УДК 621.391:519.7:510.5

А. Н. Алексейчук
Специальный факультет СБ Украины в составе Военного института телекоммуникаций и информатизации НТУУ «КПИ»

Совершенные схемы разделения секрета и конечные универсальные алгебры

Предложен метод построения совершенных схем разделения секрета по конгруэнциям конечных универсальных алгебр, обобщающий известные способы синтеза линейных схем разделения секрета над конечными полями или коммутативными кольцами.

Ключевые слова: *криптографическая защита информации, схема разделения секрета, структура доступа, универсальная алгебра.*

Введение

Схема разделения секрета (СРС) [1–4] представляет собой пару криптографических протоколов, позволяющих «распределять» секрет σ_0 (рассматриваемый как элемент некоторого абстрактного конечного множества S_0) среди участников 1, 2, …, n таким образом, чтобы только некоторые, заранее определенные (разрешенные) группы участников могли восстановить значение секрета при объединении своих компонент (проекций секрета). Схема разделения секрета называется совершенной, если любая запрещенная группа участников не может получить никакой дополнительной, к имеющейся априорной, информации о возможном значении секретного ключа, и несовершенной — в противном случае.

Важнейшим показателем практичности схемы разделения секрета является ее информационная скорость (information rate), определяемая как отношение длины секрета σ_0 к максимальной длине соответствующих ему проекций [3, 4]. При решении прикладных задач с использованием СРС, как правило, стремятся спроектировать схему разделения секрета таким образом, чтобы (при прочих равных условиях) повысить ее информационную скорость, то есть минимизировать максимальную длину проекций, хранящихся у ее участников. Наиболее «экономичными» в этом смысле среди совершенных СРС являются идеальные схемы разделения секрета, для которых длины проекций секретных ключей в точности равны длине секрета (логарифму мощности множества S_0).

Известно [5, 6], что идеальные СРС существуют не для каждой структуры доступа (совокупности разрешенных групп) на множестве участников схемы. С

другой стороны, общие методы построения совершенных СРС для произвольных монотонных структур доступа [7, 8] приводят к малопрактичным конструкциям СРС с экспоненциально малыми (от числа участников) информационными скоростями. Задачи полного описания идеальных структур доступа и разработки методов построения совершенных СРС, имеющих наибольшую (для данной структуры доступа) информационную скорость, являются в настоящее время важнейшими открытыми проблемами в области теоретического исследования схем разделения секрета [9, 10].

Большинство известных совершенных СРС (см., например, [3, 4, 11–13]) представляют собой линейные схемы, в которых секретные ключи и их проекции являются элементами конечномерных векторных пространств над конечным полем, а вычисление проекций осуществляется с помощью линейных преобразований, применяемых к секретным ключам и вспомогательным случайным данным. Простота построения, изучения свойств и разнообразие приложений линейных СРС над конечными полями обусловливают повышенное внимание, уделяемое этим схемам в современных теоретических и прикладных исследованиях [4, 9, 14].

Известен ряд обобщений линейных СРС над полями. Так, в [15–17] изучаются схемы разделения секрета (с определенными дополнительными свойствами), определяемые в терминах гомоморфизмов конечных абелевых групп или свободных модулей над коммутативным кольцом с единицей. Практически эффективные конструкции нелинейных СРС для определенных структур доступа предложены в [10]. Вместе с тем, задача построения новых классов совершенных схем разделения секрета, реализующих различные структуры доступа и имеющих приемлемые, с практической точки зрения, информационные скорости, является попрежнему актуальной.

В настоящей статье предложен общий метод построения совершенных СРС на основе систем отношений эквивалентности на конечном множестве, в частности, систем конгруэнций конечных универсальных алгебр. Показано, что каждая совершенная схема разделения секрета может быть (по существу однозначно) задана системой отношений эквивалентности, удовлетворяющих определенным условиям. В частности, если указанные отношения эквивалентности являются конгруэнциями конечной абелевой группы с операторами, представляющей собой модуль над кольцом с единицей или векторное пространство над полем, то предложенная конструкция СРС приводит к обычным линейным схемам разделения секрета [3, 11–13]. Разнообразие и особенности строения конкретных классов универсальных алгебр могут служить основанием для возможного повышения эффективности известных совершенных СРС на основе предложенного метода.

Дальнейшее изложение построено следующим образом. В п. 1 приводятся необходимые сведения об отношениях эквивалентности, универсальных алгебрах и совершенных схемах разделения секрета. Более подробную информацию по этим вопросам можно найти соответственно в [18–20] и [3–6]. В п. 2 изложены основные результаты статьи, а в п. 3 сформулированы краткие выводы и задачи дальнейших исследований.

1. Вспомогательные понятия и результаты

Пусть X — конечное множество. Напомним, что (бинарным) отношением на множестве X называется произвольное непустое подмножество декартова произведения $X^2 = X \times X$. Рефлексивное, симметричное и транзитивное отношение на множестве X называется отношением эквивалентности (ОЭ) [18].

Обозначим $\vartheta(X)$ совокупность всех ОЭ на множестве X. Известно [18], что $\vartheta(X)$ является полной решеткой относительно операций $\wedge$ и $\vee$ (пересечения и объединения отношений эквивалентности соответственно). Для любых $\rho, \varepsilon \in \vartheta(X)$ пересечение $\rho \wedge \varepsilon$ совпадает с точной нижней гранью ОЭ ρ и ε в решетке $\vartheta(X)$, то есть наибольшим отношением эквивалентности, содержащимся в каждом из отношений ρ, ε. Объединение (точная верхняя грань) $\rho \vee \varepsilon$ отношений эквивалентности ρ и ε совпадает с пересечением всех ОЭ на множестве X, содержащих одновременно ρ и ε.

Композиция $\rho \bullet \varepsilon$ отношений эквивалентности ρ и ε определяется равенством:

$$\rho \bullet \varepsilon = \{(x, y) \in X^2 \mid \exists\, z \in X\colon (x, z) \in \rho, (z, y) \in \varepsilon\}.$$

Для любых $\rho, \varepsilon \in \vartheta(X)$ справедливы включения $\rho, \varepsilon \subseteq \rho \bullet \varepsilon \subseteq \rho \vee \varepsilon$. При этом равносильны следующие утверждения [18, 20]:

(а) $\rho \bullet \varepsilon$ — отношение эквивалентности на множестве X;

(б) ОЭ ρ и ε перестановочны, то есть $\rho \bullet \varepsilon = \varepsilon \bullet \rho$;

(в) $\rho \bullet \varepsilon = \rho \vee \varepsilon$.

Далее будем отождествлять произвольное отношение эквивалентости $\rho \in \vartheta(X)$ с фактормножеством X/ρ, то есть разбиением множества X, состоящим из различных классов эквивалентности по отношению ρ. Соответственно будем отождествлять решетку $\vartheta(X)$ с решеткой всех разбиений множества X и обозначать последнюю тем же символом. Отметим, что $\vartheta(X)$ является полумодулярной решеткой с ранговой функцией

$$r(\rho) = |X| - n(\rho),\ \rho \in \vartheta(X),$$

где $n(\rho) = |X/\rho|$ — число блоков разбиения ρ [18, 19]. Условие полумодулярности решетки $\vartheta(X)$ фактически означает, что для любых $\rho, \varepsilon \in \vartheta(X)$ выполняется неравенство:

$$n(\rho \vee \varepsilon) + n(\rho \wedge \varepsilon) \geq n(\rho) + n(\varepsilon). \qquad (1)$$

Ниже используется следующая интерпретация слагаемых в формуле (1) (см. [19], стр. 33). Пусть $A_1, \ldots, A_\nu$ A_ν и $B_1, \ldots, B_\mu$ — все различные блоки разбиений ρ и ε соответственно. Рассмотрим двудольный граф $\Gamma(\rho, \varepsilon)$ на множестве вершин $\{A_1, \ldots, A_\nu, B_1, \ldots, B_\mu\}$, в котором пара вершин $\{A_i, B_j\}$ образует (неориентированное) ребро в том и только в том случае, когда $A_i \cap B_j \neq \varnothing$, $i \in \overline{1,\nu}$, $j \in \overline{1,\mu}$. Тогда числа $n(\rho) + n(\varepsilon)$, $n(\rho \wedge \varepsilon)$ и $n(\rho \vee \varepsilon)$ равны соответственно числу вершин,

числу ребер и числу связных компонент графа $\Gamma(\rho, \varepsilon)$. В частности, для любых ρ, $\varepsilon \in \vartheta(X)$ равносильны утверждения:

(а′) $\Gamma(\rho, \varepsilon)$ является полным двудольным графом;

(б′) $n(\rho \wedge \varepsilon) = n(\rho)n(\varepsilon)$;

(в′) $\rho \bullet \varepsilon = \varepsilon \bullet \rho = 1_X$, где $1_X = X^2$ — наибольший элемент решетки $\vartheta(X)$.

Пусть $\mathfrak{R}$ — универсальная алгебра с носителем X [18]. Отношение эквивалентности ρ на множестве X называется конгруэнцией алгебры $\mathfrak{R}$, если для любой операции ω: $X^n \to X$ данной алгебры и произвольных наборов $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n) \in X^n$ выполняется условие

$$((x_i, y_i) \in \rho,\ i \in \overline{1,n}) \Rightarrow (\omega(x_1, \ldots, x_n), \omega(y_1, \ldots, y_n)) \in \rho.$$

Множество $\vartheta_{\mathfrak{R}}(X)$ всех конгруэнций алгебры $\mathfrak{R}$ является подрешеткой решетки $\vartheta(X)$. Другими словами, объединение $\rho \vee \varepsilon$ и пересечение $\rho \wedge \varepsilon$ произвольных конгруэнций ρ и ε алгебры $\mathfrak{R}$ также является ее конгруэнцией [18, 20].

Алгебра $\mathfrak{R}$ называется конгруэнц-перестановочной, если для любых двух конгруэнций $\rho, \varepsilon \in \vartheta_{\mathfrak{R}}(X)$ выполняется равенство $\rho \bullet \varepsilon = \varepsilon \bullet \rho$. Отметим, что решетка $\vartheta_{\mathfrak{R}}(X)$ конгруэнц-перестановочной алгебры $\mathfrak{R}$ является модулярной, то есть неравенство (1) обращается в равенство [18, 20]. Хорошо известны многочисленные примеры конгруэнц-перестановочных алгебр. Это — группы с операторами (в частности, ассоциативные кольца, модули над кольцом с единицей, векторные пространства над полем), конечные лупы, решетки с относительными дополнениями и др. [20].

Приведем необходимые сведения о совершенных (комбинаторных) схемах разделения секрета. При этом будем придерживаться терминологии и обозначений, введенных в [6].

Пусть S_i — непустые конечные множества, $i \in \overline{0,n}$. Положим $S = S_0 \times S_1 \times \ldots \times S_n$,

$$P = \{1, 2, \ldots, n\},\ \overline{P} = P \cup \{0\},\ 2^P = \{A: A \subseteq P\}.$$

Для любых $V \subseteq S$, $A = \{i(1), i(2), \ldots, i(k)\} \subseteq \overline{P}$, где $0 \le i(1) < i(2) < \ldots < i(k) \le n$, обозначим символом V_A мультимножество, состоящее из всех k-наборов $(s_{i(1)}, s_{i(2)}, \ldots, s_{i(k)})$, полученных в результате удаления из каждого набора $(s_0, s_1, \ldots, s_n) \in V$ компонент s_i с номерами $i \notin A$. Символом $\|V_A\|$ обозначим число различных элементов мультимножества V_A.

Пусть $\Gamma \subseteq 2^P$ — некоторый монотонный класс подмножеств множества P (то есть такой, что из условий $A \in \Gamma$, $A \subseteq B \subseteq P$ следует включение $B \in \Gamma$). Согласно определению [5, 6], множество (код) $V \subseteq S$ задает совершенную схему разделения секрета с множеством секретных ключей S_0, реализующую на множестве участников P структуру доступа Γ, если выполняются следующие утверждения:

$$\|V_{A \cup 0}\| = \|V_A\| \text{ для любого } A \in \Gamma, \qquad (2)$$

$$\|V_{A\cup 0}\| = \|V_A\|\,\|V_0\| \text{ для любого } A \in 2^P/\Gamma. \tag{3}$$

Практически «распределение» секретного ключа $\sigma_0 \in S_0$ между участниками СРС V осуществляется следующим образом. Имеется доверенный центр распределения ключей (дилер), который по заданному значению σ_0 случайно и равновероятно выбирает элемент $s = (s_0, s_1, ..., s_n) \in V$ такой, что $s_0 = \sigma_0$. Затем i-му участнику СРС по защищенному каналу связи доставляется проекция s_i ключа σ_0, $i \in \overline{1,n}$. На основании условия (2) участники, принадлежащие произвольной разрешенной группе $A \in \Gamma$, совместно смогут однозначно восстановить ключ σ_0 по имеющимся у них проекциям. При этом, в силу условия (3), никакая запрещенная группа участников $A' \in 2^P/\Gamma$ не сможет получить, исходя из набора проекций $(s_i : i \in A')$, дополнительной (к имеющейся априорной) информации о ключе σ_0 [6].

Число

$$r_V = \min\{\frac{\log|S_0|}{\log|S_i|} : i \in \overline{1,n}\} \tag{4}$$

называется информационной скоростью СРС $V \subseteq S$ и является основным параметром, характеризующим практическую эффективность данной схемы разделения секрета. Известно (см., например, [3, 4, 6]), что информационная скорость произвольной совершенной СРС V не превосходит 1. В случае $r_V = 1$ схема разделения секрета V называется идеальной. Известным примером идеальной СРС является произвольная «векторная» схема разделения секрета, определяемая посредством линейного кода V над конечным полем ($S_i = \mathbf{GF}(q)$, $i \in \overline{0,n}$, V — подпространство векторного пространства $S = \mathbf{GF}(q)^{n+1}$ над полем $\mathbf{GF}(q)$) [11].

2. Метод построения совершенных СРС по конгруэнциям конечных универсальных алгебр

Докажем утверждение, характеризующее совершенные схемы разделения секрета в терминах определенных систем отношений эквивалентности на конечном множестве.

Утверждение 1. Пусть Γ — произвольная (монотонная) структура доступа на множестве P, r — вещественное число, $0 < r \le 1$. Тогда совершенная СРС, имеющая информационную скорость r и реализующая структуру доступа Γ, существует в том и только в том случае, когда существуют конечное множество X и система отношений эквивалентности $\pi_0, \pi_1, \ldots, \pi_n \in \mathfrak{I}(X)$, удовлетворяющие условиям:

$$\pi_A \overset{\text{def}}{=} \bigwedge_{i\in A}\pi_i \subseteq \pi_0 \text{ для любого } A \in \Gamma, \tag{5}$$

$$\pi_A \bullet \pi_0 = 1_X \text{ для любого } A \in 2^P/\Gamma, \tag{6}$$

$$r = \min\{\frac{\log n(\pi_0)}{\log n(\pi_i)} : i \in \overline{1,n}\}. \tag{7}$$

Доказательство. Пусть $V \subseteq S$ — код совершенной СРС, реализующей структуру доступа Г на множестве P, и $r_V = r$.

Положим $l = \|V\|$, $X = \{1, 2, \ldots, l\}$. Запишем слова, принадлежащие коду V, в виде прямоугольной таблицы размера $l \times (n + 1)$. Заметим, что i-й столбец данной таблицы представляет собой вектор значений некоторого отображения $\varphi_i : X \to S_i$, $i \in \overline{0,n}$. Положим $\pi_i = \mathrm{Ker}\ \varphi_i$, где $\mathrm{Ker}\ \varphi_i = \{(x, y) \in X^2 : \varphi_i(x) = \varphi_i(y)\}$ — ядро отображения φ_i ($i \in \overline{0,n}$), и покажем, что ОЭ $\pi_0, \pi_1, \ldots, \pi_n$ на множестве X удовлетворяют условиям (5)–(7).

Для любого множества $A \subseteq \overline{P}$ зададим отображение $\varphi_A : X \to S_A$, полагая

$$\varphi_A(x) = (\varphi_i(x))_{i \in A}, \ x \in X.$$

Заметим, что

$$\mathrm{Ker}\,\varphi_A(x) = \bigwedge_{i \in A} \mathrm{Ker}\,\varphi_i = \bigwedge_{i \in A} \pi_i = \pi_A, \tag{8}$$

$$n(\pi_A) = \|V_A\| \tag{9}$$

для любого $A \subseteq \overline{P}$. На основании равенств (8), (9) соотношения (2), (3) равносильны соответственно следующим соотношениям:

$$n(\pi_A \wedge \pi_0) = n(\pi_A) \text{ для любого } A \in \Gamma, \tag{10}$$

$$n(\pi_A \wedge \pi_0) = n(\pi_A) n(\pi_0) \text{ для любого } A \in 2^P/\Gamma. \tag{11}$$

Далее, в силу включения $\pi_A \wedge \pi_0 \subseteq \pi_A$ условие (10) равносильно утверждению: $\pi_A \wedge \pi_0 = \pi_A$ для любого $A \in \Gamma$, которое, в свою очередь, равносильно условию (5). В силу равносильности утверждений (а′)–(в′), приведенных в п. 1, условие (11) равносильно условию (6). Наконец, справедливость равенства (7) вытекает непосредственно из формул (4), (9) и равенства $|S_i| = \|V_i\|$, $i \in \overline{0,n}$.

Итак, существование совершенной СРС V такой, что $r_V = r$, реализующей структуру доступа Г, влечет существование конечного множества X и ОЭ $\pi_0, \pi_1, \ldots, \pi_n \in \vartheta(X)$, удовлетворяющих условиям (5)–(7).

Докажем обратное утверждение. Пусть π_0, π_1, …, π_n — отношения эквивалентности на конечном множестве X, для которых выполняются условия (5)–(7). Положим $S_i = X/\pi_i$ и обозначим φ_i каноническую проекцию множества X на множество S_i, $i \in \overline{0,n}$. Из векторов значений отображений φ_0, φ_1, …, φ_n составим таблицу V, полагая V_i равным вектору значений отображения φ_i, $i \in \overline{0,n}$. Заметим, что на основании рассуждений, изложенных в первой части доказательства, построенный код V задает совершенную СРС, обладающую требуемыми свойствами. Утверждение доказано.

Полученный результат позволяет предложить общий метод построения совершенных схем разделения секрета на основе конгруэнций конечных универсальных алгебр. Суть метода раскрывается в формулировках следующих утверждений.

Утверждение 2. Пусть $\mathfrak{R}$ — конечная алгебра с носителем X, π_0, π_1, …, π_n — конгруэнции алгебры $\mathfrak{R}$ такие, что

$$(i)\ \pi_0 \bullet (\bigwedge_{i\in A} \pi_i) = (\bigwedge_{i\in A} \pi_i) \bullet \pi_0 \text{ для любого } A \subseteq P = \{1, 2, \ldots, n\},$$

$$(ii)\ \pi_0 \text{ — максимальная конгруэнция алгебры } \mathfrak{R}.$$

Тогда система конгруэнций π_0, π_1,…, π_n задает на множестве P совершенную СРС, реализующую структуру доступа:

$$\Gamma = \{A \subseteq P: \bigwedge_{i\in A} \pi_i \subseteq \pi_0\}. \qquad (12)$$

Информационная скорость указанной СРС определяется по формуле (7).

Доказательство. Заметим, что в силу максимальности конгруэнции π_0 и равносильности условий (а)–(в), приведенных в п. 1, для любого множества $A \in 2^P / \Gamma$ выполняется равенство $(\bigwedge_{i\in A} \pi_i) \bullet \pi_0 = 1_X$. Следовательно, система конгруэнций π_0, π_1,…, π_n удовлетворяет условиям (5), (6), и на основании утверждения 1 существует совершенная СРС, имеющая информационную скорость (7) и реализующая структуру доступа (12).

Утверждение доказано.

Следствие. Пусть π_0 — максимальная, а π_1,…, π_n — произвольные конгруэнции конечной конгруэнц-перестановочной алгебры $\mathfrak{R}$. Тогда система конгруэнций π_0, π_1,…, π_n задает совершенную СРС на множестве n участников, структура доступа которой определяется по формуле (12), а информационная скорость — по формуле (7). Код V указанной СРС имеет вид:

$$V = \{(\varphi_0(x), \varphi_1(x), \ldots, \varphi_n(x)): x \in X\},$$

где φ_i — каноническая проекция алгебры $\mathfrak{R}$ на факторалгебру по конгруэнции π_i, $i \in \overline{0,n}$.

Отметим, что в частном случае, когда алгебра $\mathfrak{R}$ является абелевой группой с операторами, представляющей собой векторное пространство над конечным полем, схема разделения секрета, описанная в формулировке следствия, совпадает с «векторной» СРС Э. Брикела [11].

Утверждения 1, 2 можно непосредственно использовать для построения разнообразных «конкретных» схем разделения секрета, выбирая подходящим образом универсальную алгебру $\mathfrak{R}$ и систему отношений эквивалентности на носителе этой алгебры. Пусть, например, $\mathfrak{R}$ является модулем конечной длины над конечным коммутативным кольцом с единицей (здесь и далее модуль $\mathfrak{R}$ рассматривается как абелева группа с операторами) [20]. Положим π_i равным фактормодулю $\mathfrak{R}/\mathfrak{R}_i$, где $\mathfrak{R}_i$ — некоторый подмодуль модуля $\mathfrak{R}$, $i \in \overline{0,n}$. Пусть $\varphi_i : \mathfrak{R} \to \mathfrak{R}_i$ — канонический гомоморфизм модулей. Тогда, отождествляя фактормодуль $\pi_i = \mathfrak{R}/\mathfrak{R}_i$ с ядром гомоморфизма φ_i ($i \in \overline{0,n}$) и применяя к системе конгруэнций π_0, π_1,…, π_n модуля $\mathfrak{R}$ утверждение 1, получим, что набор гомоморфизмов $\varphi_i : \mathfrak{R} \to \mathfrak{R}_i$, $i \in \overline{0,n}$ в том и только в том случае задает совершенную схему разделения секрета со структурой доступа $\Gamma \subseteq 2^P$, когда выполняются следующие условия:

$$\bigcap_{i \in A} \operatorname{Ker} \varphi_i \subseteq \operatorname{Ker} \varphi_0 \text{ для любого } A \in \Gamma, \tag{13}$$

$$\bigcap_{i \in A} \operatorname{Ker} \varphi_i + \operatorname{Ker} \varphi_0 = \mathfrak{R} \text{ для любого } A \in 2^P/\Gamma. \tag{14}$$

Отметим, что соотношения (13), (14) характеризуют так называемые линейные совершенные СРС над конечным полем [12, 13]. По сути, аналогичные соотношения используются в [16, 17] для задания совершенных СРС над некоторыми коммутативными кольцами и группами.

В качестве еще одного возможного применения утверждения 1, укажем способ построения совершенных схем разделения секрета по определенной системе подгрупп произвольной конечной группы.

Утверждение 3. Пусть X — конечная группа, G_0 — максимальная, а G_i — произвольная подгруппа группы X, $i \in \overline{1,n}$. Пусть, далее, π_i обозначает множество различных левых смежных классов группы X по подгруппе G_i, $i \in \overline{0,n}$. Тогда при выполнении хотя бы одного из условий

(i') G_i — нормальный делитель группы X, $i \in \overline{1,n}$,

(ii') G_0 — нормальный делитель группы X

система разбиений π_0, π_1,..., π_n задает совершенную СРС *V*, реализующую структуру доступа (12). Информационная скорость СРС *V* равна:

$$r_V = \min\{\frac{\log(X : G_0)}{\log(X : G_i)} : i \in \overline{1,n}\},$$

где (*X*: *H*) обозначает индекс подгруппы *H* в группе *X*.

Доказательство. Для любого $A \subseteq P$ положим $G_A = \bigcap_{i \in A} G_i$. Заметим, что G_A является подгруппой группы *X*, и разбиение $\pi_A = \bigwedge_{i \in A} \pi_i$ совпадает с разложением группы *X* в левые смежные классы по этой подгруппе.

Пусть теперь для некоторого $A \subseteq P$ группа G_A не содержится в группе G_0. Тогда при выполнении любого из условий (*i*′), (*ii*′) произведение $G_A G_0 = G_0 G_A$ является подгруппой группы *X*, которая совпадает с *X* в силу максимальности G_0. Таким образом, на основании утверждения 1 для завершения доказательства остается убедиться в справедливости следующего утверждения.

Пусть *G* и *H* — подгруппы группы *X* такие, что *X* = *GH*, и *H* — нормальный делитель *X*. Тогда любые два левых смежных класса группы *X* по подгруппам *G* и *H* соответственно имеют непустое пересечение.

Докажем это. Пусть *xG* и *yH* — левые смежные классы группы *X* соответственно по подгруппам *G* и *H*. Из равенств *GH* = *HG* = *X* следует, что $y = g_1 h_1$, $x = h_2 g_2$ для некоторых g_1, $g_2 \in G$, $h_1, h_2 \in H$. Следовательно, $xG = h_2 G$ и (так как *H* — нормальный делитель группы *X*) $yH = g_1 H = H g_1$. Остается заметить, что $h_2 g_1 \in H g_1 \cap h_2 G = yH \cap xG$, что и требовалось доказать.

Заключение

Описанные выше конструкции совершенных схем разделения секрета свидетельствуют о большом разнообразии конкретных СРС, которые могут быть получены путем задания некоторой конечной универсальной алгебры и соответствующей системы ОЭ на ее носителе. Вместе с тем, более важным (и более трудным) является вопрос о том, насколько в действительности различны структуры доступа указанных СРС. Известно [13], что для любой монотонной структуры доступа существует реализующая ее линейная СРС над конечным полем (определяемая соотношениями (13), (14)). Однако метод построения таких СРС, изложенный в [13], в общем случае, приводит к малопрактичным конструкциям линейных схем разделения секрета, имеющих крайне малые значения информационной скорости. Вопрос о том, насколько более эффективно можно реализовать те или иные структуры доступа с помощью СРС, построенных по системам конгруэнций универсальных алгебр, отличных от конечных векторных пространств, является в настоящее время открытым.

Задача оптимизации информационной скорости совершенных схем разделения секрета, реализующих заданную структуру доступа Г, естественным образом

приводит к вопросу о том, каково наибольшее число блоков разбиения $\pi_0 \in \vartheta(X)$, удовлетворяющего (для заданных отношений эквивалентности $\pi_1,\ldots, \pi_n \in \vartheta(X)$ и монотонного класса $\Gamma \subseteq 2^P$) условиям (5), (6). Обозначим Γ_0 совокупность минимальных элементов класса Γ. Тогда на основании соотношения (5) справедливо включение

$$\pi_0 \supseteq \pi_\Gamma \overset{\text{def}}{=} \bigvee_{A\in\Gamma_0} \left(\bigwedge_{i\in A} \pi_i\right),$$

из которого следует, что $n(\pi_0) \le n(\pi_\Gamma)$. Нахождение необходимых и достаточных условий, при которых полученное неравенство обращается в равенство (то есть ОЭ $\pi_\Gamma = \pi_0$ удовлетворяет условию (6)), представляет собой практически важную, интересную задачу.

Отметим, что полученное выше алгебраическое описание совершенных СРС (см. утверждение 1) можно распространить на другие, «родственные» схемам разделения секрета, криптографические протоколы: схемы предварительного распределения ключей и схемы широковещательного шифрования [21]. Решающий шаг в этом направлении сделан в статьях [22, 23], где представлены конструкции линейных схем распределения ключей, включающие в себя, в качестве частных случаев, практически все известные ранее способы построения таких схем (см. [23]). Для того чтобы получить алгебраические варианты определений схемы предварительного распределения ключей и схемы широковещательного шифрования (по сути равносильные общепринятым теоретико-информационным определениям этих понятий [21]), достаточно отказаться от условия линейности отображений в конструкциях схем распределения ключей, предложенных в [22, 23].

1. *Blakley G.R.* Safeguarding Cryptographic Keys // Proc. AFIPS 1979 National Computer Conference. — N-Y. — 1979. — Vol. 48. — P. 313–317.

2. *Shamir A.* How to share a secret // Comm. ACM. — 1979. — Vol. 22, N 1. — P. 612–613.

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. *Brickell E.F., Davenport D.M.* On the Classification of Ideal Secret Sharing Schemes // J. Cryptology — 1991. — Vol. 4. — P. 123–134.

6. *Блейкли Р.Г., Кабатянский Г.А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. — 1997. — Т. 33. — Вып. 3. — С. 102–110.

7. *Ito M., Saito A., Nishizeki T.* Secret Sharing Scheme Realizing General Access Structure // Proc. IEEE Globecom' 87. — Tokyo. — 1987. — P. 99–102.

8. *Benaloh J., Leichter J.* Generalized Secret Sharing and Monotone Functions // Advances in Cryptology. — CRYPTO'88. — Lecture Notes in Comput. Sci. — 1990. — Vol. 403. — P. 27–35.

9. *Marti-Farre J., Padro C.* Secret Sharing Schemes on Access Structures with Intersection Number to One // Proc. Third Conf. on Security and Communication Networks'02. — Amalfi. — 2002. — Vol. 2576. — P. 354–363.

10. *Beimel A., Ishai Y.* On the Power of Nonlinear Secret Sharing // Proc. 16th Conf. on Computational Complexity. — 2001. — P. 188–202.

11. *Brickell E.F.* Some Ideal Secret Sharing Schemes // J. Combin. Math. and Combin. Comput. — 1989. — N 9. — P. 105–113.

12. *Blakley G.R., Kabatianski G.A.* Linear Algebra Approach to Secret Sharing Schemes // Error Control, Cryptology and Speech Compression. — Lecture Notes in Comput. Sci.— 1994. — Vol. 829. — P. 33–40.

13. *Simmons G.J., Jackson W., Martin K.* The Geometry of Secret Sharing Schemes // Bull. of the ICA. — 1991. — N 1. — P. 71–88.

14. *Cramer R., Damgard I., Maurer U.* General Secure Multi-Party Computation from any Linear Secret Sharing Schemes // Advances in Cryptology — EUROCRYPT'00. — Lecture Notes in Comput. Sci. — 2000. — Vol. 1807. — P. 316–334.

15. *Frankel Y., Desmedt Y.* Classification of Ideal Homomorphic Threshold Schemes over Finite Abelian Groups // Advances in Cryptology — EUROCRYPT'92. — Lecture Notes in Comput. Sci. — 1993. — Vol. 658. — P. 25–34.

16. *Cramer R., Fear S.* Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups // Advances in Cryptology — EUROCRYPT'02. — Lecture Notes in Comput. Sci. — 2002. — Vol. 2442. — P. 272–287.

17. *Cramer R., Fear S., Ishai Y., Kushilevitz E.* Efficient Multi-Party Computation over Rings // Cryptology ePrint Archive, Report 2003/030. — 2003.

18. *Кон П.* Универсальная алгебра: Пер. с англ. — М.: Мир, 1968. — 351 с.

19. *Айгнер М.* Комбинаторная теория: Пер. с англ. — М.: Мир, 1982. — 558 с.

20. *Биркгоф Г.* Теория решеток: Пер. с англ. — М.: Наука, 1984. — 568 с.

21. *Stinson D.R.* On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption // Designs, Codes and Cryptography. — 1997. — Vol. 12. — P. 215–243.

22. *Padro C., Gracio I., Martin S., Morillo P.* Linear Key Predistribution Schemes // Designs, Codes and Cryptography. — 2002. — Vol. 25. — P. 281–298.

23. *Padro C., Gracio I., Martin S., Morillo P.* Linear Broadcast Encryption Schemes // Discrete Appl. Math. — 2003. — Vol. 128. — P. 223–238.

Поступила в редакцию 07.02.2005