$\delta(G)\geq 7.$

Λ

$c\in C_2,\ C_2\in\Lambda$

$a\geq 7$ $|C_1|\geq 6$

$|C_2|\geq 6.$

УДК 003.26:51:004(075.8)

Т.В. ГАЛИБУС

РАЗДЕЛЕНИЕ СЕКРЕТА НАД ПОЛИНОМИАЛЬНЫМИ КОЛЬЦАМИ

Some new results on the modular key safeguarding over polynomial rings are obtained.

Асмус и Блюм [1] показали, что любую пороговую схему разделения секрета можно реализовать модулярно над кольцом целых чисел. Их подход основан на следующем простом наблюдении. Пусть $m_1<m_2< \ldots <m_t$ - система попарно взаимно простых модулей с условием $M_2=m_1m_2 \ldots m_k > m_{t-k+1}m_{t-k+2} \ldots m_t=M_1$, где $1\leq k\leq t$ [2].

Если теперь секрет *c* взять из промежутка (M_1, M_2), а *i*-частичным секретом считать его наименьший неотрицательный вычет по mod m_i, т. е. $c_i \equiv c \pmod{m_i}$ и сам модуль *ТПИ,* то восстановление секрета с может осуществить любая группа участников, если их не меньше *к.* Это можно сделать, решив соответствующую систему уравнений. Например, для первых *к* участников эта система принимает вид

$$x \equiv c_1 \pmod{m_1},\ x \equiv c_2 \pmod{m_2},\ \ldots,\ x \equiv c_k \pmod{m_k}.$$

Такой подход имеет ряд недостатков, связанных со структурой самого кольца $\mathbb{Z}$. Например, участники заведомо обладают неодинаковой априорной информацией о секрете с, так как их модули попарно различны. Не вполне ясно и как построить оптимальную систему модулей $m_1, m_2, \ldots, m$, хотя некоторые подходы к решению второй задачи намечены Асмусом, Блюмом и в работе [3].

Покажем, что переход от кольца $\mathbb{Z}$ к кольцу многочленов над конечным полем $F_q[x]$ оправдан и в ряде случаев позволяет избавиться от указанных недостатков, а также, что любая, не только пороговая, схема доступа может быть реализована модулярно.

Напомним, что семейство подмножеств Г произвольного множества участников *P* называется структурой доступа, если обладает свойством монотонности, т. е.

$$A \in \Gamma,\ A \subset B \subset P \Rightarrow B \in \Gamma.$$

Реализацией структуры доступа, или схемой разделения секрета, называется такой алгоритм, который позволяет вычислить некоторый секрет лишь группам участников, образующим подмножество из множества Г. Пороговая схема - лишь частный случай этого понятия.

В дальнейшем существенным является то, что в кольце $F_q[x]$, как и в кольце $\mathbb{Z}$, справедлива китайская теорема об остатках, а также следующее простое утверждение: система сравнений

$$x \equiv c_1 \pmod{m_1},\ x \equiv c_2 \pmod{m_2},\ \ldots,\ x \equiv c_k \pmod{m_k}$$

над кольцом $F_q[x]$, где F_q - конечное поле, в случае разрешимости имеет единственное решение по модулю НОК(оті(х), $m_2(x), \ldots, m_l(x)$), если под решением понимать вычет наименьшей степени.

Заметим попутно, что при произвольно выбранных модулях $m_1(x), m_2(x), \ldots, m_l(x)$ и произв$c(x) \in F_q[x]$ получается некоторая схема разделения секрета (не обязательно пороговая), если частичными секретами считать остатки от деления $c(x)$ на модули $m_1(x), m_2(x), \ldots, m_l(x)$. При этом некоторое подмножество будет разрешенным, если степень НОК соответствующих модулей будет больше deg $c(x)$. Тогда схемы доступа будем называть модулярными.

Теорема 1. Произвольная схема доступа может быть реализована модулярно над кольцом многочленов $F_q[x]$

Доказательство. Сначала произвольно выберем модули $m_1(x), m_2(x), \ldots, m_l(x)$, например, $m_1(x) = m_2(x) = \ldots = m_l(x) = 1$. Затем возьмем какое-нибудь максимальное по включению запрещенное подмножество $A \notin \Gamma$. Все модули, не входящие в *А,* домножим на некоторый неприводимый многочлен $p_1(x) \in F_q[x]$. Поскольку неприводимый многочлен может иметь любую наперед заданную степень, то таким домножением можно добиться выполнения условия: степень НОК многочленов из множества *А* меньше степени НОК многочленов из любого разрешенного. Это условие не будет нарушено и в дальнейшем, если будет взят другой неприводимый многочлен $p_2(x) \neq p_1(x)$ и другое максимальное по включению запрещенное подмножество. Всего домножений потребуется не более числа всех максимальных запрещенных подмножеств.

Секрет $c(x)$ можно взять так, чтобы выполнялось условие $M_1<\deg c(x)<M_2$, где M_1 - максимальная степень, а M_2 - минимальная степень НОК разрешенных подмножеств.

Заметим, что в ряде случаев использование неприводимых многочленов не вполне оправдано, так как семейство попарно взаимно простых многочленов потенциально может привести к реализации той же схемы, но с меньшими степенями. В самом деле, пусть $m_1(x), m_2(x), \ldots, m_l(x)$ - семейство попарно взаимно простых многочленов одинаковой степени n. Тогда, как нетрудно видеть, путем подбора секрета c его можно использовать для реализации любой (k, t)-пороговой схемы, $t \geq k$.

Поэтому попытаемся оценить максимальное число попарно взаимно простых нормированных многочленов степени n в кольце $F_q[x]$. Сюда в первую очередь следует отнести неприводимые, число которых находим по известной формуле [4]

$$N_q = \frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}.$$

Таким образом, остается лишь вычислить количество неприводимых попарно взаимно простых многочленов степени n. Нас в первую очередь интересуют максимальные по числу элементов, а не по включению семейства многочленов с этим условием. Обозначим их число через $C_q(n)$.

Теорема 2. $C_q(n) = \sum_{i=1}^{\frac{n-1}{2}} N_q(i)$ при нечетном n, а при четном n

$$C_q(n) = C_q(n-1) + \left[\frac{1}{2}N_q\left(\frac{n}{2}\right)\right].$$

Доказательство. Рассмотрим случай нечетного n, для четного n доказательство будет аналогичным. Каждый многочлен указанного семейства содержит делитель, степень которого не выше $\left[\frac{n}{2}\right]$. Поэтому $C_q(n)$ не превышает указанной суммы. Возьмем теперь приводимый нормированный многочлен из нашего семейства $f_1(x)f_2(x)$. Поскольку $\deg f_1(x)f_2(x)=n$, $\deg f_1(x)=l<\left[\frac{n}{2}\right]$, то $\deg f_2(x)=n-l$. Это означает, что для существования дополнительного многочлена $f_2(x)$ достаточно выполнения условия $N_q(l) \leq N_q(n-l)$ и что в этом случае указанная верхняя граница достижима. На самом деле верно более сильное утверждение.

Теорема 3. Функция $N_q(n)$ является строго возрастающей по n кроме случаев q=2, 3, когда она строго возрастает начиная с n=2.

Доказательство. Будем исходить из двух очевидных неравенств:

$$N_q(n) \geq \frac{1}{n}\left(q^n - \frac{q^n - q}{q-1}\right); \quad N_q(n) \leq \frac{1}{n}\left(q^n + \frac{q^n - q}{q-1}\right).$$

Тогда

$$N_q(n+1) - N_q(n) \geq \frac{1}{n(n+1)(q-1)}\left(q^{n+1}(nq - 3n - 1) + (2n+1)q\right) > 0$$

для всякого $q>3$, так как $nq \geq 3n+1$.

Для рассмотрения оставшихся случаев используем более точные оценки:

$$N_q(n) \geq \frac{1}{n}\left(q^n - \frac{q^{\left[\frac{n}{2}\right]+1} - q}{q-1}\right);\ N_q(n) \leq \frac{1}{n}\left(q^n + \frac{q^{\left[\frac{n}{2}\right]+1} - q}{q-1}\right).$$

Если $q=2$, то

$$N_2(n+1) - N_2(n) \geq \frac{1}{n(n+1)}\left((n-1)2^n - n2^{\left[\frac{n+1}{2}\right]+1} - (n+1)2^{\left[\frac{n}{2}\right]+1} + 2n + 2\right) > 0$$

начиная с $n=5$. Для $n<5$ неравенство не выполняется только для $n=1$.

Случай $q=3$ рассматривается аналогично.

В заключение отметим, что одним из основных параметров схемы разделения секрета является ее информационный уровень, который определяется как частное от деления длины секрета на максимальную длину частичного секрета в битах.

Теорема 4. Уровень информации СРС полиномиального типа в кольце $F_2[x]$ для любой структуры доступа превосходит 1/2.

Доказательство. Как и ранее, считаем степени попарно взаимно простых многочленов, используемых при построении модулярной СРС, равными n. Тогда наибольшая степень НОК многочленов, соответствующих запрещенному подмножеству участников, есть kn, где k - количество различных попарно взаимно простых многочленов, на которые домножались модули участников данного запрещенного подмножества. Следовательно, секрет выбирается из множества двоичных векторов, соответствующих промежутку $[2^{kn}, 2^{(k+1)n}]$. Частичные секреты участников - это пары многочленов степени не выше nk. Оценим отношение мощности множества секретов и множества частичных ключей:

$$\rho = \frac{\log_2(2^{kn+n} - 2^{kn})}{\log_2(2^{2kn})} > \frac{\log_2(2^{kn}2^{n-1})}{2kn} = \frac{kn+n-1}{2kn} = \frac{1}{2} + \frac{n-1}{kn} > \frac{1}{2}.$$

1. Asmuth C.A., Bloom J. // IEEE Transactions on information theory. 1983. Vol. 29. P. 156.

2. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. Мн., 2003.

3. Кошур Н.Н., Матвеев Г.В. // Вопросы информационной безопасности: Сб. науч. тр. НАН Беларуси. Мн., 2002. Вып. 1. С. 85.

4. Лидл Р., Нидеррайтер Г. Конечные поля: в 2 т. М., 1988.

Поступила в редакцию 27.06.05.

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

v^k, $k<\infty$, $\{x=(x_1, \ldots, x_m) |$ $k\}$

$m \geq (2k+1)$