ПРОБЛЕМЫ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

Материалы конференции
в МГУ 29 – 30 октября 2010 г.

Том 2

ББК 32.81В6
М34

Организация и проведение Восьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009) были поддержаны грантом РФФИ № 09-01-06106-г.

РФФИ

М34 **Материалы** Пятой международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет имени М. В. Ломоносова. 29–30 октября 2009 г. Том 2. Материалы Восьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009). — М.: МЦНМО, 2010. — 224 с.

ISBN 978-5-94057-693-8

ISBN 978-5-94057-693-8
ISBN 978-5-94057-695-2 (Том 2)

Содержание

из количества элементов в поле. Это делает невозможным сведение анализа исходной структуры к анализу структуры, мощность которой близка к квадратному корню из мощности исходной структуры. Также показано, что сложение в конечном поле хорошо перемешивает смежные классы по мультипликативной группе любого подполя и наоборот.

Литература

[1] Шеннон К. Теория связи в секретных системах. В кн.: «Работы по теории информации и кибернетике». М.: Иностранная литература, 1963.

[2] Горчинский Ю. Н. О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями. Труды по дискретной математике, М.: ТВП, 1997, т. 1, с. 67–84.

[3] Горчинский Ю. Н. Стохастические алгебры. Труды по дискретной математике, М.: ТВП, 1998, т. 2, с. 55–87.

Свойства решеток разграничения доступа, совершенные шифры и схемы разделения секрета

Е. А. Болотова, С. С. Коновалова, С. С. Титов

Теория разграничения доступа к информации содержит довольно обширную предметную область, задачи в которой могут иметь самостоятельное значение [1, 2, 3, 4]. Так, при тематическом разграничении доступа [1, 5] большой интерес представляет определение близости или удаленности различных тематик друг от друга, то есть абстрактное описание возможных метрик на множестве тематик [1, 6]. Эта задача решается легче для дистрибутивных решеток [7], например, путем вложения их в решетку подмножеств некоторого множества. Каждый элемент решетки представляется как подмножество, то есть битовая строка, и расстояние между ними естественно определять расстоянием Хэмминга. В связи с этим представляет интерес исследование абстрактных алгебраических свойств решеток безопасности, соответствующих различным иерархическим моделям безопасности, в том числе дистрибутивности, модулярности и полумодулярности, тем более что свойством полумодулярности обладают решетки подпространств матроидов [8], а матроиды, как известно, соответствуют структурам доступа при разделении секрета [9, 10]. Интересны и соотношения между решетками различных моделей безопасности [1, 5], а также соотношения и взаимодействие решеток одной и той же модели, но для компьютерных систем, изменяющихся во времени (сохранение безопасности функционирования) и в пространстве (компьютерные сети) [1, 11]. В [12], например, доказано следующее

Утверждение 1. *Если сегмент сети с решеткой уровней безопасности L_2 доверяет сегменту с решеткой L_1, то система безопасна при удаленном доступе в иерархических моделях тогда и только тогда, когда решетка L_2 изоморфна выпуклой подрешетке решетки L_1.*

При тематическом разграничении доступа представляет интерес решетка рубрикаторных идеалов [1]. Рубрикаторный идеал является множеством вершин иерархического классификатора, которое является порядко-

вым идеалом, обязательно включающим вершины-родители при вхождении в идеал полного набора их сыновей. Докажем дистрибутивность этой решетки в два шага — через приведение к бинарному дереву и устранение «посредников».

Дерево рубрик можно привести к виду бинарному, вводя «заместителей»: если $x_1, \ldots, x_n$ — все сыновья вершины y, $n > 2$, то заменим эту n-развилку на две развилки так, что x_1, z — все сыновья вершины y, причём $x_2, \ldots, x_n$ — все сыновья новой вершины z («заместителя»). Если в дереве рубрик возникают вершины, развилки которых тривиальны, то возникают «посредники» между некоторыми начальниками и подчиненными. Устраняем их так: если $x_1, \ldots, x_n$ — все сыновья вершины y, $n \geqslant 1$, а вершина y — единственный сын вершины v, то в новом дереве считаем вершины $x_1, \ldots, x_n$ всеми сыновьями вершины v, а вершина y отсутствует. Решетка рубрикаторных идеалов полученного на каждом шаге дерева, очевидно, изоморфна решетке рубрикаторного идеала исходного дерева рубрик. Рассмотрим множество листовых вершин бинарного без посредников дерева рубрик. Для рубрикаторного идеала J обозначим [1] через $\Lambda(J)$ множество его листовых вершин. Из отсутствия посредников вытекает, что Λ — инъекция. Докажем, что $\Lambda(J_1 \cup_p J_2) = \Lambda(J_1) \cup \Lambda(J_2)$. Если $a \leqslant b$, то вершина b может возникнуть из рубрикаторного замыкания тогда и только когда, когда $b \notin \Lambda(J_1)$, $b \notin \Lambda(J_2)$, но оба его непосредственных подчиненных c_1, c_2 таковы, что $c_1 \in J_1$, $c_1 \notin J_2$ и $c_2 \notin J_1$, $c_2 \in J_2$. Поскольку b — начальник для a, то, в силу бинарности, либо $a \leqslant c_1$, либо $a \leqslant c_2$, и равенство доказано. Значит, Λ — изоморфное вложение решетки рубрикаторных идеалов бинарного дерева без посредников в решётку подмножеств множества листовых вершин. Итак, доказано

Утверждение 2. *Решетка безопасности рубрикаторных идеалов при тематическом разграничении доступа дистрибутивна.*

Рассмотрим использование аппарата решеток в задачах изучения совершенных СРС [14, 13]. Для идеальных БД-совершенных СРС естественным образом возникает соответствующий схеме матроид [9, 10]. Решетка подпространств матроида, как известно, полумодулярна [4, 8]. Решетка с какими свойствами естественно возникает для неидеальных СРС? Пусть имеется V-матрица БД-совершенной СРС с n участниками, S_0 — множество секретов, S_i — множество проекций i-го участника ($i = 1, \ldots, n$) [9, 10]. Условия БД-совершенности СРС при $v_i \in S_i$ запишем в виде $\{i, j, \ldots, k\} \in \Gamma \Longrightarrow [v_i, v_j, \ldots, v_k] = v_0$, то есть $\forall \vec{s}' = (v_0', v_1', \ldots, v_n')$ $v_i' = v_i$ & $v_j' = v_j$ & ... & $v_k' = v_k \Longrightarrow v_0' = v_0$. Или, по-другому:

1. Если $\{i, j, \ldots, k\} \in \Gamma$, то для любых двух строк $\vec{s}$ и $\vec{s}'$ матрицы V этой БД-совершенной СРС таких, что $v_i' = v_i$ & $v_j' = v_j$ & ... & $v_k' = v_k$ имеем $v_0' = v_0$.
2. Пусть $\{i, j, \ldots, k\} \notin \Gamma$; тогда для любой строки $\vec{s} = (v_0, v_1, \ldots, v_n)$ матрицы V БД-совершенной СРС и любого $v_0' \in S_0$ есть такая строка $\vec{s}' = (v_0', v_1', \ldots, v_n')$, что $v_i' = v_i$, $v_j' = v_j$, ..., $v_k' = v_k$. А так как в любой строке s эти компоненты произвольны, множество индексов $\{i, j, \ldots, k\} \notin \Gamma$ не влечет за собой никакого разбиения множества строк.

Следуя [15], естественно рассмотреть на множестве строк матрицы V бинарные отношения ρ_j, $j \in \{0, 1, \ldots, n\}$: если v', $v'' \in V$, то $v' \rho_j v'' \iff \Rightarrow v_j' = v_j''$. Ясно, что это отношения эквивалентности и они задают разбиения множества строк. Точная нижняя грань $S_i \wedge S_j$: $\vec{s} \equiv \vec{s}' \iff v_i = v_i'$ & $v_j = v_j'$ — это отношение эквивалентности. Аналогично, отношение $\rho_{ij\ldots k}$: $\vec{s} \equiv \vec{s}' \iff v_i = v_i'$ & $v_j = v_j'$ & ... & $v_k = v_k'$ — отношение эквивалентности. Эти разбиения порождают подрешетку в решетке всех разбиений множества строк матрицы V. Разбиения частично упорядочены отношением измельчения. Запишем первое условие СРС и второе условие соответственно [15] в виде

1′) $\rho_i \wedge \rho_j \wedge \ldots \wedge \rho_k \leqslant \rho_0$, если $A = \{i, j, \ldots, k\} \in \Gamma$;

2′) $(\rho_i \wedge \rho_j \wedge \ldots \wedge \rho_k) \cdot \rho_0 = \mathbf{1}$ при $A = \{i, j, \ldots, k\} \notin \Gamma$,

где точка $\cdot$ обозначает произведение (композицию) бинарных отношений, $\mathbf{1}$ — единица в решетке разбиений множества строк матрицы V по отношению измельчения (то есть $\mathbf{1}$ — это всеобщая эквивалентность, разбиение, состоящее из единственного множества — множества всех строк).

Заметим, что из 2′) вытекает равенство

2″) $(\rho_i \wedge \rho_j \wedge \ldots \wedge \rho_k) \vee \rho_0 = \mathbf{1}$ при $A = \{i, j, \ldots, k\} \notin \Gamma$

ввиду определения операции верхней грани $\vee$ в решетке разбиений [4, 16]. Действительно, в решетке разбиений (см., например, [16, с. 49]) разбиение (эквивалентность) $\rho = \pi \vee \sigma$ определяется так:

$x \rho y \iff$ существует $k \geqslant 1$ и такая последовательность $x_1, \ldots, x_k$, что $x = x_1$, $y = x_k$, причем для всех $i \in \{1, 2, \ldots, k-1\}$ имеем или $x_i \pi x_{i+1}$, или $x_i \sigma x_{i+1}$.

В частности, при $k = 1$ имеем $y = x_1 = x$, так что $x \rho x$ в силу рефлексивности отношений π и σ; при $k = 2$ имеем $x \pi y$ или $x \sigma y$ влечет $x \rho y$. Значит, $\pi \vee \sigma = \mathbf{1}$ тогда и только тогда, когда для любых элементов $x, y \in X$

существует $k \geqslant 1$ и такая последовательность $x_1, \ldots, x_k$, что $x = x_1$, $y = x_k$, причем для всех $i = 1, 2, \ldots, k-1$ имеют место отношения или $x_i \pi x_{i+1}$, или $x_i \sigma x_{i+1}$.

В рассматриваемом нами случае пусть $x = (v_0, v_1, \ldots, v_n)$ и $y = (v_0'', v_1'', \ldots, v_n'')$ — две строки матрицы V нашей БД-совершенной СРС. Пусть $\{i, j, \ldots, k\} \notin \Gamma$. Положим $x_1 = x$, $x_2 = (v_0', v_1', \ldots, v_n')$, где по свойству $2'$) мы можем выбрать $v_0' = v_0''$, $v_i' = v_i$, $v_j' = v_j$, ..., $v_k' = v_k$. В наших обозначениях $\rho_{ij\ldots k} = \rho_i \wedge \rho_j \wedge \ldots \wedge \rho_k$ мы можем записать это отношение как $x_1 \rho_{ij\ldots k} x_2$. Взяв теперь $x_3 = y$, мы видим, что выполняется отношение $x_2 \equiv x_3$, то есть $x_2 \rho_0 y$. Итак, имеем $k = 3$ и последовательность $x = x_1, x_2, x_3 = y$ такую, что $x_1 \rho_{ij\ldots k} x_2$ и $x_2 \rho_0 x_3$, что означает $x(\rho_0 \wedge \rho_{ij\ldots k})y$ для произвольных строк x, y матрицы V, то есть $\rho_0 \vee (\rho_i \wedge \rho_j \wedge \ldots \wedge \rho_k) = 1$, что и требовалось. □

Отметим, что условие $2''$) есть лишь следствие условия $2'$) (то есть обратная импликация может быть ложной). Эти равенства являются двойственными к условиям принципа «всё или ничего». Итак, поскольку решетка разбиений полумодулярна [4], доказано

Утверждение 3. *Любой БД-совершенной СРС соответствует полумодулярная решетка разбиений ее строк, удовлетворяющая двойственному принципу «всё или ничего».*

Для линейной СРС этот подход означает рассмотрение подпространств, ортогональных к подпространствам L_i [9, 10], соотнесенных с участниками. Использование совершенных схем с «хорошими» свойствами представляется предпочтительным. С этой целью в [15] предложено использовать отношения эквивалентности ρ_i, представляющие собой конгруэнции универсальных алгебр с нужными свойствами. Так, решетка линейной СРС модулярна. Условие $2''$) слабее условия $2'$), которое и надо считать первичным. Равенство $\rho \cdot \sigma = \sigma \cdot \rho$ для линейной СРС, очевидно, имеет место. Рассмотрение этого вопроса [15] дает возможность для решетки, порожденной эквивалентностями ρ_i, доказать

Утверждение 4. *Пусть эквивалентности, составляющие решетку разбиений строк БД-совершенной СРС, перестановочны. Тогда эта решетка модулярна.*

Поскольку перестановочность означает наличие «достаточного» количества строк в V, такие схемы естественно назвать вполне совершенными. Отметим, что использование дистрибутивных решеток здесь невозможно из-за нарушений принципа «всё или ничего». Таким образом, абстрактные свойства решеток играют важную роль в задачах разграничения доступа и разделения секрета и могут быть применены, в том числе, к решению сформулированных в [9, 17] проблем.

Для задач разделения секрета аппарат решеток возникает через использование квазигрупп и принципа «всё или ничего» [9, 18]. Так, разделение секрета можно геометрически интерпретировать как задачу интерполяции [19] с использованием многоместных квазигрупповых операций. Теперь применим метод, описанный выше для решеток, для идеальных БД-совершенных СРС. Все множество проекций для n участников отождествим с множеством секретов S_0, $|S_0| = q$: $S_0 = S_1 = S_2 = \ldots = S_n = S$. Рассмотрим такие СРС через комбинаторную интерпретацию в терминах квазигрупп. Пусть в данном множестве участников есть разрешенное подмножество из m участников $A \in \Gamma_{\min}$, $|A| = m$. Рассмотрим пример $m = 2$, тогда $\{i, j\} \in \Gamma_{\min}$. Можно доказать, что по данным значениям s_0 и s_i значение s_j определяется однозначно, а по значениям s_0 и s_j значение s_i определяется однозначно. Таким образом, для идеальной БД-совершенной СРС определена квазигруппа [18] на множестве S с операцией $s_0 = s_i * s_j$, с однозначным правым ($s_i = s_0 / s_j$) и левым ($s_j = s_i \setminus s_0$) делением. Аналогично доказывается следующее утверждение и для m-квазигрупп, то есть которые задаются функцией $f(s_1, s_2, \ldots, s_m)$ от m переменных, биективной по каждой из переменных [20].

Утверждение 5. *В идеальной БД-совершенной СРС для каждого множества $A \in \Gamma_{\min}$, $|A| = m$, на множестве S определена m-арная операция*

$$f\colon \underbrace{S \times \ldots \times S}_{m \text{ раз}} \to S,$$

задающая m-квазигруппу.

Следующее утверждение означает, что в идеальном случае любой из участников может считаться хранителем секрета.

Утверждение 6. *Каждый цикл мощности $m+1$ матроида, соответствующего идеальной БД-совершенной СРС, определяет m-квазигруппу на S.*

Таким образом, в качестве универсальных алгебр [15] можно использовать m-квазигруппы.

Теперь рассмотрим структуры доступа, состоящие из пар элементов. Их можно задавать графами: вершинами графа являются участники, а ребра графа связывают двух участников из разрешенного множества. При этом важную роль играет группа автоморфизмов графа [21].

Рассмотрим структуры доступа, в которых есть два разрешенных множества $\{i, J_{m-1}\} \in \Gamma_{\min}$ и $\{k, J_{m-1}\} \in \Gamma_{\min}$, где $J_{m-1} = \{j_1, j_2, \ldots, j_{m-1}\}$ — общее множество участников для них. Согласно [22] для таких структур доступа участники i и k называются связанными, и фактически дилер

им выдает одну и ту же проекцию секрета (в общем же случае структуры доступа с парами эквивалентных участников не рассматриваются, что эквивалентно отсутствию в матроиде циклов длины два) [22]. Таких участников можно объединить в одну роль (например, начальника или подчиненного) [5].

Рассмотрим структуру доступа, в которой есть такие три участника i, j и k, когда j-й участник входит в оба разрешенных множества, что:

$$\begin{cases} \{i, j\} \in \Gamma_{\min}, \\ \{j, k\} \in \Gamma_{\min}, \\ \{i, k\} \notin \Gamma_{\min}. \end{cases} \tag{1}$$

С точки зрения квазигрупп данную ситуацию можно описать в терминах изотопии. А именно, пусть на множестве S определены две квазигрупповые операции $*$ и $\bullet$, раскрывающие секрет s_0 разрешенным парам участников $\{i, j\}$ и $\{k, j\}$, так что $s_0 = s_i * s_j$ и $s_0 = s_k \bullet s_j$. Тогда $s_k = f_{ik}(s_i) = f(s_i)$, и из равенства $s_i * s_j = f(s_i) \bullet s_j$ заключаем, что $x \bullet y = f^{-1}(x) * y$, то есть квазигруппа с операцией $\bullet$ получается из квазигруппы с операцией $*$ изотопией (по левому сомножителю). Поэтому справедливо

Утверждение 7. *Для структуры доступа с условием* (1) *соответствующие квазигруппы* $s_0 = s_i * s_j$ *и* $s_0 = s_k \bullet s_j$ *изотопны между собой.*

Это показывает, что идеальные схемы близки по своим свойствам к пороговым. В таком случае для структур доступа, состоящих только из пар, можно дать исчерпывающее описание, в каком случае они дают идеальную реализацию. Если для каждого участника пороговой $(2, k)$-схемы создать дубликаты, играющие одну и ту же роль, то схема станет идеальной БД-совершенной. И в общем случае, любую идеальную БД-совершенную СРС, состоящую из пар, можно получить таким образом из пороговой.

В линейном случае для пороговых СРС эти операции будут линейными. Кроме того они обладают хорошими алгебраическими свойствами. Для $m = 2$ пороговая схема Шамира $(2, n)$ геометрически представляет собой конечную аффинную плоскость. Она дает интерполяцию посредством полилинейной операции, в бинарном случае определяемой через векторное произведение

$$\vec{u} \times \vec{v} = [\vec{u}, \vec{v}] = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ x & y & z \\ a & b & c \end{vmatrix} = \vec{i}(yc - bz) - \vec{j}(xc - az) + \vec{k}(xb - ay),$$

где $\vec{u} = (x, y, z)$, $\vec{v} = (a, b, c)$; для нее справедливо тождество Якоби для векторного произведения. m-арная операция, определяемая по аналогии

с бинарной операцией, обладает хорошими свойствами, в том числе для нее доказано следующее

Утверждение 8. *Для m-линейной операции справедлив аналог тождества Якоби.*

При $m = 3$ аналог тождества Якоби для произведения из трех элементов имеет вид

$$[\vec{f}, \vec{g}, [\vec{u}, \vec{v}, \vec{w}]] = [[\vec{f}, \vec{g}, \vec{u}], \vec{v}, \vec{w}] + [\vec{u}, [\vec{f}, \vec{g}, \vec{v}], \vec{w}] + [\vec{u}, \vec{v}, [\vec{f}, \vec{g}, \vec{w}]],$$

где

$$[\vec{u}, \vec{v}, \vec{w}] = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} & \vec{\ell} \\ x & y & z & t \\ a & b & c & d \\ p & q & r & s \end{vmatrix}, \quad \vec{u} = (x, y, z, t),\ \vec{v} = (a, b, c, d),\ \vec{w} = (p, q, r, s).$$

В [23] был дан геометрический метод оценки максимально возможного числа n для СРС $(3, n)$ и как следствие была доказана теорема о несуществовании эндоморфных $U(3)$-стойких шифров с минимальным числом ключей с уравнением зашифрования $y = kf(x) + \ell$ в конечных полях нечетной характеристики.

Для случая $m = 3$ для СРС можно использовать окружности, задаваемые функциями второго порядка $(x - a)^2 + (y - b)^2 = R$. Для этого приведем решение системы

$$\begin{cases} (x_1 - a)^2 + (y_1 - b)^2 = R, \\ (x_2 - a)^2 + (y_2 - b)^2 = R, \\ (x_3 - a)^2 + (y_3 - b)^2 = R \end{cases}$$

с применением стандартных операций раскрытия скобок и вычитания тождеств:

$$\begin{cases} b = -2 \cdot \dfrac{(x_2 - x_1)(x_1 x_2 + y_3^2) + (x_3 - x_2)(x_2 x_3 + y_1^2) + (x_1 - x_3)(x_1 x_3 + y_2^2)}{(x_1 - x_3)(y_3 - y_2) - (x_2 - x_3)(y_3 - y_1)}, \\ a = -2 \cdot \dfrac{y_3^2 - y_1^2 - x_1^2 + x_3^2 + (y_3 - y_1)(-2b)}{(x_1 - x_3)}, \\ R = (x_2 - a)^2 + (y_2 - b)^2, \\ (x_1 - x_3)(y_3 - y_2) - (x_2 - x_3)(y_3 - y_1) \neq 0. \end{cases}$$

Таким образом, для характеристики поля не равной двум и когда -1 не является квадратом, в этом поле параметры a, b и R определяются однозначно и можно построить $q^2(q - 1)$ различных окружностей при $R \neq 0$ для СРС. При $R = 0$ либо уравнение окружности совпадает с уравнениями

двух прямых, либо таких точек вообще не существует. А включение последнего неравенства в систему связано с условием существования дроби, в противном случае получим, что данные три точки лежат на одной прямой. В качестве секрета можно взять координаты центра окружности (a, b) или параметр R.

Примером плоскости, состоящей из окружностей, является плоскость Мёбиуса. В [24, 17] плоскость Мёбиуса, $L-(\mu, \lambda, \sigma)$-схемы, совершенные шифры и их современные аналоги связаны между собой, поэтому представляет интерес их исследования.

Напомним, что мёбиусова (инверсная) плоскость [24] получается из евклидовой плоскости присоединением единственной идеальной точки, которая считается принадлежащей всем прямым плоскости. После такого присоединения и прямые линии, и окружности называются циклами. Для полей $GF(2^r)$ характеристики два, как известно, примером плоскости Мёбиуса является проекция овалоида $\sigma x_1x_2+\sigma x_3x_4+x_3^2+x_4^2=0$ на плоскость $x_4=0$, где $\sigma\in GF(2^r)$ таково, что многочлен $x^2+\sigma x+1$ неприводим над $GF(2^r)$. В [24] показано, что сфера с уравнением $x_1^2+x_2^2+x_3^2=x_4^2$ имеет стереографическое отображение на плоскость Мёбиуса для нечетного q. Для плоскости Мёбиуса справедлива аксиома, которая является необходимым условием $O(3)$- и $U(3)$-стойкости шифра [17].

$U(L)$-стойкий шифр (и соответствующий ему перпендикулярный массив $PA_\omega(L, \lambda, \mu)$) — шифр, стойкий к атакам на основе неупорядоченной L-кратной совокупности шифртекстов, полученных на одном ключе, а $O(L)$-стойкий шифр (и соответствующий ему массив $A_\omega(L, \lambda, \mu)$) — шифр, стойкий к атакам на основе упорядоченной L-кратной совокупности шифртекстов, полученных на одном ключе. Такие шифры являются стойкими к активным атакам злоумышленника: имитации и подмены сообщения. Их построение эквивалентно построению таблицы зашифрования определенного вида, состоящей из подстановок на множестве элементов открытого текста.

$L-(\mu, \lambda, \sigma)$-схема задается набором непустых подмножеств (блоков) некоторого множества и определяется несколькими условиями. Плоскость Мёбиуса является примером $L-(\mu, \lambda, 1)$-схемы. Заметим, что аналогичные параметры такой схемы и имитостойкого шифра имеют то же обозначение.

Для $L-(\mu, \lambda, \sigma)$-схем и $O(L)$-, $U(L)$-стойких шифров справедлив ряд утверждений: утверждение 9 определяет условие соответствия $L-(\mu, \lambda, \sigma)$-схемы массиву $O(L)$- или $U(L)$-стойкого шифра; утверждение 10 определяет условие построения неэндоморфного $O(L)$- или $U(L)$-стойкого шифра на основе $L-(\mu, \lambda, \sigma)$-схем и эндоморфного $O(L)$- или $U(L)$-стойкого шифра; утверждение 11 показывает простой способ «уменьшения» массива $PA_\omega(L, \lambda, \mu)$ (или $A_\omega(L, \lambda, \mu)$) до массива $PA_\omega(L, \lambda', \mu)$ (или $A_\omega(L, \lambda', \mu)$).

Утверждение 9. *Упорядоченное произвольным образом множество блоков $L-(\mu, \lambda, \sigma)$-схемы образует массив $PA_\omega(L, \lambda, \mu)$ (или $A_\omega(L, \lambda, \mu)$) только при условии $\sigma=\omega\cdot C_\lambda^L$ (или $\sigma=\omega\cdot A_\lambda^L$).*

Утверждение 10. *Если для каждого блока $L-(\mu, \lambda, \sigma)$-схемы множество его элементов является множеством элементов открытых текстов массива $PA_{\omega'}(L, \lambda, \lambda)$ (или $A_{\omega'}(L, \lambda, \lambda)$), то набор всех строк такого массива образует массив $PA_\omega(L, \lambda, \mu)$ (или $A_\omega(L, \lambda, \mu)$), где $\omega'=\omega/\sigma\geqslant 1$.*

Утверждение 11. *Если существует массив $PA_\omega(L, \lambda, \mu)$ (или $A_\omega(L, \lambda, \mu)$), то при $L\leqslant\lambda'<\lambda\leqslant\mu$ путем удаления любых $\lambda-\lambda'$ столбцов из него всегда можно выделить массив $PA_\omega(L, \lambda', \mu)$ (или $A_\omega(L, \lambda', \mu)$), соответственно. Обратно, если не существует массива $PA_\omega(L, \lambda', \mu)$ (или $A_\omega(L, \lambda, \mu)$), то не существует и массива $PA_\omega(L, \lambda, \mu)$ (или $A_\omega(L, \lambda', \mu)$).*

Посчитаем число ключей для построения перпендикулярного массива $PA_1(3, \lambda, \mu)$, соответствующего $U(3)$-стойкому шифру, где μ — мощность множества зашифрованных текстов, соответствующая числу всех точек плоскости Мёбиуса (q^2+1); λ — мощность множества зашифрованных текстов, соответствующая числу точек на кривой $q+1$:

$$\pi=C_\mu^3=\frac{\mu(\mu-1)(\mu-2)}{1\cdot 2\cdot 3}=\frac{(q^2+1)q^2(q^2-1)}{6}=$$
$$=q(q^2+1)\cdot\frac{(q+1)q(q-1)}{6}=q(q^2+1)\cdot C_{q+1}^3.$$

Заметим, что множитель $q(q^2+1)$ — это число всех циклов плоскости Мёбиуса, а C_{q+1}^3 — это число ключей, необходимых для построения эндоморфного $U(3)$-стойкого шифра с параметрами $\lambda=\mu=q+1$. Аналогично, число ключей и для построения неэндоморфного $O(3)$-стойкому шифра выражается через число ключей эндоморфного $O(3)$-стойкого шифра как $\tau=A_{q^2+1}^3=q(q^2+1)\cdot A_{q+1}^3$. Поэтому, чтобы построить, например, неэндоморфный $U(3)$-стойкий шифр на основе плоскости Мёбиуса, необходимо каждый ее цикл использовать вместе с соответствующим эндоморфным $U(3)$-стойким шифром. Отметим случай $L=q$: тогда эндоморфный $U(3)$-стойкий шифр задается латинским квадратом. Таким образом, частным случаем утверждения 10 является следующее

Утверждение 12. *Если множество элементов каждого цикла плоскости Мёбиуса взято за множество открытых текстов некоторого эндоморфного $U(3)$-стойкого (или $O(3)$-стойкого) шифра,*

то объединение таблиц зашифрования для всех циклов является таблицей зашифрования неэндоморфного $U(3)$-стойкого (или $O(3)$-стойкого) шифра.

Таким образом, в работе получены следующие результаты: доказана дистрибутивность решетки рубрикаторных идеалов при тематическом разграничении доступа; использован аппарат решеток для изучения СРС, рассмотрено свойство модулярности; установлена связь структур доступа с решетками, матроидами и квазигруппами; установлена связь плоскости Мёбиуса с современными аналогами совершенных шифров.

Авторы благодарят Н. А. Гайдамакина и В. А. Баранского за постановку задач и внимание к работе; М. М. Глухова, В. В. Ященко, П. Н. Девянина, Н. П. Варновского за направляющие контакты и полезные обсуждения, А. Н. Алексейчука за плодотворные дискуссии, литературные ссылки и указания на приоритеты; а также А. С. Худеньких и в целом Екатеринбургский научно-технический центр ФГУП «НПП «Гамма» за поддержку.

Литература

[1] Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во УрГУ, 2003, 327 с.

[2] Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. М.: Изд-во Молгачева С. В., 2001, 352 с.

[3] Девянин П. Н., Михальский О. О., Першаков А. С. Теоретические основы компьютерной безопасности. Учеб. пособие для ВУЗов. М.: Радио и связь, 2000, 168 с.

[4] Глухов М. М., Стеллецкий И. В., Фофанова Т. С. Структуры // Итоги науки. Алгебра. Геометрия. Топология. 1968. М.: 1970, с. 101–155.

[5] Девянин П. Н. Модели безопасности компьютерных систем. М.: Academia, 2005. 144 с.

[6] Баранский В. А. Введение в общую алгебру и ее приложения. Екатеринбург: Изд-во УрГУ, 1998, 169 с.

[7] Скорняков Л. А. Элементы теории структур. М.: Наука, 1970, 148 с.

[8] Асанов М. О., Баранский В. А., Расин В. В. Дискретная оптимизация: графы, матроиды, алгоритмы. М.–Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001, 288 с.

[9] Введение в криптографию. Под общей ред. В. В. Ященко. СПб: Питер, 2001, 288 с.

[10] Блейкли Г. Р., Кабатянский Г. А. Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации, 1997, т. 33, вып. 4, с. 102–110.

[11] Зегжда Д. П., Ивашко А. М. Технология создания безопасных систем обработки информации на основе отечественной защищенной операционной системы // Проблемы информационной безопасности. Комп. системы, 1999, № 2.

[12] Болотова Е. А., Титов С. С. Два этюда на тему разграничения доступа к информации в иерархических моделях // Проблемы теоретической и прикладной математики: Труды 39-й Всеросс. молодежной конф. Екатеринбург: УрО РАН, 2008, С. 343–347.

[13] Martí-Farre J., Padro C. Secret sharing schemes on access structures with intersection number equal to one // Discrete Appl. Math., 2006, v. 154, № 3, p. 552–563.

[14] Beimel A., Chor B. Universally ideal secret sharing schemes // IEEE Trans. on Information Theory, 1994, v. 40, № 3, p. 786–794.

[15] Алексейчук А. Н. Совершенные схемы разделения секрета и конечные универсальные алгебры // Реєстрація, зберігання і обробка даних, 2005, т. 7, № 2, с. 55–65.

[16] Липский В. Комбинаторика для программистов. М.: 1988, 200 с.

[17] Зубов А. Ю. Совершенные шифры. М.: Гелиос АРВ, 2003, 160 с.

[18] Глухов М. М. О применениях квазигрупп в криптографии // Прикладная дискретная математика, 2008, № 2(2), с. 28–33.

[19] Баутин С. П., Медведев Н. В., Титов С. С. Проблема разделения секрета на эллиптических кривых // Проблемы прикладной математики и механики: Сб. научн. тр. Екатеринбург: УрГУПС, 2008, вып. 65(148)/3, с. 160–174.

[20] Фомичев В. М. Дискретная математика и криптология. Курс лекций. М.: Диалог-МИФИ, 2003, 400 с.

[21] Зюляркина Н. Д., Махнёв А. А. Автоморфизмы полутреугольных графов с $\mu = 6$ // Проблемы теоретической и прикладной математики. Труды 40-й Всероссийской молодежной конференции. Екатеринбург: УрО РАН, 2009, с. 28–32.

[22] Martí-Farre J., Padro C. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants // Proc. of Fifth Conference on Security and Cryptography for Networks, SCN 2006, Lecture Notes in Comput. Sci., 2006, v. 4116, p. 201–215.

[23] Титов С. С., Устьянцева Н. О. Пороговые схемы разделения секрета и совершенные шифры // Проблемы теоретической и прикладной математики: Труды 39-й Всеросс. молодежной конф. Екатеринбург: УрО РАН, 2008, с. 408–412.

[24] Картеси Ф. Введение в конечные геометрии. М.: Наука, 1980, 320 с.