Таким образом, предложены подходы к реализации нелинейных ПСП и перестановок большой длины, имеющих небольшую длину ключа.

Список литературы

1. Орлов В. А., Карташова М. В. О реализации псевдослучайных перестановок и последовательностей с использованием линейных преобразований // Информационные технологии управления в социально-экономических системах. — 2009. — № 3. — С. 87–91.

ИДЕАЛЬНЫЕ МОДУЛЯРНЫЕ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

Г. В. Матвеев, Н. Н. Шенец (Минск)

Модулярные схемы разделения секрета были предложены Миньоттом [1], Асмусом и Блюмом [2]. Они основаны на решении системы сравнений в кольце целых чисел. Пусть $I = \{1, 2, \ldots, t\}$ — множество участников, а число c — *секрет*. Каждый участник $i \in I$ располагает натуральным модулем m_i и числом $s_i = c \pmod{m_i}$ — наименьшим неотрицательным вычетом секрета c по модулю m_i, которое называется *частичным секретом* участника. Тогда любое подмножество участников $A \subseteq I$ находит значение c, решая соответствующую систему сравнений. Однако правильно найдут секрет лишь те подмножества участников A, для которых выполнено условие $c < \text{НОК}[m_i, i \in A]$. Асмус и Блюм предложили приводить секрет c по дополнительному модулю m_0, что позволяет приблизить его размер к размерам частичных секретов.

С разделением секрета тесным образом связано понятие *структуры доступа*, под которой понимается семейство подмножеств Γ множества участников I, обладающее свойством монотонности, т. е. $A \in \Gamma, A \subseteq B \subseteq I \Rightarrow B \in \Gamma$. Подмножества из семейства Γ называются разрешенными. Все остальные подмножества называются запрещенными. Они образуют структуру отказа $\overline{\Gamma}$. Любая структура доступа задается набором своих минимальных по включению подмножеств $\Gamma_{\min}$, а структура отказа — максимальным по включению набором $\overline{\Gamma}_{\max}$.

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 дальнейшем модулярный подход был развит в работах [3, 4]. Он был обобщен на случай кольца полиномов $\mathbb{F}_q[x]$ над полем Галуа $\mathbb{F}_q$. Было показано, что любая структура доступа допускает модулярную реализацию в кольцах целых чисел и полиномов над полями Галуа. Получен также ответ на известный вопрос о том, какие структуры доступа могут быть реализованы с помощью попарно взаимно простых модулей. Такие структуры доступа были названы *элементарными*, они могут быть заданы с помощью линейной формы.

При построении схем разделения секрета стараются удовлетворить нескольким естественным требованиям. К их числу относится требование *совершенности*, т.е. чтобы запрещенные множества участников не получали никакой дополнительной информации к имеющейся априорной о возможном значении секрета c. Для таких схем вводится понятие *информационного уровня* ρ, который равен минимуму отношения размера сектрета к размерам частичных секретов. Известно, что $0 < \rho \leq 1$. В случае $\rho = 1$ схема называется *идеальной*. Формальные определения имеются в работе [5].

В настоящий момент для модулярных схем разделения секрета известно мало результатов, связанных с оценками их качества. Так в работе [5] была построена асимптотически совершенная и асимптотически идеальная пороговая схема над кольцом целых чисел при $m_0 \to \infty$. Отметим, что в этом кольце вообще нельзя построить совершенную модулярную схему разделения секрета. Переход же к кольцу полиномов над полем Галуа позволил преодолеть это препятствие, и в работе [4] была предложена совершенная и идеальная реализация пороговой структуры доступа. Однако для других структур доступа никаких оценок качества их модулярных реализаций до настоящего момента получено не было.

Пусть $m_1(x), m_2(x), \ldots, m_t(x) \in \mathbb{F}_q[x]$ — модули участников. Для реализации структуры доступа Γ необходимо и достаточно, чтобы выполнялось условие:

$$M_1 = \deg \max_{A \in \overline{\Gamma}} \text{НОК}[m_i(x), i \in A] < \deg \min_{A \in \Gamma} \text{НОК}[m_i(x), i \in A] = M_2.$$

Рассмотрим схему Асмуса—Блюма. Пусть $m_0(x)$ — дополнительный модуль. Тогда секрет $c(x)$ случайным образом выбирается на множестве полиномов, степень которых меньше $\deg m_0(x)$. Затем случайным образом генерируется полином $p(x)$, степень которого

меньше $M_2 - \deg m_0(x)$. В результате формируется промежуточное значение секрета $C(x) = m_0(x)p(x) + c(x)$, $\deg C(x) < M_2$. Отметим, что все значения полинома $C(x)$ равновероятны. Частичный секрет i-го участника вычисляется по формуле $s_i(x) = C(x) \pmod{m_i(x)}$.

Теорема 1. *Реализация схемы Асмуса—Блюма в кольце полиномов над полем Галуа будет совершенной тогда и только тогда, когда*:

1. НОД$(m_0(x), m_i(x)) = 1$, $\forall i \in I$.

2. $\deg m_0(x) \leq M_2 - M_1$.

Определение. Два участника i и j из множества I называются *взаимозаменяемыми*, если для любого подмножества $A \in \overline{\Gamma}_{max}$ справедливо $i \in A \Leftrightarrow j \in A$.

Взаимозаменяемым участникам можно давать одинаковые модули. При этом без потерь можно рассматривать ту же структуру доступа, заменив взаимозаменяемых участников одним участником. Поэтому мы рассматриваем структуры доступа без таких участников.

Теорема 2. *Идеальной модулярной реализацией в кольце полиномов над полем Галуа обладает только пороговая структура доступа.*

Теорема 3. *В классе элементарных непороговых структур доступа оптимальный информационный уровень равен* $1/2$. *Он достигается на структурах, задаваемых линейными формами с коэффициентами* 1 *и* 2.

Список литературы

1. Mignotte M. How to share a secret // Lecture Notes in Computer Science. Advances in cryptology (Eurocrypt'82). — 1983. — P. 371–375.

2. Asmuth C. A., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. — 1983. — V. 29. — P. 208–210.

3. Galibus T., Matveev G. Generalized Mignotte sequences in polynomial rings // Electronic Notes in Theoretical Computer Science. — 2007. — V. 186. — P. 41–46.

4. Galibus T., Matveev G., Shenets N. Some structural and security properties of the modular secret sharing // SYNASC'08. — LosAlamitos (California): IEEE Comp. Soc. Press, CPS, 2009. — P. 197–200.

5. Quisquater M., Preneel B., Vandewalle J. On the security of the threshold scheme based on the Chinese remainder theorem // Lecture Notes in Computer Science. — 2002. — V. 2274. — P. 199–210.