МОДУЛЯРНОЕ РАЗДЕЛЕНИЕ СЕКРЕТА И НУЛЬМЕРНЫЕ ИДЕАЛЫ

Т. В. Галибус

Минск, Беларусь
E-mail: tan2tan@gmail.com

В работе обобщена схема Асмуса – Блюма на случай кольца многочленов от нескольких переменных над полем Галуа. Описаны алгоритмы разделения и восстановления секрета. Доказана теорема об условии на нульмерные идеалы, пригодные для реализации пороговой схемы Асмуса – Блюма в данном кольце. Доказана теорема о количестве максимальных идеалов, пригодных для совершенной реализации пороговой схемы Асмуса – Блюма в данном кольце.

Ключевые слова: базис Гребнера, идеал, разделение секрета.

В кольце многочленов от нескольких переменных $F_q[x_1, \dots, x_n] = F_q[X]$ над полем Галуа имеются все предпосылки для определения модулярной схемы разделения секрета. В соответствии с теорией Бухбергера можно корректно определить приведение произвольного многочлена (секрета) $s(X)$ по модулю любого идеала. Для этой цели лучше всего подходят нульмерные идеалы, так как в этом случае фактор-кольцо $F_q[X]/I$ конечно, а значит, для оценки секретности применим предложен-

ный в работе [3]. Этой же причиной обусловлен и выбор поля F_q . Для восстановления секрета имеется аналог китайской теоремы об остатках.

Напомним, что в этом кольце остатки и сравнения берутся по модулю идеала, иными словами, $f(X) \equiv r(X) \pmod{I}$ означает, что f приводится к r по модулю идеала I , т. е. $f - r \in I$. Для того чтобы однозначно определить приведение многочлена по модулю идеала, достаточно выбрать некоторое мономиальное упорядочение. Результатом будет остаток от деления многочлена на соответствующий базис Гребнера [2]. Алгоритм Бухбергера позволяет отыскать базис Гребнера $G_I = (g_1, g_2, \dots, g_k)$ относительно данного мономиального упорядочения для всякого идеала I кольца $F_q[X]$. Поскольку всякий полином f приводится по модулю I с помощью базиса G_I единственным образом, то идеалы удобно задавать их базисами Гребнера [2].

Перейдем теперь к китайской теореме об остатках.

Теорема. Зафиксируем мономиальное упорядочение. Система сравнений

$$\begin{aligned} f(X) &\equiv s_1(X) \pmod{I_1}, \\ f(X) &\equiv s_2(X) \pmod{I_2}, \\ &\dots \\ f(X) &\equiv s_k(X) \pmod{I_k}, \end{aligned}$$

при попарно взаимно простых идеалах $I_1, I_2, \dots, I_k$ имеет единственное решение по модулю произведения $I_1 I_2 \dots I_k$ относительно данного мономиального упорядочения. Оно представимо в виде $F(X) \equiv \sum_{i=1}^k s_i(X) b_i(X) \pmod{I_1 I_2 \dots I_k}$,

$$\text{где } b_i(X) \equiv 1 \pmod{I_i}, b_i(X) \equiv 0 \pmod{I_j}, i \neq j.$$

Указанное решение можно построить, используя базисы Гребнера идеалов $I_1, I_2, \dots, I_k$. В самом деле, минимальный базис Гребнера суммы идеалов (I_i, I_j) содержит 1, а приведение объединенного базиса пары взаимно простых идеалов к 1 позволит нам указать такие $a_i \in I_i, a_j \in I_j$, что $a_i + a_j = 1$. Далее, $b_i(X) \equiv \prod_{j=1}^k a_j(X), i \neq j$.

Найденное решение $F(X)$ является единственным по модулю произведения всех идеалов $I_1, I_2, \dots, I_k$ относительно данного мономиального упорядочения, поэтому такой CRT-алгоритм можно использовать для модулярного восстановления секрета в кольце $F_q[X]$.

Зафиксируем некоторое мономиальное упорядочение в $F_q[X]$. Для построения обобщенной схемы Асмуса – Блюма [1] будем использовать попарно взаимно простые нульмерные идеалы $I_1, I_2, \dots, I_t$, одной и той же степени n . Понятие степени идеала обобщает понятие степени полинома. Она определяется как размерность фактор-кольца $F_q[X]/I$ как векторного пространства над полем F_q , т. е. $\deg I = \dim_{F_q} F_q[X]/I$. Секретом будем считать результат приведения $s(X)$ по дополнительному нульмерному идеалу P , такому, что $\deg P \leq n$. Предпороговое количество частичных секретов $s_i(X)$ участников схемы задается произвольно. Далее с

помощью CRT вычисляется промежуточное значение $Y(X)$, приведенное по модулю произведения k идеалов. Обозначим через $Y_A(X)$ результат приведения $Y(X)$ по модулю произведения идеалов $I_{i_1}, I_{i_2}, \dots, I_{i_l}$, соответствующих участникам из подмножества $A = \{i_1, i_2, \dots, i_l\}$. Для промежуточного секрета (k, t) -пороговой схемы должно выполняться условие $Y_A(X) = Y(X), |A| \geq k, Y_A(X) \neq Y(X), |A| < k$. При этом частичные секреты участников $s_i(X)$ являются вычетами промежуточного секрета $Y(X)$ наименьшей степени относительно данного мономиального упорядочения по модулю I_i .

Решая систему $Y(X) \equiv s_{i_j}(X) \pmod{I_{i_j}}, j = 1, 2, \dots, l$ с помощью CRT участники $i_1, i_2, \dots, i_l$ находят предполагаемое единственное приведенное значение секрета $Y(X)$ по модулю $I_{i_1}, I_{i_2}, \dots, I_{i_l}$. Значением секрета $s(X)$ является $Y(X) \pmod{P}$, т. е. результат приведения по модулю идеала P для данного мономиального упорядочения.

Найдем, какому условию должны удовлетворять попарно взаимно простые идеалы $I_1, I_2, \dots, I_t$, для того чтобы они подходили для реализации пороговой схемы Асмуса – Блюма. Мультистепенью $multi\ deg\ f$ полинома f назовем максимальный вектор степеней его мономов относительно выбранного упорядочения, а старшим членом $LT(f)$ назовем член, соответствующий моному с максимальной степенью. Обозначим через $r_i(X)$ многочлен наименьшей мультистепени относительно данного мономиального упорядочения в минимальном базисе Гребнера идеала I_i .

Теорема. Пусть нульмерные идеалы $I_1, I_2, \dots, I_t$, заданные базисами Гребнера $G(I_j), j = 1, 2, \dots, t$, таковы, что

- 1) полиномы $r_j(X), j = 1, 2, \dots, t$ попарно взаимно просты, а их мультистепени $\alpha_1(I_j)$ совпадают;
- 2) мультистепень любого другого элемента базиса Гребнера $G(I_j), j = 1, 2, \dots, t$, не равного $r_j(X)$, больше, чем $(k+1)\alpha_1$.

Тогда указанные идеалы пригодны для реализации любой (l, t) -пороговой структуры доступа, где $l \leq k$.

Для того чтобы построить совершенную схему, идеалы должны удовлетворять более сильному условию, чем равенство степеней, а именно, равенство наборов степеней базисных элементов при выбранном мономиальном упорядочении. Дадим строгое определение. Идеалы I_1, I_2 называются равноостаточными, если они обладают одним и тем же набором приведенных мономов: $RT(I_1) = RT(I_2)$. Такие идеалы позволяют пользователям схемы Асмуса – Блюма получить одно и то же количество информации о секрете, т. е. обеспечивают равноправие пользователей.

Пусть I – максимальный идеал. Зафиксируем обратное лексикографическое упорядочение $x_m > x_{m-1} > \dots > x_1$. Тогда старшие мономы базисных элементов $LT(g_k), k = 1, 2, \dots, m$ базиса Гребнера $G(I) = \{g_1, g_2, \dots, g_m\}$ являются мономами $x_1^{\beta_1} x_2^{\beta_2} \dots x_m^{\beta_m}$ соответственно [2]. Обозначим число максимальных равноостаточных идеалов с этим условием через $\bar{N}_q(\beta_1, \beta_2, \dots, \beta_m)$. Пусть также $N_q(n)$ обозначает число

неприводимых полиномов степени n в кольце полиномов одной переменной над полем F_q .

Теорема. $\overline{N}_q(\beta_1, \beta_2, \dots, \beta_m) = N_q(\beta_1)N_{q^{\beta_1}}(\beta_2) \dots N_{q^{\beta_1\beta_2 \dots \beta_{m-1}}}(\beta_m)$.

Доказательство. Пусть I – максимальный идеал. Тогда он задается единственным относительно обратного лексикографического мономиального упорядочения минимальным базисом Гребнера $G(I) = \{g_1, g_2, \dots, g_m\}$ с набором степеней базисных элементов $\beta_1, \beta_2, \dots, \beta_m$. Поэтому число таких идеалов равно числу соответствующих базисов Гребнера. Поскольку g_1 является неприводимым нормированным полиномом в $F_q[x_1]$ степени β_1 , то для его выбора имеется $N_q(\beta_1)$ возможностей. Далее, $g_2(x_1, x_2)$ является неприводимым полиномом по модулю $g_1(x_1)$. Так как его образ неприводим при каноническом эпиморфизме $F_q[x_1, x_2] \rightarrow F_q[x_1, x_2] / \langle g_1(x_1) \rangle$, то возможностей выбора для этого элемента $N_{q^{\beta_1}}(\beta_2)$ и т. д. Таким образом, имеется в точности $N_{q^{\beta_1\beta_2 \dots \beta_{i-1}}}(\beta_i)$ возможностей выбрать полином g_i в базисе $G(I) = \{g_1, g_2, \dots, g_m\}$.

Максимальными равноостаточными идеалами являются, например, идеалы симметрических отношений. Для данных идеалов мы уже построили совершенную реализацию произвольной структуры доступа [4].

ЛИТЕРАТУРА

1. *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.
2. *Becker, T.* Grebner bases. A Computational Approach to Commutative Algebra / T. Becker, V. Weispfenning. Springer-Verlag, 1993. 575 p.
3. *Quisquater, M.* On the security of the threshold scheme based on the Chinese remainder theorem / M. Quisquater, B. Preneel, J. Wandervalle // LNCS. 2002. Vol. 2274. P. 199–210.
4. *Галибус, Т. В.* Идеалы симметрических отношений и разделение секрета / Т. В. Галибус // Вест. Белорус. гос. ун-та. Сер. 1. Физика. Математика. Информатика. 2011. № 2. С. 141–143.