КОМБИНАТОРИКА НУЛЬМЕРНЫХ ИДЕАЛОВ И МОДУЛЯРНОЕ РАЗДЕЛЕНИЕ СЕКРЕТА

Т. В. Галибус, Г. В. Матвеев (Минск)

Первоначально модулярное разделение секрета изучалось лишь в кольце целых чисел [1, 2]. При таком подходе секретом считается натуральное число s, а секретом i-го участника — натуральный модуль m_i и наименьший неотрицательный вычет s по этому модулю $s = s_i(\mathrm{mod} m_i)$. Группа участников A пытается восстановить секрет, решая систему сравнений $x \equiv s_i(\mathrm{mod} m_i), i \in A$.

Этот подход выдвинул несколько задач комбинаторного характера, касающихся построения модулей m_i и секрета s. Некоторые из них проще решаются в кольце полиномов $F_q[x]$ над полем Галуа [3, 4]. Сейчас мы предлагаем обобщение модулярного подхода на случай кольца полиномов от нескольких переменных $F_q[X]$, где $X = (x_1, x_2, .., x_m)$. В этом кольце есть все необходимое для модулярного разделения секрета. В качестве секрета берется полином $S(X) \in F_q[X]$, а в качестве модуля участника — нульмерный идеал I. В этом случае корректно определен вычет секрета по модулю идеала $S(X)(\mathrm{mod} I)$, при условии, что задано мономиальное упорядочение, а для восстановления секрета имеется CRT-алгоритм [5].

Будем говорить, что на множестве участников $\mathcal{P} = \{1, 2, ..., t\}$ задана структура доступа, если указано семейство Γ разрешенных подмножеств. Все остальные подмножества называются запрещенными. Предполагается выполненным условие монотонности $A \in \Gamma, A \subset A' \Rightarrow A' \in \Gamma$. Пусть I — нульмерный идеал в кольце $F_q[X]$. Назовем его степенью размерность фактор-кольца как векторного пространства над полем F_q, т.е. $\deg I = \dim_{F_q} F_q[X]/I$. Укажем несколько свойств нульмерных идеалов, аналогичных свойствам неприводимых полиномов, которые затем применяются для построения модулярных реализаций структур доступа. Первые два из них скорее всего известны, но мы не нашли ссылку.

Теорема 1. *Пусть I_1, I_2 — нульмерны и взаимно просты. Тогда* $\deg I_1 I_2 = \deg I_1 + \deg I_2$.

Доказательство следует из известного варианта CRT: $R/I_1 I_2 \cong R/I_1 \oplus R/I_2$.

Обозначим через $N_q(n)$ число нормированных неприводимых полиномов степени n в кольце $F_q[x]$, а через $\overline{N}_q(n)$ — число максимальных идеалов степени n в кольце $F_q[X]$.

Теорема 2. $\overline{N}_q(n) = N_{q^n}(n)$.

Доказательство. В классическом случае формула для $N_q(n)$ выводится из того, что $q^n = \deg\prod_{\deg f|n} f(x)$, где произведение распространено на все неприводимые полиномы $f(x), \deg(f(x))|n$. Применяя теорему 1, можно показать, что $\deg\prod_{\deg I|n} I = q^{mn}$, а затем применить обращение Мебиуса.

Обозначим через $C_q(n)$ максимальное число попарно взаимно простых радикальных идеалов степени n в кольце $F_q[X]$.

Теорема 3. $\overline{C}_q(n) = \sum_{l\leq\frac{n}{2}} N_{q^n}(l) + N_{q^m}(n)$, *при нечетном* n.

$\overline{C}_q(m) = \sum_{l\leq\frac{m-2}{2}} N_{q^m}(l) + [\frac{1}{2}N_{q^m}(\frac{n}{2})] + N_{q^m}(n)$, *при четном* n.

В случае $m = 1$ это утверждение доказано нами в работах [3, 4]. В общем случае, рассуждения легко обобщаются. Надо только воспользоваться тем, что для радикального идеала примарные компоненты являются максимальными идеалами.

Перейдем сейчас к модулярной реализации схемы доступа на множестве участников P. Напомним, что для модулярной реализации по Миньотту необходимо чтобы модули участников $P_1, P_2, ..., P_t$ и секрет $S(X) \in F_q[X]$ были такими, чтобы выполнялось условие:

$$S(X) = S(X)(\mathrm{mod}\bigcap_{i\in A} P_i), A \in \Gamma; S(X) \neq S(X)(\mathrm{mod}\bigcap_{i\in A} P_i), A \notin \Gamma,$$

где правая часть — результат приведения секрета $S(X)$ по указанному идеалу. Другими словами, секрет $S(X)$ должен быть приведен по модулю произведения для всех разрешенных подмножеств и не является таковым для запрещенных. Напомним, что для всякого идеала $I \in F_q[X]$ приведенными являются лишь линейные комбинации приведенных мономов из $RT(I)$ [5].

Имеется еще модулярная реализация и в смысле Асмуса—Блюма, отличающаяся тем, что секрет приводится по дополнительному модулю [1].

Теорема 4. *Любая схема доступа* Γ *имеет модулярные реализации в любом кольце* $F_q[X]$ *по Миньотту и Асмусу — Блюму.*

Доказательство. Рассмотрим случай реализации по Миньотту. Выберем сначала попарно взаимно простые нульмерные идеалы $P_1, P_2, ..., P_l$, где l — число максимальных по включению запрещенных подмножеств. По теореме 3 это возможно в любом кольце $F_q[X]$. Более того, можно считать, что все идеалы $P_1, P_2, .., P_l$ — одной степени. Первоначально присвоим каждому участнику единичный идеал. Берем затем какое-нибудь максимальное по включению запрещенное множество B и модули всех участников, не входящих в B, умножаем на идеал P_1. Поступаем так с каждым максимальным запрещенным подмножеством. В результате всех умножений имеем следующее.

Для всякого разрешенного множества участников A пересечение (произведение) всех их модулей (идеалов) будет равно произведению $P_1P_2..P_l$, а для всякого запрещенного B соответствующее пересечение будет собственным делителем этого произведения. С точностью до нумерации, можно сказать, что $\bigcap_{i\in B} P_i = P_1P_2...P_{l_1}$, где $l_1 < l$. Следовательно, $RT(P_1P_2...P_{l_1}) \subset RT(P_1P_2...P_l)$.

Для каждого максимального запрещенного множества B выберем по одному моному $S_B(X)$ из $RT(P_1P_2...P_l)\backslash RT(P_1P_2...P_{l_1})$, а в качестве самого секрета возьмем линейную комбинацию мономов $S_B(X)$. Таким образом, полином $S(X)$ будет приведенным по $\mathrm{mod}(\bigcap_{i\in A} P_i)$ и неприведенным по $\mathrm{mod}(\bigcap_{i\in B} P_i)$. Один из мономов $S_B(X)$ может подходить для нескольких запрещенных множеств B. Поэтому общее число мономов секрета $S(X)$ не превосходит l.

Замечание. Теоремы 1–3 отчасти объясняют, почему мы используем лишь нульмерные идеалы.

Список литературы

1. Asmuth C. A., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. — 1983. — V. 29. — P. 156–169.

2. Mignotte M. How to share a secret // Lecture Notes in Computer Science. — 1983. — V. 149. — P. 371–375.

3. Galibus T., Matveev G. Generalized mignotte sequences in polynomial rings // Electronic Notes on Theoretical Computer Science. — 2007. — V. 186. — (To appear).

4. Galibus T., Matveev G. Mignotte sequences in polynomial rings // Proc. of ICS 2006, International Workshop on Information and Computer Security (Timisoara, Romania). — 2006. — P. 39–44.

5. Becker T., Weispfenning V. Gröbner Bases // A computational approach to commutative algebra. — Springer-Verlag, 1993.