УДК 003.26:51:004(075.8)

Т.В. ГАЛИБУС

ИДЕАЛЫ СИММЕТРИЧЕСКИХ ОТНОШЕНИЙ И СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

We prove some properties of the ideals of symmetrical relations. These properties allow us to use such ideals for the secret sharing scheme generation. We construct the general secret sharing scheme, where the shares of the participants are the combined ideals of symmetrical relations. We study the security of the proposed scheme as well.

Модулярное разделение секрета основано на следующем простом наблюдении [1, 2]. Пусть $m_1 < m_2 < ... < m_l$ – система попарно взаимно простых натуральных модулей. Если секретом является некоторое натуральное число c, а секретом i-го участника, $i \in P = \{1,2, ..., l\}$, является наименьший неотрицательный вычет c по модулю m_i, т. е. $c_i \equiv c \pmod{m_i}$, то группа участников $A \subseteq P$ восстанавливает исходный секрет c путем решения системы сравнений $x \equiv c_i \pmod{m_i}$, $i \in A$. Это можно сделать, например, с помощью китайской теоремы об остатках. При этом правильно найдет секрет c лишь та группа участников A, для которой выполнено условие $c < \prod_{i \in A} m_i$. Тот же принцип используется при построении схемы разделения секрета над кольцом полиномов от одной [3–5] до нескольких переменных. В данной работе мы рассматриваем специальный класс идеалов в применении к модулярному разделению секрета.

Пусть F_q – конечное поле. Пусть f – сепарабельный полином степени n в кольце $F_q[x]$. Положим $\Omega = (\alpha_1, \alpha_2, ..., \alpha_n)$, где $\alpha_1, \alpha_2, ..., \alpha_n$ – корни полинома f в алгебраическом замыкании $\overline{F_q}$.

Обозначим через S_n симметрическую группу и определим ее действие на Ω следующим образом:

$$\forall \sigma \in \Sigma_n, \sigma.\Omega = (\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}).$$

Определение 1. Идеалом симметрических отношений многочлена f называется идеал $I \in F_q[x_1, x_2, ..., x_n]$, аннулирующий любую подстановку $\sigma.\Omega$ корней f:

$$I = \{p(x_1, x_2, ..., x_n) \mid p\left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, ..., \alpha_{\sigma(n)}\right) = 0, \forall \sigma \in S_n\}.$$

Эти идеалы обладают свойством эквипроективности [6], а их произведения – свойством триангулируемости, которое позволяет использовать их для построения совершенных модулярных реализаций общих структур доступа. Зафиксируем обратное лексикографическое мономиальное упорядочение $x_1 < x_2 < \ldots < x_n$ в кольце $F_q\left[x_1, x_2, ..., x_n\right]$.

Утверждение 1 (Обри – Валибуз [6]). Идеал симметрических отношений $I \in F_q[x_1, x_2, ..., x_n]$ обладает треугольным базисом Гребнера, т. е. базисом вида

$$\{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, x_2, \ldots, x_n)\},\ LT(f_i) = x_i^{d_i},$$

где $LT(f_i)$ обозначает старший член многочлена f_i. При этом $f_1(x_1) = f(x_1)$, $d_i = n - i + 1$, $i = \overline{1,n}$.

Многообразие такого идеала I обладает свойством эквипроективности.

Определение 2. Пусть $\pi_i(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_i)$. Многообразие $V \in \overline{F_q}^n$ называется эквипроективным, если для любой точки $M \in V_i = \pi_i(V)$, $i = 1,2, \ldots, n-1$, число прообразов $c_i(V) = |\pi^{-1}(M)|$ зависит лишь от i.

Утверждение 2 (Обри – Валибуз [6]). Идеал эквипроективного многообразия $V \in \overline{F_q}^n$ обладает треугольным базисом Гребнера $T = \{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, x_2, \ldots, x_n)\}$, причем $c_i(V) = d_{i+1}d_{i+2}\ldots d_n$, $i = 1, 2, \ldots, n-1$, где $\deg(f_i) = d_i$.

Утверждение 3. (Обри – Валибуз [6]). Многообразие идеала симметрических отношений эквипроективно и состоит из всех перестановок набора корней многочлена f и только их.

Далее, пусть $I_1, I_2, ..., I_k$ – набор идеалов симметрических отношений, соответствующий набору попарно взаимно простых сепарабельных многочленов $g_1, g_2, ..., g_k$, $\deg g_i = n$, $i = 1,2,\ldots,k$.

Теорема 1. *Произведение идеалов $I_1 I_2 \ldots I_k$ обладает треугольным базисом* $\{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, x_2, \ldots, x_n)\}$, *где* $f_1(x_1) = g_1(x_1) g_2(x_1) \ldots g_k(x_1)$, $d_i = n - i + 1$, $i = \overline{2,n}$.

Доказательство. Во-первых, заметим, что поскольку g_i попарно взаимно простые сепарабельные полиномы, то многообразия их идеалов симметрических отношений не имеют точек пересечения по всем компонентам (все корни всех многочленов попарно различны). Значит, $V(I_1, I_2, ..., I_k)$ содержит $kn!$ элементов, поскольку каждое многообразие содержит все подстановки n-вектора.

Легко видеть, что поскольку все многообразия $V(I_1)$, $V(I_2),\ldots,V(I_k)$ эквипроективны с одинаковыми параметрами c_i, то их объединение также эквипроективно с теми же параметрами. Из утверждения 2 следует, что $d_i = c_{i-1}(V(I))/c_i(V(I)) = n-i+1,\ \ i=\overline{2,n}.$

Нам осталось показать, что $f_1(x_1) = g_1(x_1)g_2(x_1)\ldots g_k(x_1)$. Это следует из утверждения 1 и попарной взаимной простоты многочленов $g_1(x_1), g_2(x_1),\ldots, g_k(x_1)$. В самом деле, любой многочлен $p(x_1) \in I_1 I_2 \ldots I_k$ кратен $f_1^{(i)}(x_1) = g_i(x_1),\ i=\overline{1,k}.$ Теорема доказана.

Покажем, что идеалы $I_1, I_2,\ldots,I_k$ можно использовать для построения общей структуры доступа. Напомним, что структурой доступа называется семейство подмножеств **Γ** множества участников $P = \{1,2,...,l\}$, обладающее свойством монотонности, т. е. $A \in \Gamma,\ A \subset B \subset P \Rightarrow B \in \Gamma$. Подмножества из семейства **Γ** называются разрешенными. Все остальные подмножества называются запрещенными. Они образуют структуру отказа $\mathbf{\Gamma}^*$.

В [3, 5] нами было показано, что любая структура доступа делает возможной модулярную реализацию в кольцах целых чисел и полиномов. Под модулярной реализацией произвольной структуры доступа мы понимаем систему данных $\left(S, \{s_i, m_i\}, i=\overline{1,l}\right)$, где S – секрет схемы, а $\{s_i, m_i\}$ – модули участников и соответствующие им частичные секреты такие, что лишь разрешенные множества участников смогут восстановить S, объединив свои частичные секреты. Следующая теорема показывает, что такая же реализация возможна в кольце $F_q[x_1, x_2, \ldots, x_n]$ в случае, если модулями участников являются специальные произведения идеалов симметрических отношений $I_1, I_2,\ldots,I_k$, соответствующих попарно взаимно простым сепарабельным полиномам одной степени $g_1, g_2, \ldots, g_k$, $\deg g_i = n$, $i = 1,2, \ldots, k$. Частичными секретами являются вычеты по соответствующим произведениям идеалов.

Теорема 2. *Произвольная структура доступа* **Γ** *обладает модулярной реализацией по Миньотту и по Асмусу – Блюму в кольце* $F_q[x_1, x_2, \ldots, x_n]$.

Доказательство. Рассмотрим случай реализации по Миньотту. Пусть $I_1, I_2,\ldots,I_k$ – набор идеалов симметрических отношений, соответствующих попарно взаимно простым сепарабельным полиномам одной степени $g_1, g_2, \ldots, g_k$, $\deg g_i = n$, $i = 1,2,\ldots,k$. Здесь k – число максимальных по включению запрещенных подмножеств. Если степень n достаточно велика, мы всегда можем выбрать любое количество сепарабельных полиномов данной степени в кольце $F_q[x]$, а значит, и соответствующих им идеалов. Из теоремы 1 следует, что все идеалы $I_1, I_2,\ldots,I_k$ обладают одной и той же степенью $n!$. Пусть все участники вначале обладают единичными идеалами. Рассмотрим некоторое максимальное по включению запрещенное подмножество B. Модули всех участников, не входящих в B, мы домножаем на I_1. Далее мы поступаем аналогичным образом со всеми оставшимися максимальными по включению запрещенными подмножествами.

После всех домножений произведение идеалов $I_1 I_2 \ldots I_k$ будет общим модулем всякого разрешенного подмножества участников. Для всякого же запрещенного хотя бы один множитель в аналогичном произведении отсутствует, т. е. модуль запрещенного подмножества является собственным делителем данного произведения, а значит, общим секретом участников такого подмножества является $I_{i_1} I_{i_2} \ldots I_{i_{k_1}}$, $k_1 < k$. Отметим, что всякое $RT\left(I_{i_1} I_{i_2} \ldots I_{i_{k_1}}\right) \subset RT(I_1 I_2 \ldots I_k)$ в силу того, что идеалы симметрических отношений являются нульмерными. Под $RT(I)$ мы понимаем множество приведенных мономов данного идеала.

В качестве секрета $S(x_1, x_2, \ldots, x_n)$ модулярной схемы Миньотта выбирается линейная комбинация мономов $S_B(x_1, x_2, \ldots, x_n) \in RT(I_1 I_2 \ldots I_k) \setminus RT\left(I_{i_1} I_{i_2} \ldots I_{i_{k_1}}\right)\ \forall B$ – максимального по включению запрещенного подмножества. По построению полином $S(x_1, x_2, \ldots, x_n)$ является приведенным по модулю $(I_1 I_2 \ldots I_k)$ и не приведенным по модулю всякого произведения запрещенного $(I_{i_1} I_{i_2} \ldots I_{i_{k_1}})$, где $k_1 < k$.

Частичные секреты участников $S_i(x_1, x_2, \ldots, x_n)$ вычисляются как остатки секрета $S(x_1, x_2, \ldots, x_n)$ по модулям соответствующих произведений идеалов m_i.

Для случая схемы Асмуса – Блюма модули участников строятся аналогичным образом, а секрет $S(x_1, x_2, \ldots, x_n)$ выбирается из множества $RP(P)$, где P – идеал симметрических отношений степени n с сепарабельным многочленом $g_0(x)$, $(g_0, g_i) = 1$, $i = 1,2, ..., k$. Под $RP(I)$ мы понимаем множество приведенных по модулю I полиномов, т. е. линейных комбинаций мономов из $RT(I)$.

Затем выбирается промежуточный секрет $Y(x_1, x_2, \ldots, x_n) \in RP(I_1 I_2 \ldots I_k)$. Для этого секрет $S(x_1, x_2, \ldots, x_n)$ дополняется произвольными полиномами из $P \cap RP(I_1 I_2 \ldots I_k)$. Таким образом, промежуточное значение секрета $Y(x_1, x_2, \ldots, x_n) = S(x_1, x_2, \ldots, x_n) + p(x_1, x_2, \ldots, x_n)$, где $p(x_1, x_2, \ldots, x_n)$ – полином из идеала P. Частичные секреты вычисляются как остатки $Y(x_1, x_2, \ldots, x_n)$ по модулям соответствующих идеалов.

Преимущество идеалов симметрических отношений заключается в том, что множества приведенных мономов произведения таких идеалов обладают свойством монотонного роста по включению. Это позволяет нам доказать следующую теорему о совершенности общей схемы разделения секрета с использованием идеалов симметрических отношений. Под совершенной модулярной реализацией мы понимаем такую схему, в которой каждому набору частичных секретов участников запрещенного подмножества B соответствует одинаковое количество возможных значений секрета $S(x_1, x_2, \ldots, x_n) \in RP(P)$. Это определение обобщает аналогичное определение, приведенное в [7].

Теорема 3. *Общая схема разделения секрета Асмуса – Блюма в кольце $F_q[x_1, x_2, \ldots, x_n]$ с модулями участников, построенными согласно теореме 2, является совершенной.*

Доказательство. В случае реализации по Асмусу – Блюму секрет $S(x_1, x_2, \ldots, x_n) \in RP(P)$.

Пусть B – запрещенное множество участников, $S(B)$ – их частичные секреты, а $I_1 I_2 ... I_{k_1}$, $k_1 < k$, – их общий модуль. Для доказательства теоремы нам необходимо показать, что количество полиномов в $S(B)$ не зависит от фиксированного значения полинома $S(x_1, x_2, \ldots, x_n)$.

Во-первых, отметим, что после объединения частичных секретов участники из B могут получить промежуточное значение $Y_B(x_1, x_2, \ldots, x_n) \in S(B)$, которое является приведенным по модулю $I_1 I_2 ... I_{k_1}$. Таким образом, любому $Y_B(x_1, x_2, \ldots, x_n)$ соответствует одинаковое количество возможных истинных значений $Y(x_1, x_2, \ldots, x_n)$:

$$Y(x_1, x_2, \ldots, x_n) \in \{Y_B(x_1, x_2, \ldots, x_n) + I_1 I_2 ... I_{k_1} \cap RP(I_1 I_2 ... I_k)\}.$$

Заметим, что $Y(x_1, x_2, \ldots, x_n)$ выбирается их множества $\{S(x_1, x_2, \ldots, x_n) + P \cap RP(I_1 I_2 \ldots I_k)\}$, мощность которого не зависит от выбранного полинома $S(x_1, x_2, \ldots, x_n)$ в силу того, что выполняется включение $RT(P) \subset RT(I_1 I_2 \ldots I_k)$.

Таким образом, для любого фиксированного значения секрета $S(x_1, x_2, \ldots, x_n)$ число полиномов в $S(B)$ есть $|P I_1 I_2 ... I_{k_1} \cap RP(I_1 I_2 ... I_k)|$. Мощность данного множества не зависит от выбора $S(x_1, x_2, \ldots, x_n)$ в силу того, что $RT(P I_1 I_2 ... I_{k_1}) \subseteq RT(I_1 I_2 ... I_k)$. Мы доказали совершенность схемы.

1. Mignotte M. // Advances in cryptology. Eurocrypt'82, LNCS. 1982. P. 371.
2. Asmuth C.A., Bloom J.A. // IEEE Transactions on Information Theory. 1983. Vol. 29. P. 156.
3. Galibus T., Matveev G. // ENTCS. 2007. Vol. 186.
4. Galibus T., Matveev G., Shenets N. // Proc. of SYNASC'08. Los Alamitos, 2009. P. 197.
5. Галибус Т.В. Разделение секрета над полиномиальными кольцами // Вестн. БГУ. Сер. 1. 2006. № 2. С. 97.
6. Aubry P., Valibouze A. // J. Symbolic Computation. 2000. Vol. 30. P. 635.
7. Quisquater M., Preneel B., Vandewalle J. // LNCS. 2002. Vol. 2274. P. 199.

Поступила в редакцию 17.03.11.

Татьяна Васильевна Галибус – соискатель кафедры методов математического моделирования и анализа данных. Научный руководитель – кандидат физико-математических наук, доцент кафедры высшей математики Г.В. Матвеев.