ОБ ИДЕАЛЬНЫХ МОДУЛЯРНЫХ СХЕМАХ РАЗДЕЛЕНИЯ СЕКРЕТА В КОЛЬЦАХ МНОГОЧЛЕНОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

Н. Н. Шенец

НИИ прикладных проблем математики и информатики
Минск, Беларусь
E-mail: Shenets.N@gmail.com

В работе рассматривается модулярное разделение секрета в кольцах многочленов от нескольких переменных над полями Галуа. Получен критерий совершенности модулярных схем в этих кольцах и показано, что идеальными являются только пороговые схемы разделения секрета.

Ключевые слова: секрет, схема разделения секрета, модулярный подход, идеал, идеальность, совершенность.

ВВЕДЕНИЕ

Разделение секрета – молодое направление в криптографии. Его суть состоит в решении следующей задачи: необходимо так распределить некоторую важную информацию (секрет) $c \in S$ между участниками из множества $J = \{1, 2, ..., t\}$, чтобы лишь заранее определенные подмножества (разрешенные) могли правильно восстановить секрет, а остальные (запрещенные) не имели такой возможности. Разрешенные подмножества участников вместе образуют структуру доступа $\Gamma \subseteq 2^J$, обладающую свойством монотонности: $A, B \subseteq J, A \in \Gamma, A \subseteq B \Rightarrow B \in \Gamma$. Структура доступа называется (k, t)-пороговой, если разрешенными подмножествами являются все подмножества, содержащие k либо более участников.

Первые решения основной задачи были предложены Шамиром [1] и Блэйкли [2] в 1979 г. для пороговых структур доступа. В 1983 г. Миньотт [3], Асмут и Блум [4] заложили модулярный подход в разделении секрета. Секретом является некоторое целое число $c \in \mathbb{Z}$, а частичным секретом s_i участника i – его вычет по некоторому модулю m_i. Для восстановления секрета участники решают систему сравнений $c \equiv s_i (\mathrm{mod}\, m_i)$, $i \in A \subseteq J$. В дальнейшем модулярный подход изучался в работах [5–7]. В частности, он был обобщен на кольцо многочленов от одной переменной над полем Галуа.

Для схем разделения секрета были разработаны критерии качества [8] – совершенность и идеальность. Предполагается, что секрет равномерно распределен на множестве S. Схема разделения секрета (СРС) называется совершенной, если запрещенное подмножество участников не получает никакой дополнительной информации о секрете, кроме априорной. Другими словами, распределение секрета остается равномерным и при наличии частичных секретов участников из запрещенного подмно-

жества. Идеальными являются совершенные схемы, в которых размеры секрета и частичных секретов совпадают.

В [7] был получен критерий совершенности модулярных схем Асмута – Блума в кольце многочленов от одной переменной над полями Галуа, а также показано, что идеальной реализацией обладают только пороговые структуры доступа. В настоящей работе мы обобщим эти результаты на кольцо многочленов от нескольких переменных.

ОБОБЩЕННАЯ СХЕМА АСМУТА – БЛУМА В КОЛЬЦЕ МНОГОЧЛЕНОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

Рассмотрим кольцо многочленов от нескольких переменных $\mathbb{F}_q[X]$, $X=(x_1,\ldots,x_n)$, над полем Галуа $\mathbb{F}_q$. Пусть зафиксирован некоторый мономиальный порядок. Тогда приведение многочлена по модулю идеала определено однозначно. Пусть $I_1, I_2, \ldots, I_t$ – нульмерные идеалы, а $s_1(X), s_2(X), \ldots, s_t(X) \in \mathbb{F}_q[X]$ — некоторые многочлены. Тогда справедливо утверждение: система сравнений

$$\begin{cases} c(X) \equiv s_1(X) \bmod I_1 \\ c(X) \equiv s_2(X) \bmod I_2 \\ \ldots \\ c(X) \equiv s_t(X) \bmod I_t \end{cases}$$

либо несовместна, либо имеет единственное решение по модулю наименьшего общего кратного (НОК) идеалов $I_1, I_2, \ldots, I_t$. В случае, если идеалы попарно взаимно простые, т. е. $I_i + I_j = 1, \forall i \neq j$, имеем обобщенную китайскую теорему об остатках (CRT), причем решение системы всегда существует.

Рассмотрим сначала обобщение схемы Миньотта. Секретом будет некоторый многочлен $C(X)$, участнику i выдается модуль I_i и частичный секрет $s_i(X) = C(X) \bmod I_i$. Для реализации структуры доступа необходимо и достаточно, чтобы секрет $C(X)$ был приведенным по модулю НОК идеалов из любого разрешенного подмножества участников и не являлся таковым для запрещенных подмножеств.

В обобщенной схеме Асмута – Блума присутствует дополнительный модуль I_0, а секретом является $c(X) = C(X) \bmod I_0$. В этой схеме $C(X)$ называется промежуточным секретом. Далее будем рассматривать только схему Асмута – Блума, так как схема Миньотта не может быть совершенной ни при каких условиях.

В [9] был предложен алгоритм построения модулей для реализации произвольной структуры доступа в кольце многочленов от нескольких переменных над полем Галуа.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Исследуем схему Асмута – Блума в кольце $\mathbb{F}_q[X]$. Обозначим через $RT(I)$ множество мономов, приведенных по модулю I, а через $RP(I)$ – линейную оболочку $RT(I)$. Пусть также $I^B = \text{НОК}[I_i, i \in B]$, а $M_2 = \bigcap_{B \in \Gamma} RT(I^B)$ – множество мономов, ле-

жащих в пересечении RT идеалов всех разрешенных подмножеств. Отметим, что промежуточный секрет $C(X) \in RP(M_2)$.

Теорема 1. Схема Асмута – Блума в кольце $\mathbb{F}_q[X]$ совершенна тогда и только тогда, когда выполнены следующие условия:

1) $I_0 + I_i = 1, \forall i \in J$.

2) $\forall A \notin \Gamma : RT(I^A I_0) \subseteq M_2$.

Доказательство. Докажем сначала необходимость. Пусть есть совершенная схема Асмута – Блума, но первое условие теоремы не выполнено, т. е. существует $I_i : I_i + I_0 = D \neq 1$. Тогда множество возможных значений секрета для такого участника можно сузить: $c(X) \equiv s_i(X) \bmod D$. Следовательно, схема несовершенна – получили противоречие.

Пусть первое условие выполнено, но не выполнено 2-е, т. е. существует запрещенное подмножество A такое, что $RT(I^A I_0) \not\subset M_2$. Иными словами, существует моном $m \in RT(I^A I_0) \setminus M_2$. Рассмотрим многочлен $g(X) = s^A(X) + \left(m - m(\bmod I^A)\right) =$ $= s^A(X) + f_m(X)$, где $s^A(X)$ – общий частичный секрет, восстановленный участниками из подмножества A. Заметим, что многочлен $f_m(X) \in I^A$, $f_m(X) \in RP(I^A I_0)$ и содержит моном m. Следовательно, $g(X) \in RP(I^A I_0)$. Положим $c' = g(X) \bmod I_0$. Согласно CRT, для системы

$$\begin{cases} C(X) \equiv s^A(X) \bmod I^A \\ C(X) \equiv c'(X) \bmod I_0 \end{cases}$$

существует единственное решение в $RP(I^A I_0)$, но по построению этим решением является многочлен $g(X)$. С другой стороны, $m \in g(X) \notin RP(M_2)$, а значит, значение $c'(X)$ для секрета невозможно – опять получили противоречие.

Докажем достаточность. Пусть условия теоремы выполнены. Покажем, что секрет остается равномерно распределенным и при наличии частичных секретов из запрещенного подмножества. Рассмотрим произвольное запрещенное подмножество $A \notin \Gamma$ и множество многочленов $V = \{s^A(X) + f(X) \mid f(X) \in I^A, f(X) \in LP(M_2)\}$ — множество возможных значений промежуточного секрета. Зафиксируем некоторое значение секрета $c^j(X) \in RP(I_0)$. Тогда существует единственный многочлен $g^j(X) \in LP(I^A I_0)$, такой, что $g^j(X) \equiv s^A(X) \bmod I^A, g^j(X) \equiv c^j(X) \bmod I_0$ (согласно CRT).

Если $RT(I^A I_0) = M_2$, то каждому значению секрета соответствует единственный промежуточный секрет из множества V, т. е. секрет остается равномерно распределенным при наличии частичных секретов из подмножества A.

Пусть $RT(I^A I_0) \subset M_2$. Каждому многочлену $f(X) \in RP(M_2)$, содержащему хотя бы один моном из $M_2 \setminus RT(I^A I_0)$, поставим в соответствие многочлен $\overline{f}(X) = f(X) - f(X) \bmod (I^A I_0) \neq 0$. Очевидно, что $\overline{f}(X) \in I^A I_0$. Тогда каждому значению секрета $c^j(X) \in RP(I_0)$ соответствует множество промежуточных секретов $C^j = \{g^j(X), g^j(X) + \overline{f}(X) \mid \overline{f}(X) \in I^A I_0, \overline{f}(X) \in RP(M_2)\} \subset V$. Очевидно, что множе-

ства C^j равномощные. Следовательно, в множестве V для каждого значения секрета существует одинаковое число возможных значений промежуточного секрета, что влечет равномерное распределение секрета и при наличии частичных секретов из запрещенного подмножества.

Теорема доказана.

Далее рассматриваем структуры доступа, в которых отсутствуют взаимозаменяемые участники [7].

Теорема 2. Идеальной модулярной реализацией в кольце $\mathbb{F}_q[X]$ обладает только пороговая структура доступа.

Доказательство. Пусть есть совершенная и идеальная схема Асмута – Блума. Это значит, что выполнены условия теоремы 1 и, кроме того, $\deg I_i = \deg I_j = \deg I_0$, $\forall i, j$. Покажем, что $I_i + I_j = 1, \forall i \neq j$, откуда будет следовать, что структура доступа–пороговая, так как в этом случае $\deg I_i I_j = \deg I_i + \deg I_j$ и выполняется условие 2 теоремы 1.

Рассмотрим произвольное максимальное по включению запрещенное подмножество участников $A \in \overline{\Gamma}_{\max}$, т. е. $\forall i \notin A \Rightarrow A \cup \{i\} \in \Gamma$. Тогда, с одной стороны, $\deg \text{НОК}[I^A, I_i] \geq |M_2|$, так как $M_2 \subseteq RT(\text{НОК}[I^A, I_i])$. С другой стороны, $RT(I^A I_0) \subseteq M_2$, $\deg I^A + \deg I_0 \leq |M_2|$ и $\deg I_i = \deg I_0$, откуда следует, что $I^A + I_i = 1$, $RT(I^A I_i) = RT(I^A I_0) = M_2$. Таким образом, модуль участника, не входящего в максимальное запрещенное подмножество, взаимно прост с модулями участников из этого подмножества. Заметим также, что из-за отсутствия в структуре доступа взаимозаменяемых участников выполняется $\forall i, j \in J$, $\exists A \in \overline{\Gamma}_{\max} : i \in A, j \notin A$.

Теорема доказана.

Таким образом, мы получили критерий совершенности и охарактеризовали все идеальные модулярные схемы разделения секрета в кольце многочленов от нескольких переменных над полем Галуа. Эти результаты являются обобщением результатов, полученных в работе [7] для случая кольца многочленов от одной переменной.

ЛИТЕРАТУРА

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

2. *Blakley, G.* Safeguarding cryptographic keys / G. Blakley // Proc. AFIPS nat. comp. conf. New York, 1979. Vol. 48. P. 313–317.

3. *Mignotte, M.* How to share a secret / M. Mignotte // LNCS. 1982. Vol. 189. P. 371–375.

4. *Asmuth, C. A.* A modular approach to key safeguarding / C. A. Asmuth, J. Bloom // IEEE Trans. on inf. theory. 1983. Vol. 29. P. 156–169.

5. *Шенец, Н. Н.* Многомерное модулярное разделение информации / Н. Н. Шенец // Информатика. 2007. № 4(16). С. 125–132.

6. *Galibus, T.* Some structural and security properties of the modular secret sharing / T. Galibus, G. Matveev, N. Shenets // SYNASC'2008. IEEE Comp. Soc., CPS, Los~Alamitos, 2009. P. 197–200.

7. *Шенец, Н. Н.* Об информационном уровне модулярных схем разделения секрета / Н. Н. Шенец // Докл. Нац. акад. наук Беларуси. Сер. физ.-мат. наук. 2010. Т. 54, № 6. С. 9–12.

8. *Stinson, D. R.* Cryptography: theory and practice / D. R. Stinson. N.Y.: CRC Press, 2002. 512 p.

9. *Галибус, Т. В.* Комбинаторика нульмерных идеалов и модулярное разделение секрета / Т. В. Галибус, Г. В. Матвеев // 9 Междунар. науч. семинар «Дискретная математика и ее приложения». М. 2007. С. 424–426.