ИНФОРМАТИКА

2007 **октябрь-декабрь** **№ 4**

ЗАЩИТА ИНФОРМАЦИИ

УДК 003.26

Т.В. Галибус

МОДУЛЯРНАЯ РЕАЛИЗАЦИЯ СПЕЦИАЛЬНЫХ СТРУКТУР ДОСТУПА

Рассматриваются способы построения модулей и распределения частичной информации для модулярного разделения секрета в специальных случаях. Предлагаются алгоритмы для построения целочисленных и полиномиальных модулей для пороговых и парных структур доступа, в частности алгоритм модулярной реализации парных структур доступа над кольцом целых чисел и алгоритм идеальной реализации некоторых парных структур над кольцом многочленов. Показываются адаптационные возможности модулярного разделения секрета над кольцом многочленов.

Введение

Теория разделения информации как направление современной криптографии впервые была выдвинута в 1979 г. в основополагающих работах Дж. Блейкли [1] и А. Шамира [2]. В зарубежных публикациях чаще говорят о разделении «секрета», а не информации. Под этим имеют в виду, как правило, секретный PIN-код, позволяющий пользоваться банкоматом, мобильным телефоном, кодовым замком и т. д. В настоящей работе в основном используется западный аналог указанного термина. Основная задача теории разделения секрета состоит в том, чтобы распределить некоторую важную информацию среди данной группы лиц. При этом лишь заранее определенные подмножества, объединив свои частичные секреты, могут восстановить истинное значение секрета.

В работах К. Асмуса, Дж. Блюма [3] и М. Миньотта [4] были намечены основы модулярного подхода к решению основной задачи в кольце целых чисел. В этом кольце в качестве секрета c можно взять некоторое целое число, а в качестве частичного секрета участника – вычет c по некоторому модулю. Восстановление секрета в таких схемах, которые называются *модулярными*, осуществляют путем решения системы сравнений, чаще всего с помощью китайской теоремы об остатках. Следует отметить, что схема Шамира, по существу, также является модулярной.

Дадим ключевое определение в теории разделения секрета. Пусть $P=\{1, 2, ..., t\}$ – множество участников схемы разделения секрета (СРС).

Определение. *Под структурой доступа* Γ *схемы разделения секрета будем понимать любое монотонное семейство подмножеств множества P, т. е.*

$$A \in \Gamma; A \subset B \subset P \Rightarrow B \in \Gamma.$$

Под реализацией структуры доступа Γ понимают такой алгоритм (или СРС), который позволяет восстанавливать секрет лишь для подмножеств участников, содержащихся в Γ. Отметим, что в классических подходах к разделению секрета, как правило, рассматривается лишь случай (k, t)-пороговой схемы доступа, т. е. такой, в которой разрешенными подмножествами являются все l-подмножества из множества t участников, где $l \geq k$. Число k называют *порогом*.

Целью изучения схем разделения секрета является не только исследование наиболее приемлемых моделей (структур доступа), но и поиск возможностей по реализации произвольных схем с заданными свойствами. Так, в работе [5] показано, как можно реализовать модулярно так называемые купейные («compartmented» в англоязычной литературе) структуры доступа. В этих схемах участники разбиваются на некоторые подмножества (купе), и, помимо общего порога, в каждом из этих подмножеств вводится свой порог. Секрет может быть восстановлен только в том случае, когда количество участников из любого купе больше купейного порога, а всех участников больше общего порога. В работе [6] было показано, что

модулярный подход пригоден для реализации произвольной структуры доступа. Это является обобщением предложенной С. Ифтене купейной структуры [5]. Однако не всегда общий подход является удобным для применения. Например, в настоящей статье предлагается специальный способ модулярной реализации так называемой парной структуры доступа над кольцом целых чисел, требующий меньшего числа операций, чем при применении общего алгоритма. Под парными понимаются структуры, у которых максимальными по включению запрещенными множествами являются все одноэлементные множества и некоторые пары. Эти схемы образуют более широкий класс, чем (2, n)- и (3, n)-пороговые.

В настоящей работе рассматриваются вопросы оценки качества схем разделения секрета для различных структур доступа, необязательно являющихся пороговыми. При разработке схем разделения секрета необходимо удовлетворить нескольким естественным требованиям. К их числу, в первую очередь, относится требование *идеальности*, т. е. размер частичного секрета c_i должен быть равен размеру основного секрета c для любого $i = 1, \ldots, t$. С другой стороны, желательно, чтобы неразрешенные множества участников не получали никакой дополнительной информации к имеющейся априорной о возможном значении секрета c. Такие схемы называют *совершенными*. В работе приводятся некоторые реализации специальных структур доступа над кольцом многочленов, удовлетворяющие данным требованиям совершенности и идеальности. В частности, рассматриваются реализации парных структур доступа над этим кольцом. Отметим, что модулярное разделение секрета в кольце целых чисел не обладает свойствами идеальности и совершенности. Такие СРС обладают наилучшими свойствами, если модули выбраны попарно взаимно простыми и как можно более близкими [7, 8].

В работе показано также, что в условиях модулярного подхода над кольцом многочленов можно успешно строить СРС с адаптационными свойствами. Это значит, что при добавлении новых участников и изменении порога можно использовать старую схему с небольшой модификацией.

1. Модулярная схема разделения секрета

Для дальнейшего рассмотрения специальных реализаций структур доступа напомним общий принцип модулярного разделения секрета К. Асмуса и Дж. Блюма [3] для (k, t)-пороговой СРС.

Рассмотрим систему $p < m_1 < m_2 < \ldots < m_t$ попарно взаимно простых модулей, для которой выполнено условие

$$\prod_{i=1}^{k} m_i > p \prod_{i=1}^{k-1} m_{t-i+1}.$$

Положим $M_1 = \prod_{i=1}^{k-1} m_{t-i+1}$, $M_2 = \prod_{i=1}^{k} m_i$. Пусть секрет c выбирается так, что $0 < c < p$. Пусть также $y=c+Ap$, где A – произвольное целое из промежутка [M_1, M_2/p). Тогда в качестве частичного секрета для i-го участника возьмем $c_i = y \pmod{m_i}$, т. е. наименьший неотрицательный вычет y по модулю m_i. Для восстановления секрета c применяем китайскую теорему об остатках, а затем приводим полученный результат по модулю p. Такая схема отличается от схемы, предложенной М. Миньоттом [4], лишь введением дополнительного модуля p, по которому приводится секрет. Это незначительное изменение позволяет несколько приблизить размер исходного секрета к размеру частичного секрета.

В работах [6, 9] предложено естественное обобщение рассмотренной схемы на случай кольца многочленов от одной переменной над полем Галуа $F_q[x]$. Единственным отличием схемы является то, что вместо последовательных взаимно простых модулей выбираются попарно взаимно простые полиномы одной степени: $p_0(x)$, …, $p_t(x)$. Секрет $s(x)$ выбирается как вычет по модулю $p_0(x)$. Частичными секретами являются вычеты $s_1(x)$, …, $s_t(x)$ по соответствующим модулям.

Поскольку степени полиномов равны, то каждый участник получает частичный секрет фактически из того же множества, что и секретное значение $s(x)$, так как это вычеты по модулям

многочленов одной и той же степени. Таким образом, участники не получают никакой информации о секрете, поскольку пространство возможных значений истинного секрета не сужается.

Отметим, что в случае модулярной реализации общих структур доступа при использовании подхода К. Асмуса и Дж. Блюма условие попарной взаимной простоты модулей можно ослабить. Для корректного построения СРС достаточно лишь того, чтобы наименьшее общее кратное (НОК) многочленов любых запрещенных подмножеств было меньше НОК многочленов любых разрешенных подмножеств. Далее будем пользоваться этим обобщением, сохраняя прежнее название – схемы Асмуса–Блюма.

2. Генерация полиномиальных модулей для семейств пороговых СРС

Отметим, что различные способы построения модулей для пороговых схем над кольцом целых чисел были предложены ранее в работе [8]. Теорема 1 показывает, что при переходе к кольцу многочленов $F_2[x]$ над двоичным полем появляется возможность строить системы модулей, реализующие не одну, а целое семейство пороговых схем $(1, n)$, $(2, n)$, ..., (n, n). В работе [6] автором указывался один подход к генерации максимальной по включению системы подходящих модулей. Данный способ удобен для реализации любой пороговой структуры доступа для любого числа n участников.

Теорема 1. *Пусть $t = n!$. Тогда многочлены $x^t + x + 1$, $x^t + x^2 + 1,...,x^t + x^n + 1 \in F_2[x]$ попарно взаимно просты и, значит, пригодны для реализации семейства пороговых СРС:*

$$(1, m), (2, m),.., (m, m), \ \forall m, 1 < m \le n.$$

Доказательство. Пусть $d(x) = \text{НОД}(x^t + x^i + 1, x^t + x^j + 1)$, где $i > j$. Очевидно, $d(x)$ делит сумму $x^i + x^j = x^j (x^{i-j}+1)$ этих многочленов. С другой стороны, у триномов из условия теоремы 0 и 1 не являются корнями. Поэтому $d(x) \mid x^{i-j} + 1$. Поскольку t делится на $i - j$, то $d(x) \mid x^t + 1$. Также $d(x) \mid x^t + x^j + 1$, поэтому $d(x)$ делит и x^i. Последнее означает, что $d(x) = 1$.

В связи с тем что в случае кольца $F_2[x]$ условие для степеней многочленов $\deg M_2 \ge \deg p + \deg M_1$ является аналогом условия $M_2 \ge p M_1$ для случая кольца целых чисел, то, подставив степени, получим очевидное условие $kn \ge \deg p + (k-1)n$. ■

3. Реализация парных структур доступа над кольцом целых чисел

Рассмотрим схемы разделения секрета для парных структур доступа над кольцом целых чисел. Напомним, что парной называется структура доступа, у которой максимальными по включению запрещенными являются все одноэлементные множества и некоторые пары. Во-первых, указывается специальная реализация произвольной парной структуры доступа, которая требует выполнения меньшего числа операций. Во-вторых, описываются все возможные парные структуры доступа, которые реализуются попарно взаимно простыми модулями.

Теорема 2. *Любая парная структура доступа допускает модулярную реализацию над кольцом целых чисел.*

Доказательство. Обозначим НОК $[a, b]$ через $[a, b]$, а НОД (a, b) через (a, b). Сначала докажем одно вспомогательное утверждение. Пусть различные натуральные i, j удовлетворяют условию $i, j \le n$, тогда $(n! + i, n! + j) = (i, j)$. В самом деле, многократно применяя свойство $a = bq + r \Rightarrow (a, b) = (b, r)$, имеем $(n! + i, n! + j) = (n! + + i, n! + j - n! - i) = (n! + i, j - i) = (i, j - i) = (i, j)$.

Далее вместо n возьмем большее m так, чтобы в промежутке $(1, m)$ было достаточно много простых чисел. Пусть p, q – различные простые числа из этого промежутка. Тогда $[m! + p, m! + q] = (m!)^2 + (p + q)m! + pq$.

Аналогичная формула имеет место и для составных p и q, если $(p, q) = 1$. Если же $(p, q) = d > 1$, то $[m! + p, m! + q] = ((m!)^2)/d + ((p + q) m!)/d + [p, q]$.

Если теперь секрет c брать вблизи $(m!)^2$, то величина $[m! + p, m! + q]$ при взаимно простых p, q будет больше c, а при не взаимно простых p, q – меньше c.

Таким образом, осталось доказать следующее утверждение: всегда можно найти заданное число различных натуральных $m_1, m_2, ..., m_t$ так, чтобы заранее указанные пары были взаимно простыми, а остальные нет.

Поступим так. Изначально в качестве $m_1, m_2, ..., m_t$ возьмем систему простых чисел. Все простые сейчас и далее, разумеется, меньше m, а также попарно различны. Если надо, чтобы $(m_1, m_2) > 1$, то домножим m_1 и m_2 на новое простое. Такое домножение не изменит другие наибольшие общие делители. Далее поступаем аналогично, используя каждый раз новое простое. ■

Указанный способ генерации модулей является более подходящим для парных структур доступа, чем общий способ реализации произвольных структур доступа, полученный в работе [9]. Дело в том, что применение специального метода требует только двух домножений, а общий алгоритм требует t–2 домножений для каждой пары запрещенных, где t – число участников.

Отметим еще одну особенность модулярных схем в кольце целых чисел. Дело в том, что первоначально пороговые схемы строились с использованием попарно взаимно простых модулей. Возникает естественный вопрос о том, какие вообще СРС могут задавать системы указанных модулей. Проще всего на этот вопрос ответить для случая парной СРС. Парную СРС удобно характеризовать ее матрицей $A = (a_{ij})$, где $a_{ij} = 1$, если пара (i, j) разрешена, в противном случае $a_{ij} = 0$. Пары (i, i) не рассматриваются и поэтому полагают $a_{ii} = 0$.

С учетом выбранных обозначений укажем необходимое условие реализуемости парных СРС с попарно взаимно простыми модулями.

Теорема 3. *Если парная структура доступа для t участников реализуется модулярно системой попарно взаимно простых модулей, то ее матрица имеет вид* $A = (a_{ij})$, *где* $a_{ij} = 1$ *влечет* $a_{kl} = 1$, *если* $k \le i$, $l \le j$, $k \ne l$.

Доказательство. Во-первых, отметим следующее свойство данной структуры доступа: не существует таких двух пар участников, что $\{x_i, x_j\}$ и $\{x_k, x_l\}$ запрещены, а $\{x_i, x_k\}$ и $\{x_j, x_l\}$ разрешены. В противном случае окажется, что $m_i m_j < m_i m_k$, $m_l m_j > m_l m_k$, а значит, $m_i m_j m_l m_k < m_i m_j m_l m_k$.

Следовательно, путем перестановки участников (т. е. строк и столбцов матрицы A) можно привести матрицу к виду, когда во всех строках и столбцах $a_{ij} \le a_{i-1j}$, $a_{ij} \le a_{ij-1}$. Это и означает, что выполняется условие теоремы. ■

4. Идеальная реализация парных структур доступа над кольцом многочленов

Докажем, что существует реализация парных структур доступа уже над кольцом многочленов таким образом, чтобы построенные модули имели равные степени, т. е. размер всех пространств частичных секретов был равен размеру пространства секретов. Напомним, что такая реализация СРС называется идеальной. На самом деле, существуют структуры доступа, для которых невозможно построить идеальную СРС [10]. В этом случае вводится специальная характеристика уровня информации. Если размеры частичных секретов в r раз превосходят размер секрета, то такая реализация называется реализацией с *уровнем информации* $1/r$. В полном объеме вопрос об идеальной модулярной реализуемости произвольных структур доступа еще не решен.

Пусть $C_q(n)$ – максимальное количество попарно взаимно простых полиномов степени n со старшим коэффициентом 1. $C_q(n)$ определяет количество участников пороговой полиномиальной модулярной СРС. В работе [6] была найдена точная формула для $C_q(n)$, а также указан способ построения максимального семейства $C_q(n)$ попарно взаимно простых многочленов степени n.

Теорема 4. *Пусть степени многочленов участников равны n. Тогда любая парная структура доступа с непересекающимися парами запрещенных подмножеств допускает идеальную реализацию схемы Асмуса–Блюма в кольце многочленов* $F_q[x]$ *с количеством участников* $t \le 2C_q(n)$.

Доказательство. Напомним, что каждый участник схемы должен обладать полиномом $p_i(x)$, $(p_i(x), p_j(x)) = 1$. Поскольку согласно условию теоремы любой участник принадлежит не

более чем одной паре запрещенных подмножеств, то можно считать равными полиномы, принадлежащие участникам одной пары, т. е.

$$\{i, j\} \notin \Gamma \Rightarrow p_i(x) = p_j(x) = p_{ij}(x),$$

а значит, $\deg(p_{ij}(x), p_{ij}(x)) = n$ для всякого запрещенного подмножества $\{i, j\}$.

Отметим, что при этом разность степеней НОК любых разрешенных и запрещенных подмножеств не менее n. Поэтому всегда можно выбрать дополнительный модуль $p_0(x)$ степени n, определяющий секрет, а значит, размеры пространства секретов совпадают с размером пространства частичных секретов и схема является идеальной. ■

К сожалению, для произвольных парных структур доступа с пересекающимися парами участников пока не удалось получить идеальной реализации, однако в работе [6] предлагается модулярная реализация такой структуры над кольцом многочленов, позволяющая несколько улучшить оценку уровня информации в схеме Асмуса–Блюма по сравнению с общим алгоритмом реализации произвольной структуры доступа над любым евклидовым кольцом.

Назовем глубиной парной структуры доступа максимальное количество запрещенных пар, которым принадлежит каждый участник.

Теорема 5. *Пусть степени многочленов участников равны n. Тогда любая парная структура доступа с глубиной s допускает реализацию схемы разделения секрета Асмуса–Блюма с уровнем информации* $1/s$ *в кольце многочленов* $F_q[x]$*, если степени модулей удовлетворяют условию* $n > sC_t^2$.

Доказательство. Пусть некоторый участник присутствует в s запрещенных парах. Каждой запрещенной паре необходимо поставить в соответствие единственный общий делитель. Поэтому у многочленов, участвующих в схеме, должно быть не менее s различных неприводимых делителей. Количество различных пар не превышает C_t^2. Поэтому условие для степени любого общего делителя пары многочленов $n/s > C_t^2$ гарантирует реализуемость любой парной структуры доступа с глубиной s. При этом разница степеней НОК разрешенных и запрещенных подмножеств не превышает n/s. Очевидно, что уровень информации при этом не менее $1/s$. ■

Возможность идеальной реализации позволяет разделить секрет более эффективно в том смысле, что для хранения исходного секрета требуется не больше памяти, чем для хранения частичного секрета. Таким образом, найдены структуры доступа, реализуемые идеально, а также оценен уровень информации в специальных реализациях парных структур доступа.

5. Адаптационные свойства модулярного разделения секрета над кольцом многочленов

Одной из задач в практической реализации разделения секрета является указание возможности перехода от одной структуры доступа к другой с наименьшим количеством изменений в уже реализованной СРС [11, 12]. Модулярное разделение секрета над кольцом многочленов в силу равенства степеней модулей обладает в этом смысле некоторыми преимуществами по сравнению с классическим подходом. Рассмотрим адаптацию СРС к изменению порога или добавлению участников. Зачастую такие операции требуют изменения большого количества информации в схеме, однако в случае модулярной схемы над кольцом многочленов в этом нет необходимости.

Свойство 1. *Пусть n – степени модулей участников СРС, а их количество* $t < C_q(n) - 1$. *Тогда добавление нового участника к модулярной схеме разделения секрета над* $F_q[x]$ *не потребует изменения уже распределенных частичных секретов и модулей.*

Доказательство. При добавлении одного участника проверяется, можно ли обеспечить ему модуль степени n. Поскольку количество попарно взаимно простых полиномов степени n не превосходит $C_q(n)$, то нет необходимости менять уже имеющиеся модули, пока количество участников не достигло $C_q(n)$. В качестве частичных секретов новых участников берутся остатки от деления секрета на выбранные новые модули. Уже имеющиеся частичные секреты при этом не меняются. ■

Свойство 2. *Пусть имеется полиномиальная модулярная* (k, t)*-пороговая СРС. Тогда переход к любой* (k', t)*-пороговой СРС,* $1 \le k' \le t$, *не потребует изменения модулей участников, а лишь их частичных секретов.*

Доказательство. При изменении порога в схеме Асмуса–Блюма необходимо лишь переопределить количество тех участников, для которых частичные секреты выбраны произвольно. Следовательно, частичные секреты оставшихся участников вычисляются заново относительно соответствующих модулей. Таким образом, один и тот же набор модулей подходит для реализации всех пороговых структур доступа для имеющегося множества участников. ■

Заключение

В работе рассмотрены некоторые специальные свойства модулярного разделения секрета, такие как идеальная реализуемость парных структур доступа над кольцом многочленов, изменение порога и добавление участников. На практике это означает, что построенная схема более применима для сетевых систем с большим числом участников, в которых необходимо хранить большие объемы информации. Указан также способ генерации модулей для пороговых схем разделения секрета над кольцом многочленов. Таким образом, дальнейшее исследование модулярного разделения секрета целесообразно, так как при небольших модификациях общего подхода реализация оказывается более оптимальной в смысле сложности алгоритмов и хранения информации, что обусловливает возможность ее применения на практике для построения схем электронного голосования или процедуры пороговой цифровой подписи. Это оправдано еще и тем, что модулярный подход к разделению секрета является более эффективным с точки зрения теории сложности, чем классическая схема Шамира. В самом деле, еще в работе [3] показано, что вычислительная сложность восстановления секрета в модулярной схеме разделения секрета с использованием CRT-алгоритма равна $O(t)$, в то время как сложность восстановления секрета с использованием интерполяционной формулы Лагранжа в схеме, предложенной А. Шамиром [4], равна $O(t \log_2 t)$.

Список литературы

1. Blakley, G. Safeguarding cryptographic keys / G. Blakley // AFIPS 1979 Nat. Computer. – 1979. – Vol. 48. – P. 313–317.

2. Shamir, A. How to Share a Secret / A. Shamir // Comm. ACM. – 1979. – Vol. 22. – P. 612–613.

3. Asmuth, C.A. A modular approach to key safeguarding / C.A. Asmuth, J. Bloom // IEEE Trans. on IT. – 1983. – Vol. 29. – P. 156–169.

4. Mignotte, M. How to share a secret / M. Mignotte. – 1982. – Vol. 1981. – P. 371–375.

5. Iftene, S. Compartmented Secret Sharing Based on the Chinese Remainder Theorem / S. Iftene // Cryptology ePrint Archive [Electronic resource]. – 2005. – № 408. – Mode of access: http://eprint.iacr.org/2005/408.pdf. – Date of access: 20.11.2006.

6. Galibus, T. Generalized Mignotte Sequences in Polynomial Rings / T. Galibus, G. Matveev // ENTCS. – 2006. – Vol. 186. – P. 39–44.

7. Quisquater, M. On the security of the threshold scheme based on the Chinese remainder theorem / M. Quisquater, B. Preneel, J. Vandewalle // LNCS. – 2002. – Vol. 2274. – P. 199–210.

8. Кошур, Н.Н. Генерация модулей для пороговых схем / Н.Н. Кошур, Г.В. Матвеев // Вопросы информационной безопасности: сб. науч. тр. – 2002. – № 1. – С. 85–88.

9. Галибус, Т.В. Разделение секрета над полиномиальными кольцами / Т.В. Галибус // Вестник БГУ. Сер. 1. – 2006. – № 2. – С. 97–100.

10. Stinson, D.R. Cryptography: Theory and Practice / D.R. Stinson. – London: CRC Press, 1995. – 512 p.

11. Desmedt, Y. Redistributing secret shares to new access structures and its applications: technical report № ISSE TR-97-01 / Y. Desmedt, S. Jajodia. – George Mason University. USA, 1997. – 23 p.

12. Frankel, Y. Adaptive security for the additive-sharing based proactive RSA / Y. Frankel, P. MacKenzie, M. Yung // LNCS. – 2001. – Vol. 1992. – P. 240–263.
13. Ященко, В.В. Введение в криптографию / В.В. Ященко. – СПб.: МЦНМО, 2001. – 431 с.

Поступила 13.12.06

Белорусский государственный университет,
Минск, пр. Независимости, 4
e-mail: galibus@bsu.by

T.V. Galibus

MODULAR REALIZATION OF SPECIFIC ACCESS STRUCTURES

Several specific algorithms to construct the polynomial modulies for realization of a secret sharing scheme with optimal cryptographic properties is proposed. In particular, the modulies for the threshold and paired access structures are constructed. The problem of adapting the modular secret sharing scheme is considered.