m$, $q = 1, 2$, могут быть явно выражены через множества вида (5), образующие иерархию доступа исходной *d*-СРСМС $\rho(G)$.

Теорема 3. Для любого $\tau \mid m$ и $q = 1, 2$ семейство $\Psi^{(q)}(\tau)$ является разбиением множества 2^P. При этом для любого $t \mid m$:

$$\Psi_t^{(1)}(\tau) = \bigcup \{\widetilde{\Psi}_f : f \mid m,\ [f,\tau] = t\}\,, \tag{16}$$

$$\Psi_t^{(2)}(\tau) = \bigcup \{\widetilde{\Psi}_f : f \mid m,\ \frac{f}{(f,\tau)} = t\}\,. \tag{17}$$

Доказательство. Первое утверждение теоремы следует непосредственно из определения множеств $\Psi_t^{(q)}(\tau)$, $t \mid m$.

Для доказательства равенства (16) достаточно показать, что для любых $f \mid m$, $A \in \widetilde{\Psi}_f$ число $t = [f,\tau]$ является наименьшим натуральным делителем числа *m*, для которого участники коалиции *A* могут однозначно восстановить элемент *ts*

по секретным значениям π_l, $l \in A$ и сообщению B вида (14). Убедимся в справедливости этого утверждения.

Заметим, что в силу условия $A \in \widetilde{\Psi}_f$ и формул (1), (2), (5) f является наименьшим делителем числа m, для которого участники коалиции A могут однозначно восстановить элемент $fb(a_1, \ldots, a_k)$ по известным им значениям π_l, $l \in A$. Умножая равенство (14) на $t = [f, \tau]$, получим $tB = g_{0,n+1} ts + \dfrac{[f,\tau]}{f} fb(a_1,\ldots,a_k) +$ $+ \dfrac{[f,\tau]}{\tau}(mr)$, откуда следует, что

$$ts = (g_{0,n+1})^{-1}(tB - \frac{[f,\tau]}{f} fb(a_1,\ldots,a_k)). \qquad (18)$$

Итак, зная $fb(a_1, \ldots, a_k)$ и B, участники коалиции A восстановят ts по формуле (18).

Пусть теперь t_1 — произвольный делитель числа m, для которого элемент $t_1 s$ однозначно определяется значениями π_l, $l \in A$ и сообщением (14). Покажем, что $t \mid t_1$.

Прежде всего, заметим, что $\tau \mid t_1$, поскольку в противном случае на основании равенства $B = g_{0,n+1}(s + (g_{0,n+1})^{-1} \dfrac{m}{\tau}) + b(a_1,\ldots,a_k) + \dfrac{m}{\tau}(r-1)$, вытекающего из формулы (14), существует, по крайней мере, два различных элемента, $t_1 s$ и $t_1(s + (g_{0,n+1})^{-1} \dfrac{m}{\tau})$, соответствующих заданным π_l, $l \in A$, и B. Далее, умножая равенство (14) на t_1, получим соотношение $t_1 B = g_{0,n+1} t_1 s + t_1 b(a_1,\ldots,a_k)$, из которого, согласно условию $A \in \widetilde{\Psi}_f$, следует, что $f \mid t_1$. Итак, $t = [f, \tau] \mid t_1$, что и требовалось доказать.

Аналогичным образом доказывается равенство (17).

В заключение рассмотрим пример, позволяющий более наглядно проиллюстрировать изложенные выше результаты.

Пусть $m = p^d$, где p — простое число, $d \geq 2$, $\rho(G)$ — линейная над кольцом $R = \mathbf{Z}/(p^d)$ схема разделения d секретных ключей с многоадресным сообщением, соответствующая матрице G вида (1).

Согласно теореме 1, иерархия доступа d-СРСМС $\rho(G)$ состоит из $d + 1$ попарно непересекающихся классов (уровней) $\widetilde{\Psi}_{p^i}$, $i \in \overline{0,d}$, находящихся во взаимно однозначном соответствии с делителями числа p^d. При этом, если $\widetilde{\Psi}_{p^i} \neq \varnothing$, то участники каждой коалиции $A \in \widetilde{\Psi}_{p^i}$, расположенной на i-м уровне иерархии доступа, могут однозначно восстановить по значениям π_l, $l \in A$, и сообщению B вида (4) ровно $d - i$ секретных ключей $s_0, s_1, \ldots, s_{d-i-1} \in \mathbf{GF}(p)$ из набора $s = (s_i: i \in \overline{0, d-1})$, распределяемого дилером. В частности, произвольная коалиция уча-

стников, находящаяся на i-м уровне, $i \in \overline{0, d-1}$, имеет доступ ко всей секретной информации, зашифрованной на ключах, однозначно восстанавливаемых коалициями, расположенными на более «низких» уровнях (с номерами $j > i$).

Предположим, что после завершения первого этапа d-СРСМС $\rho(G)$ требуется ограничить «права доступа» коалиций, расположенных на уровнях с номерами 0, 1, …, $\nu - 1$, переведя все указанные коалиции на ν-й уровень иерархии доступа d-СРСМС $\rho(G)$, и при этом сохранить «права доступа» каждой коалиции, находящейся на уровне с номером $j \in \overline{\nu, d}$. Для решения этой задачи дилер фиксирует $\tau = p^{\nu}$ и передает участникам сообщение B вида (14) по широковещательному каналу связи. Тем самым на множестве участников формируется новая иерархия доступа $\Psi^{(1)}(\tau)$, состоящая из непустых множеств вида (16). Нетрудно видеть, что эта иерархия доступа состоит из $d - \nu + 1$ уровней вида

$$\Psi^{(1)}_{p^{\nu}}(p^{\nu}) = \bigcup_{i=0}^{\nu} \widetilde{\Psi}_{p^i}\,,\ \Psi^{(1)}_{p^{\nu+1}}(p^{\nu}) = \widetilde{\Psi}_{p^{\nu+1}}\,,\ \ldots,\ \Psi^{(1)}_{p^{d}}(p^{\nu}) = \widetilde{\Psi}_{p^{d}}$$

и, следовательно, удовлетворяет сформулированным выше ограничениям на «права доступа» коалиций участников.

Пусть теперь ставится задача переместить каждую коалицию участников на ν уровней «вверх» (с i-го на $(i - \min\{i, \nu\})$-й уровень иерархии доступа $\widetilde{\Psi}$, $i \in \overline{0, d}$) после выполнения первого этапа d-СРСМС $\rho(G)$. В этом случае дилер фиксирует $\tau = p^{\nu}$ и передает участникам d-СРСМС сообщение B вида (15). На основании равенства (17) сформированная таким образом новая иерархия доступа $\Psi^{(2)}(\tau)$ состоит из $d - \nu + 1$ уровней следующего вида:

$$\Psi^{(2)}_{p^{0}}(p^{\nu}) = \bigcup_{i=0}^{\nu} \widetilde{\Psi}_{p^i}\,,\ \Psi^{(2)}_{p^{1}}(p^{\nu}) = \widetilde{\Psi}_{p^{\nu+1}}\,,\ \ldots,\ \Psi^{(2)}_{p^{d-\nu}}(p^{\nu}) = \widetilde{\Psi}_{p^{d}}\,.$$

Коалиции, находящиеся на уровне $\Psi^{(2)}_{p^{0}}(p^{\nu})$ новой иерархии доступа, могут однозначно восстановить все секретные ключи s_i, $i \in \overline{0, d-1}$; коалиции, расположенные на следующем уровне $\Psi^{(2)}_{p^{1}}(p^{\nu})$, могут восстановить ключи с номерами $i \in \overline{0, d-2}$ и т.д. Наконец, участники произвольной коалиции $A \in \Psi^{(2)}_{p^{d-\nu}}(p^{\nu})$, не имеющие никакой апостериорной информации о ключах s_i ($i \in \overline{0, d-1}$) в исходной d-СРСМС $\rho(G)$, получат возможность восстановить ключи с номерами $i \in \overline{0, d-\nu-1}$.

Подчеркнем, что все представленные выше схемы разделения нескольких секретов с многоадресным сообщением являются, безусловно, стойкими, то есть

обеспечивают (в рамках принятой модели) невозможность получения каких-либо сведений о соответствующих секретных ключах независимо от ограничений на производительность вычислительных средств участников *d*-СРСМС или внешнего (пассивного) противника.

1. *Simmons G.J.* How to (Really) Share a Secret // Advances in Cryptology — CRYPTO'88. — Lecture Notes in Comput. Science, 1990. — P. 390–448.

2. *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. — Vol. 435. — P. 286–298.

3. *Martin K.* Discrete Structures in the Theory of Secret Sharing. — PhD Th. — University of London. — 1991.

4. *Blundo C.*, *Cresti A.*, *De Santis A.*, *Vaccaro U.* Fully Dynamic Secret Sharing Schemes // Advances in Cryptology — CRYPTO'93. — Lecture Notes in Comput. Science, 1994. — P. 110–125.

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

Поступила в редакцию 30.01.2006