УДК 003.26:51:004(075.8)

Т.В. ГАЛИБУС, Н.Н. ШЕНЕЦ

ЭЛЕМЕНТАРНЫЕ МОДУЛЯРНЫЕ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

The special modular secret sharing schemes are constructed over the ring of integers. The access structure is paired i. e. maximal unauthorized subsets are some single participants and the pairs of participants. We prove that such access structure can be realized by means of modular secret sharing scheme with the co-prime moduli and provide the algorithm of constructing such moduli for any given paired structure.

В основе модулярного разделения секрета лежит следующее простое наблюдение, принадлежащее С. Асмусу, Д. Блюму [1] и М. Миньотту [2]. Пусть $m_1 < m_2 < ... < m_t$ – система попарно взаимно простых натуральных модулей. Если секретом является некоторое натуральное число c, а секретом i-го участника, $i \in P = \{1, 2, ..., t\}$, – наименьший неотрицательный вычет c по модулю m_i, т. е. $c_i \equiv c \pmod{m_i}$, то восстановление исходного секрета c группой участников $A \subseteq P$ осуществляется путем решения системы сравнений $x \equiv c_i \pmod{m_i}$, $i \in A$. Это можно сделать, например, с помощью китайской теоремы об остатках. При этом правильно найдет секрет c лишь та группа участников A, для которой выполнено условие $c < \prod_{i \in A} m_i$.

Напомним, что структурой доступа называется семейство подмножеств Γ множества участников $P = \{1, 2, ..., t\}$, обладающее свойством монотонности, т. е. $A \in \Gamma, A \subset B \subset P \Rightarrow B \in \Gamma$. Подмножества из семейства Γ называются разрешенными, все остальные подмножества – запрещенными. Они образуют структуру отказа Γ^*. Для них выполняется двойственное условие монотонности $A \in \Gamma^*, B \subset A \subset \Gamma^* \Rightarrow B \in \Gamma^*$.

Важным частным случаем структуры доступа является (k, t)-пороговая структура доступа. Здесь разрешенным будет всякое подмножество A, если $|A| \geq k$, для некоторого k, $1 \leq k \leq t$.

В работах [3], [4] было показано, что любая структура доступа допускает модулярную реализацию в кольцах целых чисел и полиномов от любого числа переменных над полем Галуа. При этом, однако, используются произвольные модули, а не только попарно взаимно простые.

Вместе с тем до настоящего времени остается нерешенным вопрос о том, какие структуры доступа помимо пороговых допускают модулярную реализацию с помощью попарно взаимно простых модулей. Этот вопрос уже обсуждался в печати [5]. Он возник потому, что с взаимно простыми модулями легче работать, поскольку в этом случае секрет восстанавливается применением китайской теоремы об остатках.

Основной целью данной статьи является частичное решение этого вопроса. Далее будет удобно называть схему разделения секрета (СРС) с попарно взаимно простыми модулями *элементарной*, поскольку такие схемы тесно связаны со структурами доступа специального вида.

Определение 1. Структуру доступа Γ на множестве участников P назовем *связной*, если для любой упорядоченной четверки попарно непересекающихся подмножеств $A_1, A_2, A_3, A_4 \subseteq P$ выполняется следующее условие: среди подмножеств $A_1 \cup A_2$, $A_3 \cup A_4$, $A_1 \cup A_3$, $A_2 \cup A_4$ не может быть двух разрешенных $A_1 \cup A_2$, $A_3 \cup A_4$ и двух запрещенных $A_1 \cup A_3$, $A_2 \cup A_4$.

Отметим, что в любой структуре доступа имеются минимальные по включению подмножества участников. Будем называть семейство всех таких подмножеств базисом структуры доступа. Можно определить и базис структуры отказа как семейство максимальных по включению запрещенных подмножеств участников.

Определение 2. Структура доступа Γ на множестве участников P называется парной, если базис структуры отказа Γ_2 состоит из некоторого семейства подмножеств $\{X\}$, где $|X| \leq 2$, т. е. в него входят лишь отдельные участники и их пары.

Таким образом, парная структура доступа есть обобщение (2, t)-пороговой.

Лемма 1. Если структура доступа реализуется с помощью элементарной модулярной СРС, то она является связной.

Доказательство. Прежде всего отметим, что в случаях $t = 2$ и $t = 3$ все структуры доступа являются связными, поскольку при этом не существует четырех попарно непересекающихся подмножеств участников. Общий случай будем доказывать от противного. Рассмотрим соответствующую четверку подмножеств участников A_1, A_2, A_3, A_4. Допустим, что структура доступа не является связной. Это означает, что $A_1 \cup A_2$ и $A_3 \cup A_4$ запрещены, а $A_1 \cup A_3$ и $A_2 \cup A_4$ разрешены. Обозначим произведение попарно взаимно простых модулей, соответствующее множеству A_i, через M_i. Тогда окажется, что $M_1 M_2 < M_1 M_3$ и $M_2 M_4 > M_3 M_4$. Разделив первое неравенство на второе, будем иметь противоречие $M_1 / M_4 < M_1 / M_4$.

Таким образом, получено необходимое условие элементарности. Нашей целью является доказательство достаточности этого условия для парных структур доступа. Нам понадобится одно свойство парных связных структур доступа.

Лемма 2. Пусть на множестве участников $P = \{1, 2, ..., t\}$ задана парная связная структура доступа. Тогда существуют попарно взаимно простые модули $m_1, m_2, ..., m_t$ такие, что произведение модулей, отвечающих разрешенному множеству вида $X \cup \{l\}$, будет всегда больше любого произведения, отвечающего запрещенному $X \cup \{j\}$.

Доказательство. Если $X = \varnothing$, то мы имеем дело с разрешенным участником l и запрещенным участником j. Если всем разрешенным участникам раздать модули, которые будут больше секрета, то условие $m_l > M_A$ будет выполняться автоматически сразу для всех запрещенных подмножеств $A \in \Gamma^*$ и, в частности, для запрещенных участников. Естественно, такие модули формируются после нахождения подходящих модулей для запрещенных участников и их пар. Поэтому далее рассматриваем только запрещенных участников.

Пусть $X \neq \varnothing$, т. е. $|X| = 1$. Все пары, которые отличаются лишь одним участником в составе, т. е. пары вида $\{l, j\}$, $l, j \in P, j \neq l$, задают некое условие на модули. Иными словами, если $\{l, j_1\}$ разрешена, а $\{l, j_2\}$ запрещена, то $m_{j_1} > m_{j_2}$.

Последовательно рассматривая пары участников с этим условием, мы сможем указать порядок попарно взаимно простых модулей такой, что произведение их, соответствующее разрешенному $\{l\}\cup\{j_1\}$, будет всегда больше произведения, соответствующего любому запрещенному $\{l\}\cup\{j_2\}$.

Покажем, что порядок будет задан корректно, т. е. не существует последовательности различных индексов $i_1, i_2, ..., i_s$ такой, что $m_{i_1} > m_{i_2} > ... > m_{i_s} > m_{i_1}$. Докажем это утверждение индукцией по s – длине цепочки.

В случае $s = 2$ получаем $m_{i_1} > m_{i_2}$, $m_{i_2} > m_{i_1}$, откуда следует, что подмножества $\{l\}\cup\{i_1\}$, $\{l'\}\cup\{i_2\}$ являются разрешенными, а $\{l\}\cup\{i_2\}$, $\{l'\}\cup\{i_1\}$ – запрещенными для некоторых участников l и l'. Однако для связной структуры доступа это невозможно.

Теперь предположим, что не существует цепочек длины k, $k \geq 2$, и докажем, что также не существует цепочки длины k+1. Имеем последовательность неравенств $m_{i_1} > m_{i_2} > ... > m_{i_{k+1}} > m_{i_1}$. Это равносильно тому, что существует набор модулей $m_{j_1}, m_{j_2}, ..., m_{j_{k+1}}$ такой, что выполнено $m_{j_1} m_{i_1} > m_{j_1} m_{i_2}; m_{j_2} m_{i_2} > m_{j_2} m_{i_3}; ...; m_{j_{k+1}} m_{i_{k+1}} > m_{j_{k+1}} m_{i_1}$. Другими словами, пары $\{i_l, j_l\}$ разрешены, а пары $\{i_{l \bmod(k+1)+1}, j_l\}$ запрещены, $l = \overline{1, k+1}$. Очевидно, что $m_{j_l} \neq m_{j_{l \bmod(k+1)+1}}$, $l = \overline{1, k+1}$, так как в этом случае пара $\{i_{l \bmod(k+1)+1}, j_l\}$ одновременно и разрешена, и запрещена.

Далее покажем, что $m_{j_l} \neq m_{i_n} \ \forall\, l, n = \overline{1, k+1}$. Действительно, пусть $m_{j_l} = m_{i_n}$ для некоторых l и n. Очевидно, что $l \neq n$. Рассмотрим два неравенства

$$\begin{cases} m_{j_{l-1}} m_{i_{l-1}} > m_{j_{l-1}} m_{i_l}, \\ m_{i_l} m_{i_n} > m_{i_n} m_{i_{l \bmod(k+1)+1}}. \end{cases}$$

Если $l = 1$, то $l - 1$ полагается равным $k + 1$. Рассмотрим участников $\{j_{l-1}, i_{l-1}, i_l, i_n\}$. Они все различны, поскольку $j_{l-1} \neq i_{l-1} \neq i_l \neq i_n = j_l \neq j_{l-1}$. Пары $\{j_{l-1}, i_{l-1}\}$ и $\{i_l, i_n\}$ разрешены, а пара $\{j_{l-1}, i_l\}$ запрещена. Поскольку структура доступа связная, то пара $\{i_n, i_{l-1}\}$ является разрешенной. Но тогда мы можем уменьшить длину цепочки, так как из сказанного следует, что $m_{i_{l-1}} > m_{i_{l \bmod(k+1)+1}}$. Получили противоречие с тем, что не существует цепочки длины k.

Таким образом, показано, что $m_{j_l} \neq m_{i_n} \ \forall\, l, n = \overline{1, k+1}$. Теперь рассмотрим два первых неравенства

$$\begin{cases} m_{i_1} m_{j_1} > m_{j_1} m_{i_2}, \\ m_{i_2} m_{j_2} > m_{i_3} m_{j_2}. \end{cases}$$

Пары $\{i_1, j_1\}$ и $\{i_2, j_2\}$ разрешены, а пара $\{j_1, i_2\}$ запрещена. Следовательно, пара $\{i_1, j_2\}$ должна быть разрешенной. Но тогда мы опять уменьшаем длину цепочки, так как получаем $m_{i_1} m_{j_2} > m_{j_2} m_{i_3} \Rightarrow m_{i_1} > m_{i_3}$, что противоречит предположению индукции. Лемма доказана.

Далее перенумеруем участников в порядке возрастания их модулей, согласно предыдущей лемме.

В работе [4] были получены результаты по реализации модулярных СРС в кольце полиномов $\mathbb{F}_q[x]$ над полем Галуа $\mathbb{F}_q$. Оказывается, что элементарные модулярные схемы разделения секрета в кольце целых чисел $\mathbb{Z}$ и в кольце $\mathbb{F}_q[x]$ связаны между собой, что отражает следующая

Теорема 1. Структура доступа реализуется элементарной модулярной СРС над кольцом полиномов $\mathbb{F}_q[x]$ тогда и только тогда, когда она реализуется элементарной СРС над кольцом целых чисел $\mathbb{Z}$.

Доказательство. Пусть задана структура доступа Γ и соответствующая элементарная реализация над кольцом $\mathbb{F}_q[x]$. При этом неравенство Миньотта для произведений $\prod_{i \in A, A \subseteq \Gamma} m_i > \prod_{j \in A, A \not\subset \Gamma} m_j$ трансформируется в неравенство для сумм степеней полиномов $\sum_{i \in A \in \Gamma} \deg m_i > \sum_{j \in A \notin \Gamma} \deg m_j$.

Положим $t' = \sum_{i=1}^{t} \deg m_i$ и рассмотрим $\left(\left\lceil \frac{t'}{2} \right\rceil, t'\right)$-пороговую схему над кольцом $\mathbb{Z}$. Эта схема является, как нетрудно заметить, (k, t')-пороговой при любом k. Тогда для элементарной реализации исходной структуры доступа над кольцом $\mathbb{Z}$ достаточно взять следующие модули: $\bar{m}_i = \prod_{j=1}^{\deg m_i} m'_{s+j}$, где $s = \sum_{l=1}^{i-1} \deg m_l$.

Обратное утверждение доказывается при помощи логарифмирования, причем для достижения необходимого числа попарно взаимно простых полиномов одной степени достаточно лишь увеличить степени всех модулей на некоторую константу. Теорема доказана.

Теорема 2. Существует элементарная модулярная реализация всякой парной связной структуры доступа.

Доказательство. Парная связная структура доступа задается набором максимальных запрещенных подмножеств $\{X_k\}$, $|X_k| \le 2$.

Согласно лемме 2 можно выбрать попарно взаимно простые модули $m_1 < m_2 < \ldots < m_t$ так, что произведения модулей разрешенных и запрещенных подмножеств, отличающихся лишь одним участником, упорядочены нужным нам образом.

Осталось показать, что, меняя модули, но сохраняя их порядок $m_1 < m_2 < \ldots < m_t$, можно добиться выполнения неравенства Миньотта для произведений

$$\prod_{i \in A, A \subseteq \Gamma} m_i > \prod_{j \in A, A \not\subset \Gamma} m_j.$$

Тем самым обеспечивается наличие промежутка для выбора секрета между наибольшим произведением модулей запрещенных участников и наименьшим произведением модулей разрешенных.

Рассмотрим варианты, которые не подпадают под действие леммы 2. Про разрешенных участников уже было сказано, поэтому их мы не рассматриваем. Из рассмотрения исключим также запрещенных участников и пары, содержащие их. Тогда для всех оставшихся участников существует, как минимум, одна запрещенная пара, его содержащая.

Пусть $\{i, j\}$ – запрещенная пара, $\{k, l\}$ – разрешенная пара, причем i, j, k, l попарно различны. Пусть при этом выполняется неравенство $m_i m_j > m_k m_l$. Рассмотрим пары $\{i, l\}$, $\{j, k\}$.

Во-первых, пары $\{i, l\}$, $\{j, k\}$ могут быть одновременно либо запрещенными, либо разрешенными. Пусть обе эти пары разрешены. Случай двух запрещенных пар рассматривается аналогично. Поскольку неравенство $m_i m_j < m_k m_l$ не выполняется, то с учетом выбора модулей при этом $m_i m_j < m_i m_l$, $m_i m_j < m_j m_k \Rightarrow m_j < m_l$, $m_i < m_k \Rightarrow m_i m_j < m_k m_l$. Получено противоречие.

Во-вторых, пусть пара $\{i, l\}$ запрещена, а $\{j, k\}$ разрешена. Отсюда сразу получаем, что $m_k > m_i$. Покажем, что условие связности обеспечивает корректность упорядочения таких пар, т. е. случай $m_l < m_i < m_k < m_j$ невозможен. Любое другое упорядочение этих модулей будет корректным.

Предположим, что $m_k < m_j$. Пара $\{k, l\}$ разрешена, поэтому разрешена и пара $\{j, l\}$. Тогда $m_i < m_l$. Если $\{j, l\}$ запрещена, то получаем противоречие $m_k > m_j$, что невозможно в силу леммы 2. Аналогично показывается, что если $m_i > m_l$, то $m_k > m_j$.

Таким образом, условие связности обеспечивает корректность упорядочения пар. Отметим, что если два участника s и p *равнозначны*, т. е. для любого x пары $\{s, x\}$ и $\{p, x\}$ однотипны, то между ними не будет установлено отношение по лемме 2. Будем вместо равнозначных участников рассматривать одного, но учитывая при этом пары $\{s, p\}$, образованные двумя такими участниками. Таким образом, оставшиеся участники строго упорядочены относительно друг друга. При этом в случае пороговой структуры доступа останется только один участник, поскольку в такой структуре все участники равнозначны. Поэтому далее не рассматриваем пороговую структуру.

Для построения модулей воспользуемся теоремой 1. Сначала пронумеруем модули в порядке их возрастания $m_1 < m_2 < \ldots < m_t$ и поставим каждому в соответствие натуральное число $P_i = i$, $i = \overline{1, t}$. Число P_i есть не что иное, как степень полинома, соответствующего модулю m_i. Далее упорядочим в обратном лексикографическом порядке пары из базисов разрешенных и запрещенных множеств соответственно. При этом первый модуль в паре всегда меньше второго либо равен ему. Предлагается следующий алгоритм изменения чисел P_i, чтобы удовлетворить неравенство Миньотта.

На первом шаге выбирается минимальная разрешенная пара $\{i_1, i_2\}$. Среди всех запрещенных пар выбираются все $\{j_1, j_2\}$ такие, что $i_1 \le j_1 \le j_2 < i_2$. Если таких пар нет, переходим на следующий шаг. Пусть такие пары есть, и $g_1 = \min\limits_{\{j_1, j_2\}}(P_{i_1} + P_{i_2} - P_{j_1} - P_{j_2})$. Если $g_1 \le 0$, то увеличим все числа P_i, $i \ge i_2$, на число (s–g_1). Здесь s – некоторый заранее заданный порог, $s > 0$. При этом все запрещенные пары $\{j_1, j_2\}, j_2 \le i_2$, будут иметь меньшее значение, чем пара $\{i_1, i_2\}$, а следовательно, и меньшее, чем любая разрешенная пара $\{i, i_2\}, i > i_1$.

На следующем шаге увеличиваем значение i_2 на единицу. Сначала находим минимальную разрешенную пару $\{i_1, i_2\}$ и выполняем те же действия, что и на первом шаге. Далее находим максимальную запрещенную пару $\{j_1, i_2\}$. Ясно, что $j_1 < i_1$, так как упорядочение пар корректно. Просматриваем все разрешенные пары $\{l_1, l_2\}$, попавшие в полуинтервал $(j_1, i_2]$. Находим число $g_2 = \min\limits_{\{l_1, l_2\}}(P_{l_1} + P_{l_2} - P_{j_1} - P_{i_2})$, и если $g_2 \le 0$, то увеличиваем все P_i, $i \ge \min\limits_{\{l_1, l_2\}} l_1$, на число ($s$–$g_2$). Очевидно, что после таких сдвигов значения всех рассмотренных разрешенных пар будет больше просмотренных запрещенных.

Продолжаем описанную выше процедуру до тех пор, пока не просмотрим все пары. При этом порядок модулей не нарушается, а неравенство Миньотта выполняется, причем зазор между разрешенными и запрещенными парами не меньше s. Обозначим максимальное значение запрещенных пар через M_1, а минимальное значение разрешенных – через M_2. Тогда $M_2 - M_1 \ge s$.

Теперь рассмотрим запрещенных участников. Всем им дадим одно и то же значение $\boldsymbol{P}$, так как они равнозначны. Необходимо, чтобы $\boldsymbol{P} + P_i \ge M_2$ для любого $i = \overline{1, t}$. Этого легко добиться, если положить $\boldsymbol{P} = M_2 - \min\limits_i P_i$. Для разрешенных участников положим $P_p = M_2$. Далее применяем рассуждения из теоремы 1 с учетом числа равнозначных участников.

Таким образом, утверждение теоремы (существование общего промежутка для выбора секрета) доказано.

В качестве примера рассмотрим все парные структуры доступа над множеством $P = \{1, 2, 3, 4\}$ из 4 участников, реализуемые в рамках элементарных модулярных СРС (таблица).

Парные элементарные структуры доступа для 4 участников

Набор максимальных запрещенных подмножеств	Упорядочение модулей
1. (1,4),(2,4),(3,4) – пороговые	Произвольное
2. {1,2} (одна пара)	$m_1, m_2 < m_3, m_4$
3. {1,2}, {1,3} (две пересекающиеся пары)	$m_1 < m_2, m_3 < m_4$
4. {1}, {2,3} (один участник и одна пара)	$m_1 < m_2, m_3 < m_4$
5. {1} (один участник)	$m_1 < m_2, m_3, m_4$
6. {1}, {2} (два участника)	$m_1, m_2 < m_3, m_4$
7. {1}, {2}, {3} (три участника)	$m_1, m_2, m_3 < m_4$
8. {1}, {2}, {3,4} (два участника и одна пара)	$m_3, m_4 < m_1, m_2$
9. {1}, {2,3}, {2,4} (один участник и две пересекающиеся пары)	$m_2 < m_3, m_4 < m_1$
10. {1}, {2,3}, {2,4}, {3,4} (один участник и три пересекающиеся пары)	$m_2, m_3, m_4 < m_1$
11. {1,2}, {1,3}, {2,3} (три пересекающиеся пары – вариант 1)	$m_1, m_2, m_3 < m_4$
12. {1,2}, {1,3}, {1,4} (три пересекающиеся пары – вариант 2)	$m_1 < m_2, m_3, m_4$
13. {1,2}, {1,3}, {1,4}, {2,3} (четыре пары)	$m_1 < m_2, m_3 < m_4$
14. {1,2}, {1,3}, {1,4}, {2,3} ,{2,4} (пять пар)	$m_1, m_2 < m_3, m_4$

Таким образом, нам удалось построить обобщение модулярной СРС, которое может применяться для реализации непороговых структур доступа. В частности, дан исчерпывающий ответ на вопрос о том, какие парные структуры доступа могут быть реализованы с помощью элементарных модулярных СРС. Отметим также, что при достаточно близких модулях схема обладает лучшими свойствами согласно критериям, предложенным в работе [6].

1. Asmuth C.A., Bloom J. // IEEE Transactions on Information Theory. 1983. Vol. 29. P. 156.
2. Mignotte M. Advances in cryptology – Eurocrypt'82 // LNCS. 1982. P. 371.
3. Galibus T., Matveev G. // ENTCS. 2007. Vol. 186. URL: www.elsevier.com/locate/entcs. P. 41.
4. Галибус Т.В. // Вестн. БГУ. Сер. 1. 2006. № 2. С. 97.
5. Iftene S. // Cryptology ePrint Archive. 2005. URL: http://eprint.iacr.org/2005/408.pdf
6. Quisquater M., Preneel B., Vandewalle J. // LNCS. 2002. Vol. 2274. P. 199.

Поступила в редакцию 17.01.08.

Татьяна Васильевна Галибус **–** аспирант кафедры методов математического моделирования и анализа данных. Научный руководитель – кандидат физико-математических наук, доцент кафедры высшей математики Г.В. Матвеев.

Николай Николаевич Шенец **–** аспирант кафедры методов математического моделирования и анализа данных. Научный руководитель – Г.В. Матвеев.