УДК 004.056.53 (*003.26*)

Н.Н. ШЕНЕЦ

МОДУЛЯРНОЕ РАЗДЕЛЕНИЕ СЕКРЕТА И СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

The modular secret sharing scheme with consecutive moduli is constructed. The homomorphic property of modular scheme is proved. The electronic voting scheme based on perfect and ideal modular scheme is constructed.

Основы теории разделения секрета были заложены в 1979 г. в работах Д. Блейкли [1] и А. Шамира [2]. Они предложили первые решения основной задачи, которая заключается в следующем: среди группы лиц необходимо так распределить некоторый важный *секрет*, чтобы лишь заранее определенные подмножества, объединив свои *частичные секреты*, смогли восстановить истинное значение секрета. Эти подмножества участников называются *разрешенными*, а все вместе они образуют *структуру доступа*.

Роль новой теории в последующие годы неуклонно возрастала, поскольку появилось несколько важных приложений. Так, например, Дж. Беналоу [3] предложил использовать разделение секрета в системах электронного голосования. При этом голосующий может сохранить свое мнение в тайне, высказывая его в «разделенном» виде.

В настоящее время предложено несколько способов решения основной задачи. Одним из них является *модулярный подход*, предложенный К. Асмусом, Дж. Блюмом [4] и М. Миньоттом [5]. Он основан на решении системы сравнений в кольце целых чисел. Пусть $I = \{1, 2, ..., t\}$ – множество участников, а число c – секрет. Дадим каждому участнику $i \in I$ натуральный модуль m_i и число $s_i = c (\mathrm{mod}\, m_i)$ – наименьший неотрицательный вычет секрета c по модулю m_i, которое называется *частичным секретом* участника. Тогда любая группа участников $A \subseteq I$ может попытаться найти значение c, решая соответствующую систему сравнений. Однако правильно найдут секрет лишь те группы участников A, для которых выполнено условие $c < \mathrm{НОК}[m_i, i \in A]$. К. Асмус и Дж. Блюм предложили приводить секрет c по дополнительному модулю m_0, что позволяет приблизить его размер к размерам частичных секретов. В дальнейшем модулярный подход был развит в работах [6, 7]. Он был обобщен на случай кольца полиномов $\mathbb{F}_q[x]$ над полем Галуа $\mathbb{F}_q$. Было показано, что для любой структуры доступа существует модулярная реализация в кольцах целых чисел и полиномов над полями Галуа.

Имеются также критерии оценки качества схем разделения секрета (СРС): *совершенность* и *идеальность* [8]. В [6] построена идеальная модулярная пороговая схема разделения секрета, а в [7] получен критерий совершенности модулярных схем в кольце полиномов от одной переменной над полем Галуа. Отметим, что в кольце целых чисел возможна лишь асимптотическая совершенность и асимптотическая идеальность модулярных СРС [9].

Целью данной работы является построение новых алгоритмов разделения секрета для пороговой структуры доступа в кольце целых чисел, а также разработка протокола электронного голосования с использованием идеальной модулярной пороговой схемы.

1. Пороговые схемы с последовательными модулями в кольце целых чисел. Пусть a, a+1,…, a+t–1 – последовательные натуральные числа. Для построения модулярной (k, t)-пороговой модулярной СРС необходимо, чтобы эти числа удовлетворяли условию

$$\max_{i_1,\ldots,i_{k-1}} \mathrm{НОК}(a+i_1,\ldots,a+i_{k-1}) < \min_{j_1,\ldots,j_k} \mathrm{НОК}(a+j_1,\ldots,a+j_k). \qquad (1)$$

Лемма 1. *Пусть* $a, a+1, \ldots, a+t-1$ *– последовательные натуральные числа и пусть* $a+i_1, a+i_2, \ldots, a+i_s$ *– некоторые* $s < t$ *из этих чисел. Тогда справедливо неравенство*

$$(a+i_1)(a+i_2)\cdot\ldots\cdot(a+i_s) \le (t-1)^{s(s-1)/2}\,\mathrm{НОК}(a+i_1, a+i_2, \ldots, a+i_s). \qquad (2)$$

Доказательство. Рассмотрим цепочку неравенств:

$$\mathrm{НОК}(a+i_1,\ldots,a+i_s) = \frac{(a+i_1)\cdot\mathrm{НОК}(a+i_2,\ldots,a+i_s)}{\mathrm{НОД}(a+i_1, \mathrm{НОК}(a+i_2,\ldots,a+i_s))} \ge \frac{(a+i_1)\cdot\mathrm{НОК}(a+i_2,\ldots,a+i_s)}{\mathrm{НОД}(a+i_1, \prod_{j=2}^{s}(a+i_j))} \ge$$

$$\ge \frac{(a+i_1)\cdot\mathrm{НОК}(a+i_2,\ldots,a+i_s)}{\prod_{j=2}^{s}\mathrm{НОД}(a+i_1,(a+i_j))} \ge \frac{(a+i_1)\cdot\mathrm{НОК}(a+i_2,\ldots,a+i_s)}{(t-1)^{s-1}} \ge \ldots \ge \frac{\prod_{j=1}^{s}(a+i_j)}{(t-1)^{s(s-1)/2}}.$$

Таким образом, лемма доказана.

Теперь найдем, при каких a выполняется неравенство (1).

Теорема. *Для того чтобы выполнялось неравенство* (1)*, достаточно число a выбрать из условия*

$$a \geq e \cdot (t-1)^{k(k-1)/2}. \tag{3}$$

Доказательство. Используя лемму 1 и очевидное неравенство

$$\text{НОК}(a+i_1,\ldots,a+i_s) \leq (a+i_1)\cdots(a+i_s),$$

усилим условие (2) и потребуем выполнения следующего неравенства:

$$(a)\cdots(a+k-1) \geq (t-1)^{k(k-1)/2}(a+t-1)\cdots(a+t-k). \tag{4}$$

Тогда очевидно, что $a > (t-1)^{k(k-1)/2}$. Положим $a = \alpha \cdot (t-1)^{k(k-1)/2}$. Рассмотрим цепочку очевидных неравенств:

$$\frac{(a+t-1)\cdots(a+t-k)}{(a+1)\cdots(a+k-1)} \leq \left(\frac{a+t-1}{a}\right)^{k-1} = \left(1+\frac{1}{\alpha(t-1)^{k(k-1)/2-1}}\right)^{k-1} \leq \left(1+\frac{1}{k-1}\right)^{k-1} < e.$$

Таким образом, для всех $\alpha \geq e$ неравенство (4) выполняется, а следовательно, верно и неравенство (1).

Теперь покажем, что если неравенство (4) верно для некоторого a, то оно верно и для a+1. Обозначим

$$X(a) = a(a+1)\cdots(a+k-1),\ \ Y(a) = (t-1)^{k(k-1)/2}(a+t-1)(a+t-2)\cdots(a+t-k).$$

Рассмотрим отношение

$$\frac{X(a+1)}{Y(a+1)} = \frac{X(a)}{Y(a)} \cdot \left(\frac{(a+k)\cdot(a+t-k)}{a\cdot(a+t)}\right) = \frac{X(a)}{Y(a)}\left(1+\frac{k(t-k)}{a(a+t)}\right) \geq \frac{X(a)}{Y(a)} > 1.$$

Теорема доказана.

Таким образом, найдено условие, при котором можно построить схему Миньотта на последовательных модулях.

2. Системы электронного голосования на основе схем разделения секрета. Схемы электронного голосования (СЭГ) впервые были предложены Чаумом [9] в 1981 г. В последнее время проводятся многочисленные исследования в этой области. Во многих странах уже приняты открытые стандарты электронного голосования. На многих международных научных конференциях данной тематике посвящены целые секции.

Мы рассмотрим лишь голосование **да/нет**, однако отметим, что представленные методы легко распространить на случай параллельных выборов или случай большого количества выбора в голосовании.

Наиболее важными критериями качества схемы электронного голосования являются следующие:

1. *Корректность* – результат голосования, вычисленный согласно алгоритму, лежащему в основе схемы электронного голосования, должен совпадать с истинным результатом голосования.

2. *Приватность* гарантирует, что никакое подмножество избирателей или доверительных лиц не может связать голос избирателя с ним самим.

3. *Доступность* – любой заранее определенный участник схемы обладает правом голоса.

2.1 СЭГ, основанные на гомоморфных схемах разделения секрета. Впервые определение гомоморфной схемы разделения секрета ввел Беналоу [3]. Интуитивно в такой схеме композиции частичных секретов являются частичными секретами композиции секретов. Дадим формальное определение.

Пусть S – множество значений секрета и пусть $S_1,\ldots,S_t$ – множества значений частичых секретов участников. Рассмотрим некоторые бинарные операции $\odot$ и $\otimes_1,\ldots,\otimes_t$ над этими множествами. Обозначим через Recover $(s_1,s_2,\ldots,s_t)$ функцию восстановления секрета, а через $\text{Share}(c,\Gamma)$ – функцию его разделения, Γ – заданная структура доступа. Говорят, что схема разделения секрета, реализующая структуру доступа Γ, является $(\odot,\otimes_1,\ldots,\otimes_t)$-**гомоморфной**, если для любых двух секретов $c_1,c_2 \in S$ справедливо

$$c_1 \odot c_2 = \text{Recover}(s_1^1 \otimes_1 s_1^2, s_2^1 \otimes_2 s_2^2, \ldots, s_t^1 \otimes_t s_t^2), \tag{5}$$

где $(s_1^1,s_2^1,\ldots,s_t^1) = \text{Share}(c_1,\Gamma)$, а $(s_1^2,s_2^2,\ldots,s_t^2) = \text{Share}(c_2,\Gamma)$.

В случае если $S_1 = S_2 = \ldots = S_t = S_{\text{shares}}$ и $\otimes_1 = \ldots = \otimes_t = \otimes$, $(\odot, \otimes_1, \ldots, \otimes_t)$-гомоморфная схема разделения секрета называется $(\odot, \otimes)$-гомоморфной.

Это свойство схем разделения секрета позволяет использовать их в процессе построения схемы электронного голосования. Докажем, что модулярная схема обладает свойством гомоморфности.

Лемма 2. *Схема разделения секрета Асмус – Блюма с попарно взаимно простыми модулями одной степени в кольце полиномов от одной переменной над полем Галуа* $\mathbb{F}_q$ *обладает свойством* $(+,+)$*-гомоморфности.*

Доказательство. Напомним, что в схеме Асмуса – Блюма секрет вычисляется согласно китайской теореме об остатках:

$$c_1(x) = C_1(x) (\mathrm{mod}\, m_0(x)),$$
$$c_2(x) = C_2(x) (\mathrm{mod}\, m_0(x)).$$

Здесь C_1, C_2 – промежуточные секреты, соответствующие секретам c_1 и c_2. По свойствам сравнений

$$c_1(x) + c_2(x) = C_1(x) + C_2(x) (\mathrm{mod}\, m_0(x)).$$

Далее, сумма $C_1(x) + C_2(x)$ аналогичным образом соответствует суммам частичных секретов $s_i^1(x) + s_i^2(x)$. При этом важно, что попарно взаимно простые модули схемы разделения секрета остаются прежними. Это является необходимым условием гомоморфности. Лемма доказана.

Пусть голосующие в схеме электронного голосования обозначены через $V_1, \ldots, V_m$, выборные представители – через $A_1, \ldots, A_t$. В данных СЭГ есть еще главное доверительное лицо A, задача которого заключается в подведении итогов голосования. Значения v_{yes} и v_{no} присваиваются голосам **да** и **нет** соответственно. Исходя из модели схемы электронного голосования по Беналоу [3], процесс голосования включает следующие этапы:

1. Каждый голосующий участник схемы разделяет свой голос (секрет) на составляющие (частичные секреты) по соответствующей ему схеме разделения секрета со свойством $(+,+)$-гомоморфности и посылает частичные секреты выборным представителям.

2. Выборные представители складывают полученные ими голоса. По свойству $(+,+)$-гомоморфности суммы голосов являются частичными секретами соответствующего итога выборов, а, значит, сумма голосов может быть посчитана без нарушения приватности схемы.

3. Главное доверительное лицо вычисляет конечный итог голосования, используя набор частичных сумм голосов, переданный ему выборными представителями.

2.2. СЭГ на основе модулярной схемы разделения секрета. Дадим формальное описание процесса электронного голосования с использованием полиномиального модулярного разделения секрета. Прежде всего отметим, что в данном кольце мы можем указать способ реализации любой пороговой структуры доступа для t участников, задав для нее некую полиномиальную последовательность Миньотта $(m_1(x), \ldots, m_t(x))$ или Асмуса – Блюма $(m_0(x), m_1(x), \ldots, m_t(x))$. Пусть в схеме участвуют голосующие $V_1, \ldots, V_m$, выборные представители $A_1, \ldots, A_t$ и главное доверительное лицо A.

Предварительные действия

1. Главное доверительное лицо A выбирает некоторую авторизованную (k,t)-пороговую структуру доступа Γ для выборных представителей, генерирует и публикует последовательность Асмуса – Блюма $(m_0(x), m_1(x), \ldots, m_t(x))$ попарно взаимно простых модулей одной и той же степени n.

2. Главное доверительное лицо A публикует значения v_{yes} и v_{no}, где $v_{\text{yes}}, v_{\text{no}} \in \mathbb{F}_q[x]$ – нормированные многочлены, $\deg v_{\text{yes}}(x) < n$, $\deg v_{\text{no}}(x) < n$.

Конструирование бюллетеней

1. Каждый голосующий V_j выбирает маску выборов $b_j(x) \in \mathbb{F}_q[x]$, $0 < \deg b_j(x) < n$, для своего голоса $v_j(x) \in \{v_{\text{yes}}(x), v_{\text{no}}(x)\}$ и формирует бюллетень $B_j(x) = v_j(x) + b_j(x)$. Далее он случайным образом генерирует полином $p_j(x) \in \mathbb{F}_q[x]$, $\deg p_j(x) < (k-1)n$, и вычисляет промежуточный бюллетень $CB_j(x) = p(x)m_0(x) + B_j(x)$.

2. Каждый голосующий V_j секретно пересылает подбюллетень $B_{ji}(x) = CB_j(x)(\mathrm{mod}\, m_i(x))$ выборному представителю A_i для всех $1 \le j \le m$ и для всех $1 \le i \le t$.

Подсчет бюллетеней

1. По истечении отведенного на конструирование бюллетеней времени каждый выборный представитель A_i вычисляет частичный «замаскированный» результат выборов $T_i(x) = \sum_{j=1}^{m} B_{ji}(x)(\mathrm{mod}\, m_i(x))$ и секретно посылает его главному доверительному лицу A для всех $1 \le i \le t$.

2. Главное доверительное лицо A получает окончательный «замаскированный» итог $T(x) = \sum_{j=1}^{m} B_j(x)$, решая следующую систему с использованием китайской теоремы об остатках:

$$C(x) \equiv T_i(x)(\mathrm{mod}\, m_i(x)), i \in D,$$

для некоторого разрешенного подмножества D, и затем $T(x) = C(x)(\mathrm{mod}\, m_0(x))$. В силу того что обобщенная схема Асмуса – Блюма $(+_{m_0}, +_{m_1}, \ldots, +_{m_t})$-гомоморфна, значения $T_1(x), \ldots, T_t(x)$ являются частичными секретами $T(x)$.

Голосование

По истечении отведенного на подсчет бюллетеней времени каждый голосующий V_j, $1 \le j \le m$, секретно пересылает свою маску $b_j(x)$ главному доверительному лицу A.

Подсчет голосов

1. По истечении отведенного на голосование времени главное доверительное лицо A вычисляет сумму голосов $R(x) = \sum_{j=1}^{m} v_j(x)$ как $R(x) = T(x) - \sum_{j=1}^{m} b_j(x)$.

2. Количество ответов **да** и **нет** может быть получено как решение уравнения $v_{\mathrm{yes}}(x)z + v_{\mathrm{no}}(x)y = R(x)$. Если значения $v_{\mathrm{yes}}(x)$ и $v_{\mathrm{no}}(x)$ выбираются так, что $\deg v_{\mathrm{yes}}(x) < \deg v_{\mathrm{no}}(x)$, то это решение можно найти следующим образом: $t_{\mathrm{no}} = a_{\deg R(x)}$, где $a_{\deg R(x)}$ – старший коэффициент многочлена $R(x)$, $t_{\mathrm{yes}} = \tilde{a}_{\deg P(x)}$, где $\tilde{a}_{\deg P(x)}$ – старший коэффициент многочлена $P(x) = R(x) - t_{\mathrm{no}} v_{\mathrm{no}}(x)$. Отметим, что порядок поля q должен быть достаточно большим, $q > m$. Главное доверительное лицо A публикует результат голосования $(t_{\mathrm{yes}}, t_{\mathrm{no}})$.

Эта схема электронного голосования обладает следующими свойствами: приватность и устойчивость.

Таким образом, нами построена схема электронного голосования на основе полученной ранее модулярной схемы разделения секрета, обладающей свойствами совершенности и идеальности.

1. Blakley G. // Proc. AFIPS nat. comp. conf. New York, 1979. Vol. 48. P. 313.
2. Shamir A. // Comm. of the ACM. 1979. Vol. 22. P. 612.
3. Benaloh J. // LNCS. 1987. Vol. 263. P. 251.
4. Asmuth C., Bloom J. // IEEE Transactions on Information Theory. 1983. Vol. 29. P. 156.
5. Mignotte M. // Advances in cryptology – Eurocrypt'82, LNCS. 1982. P. 371.
6. Galibus T., Matveev G., Shenets N. // SYNASC'2008: 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, IEEE Comp. Soc., CPS / Ed. by V. Negru et al. Los Alamitos, 2009. P. 197.
7. Шенец Н.Н. // Докл. НАН Беларуси. Сер. физ.-мат. наук. 2010. Т. 54. № 6. С. 9.
8. Stinson D.R. Cryptography: theory and practice. 2-nd ed. New York, 2002.
9. Quisquater M., Preneel B., Vandewalle J. // LNCS. 2002. Vol. 2274. P. 199.

Поступила в редакцию 23.12.10.

Николай Николаевич Шенец **–** младший научный сотрудник НИИ прикладных проблем математики и информатики БГУ.