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

Совершенная схема множественного разделения секрета над кольцом вычетов по модулю *m*

Предложена конструкция совершенной схемы множественного разделения секрета, основанная на линейных преобразованиях над кольцом вычетов целых чисел. Установлены необходимые и достаточные условия существования рассматриваемой схемы и описан алгоритм ее построения для произвольной заранее определенной иерархии доступа. Полученные результаты обобщают известные ранее утверждения о свойствах линейных схем разделения секрета над конечными полями, векторными пространствами и кольцами Галуа.

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

Введение

Схема множественного разделения секрета (multi-secret sharing scheme — СМРС) [1, 2] представляет собой криптографический протокол, позволяющий «разделять» одновременно несколько секретных ключей (секретов) среди участников схемы таким образом, чтобы только заранее определенные подмножества (коалиции) участников могли восстановить значения определенных ключей при объединении своих компонент (проекций секретов). Если при этом участники каждой коалиции не получают никакой апостериорной информации об остальных ключах (к которым, согласно протоколу, они не имеют права доступа), то соответствующая СМРС называется совершенной [2].

Естественный тривиальный способ задания СМРС состоит в построении нескольких обычных схем разделения секрета (СРС) [3, 4], каждая из которых независимо от остальных используется для разделения «своего» секретного ключа из заданной совокупности ключей. Как правило, такое решение оказывается малопрактичным, поскольку участникам СМРС приходится хранить большой объем секретной информации.

Разработке эффективных способов построения СМРС, исследованию их свой-

ств и возможных применений при решении различных прикладных задач посвящены работы [1, 2, 5–7] и др. В [2] предложена общая теоретико-информационная модель СМРС и получены нижние границы количества информации, хранящейся у участников произвольной схемы множественного разделения секрета.

В настоящей статье предлагается конструкция совершенной СМРС, которая отличается от изложенных в [1, 2] и является прямым обобщением «векторных» схем разделения секрета над конечными полями [8] и примарными кольцами вычетов [9]. Охарактеризованы иерархии доступа предложенных СМРС (см. ниже теоремы 1 и 2) и получены необходимые и достаточные условия существования СМРС данного типа для произвольной заранее определенной иерархии доступа (теоремы 3, 4). Предложен алгоритм построения линейной схемы множественного разделения секрета для заданной иерархии доступа, обобщающий известный ранее алгоритм построения «векторной» СРС над конечным полем [10]. Также обобщен ряд результатов, изложенных в [9, 10].

Определение и характеризация иерархии доступа предлагаемой схемы множественного разделения секрета

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

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

Зафиксируем матрицу

$$G = \left(\begin{array}{c|c} 1 & \\ 0 & \\ \vdots & G' \\ 0 & \end{array}\right)$$

размера $k \times (n + 1)$ над кольцом R ($k, n \geq 2$), которой следующим образом поставим в соответствие схему множественного разделения секрета $\sigma(G)$, реализующую распределение наборов секретных ключей $(s_{ij}) \in S$, $i \in \overline{0,d_j - 1}$, $j \in \overline{1,w}$, участникам, принадлежащим множеству $P = \{1, 2, \ldots, n\}$.

Пусть (s_{ij}) — произвольный элемент множества S. Тогда для нахождения проекций ключей s_{ij} ($i \in \overline{0,d_j - 1}$, $j \in \overline{1,w}$) дилер СМРС применяет следующий алгоритм.

1. Вычисляет элементы:

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

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

3. Независимо, случайно и равновероятно выбирает элементы $a_1, \ldots, a_{k-1} \in R$ и вычисляет вектор $(s, \pi_1, \ldots, \pi_n) = (s, a_1, \ldots, a_{k-1})G$, последние n координат которого объявляются проекциями ключей s_{ij} ($i \in \overline{0,d_j-1}$, $j \in \overline{1,w}$); при этом элемент $\pi_i \in R$ доставляется i-му участнику СМРС $\sigma(G)$, $i \in \overline{1,n}$.

Назовем описанную СМРС *линейной схемой множественного разделения секрета над кольцом* R. Отметим, что в частном случае $w = 1$, $d_1 = 1$ эта СМРС представляет собой обычную «векторную» схему разделения секрета над конечным (простым) полем [8]. При выполнении условий $w = 1$, $d_1 \geq 2$ шаг 3 изложенного выше алгоритма аналогичен процедуре вычисления проекций (одного) секретного ключа в несовершенной схеме разделения секрета над кольцом Галуа [9]. Представленные ниже результаты обобщают ряд утверждений, полученных в [9, 10], на класс линейных схем множественного разделения секрета над кольцом вычетов R.

Покажем, что $\sigma(G)$ является совершенной СМРС (в смысле определения [2]).

Предварительно введем ряд обозначений. Для любого $A \subseteq P \cup \{0\}$ обозначим символом G_A подматрицу матрицы G, состоящую из ее столбцов с номерами из множества A. В частном случае $A = \{i\}$, $i \in \overline{0,n}$, будем писать G_i вместо $G_{\{i\}}$. Для любой матрицы U над кольцом R обозначим $\langle U \rangle_R$ и $M(U)$ соответственно R-модули, порожденные столбцами и строками матрицы U. Отметим, что поскольку R является конечным евклидовым кольцом, то

$$\#\langle U \rangle_R = \#M(U) \tag{2}$$

для любой матрицы U над R [11] (здесь и далее символом $\#M$ обозначается мощность произвольного конечного множества M).

Для любого делителя $t = p_1^{l_1} \cdots p_w^{l_w}$ числа m ($0 \leq l_j \leq d_j$, $j \in \overline{1,w}$) обозначим $\tilde{\Sigma}_t$ совокупность всех множеств A участников СМРС $\sigma(G)$, которые при объединении своих проекций могут восстановить ровно $d_j - l_j$ младших p_j-х разрядов числа s_j вида (1), $j \in \overline{1,w}$. Назовем совокупность множеств $\tilde{\Sigma} = \{\tilde{\Sigma}_t : t \mid m\}$ *иерархией доступа* схемы множественного разделения секрета $\sigma(G)$.

Следующая теорема, обобщающая один из результатов статьи [9], устанавливает свойство совершенности СМРС $\sigma(G)$ и описывает строение ее иерархии доступа.

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

$$\tilde{\Sigma}_t = \{A \subseteq P: tR = I_G(A)\}, \tag{3}$$

где

$$I_G(A) = \{r \in R: rG_0 \in \langle G_A \rangle_R\}, A \subseteq P. \tag{4}$$

При этом для любого $A \in \widetilde{\Sigma}_t$:

$$\#M(G_{A\cup\{i\}}) = \#M(G_A)t. \tag{5}$$

Доказательство. Из определения иерархии доступа СМРС $\sigma(G)$ следует, что если t является образующей идеала (4), то множество A принадлежит совокупности $\widetilde{\Sigma}_t$. Поэтому для доказательства первого утверждения теоремы достаточно убедиться в справедливости включения:

$$\widetilde{\Sigma}_t \subseteq \{A \subseteq P: tR = I_G(A)\}. \tag{6}$$

Пусть $A \in \widetilde{\Sigma}_t$. Тогда, согласно определению совокупности $\widetilde{\Sigma}_t$, участники, входящие во множество A, могут однозначно восстановить произведение ts по имеющимся у них проекциям элемента $s \in R$, вычисляемого на шаге 2 описанного выше алгоритма. Отсюда следует равенство $\#M((tG_0, G_A)) = \#M(G_A)$, из которого на основании формулы (2) и теоремы о гомоморфизме модулей [11] вытекают следующие соотношения:

$$\#\langle G_A\rangle_R = \#(\langle G_A\rangle_R + \langle tG_0\rangle_R) = \frac{\#\langle G_A\rangle_R \#\langle tG_0\rangle_R}{\#(\langle G_A\rangle_R \cap \langle tG_0\rangle_R)} = \frac{m\,\#\langle G_A\rangle_R}{t\,\#(\langle G_A\rangle_R \cap \langle tG_0\rangle_R)},$$

$$\#(\langle G_A\rangle_R \cap \langle tG_0\rangle_R) = \frac{m}{t} = \#\langle tG_0\rangle_R,\ \langle G_A\rangle_R \cap \langle tG_0\rangle_R = \langle tG_0\rangle_R.$$

Итак, $tG_0 \in \langle G_A\rangle_R$, откуда в силу равенства (4) следует, что $tR \subseteq I_G(A)$. Предположим, что $I_G(A) = t_1R$, где t_1 — собственный делитель числа $t = p_1^{l_1} \cdots p_w^{l_w}$. Тогда на основании включения $t_1G_0 \in \langle G_A\rangle_R$ участники из множества A смогут восстановить по имеющимся у них проекциям произвольного элемента $s \in R$ произведение t_1s и найти, по крайней мере, для одного значения $j \in \overline{1,w}$ более чем $d_j - l_j$ младших p_j-х разрядов числа s_j (см. формулу (1)). Однако, это противоречит определению совокупности $\widetilde{\Sigma}_t$.

Таким образом, имеет место равенство $tR = I_G(A)$, откуда вытекает соотношение (6), а, значит, и формула (3). Доказательство формулы (5) проводится аналогично с использованием равенства (2) и теоремы о гомоморфизме модулей.

Теорема доказана.

Отметим, что, согласно равенствам (3), (5), для любого делителя $t = p_1^{l_1} \cdots p_w^{l_w}$ числа m участники СМРС $\sigma(G)$, входящие в произвольное множество $A \in \widetilde{\Sigma}_t$, не получат никакой апостериорной информации о секретных ключах s_{ij} с номерами $d_j - l_j < i \le d_j - 1,\ j \in \overline{1,w}$ (и полностью восстановят ключи s_{ij} при $0 \le i \le d_j - l_j$,

$j \in \overline{1,w}$). Таким образом, $\sigma(G)$ является совершенной схемой множественного разделения секрета.

Покажем, что исследование свойств предложенной СМРС над кольцом R сводится к исследованию свойств аналогичных СМРС над примарными кольцами вычетов R_j, $j \in \overline{1,w}$, изоморфными прямым слагаемым кольца R.

Для любого $j \in \overline{1,w}$ обозначим $G^{(j)} = G(\mathrm{mod}\, p_j^{d_j})$ матрицу над кольцом R_j, полученную в результате применения естественного гомоморфизма из R в R_j к элементам матрицы G. Пусть $\sigma(G^{(j)})$ — СМРС, соответствующая матрице $G^{(j)}$; $\tilde{\Sigma}^{(j)} = \{\tilde{\Sigma}_l^{(j)} : l \in \overline{0,d_j}\}$ — иерархия доступа указанной СМРС. Отметим, что на основании теоремы 1

$$\tilde{\Sigma}_l^{(j)} = \{A \subseteq P: l = \min\{\nu \in \overline{0,d_j} : p_j^{\nu} G_0 \in \langle G_A \rangle_R + p_j^{d_j} R^{(k)}\}\},\ j \in \overline{1,w}, \qquad (7)$$

где символом $R^{(k)}$ обозначен модуль k-мерных вектор-столбцов над кольцом R.

Теорема 2. Для любого делителя $t = p_1^{l_1} \cdots p_w^{l_w}$ числа m выполняется равенство:

$$\tilde{\Sigma}_t = \tilde{\Sigma}_{l_1}^{(1)} \cap \tilde{\Sigma}_{l_2}^{(2)} \cap \ldots \cap \tilde{\Sigma}_{l_w}^{(w)}. \qquad (8)$$

Доказательство. Следует непосредственно из соотношений (3), (4), (7).

Итак, на основании равенства (8) СМРС $\sigma(G)$ над кольцом R по существу представляет собой w «независимых» схем множественного разделения секрета $\sigma(G_1)$, …, $\sigma(G_w)$ над примарными кольцами вычетов R_1, …, R_w с иерархиями доступа $\tilde{\Sigma}^{(1)}$, …, $\tilde{\Sigma}^{(w)}$ соответственно. Ниже показано как этот результат может быть использован для решения задач о существовании и построении линейной СМРС над кольцом R, имеющей заранее определенную иерархию доступа.

Критерий существования линейной схемы множественного разделения секрета для данной иерархии доступа

Пусть для каждого делителя t числа m задана совокупность $\Sigma(t)$ подмножеств множества P, где $\Sigma(t_1) \cap \Sigma(t_2) = \varnothing$ при $t_1 \neq t_2$ и $\bigcup_{t|m} \Sigma(t) = 2^P$. 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:

$$\Sigma_l^{(j)} = \bigcup_{t \in D_{lj}} \Sigma(t),\ j \in \overline{1,w},\ l \in \overline{0,d_j}. \qquad (9)$$

Положим $\Sigma = \{\Sigma(t) : t \mid m\}$, $\Sigma^{(j)} = \{\Sigma_l^{(j)} : l \in \overline{0,d_j}\}$, $j \in \overline{1,w}$.

Из равенств (3), (7)–(9) вытекает следующий результат.

Теорема 3. Тогда и только тогда существует линейная над кольцом R схема множественного разделения секрета с иерархией доступа $\tilde{\Sigma} = \Sigma$, когда для любого $j \in \overline{1, w}$ существует линейная СМРС над кольцом R_j, иерархия доступа которой равна $\Sigma^{(j)}$.

Критерий существования линейной СМРС над кольцом вычетов по примарному модулю, имеющей заданную иерархию доступа, устанавливает следующая теорема (доказательство которой выходит за рамки данной статьи). Отметим, что в частном случае $d = 1$ справедливость этой теоремы вытекает из результатов, изложенных в [10].

Теорема 4. Пусть $m = p^d$ — примарное число, $\Sigma = \{\Sigma(i) : i \in \overline{0, d}\}$ — совокупность попарно непересекающихся подмножеств множества 2^P (случай $\Sigma(i) = \varnothing$ не исключается), $A_{i,1},\ldots,A_{i,r_i}$ — все минимальные (относительно включения) элементы класса $\Sigma(i)$, $i \in \overline{0, d}$.

Тогда для существования линейной над кольцом $R = \boldsymbol{Z}/(p^d)$ СМРС с иерархией доступа Σ необходимо и достаточно выполнение следующих условий.

1. $\varnothing \in \Sigma(d)$.

2. Для любого $i \in \overline{0, d}$ класс множеств $\Delta(i) = \bigcup_{j=0}^{i} \Sigma(j)$ является монотонным (то есть из условий $A \in \Delta(i)$, $B \in 2^P$, $A \subseteq B$ следует, что $B \in \Delta(i)$).

3. Существует матрица C над кольцом R, состоящая из $r = r_0 + \ldots + r_{d-1}$ строк $\overrightarrow{c_{i,j}} = \left(p^i, \overrightarrow{f_{i,j}}\right)$, где $\overrightarrow{f_{i,j}} \in R^n$, $i \in \overline{0, d-1}$, $j \in \overline{1, r_i}$, такая, что:

(а) для любых $i \in \overline{0, d-1}$, $j \in \overline{1, r_i}$ множество номеров ненулевых координат вектора $\overrightarrow{f_{i,j}}$ равно $A_{i,j}$;

(б) для любого $i \in \overline{0, d-1}$ и произвольного максимального (относительно включения) элемента X класса $2^P \setminus \Delta(i)$ совместна система линейных уравнений (СЛУ)

$$C_{\overline{X}} x^{\downarrow} = p^{d-(i+1)} c_0^{\downarrow} \qquad (10)$$

над кольцом R, где $C_{\overline{X}}$ — подматрица матрицы C, состоящая из ее столбцов с номерами из множества $\overline{X} = P \setminus X$; $c_0^{\downarrow}$ — столбец матрицы C с номером, равным 0.

При выполнении условий 1–3, в качестве строк матрицы G, задающей СМРС с иерархией доступа Σ, можно взять элементы подходящей системы образующих модуля решений СЛУ $Cx^{\downarrow} = 0^{\downarrow}$ над кольцом R.

Итак, утверждения теорем 3 и 4 дают исчерпывающий ответ на вопрос о необходимых и достаточных условиях, при которых существует линейная схема

множественного разделения секрета над кольцом вычетов по модулю m, имеющая произвольную заранее определенную иерархию доступа.

Алгоритм построения линейной схемы множественного разделения секрета для данной иерархии доступа

Пусть даны натуральное $m = p_1^{d_1} \cdots p_w^{d_w}$ и совокупности $\Delta(i, j) = \{B_1(i, j), \ldots, B_{q_{ij}}(i, j)\}$ попарно не содержащих друг друга подмножеств множества P, $i \in \overline{0, d_j - 1}$, $j \in \overline{1, w}$.

Требуется установить, существует ли схема множественного разделения секрета $\sigma(G)$ над кольцом $R = \mathbf{Z}/(m)$, удовлетворяющая следующему условию: для любых $i \in \overline{0, d_j - 1}$, $j \in \overline{1, w}$ элементы множества $\Delta(i, j)$ и только они являются минимальными (относительно включения) коалициями участников, которые при объединении своих проекций заведомо могут восстановить секретные ключи s_{lj} с номерами $0 \le l \le d_j - i$ (и, возможно, некоторые другие ключи из набора $(s_{ij}) \in S$, $i \in \overline{0, d_j - 1}$, $j \in \overline{1, w}$). В случае существования такой СМРС требуется построить определяющую ее матрицу G.

Ниже предлагается алгоритм решения поставленной задачи, основанный на утверждениях теорем 3 и 4.

Алгоритм состоит из двух этапов, на первом из которых для каждого $j \in \overline{1, w}$ проверяется существование и (в случае положительного результата проверки) строится матрица $G^{(j)}$ над кольцом R_j такая, что для любого $i \in \overline{0, d_j - 1}$ совокупность минимальных коалиций участников СМРС $\sigma(G^{(j)})$, способных восстановить не менее, чем $d_j - i$ младших p_j-х разрядов числа s_j вида (1), совпадает с множеством $\Delta(i, j)$. На втором этапе по найденным матрицам $G^{(j)}$, $j \in \overline{1, w}$, с использованием известного алгоритма, основанного на китайской теореме об остатках [12], вычисляются элементы искомой матрицы G над кольцом R, удовлетворяющей условию $G^{(j)} \equiv G \pmod{p_j^{d_j}}$, $j \in \overline{1, w}$.

Приведем более подробное описание первого этапа предлагаемого алгоритма. Этот этап состоит из трех шагов, выполняемых последовательно для каждого $j \in \overline{1, w}$.

Обозначим $\mu(\Delta(i, j)) = \{A \subseteq P \mid \exists\, B \in \Delta(i, j)\colon A \supseteq B\}$ монотонный класс подмножеств множества P с базисом $\Delta(i, j)$, $i \in \overline{0, d_j - 1}$, положим:

$$\Sigma(0, j) = \mu(\Delta(0, j)),\ \Sigma(i, j) = \mu(\Delta(i, j)) \setminus \mu(\Delta(i - 1, j)),\ i \in \overline{1, d_j - 1}.$$

На первом шаге по заданным совокупностям $\Delta(i, j)$, $i \in \overline{0, d_j - 1}$, строятся множества $\Sigma^0(i, j)$ и $\overline{\Delta^1}(i, j)$, состоящие из всех минимальных элементов класса $\Sigma(i, j)$ и всех максимальных элементов класса $2^P \setminus \mu(\Delta(i, j))$ соответственно,

$i \in \overline{0, d_j - 1}$.

Заметим, что $\Sigma^0(0, j) = \Delta(0, j)$. При $i \in \overline{1, d_j - 1}$ для построения множества $\Sigma^0(i, j)$ для каждого $v \in \overline{1, q_{ij}}$ проверяется условие

$$B_v(i, j) \supseteq B_\mu(i-1, j),\ \mu \in \overline{1, q_{i-1, j}}\,. \tag{11}$$

Если условие (11) выполняется, то $B_v(i, j) \in \Sigma^0(i, j)$, в противном случае — $B_v(i, j) \notin \Sigma^0(i, j)$. Временная сложность построения всех множеств $\Sigma^0(i, j)$, $i \in \overline{0, d_j - 1}$, составляет $\sum_{i=1}^{d_j - 1} q_{ij} q_{i-1, j}$ операций проверки включения множеств друг в друга.

Для построения множеств $\overline{\Delta}^1(i, j)$, $i \in \overline{0, d_j - 1}$, обозначим M_1 (i, j), …, $M_{s_{ij}}(i, j)$ все минимальные (относительно включения) подмножества множества P такие, что $M_k(i, j) \cap B_t(i, j) \neq \varnothing$ для всех $k \in \overline{1, s_{ij}}$, $t \in \overline{1, q_{ij}}$. Заметим, что справедливо следующее равенство:

$$\overline{\Delta}^1(i, j) = \{P \setminus M_1(i, j), \ldots, P \setminus M_{s_{ij}}(i, j)\}. \tag{12}$$

Временная сложность основанного на формуле (12) алгоритма построения множеств $\overline{\Delta}^1(i, j)$, $i \in \overline{0, d_j - 1}$, составляет не более $2^n n d_j$ двоичных операций (сравнения булевой переменной с нулем).

На втором шаге осуществляются проверка существования и построение (в случае существования) матрицы $C^{(j)}$ над кольцом R_j, удовлетворяющей условиям 3(а), 3(б) теоремы 4. Не останавливаясь, в силу ограничений на объем статьи, на детальном описании этих процедур, отметим, что матрица $C^{(j)}$ формируется строка за строкой, по методу поиска с возвращением. Каждая очередная строка этой матрицы выбирается в соответствии с условием 3(а), после чего для полученной (текущей) матрицы проверяется совместность систем линейных уравнений вида (10) над кольцом R_j. Если все указанные СЛУ совместны, выбирается следующая строка матрицы $C^{(j)}$ и т.д. Проверка совместности и построение (в случае совместности) общих решений СЛУ вида (10) осуществляются с использованием известного алгоритма Дж. Смита [11]. Если все СЛУ (10) над кольцом R_j, соответствующие текущей матрице, совместны, то совокупность их общих решений сохраняется и используется при проверке совместности и вычислении общих решений новых СЛУ, соответствующих матрице, полученной в результате добавления к текущей матрице очередной (новой) строки.

Можно показать, что временная сложность процедур, выполняемых на втором шаге первого этапа алгоритма, составляет не более

$$T_j(n) = \left(6n^2 + 5n - 1\right)\sum_{i=0}^{d_j - 1}\left|\overline{\Delta}^{-1}(i, j)\right|\left(p_j{}^{d_j} - 1\right)^{\left(\sum_{i=0}^{d_j-1}\sum_{t=1}^{r_{ij}}|A_t(i,j)|-n\right)} d_j^{\,n} \qquad (13)$$

арифметических операций (сложения, вычитания, умножения, обращения) в кольце R_j.

Третий шаг заключается в построении матрицы $G^{(j)}$ путем вычисления общего решения СЛУ $C^{(j)}x^{\downarrow} = 0^{\downarrow}$ над кольцом R_j с помощью алгоритма Смита [11]. Трудоемкость этого шага оценивается сверху величиной, равной $\frac{10}{3}n^3 - 2n^2 - \frac{1}{3}n$ арифметическим операциям (сложения, вычитания, умножения, обращения) в кольце R_j.

Отметим, что основной вклад в трудоемкость первого этапа, равно как и всего алгоритма в целом, вносит выполняемая на втором шаге процедура поиска с возвращением, временная сложность которой (для каждого $j \in \overline{1, w}$) определяется по формуле (13).

Заключение

В настоящей статье предложена линейная схема множественного разделения секрета над кольцом вычетов по модулю m, обобщающая известные конструкции «векторных» СРС над конечными полями [8] и примарными кольцами вычетов [9]. Дано явное описание иерархии доступа предложенной СМРС; в частности, показано, что ее элементы находятся во взаимно однозначном соответствии с делителями числа m. На основе полученного критерия существования линейной СМРС для заданной иерархии доступа разработан алгоритм построения такой СМРС, обобщающий ранее известный алгоритм построения «векторной» СРС над конечным полем [10].

Следует отметить, что очевидными достоинствами предложенной СМРС являются ее совершенность и простота (алгоритмическая эффективность) процедур вычисления проекций секретных ключей и восстановления их соответствующими коалициями участников схемы. Важной, с практической точки зрения, является задача нахождения необходимых и достаточных условий, при которых линейная схема множественного разделения секрета является оптимальной (среди всех СМРС, реализующих данную иерархию доступа) по критерию минимума наибольшей из длин проекций секретных ключей, хранящихся у участников СМРС. Решение этой задачи авторы предполагают изложить в отдельной статье.

1. *Jackson W.-A., Martin K.M., O'Keefe C.M.* Multisecret Threshold Schemes // Advances in Cryptology — CRYPTO'93. — Lecture Notes in Computer Science. — Vol. 773. — P. 126–135.

2. *Blundo C., De Santis A., Di Crescenzo G., Gaggia A.G., Vaccaro U.* Multi-Secret Sharing Schemes // Advances in Cryptology — CRYPTO'95. — Lecture Notes in Computer Science. — Vol. 832. — P. 150–163.

3. *Stinson D.R.* An Explication of Secret Sharing Schemes // Designs, Codes and Cryptography. — 1992. — Vol. 2. — P. 357–390.

4. *Seberry J., Charnes Ch., Pieprzyk J., Safavi-Naini R.* 41 Crypto Topics and Application. CRC Handbook of Algorithms and Theory of Computation. — CRC Press: Baca Raton, 1999. — P. 1–51.

5. *Franklin M., Yung M.* Communication Complexity of Secure Computation // Proceedings of 24th Annual ACM Symposium on Theory of Compruting, 1992. — P. 699–710.

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

7. *Blundo C., De Santis A., Vaccaro U.* Efficient Sharing of Many Secrets // Proceedings of STACS'93. — Lecture Notes in Computer Science. — Vol. 665. — P. 692–703.

8. *Brickell E.F.* Some Ideal Secret Sharing Schemes // J. Combin. Math. and Combin. Comput. — 1989. — № 9. — P. 105–113.

9. *Ashikhmin A., Barg A.* Minimal Vectors in Linear Codes // IEEE Trans. on Inform. Theory. — 1998. — Vol. 5. — P. 2010–2018.

10. *Van Dijk M.* A Linear Construction of Perfect Secret Sharing Schemes // Advances in Cryptology — EUROCRYPT'94. — Lecture Notes in Comput. Science. — Vol. 950. — P. 23–34.

11. *Елизаров В.П.* Конечные кольца. Основы теории. — М., 1993. — 255 с.

12. *Ноден П., Китте К.* Алгебраическая алгоритмика: Пер. с франц. — М.: Мир, 1999. — 720 с.

Поступила в редакцию 30.09.2005