УДК 621.391:519.7

А. Н. Алексейчук[1], Ю. Е. Бояринова[2]
[1]Институт специальной связи и защиты информации НТУУ «КПИ»
ул. Московская, 45/1, 01011 Киев, Украина
[2]Институт проблем регистрации информации НАН Украины
ул. Н. Шпака, 2, 03113 Киев, Украина

Модулярная схема разделения секрета над кольцом гауссовых целых чисел

Предложена конструкция модулярной схемы разделения секрета над кольцом гауссовых целых чисел, обладающей большей вычислительной стойкостью по сравнению с известной целочисленной модулярной схемой разделения секрета.

Ключевые слова: *модулярная схема разделения секрета, вычислительная стойкость, кольцо гауссовых целых чисел.*

Введение

Одна из первых модулярных схем разделения секрета (СРС) предложена в [1]. В этой схеме каждому участнику $i \in \overline{1,n}$ ставится в соответствие положительное целое число (модуль) m_i', а i-я проекция ключа $s_0' \in \mathbf{Z}$, выбираемого случайно и равновероятно из некоторого фиксированного конечного интервала на числовой прямой, определяется как остаток от деления s_0' на m_i'. В [1] показано, что при определенном способе задания чисел $m_1', \ldots, m_n'$ описанная конструкция позволяет реализовать (k, n)-пороговую структуру доступа на множестве участников $P = \{1, 2, \ldots, n\}$ для любого $2 \le k \le n$. Впоследствии ряд модификаций и обобщений описанной СРС исследован в [2–5]. Отметим, что основным преимуществом этих схем разделения секрета по сравнению с идеальными пороговыми СРС [6] является меньшая временная сложность восстановления секретных ключей разрешенными коалициями участников [4].

Возможность построения модулярных СРС над коммутативными кольцами, отличными от кольца $\mathbf{Z}$, по аналогии с конструкцией [1], исследовалась в [7–9]. В частности, в [8] предложены модулярные СРС над кольцом многочленов $\mathbf{GF}(2)[x]$, а в [9] описаны эффективные алгоритмы восстановления ключей разрешенными коалициями участников модулярных СРС над кольцами целых гауссовых, двойных или дуальных чисел.

При анализе стойкости схем разделения секрета, построенных над кольцом гауссовых целых чисел $\mathbf{Z}[i]$, выяснилось, что указанные СРС имеют, по существу, такую же вычислительную стойкость, что и их целочисленные аналоги — модулярные СРС, описанные в [1]. Таким образом, непосредственное «обобщение» конструкции [1] с кольца целых на кольцо гауссовых целых чисел не приводит к более эффективным, с точки зрения стойкости или практичности, схемам разделения секрета.

В настоящей статье предложена модулярная СРС над кольцом $\mathbf{Z}[i]$, свободная от указанных недостатков. Получены аналитические оценки параметров, характеризующих стойкость предложенной СРС, и показано, что новая схема разделения секрета является (в ряде случаев — существенно) более стойкой по сравнению с целочисленной модулярной СРС [1].

Основные понятия и вспомогательные результаты

Обозначим $Z[i] = \{a_1 + a_2 i : a_1, a_2 \in Z, i^2 = -1\}$ кольцо гауссовых целых чисел. Известно, что это кольцо является евклидовым относительно нормы $N(a) = |a|^2$, $a \in \mathbf{Z}[i]$. Более того, справедливо следующее утверждение (см., например [10], стр. 23).

Лемма 1. Для любых $a,\ b \in \mathbf{Z}[i],\ b \neq 0,$ существуют элементы $q, r \in \mathbf{Z}[i]$ такие, что $a = bq + r,\ \left|\mathrm{Re}(\frac{r}{b})\right| \le \frac{1}{2},\ \left|\mathrm{Im}(\frac{r}{b})\right| \le \frac{1}{2}$; в частности, $N(r) \le \frac{1}{2} N(b).$

Используя известные результаты о строении неприводимых элементов кольца $\mathbf{Z}[i]$ ([10], стр. 149–151), нетрудно убедиться в справедливости такого утверждения.

Лемма 2. Пусть $a = a_1 + i a_2,\ b = b_1 + i b_2 \in \mathbf{Z}[i]$, где $(a_1, a_2) = (b_1, b_2) = (N(a), N(b)) = 1,\ N(a) > 1,\ N(b) > 1$ (символ (u, v) обозначает наибольший общий делитель целых чисел u и v). Тогда, если $c = ab = c_1 + c_2 i$, то $(c_1, c_2) = 1$.

Обозначим $\rho(N)$ число целочисленных решений (x, y) неравенства $x^2 + y^2 \le N$, где $N > 0$. Доказательство следующего утверждения можно найти в [11], стр. 64.

Лемма 3. Для любого $N \ge 2$ справедливы неравенства:

$$\pi(\sqrt{N} - \sqrt{2})^2 < \rho(N) < \pi(\sqrt{N} + \sqrt{2})^2. \qquad (1)$$

Отметим, что верхняя оценка (1) имеет место для всех $N > 0$.

Определение модулярной схемы разделения секрета

Пусть n и k — натуральные числа, $2 \le k \le n$, $m_1, m_2, \ldots, m_n$ — необратимые элементы кольца $\mathbf{Z}[i]$. Обозначим $P = \{1, 2, \ldots, n\}$, $m_A = \prod_{i \in A} m_i$ для любого $A \subseteq P$,

$$M_1 = \max_{A\subseteq P:|A|=k-1} N(m_A),\ M_2 = \min_{A\subseteq P:|A|=k} N(m_A). \qquad (2)$$

Предположим, что элементы m_1, m_2, ..., m_n удовлетворяют следующим условиям:

(а) $(\mathrm{Re}(m_i),\mathrm{Im}(m_i))=1,\ i\in\overline{1,n}$;

(б) $(N(m_i),N(m_j))=1,\ \ i,j\in\overline{1,n},\ i\neq j$;

(в) $4<M_1<\frac{1}{36}M_2$.

Для любого $x\in\mathbf{R}$ обозначим $[x]$ целую часть числа x. Положим:

$$S_0=\{s_0\in\mathbf{Z}:|s_0|\le\left[\frac{1}{2}\sqrt{M_2}\right]-1\}, \qquad (3)$$

$$S=\{s\in\mathbf{Z}[i]:\frac{1}{4}M_1\le N(s)<\frac{1}{4}M_2\}. \qquad (4)$$

По указанным элементам m_1, m_2, ..., m_n построим схему разделения секрета для множества секретных ключей S_0 на множестве участников P.

Пусть $s^{(0)}\in S_0$ — произвольный секретный ключ. Тогда для нахождения проекций $c_1,\dots,c_n\in\mathbf{Z}[i]$ ключа $s^{(0)}$ дилеру СРС необходимо выполнить следующий алгоритм:

1) выбрать случайно и равновероятно элемент $s^{(1)}\in\mathbf{Z}$, удовлетворяющий условию

$$\frac{1}{4}M_1-\left|s^{(0)}\right|^2<\left|s^{(1)}\right|^2<\frac{1}{4}M_2-\left|s^{(0)}\right|^2$$

или, другими словами, условию

$$s\overset{\text{def}}{=}s^{(0)}+s^{(1)}i\in S; \qquad (5)$$

2) вычислить c_i как остаток от деления s на m_i в кольце $\mathbf{Z}[i]$.

Отметим, что в силу условия (в) выбор элемента $s^{(1)}$ на первом шаге описанного алгоритма всегда возможен. Обозначим построенную схему разделения секрета $\Sigma(m_1,m_2,\dots,m_n)$. Отметим, что число различных секретных ключей в этой схеме равно:

$$|S_0|=2\left[\frac{1}{2}\sqrt{M_2}\right]-1<\sqrt{M_2}\ . \qquad (6)$$

Покажем, что $\Sigma(m_1, m_2, ..., m_n)$ является (k, n)-пороговой СРС. Предварительно введем ряд дополнительных обозначений.

Зафиксируем произвольный ключ $s^{(0)} \in S_0$ и соответствующий ему набор проекций $(c_1, ..., c_n)$. Для любого $A \subseteq P$ обозначим X_A множество решений системы сравнений (СС)

$$x \equiv c_i (\mathrm{mod}\, m_i), i \in A \tag{7}$$

над кольцом $\mathbf{Z}[i]$. Зафиксируем произвольное решение x_A СС (7), удовлетворяющее условию:

$$\left|\mathrm{Re}(\frac{x_A}{m_A})\right| \le \frac{1}{2}, \quad \left|\mathrm{Im}(\frac{x_A}{m_A})\right| \le \frac{1}{2}. \tag{8}$$

Отметим, что, согласно лемме 1, такое решение всегда существует, и может быть получено как остаток от деления любого фиксированного решения СС (7) на элемент m_A. Кроме того, на основании условия (б), множество X_A имеет следующий вид:

$$X_A = \{x_A + rm_A : r \in \mathbf{Z}[i]\}. \tag{9}$$

При этом элемент s вида (5) удовлетворяет системе сравнений (7), то есть принадлежит множеству (9).

Пусть $A \subseteq P$, $|A| = k$. Покажем, что участники, входящие в коалицию A, могут однозначно восстановить элемент s вида (5) по набору проекций $(c_i : i \in A)$ и, следовательно, найти ключ $s^{(0)}$ по формуле $s^{(0)} = \mathrm{Re}(s)$. Для этого достаточно убедиться в том, что любое решение x_A СС (7), удовлетворяющее условию (8), равно элементу s.

Предположим противное: $x_A \neq s$. Тогда в силу соотношений $x_A \in X_A$, $s \in X_A$ элемент m_A делит разность $s - x_A$ в кольце $\mathbf{Z}[i]$ и, следовательно,

$$\left|\mathrm{Re}(\frac{s - x_A}{m_A})\right| \ge 1 \ \textit{или} \ \left|\mathrm{Im}(\frac{s - x_A}{m_A})\right| \ge 1. \tag{10}$$

С другой стороны, поскольку $s \in S$, то на основании равенства (4) $N(s) < \frac{1}{4} M_2 \le \frac{1}{4} N(m_A)$, то есть $N(\frac{s}{m_A}) < \frac{1}{4}$. Отсюда, используя неравенства (8), получим:

$$\left|\mathrm{Re}(\frac{s-x_A}{m_A})\right| \le \left|\mathrm{Re}(\frac{s}{m_A})\right| + \left|\mathrm{Re}(\frac{x_A}{m_A})\right| < \frac{1}{2}+\frac{1}{2}=1,$$

$$\left|\mathrm{Im}(\frac{s-x_A}{m_A})\right| \le \left|\mathrm{Im}(\frac{s}{m_A})\right| + \left|\mathrm{Im}(\frac{x_A}{m_A})\right| < \frac{1}{2}+\frac{1}{2}=1.$$

Но эти соотношения противоречат условию (10). Таким образом, исходное предположение $x_A \neq s$ неверно, что и требовалось доказать.

Итак, на основании вышеизложенного можно предположить следующий алгоритм восстановления ключа $s^{(0)}$ участниками коалиции A, где $|A| = k$:

1) найти хотя бы одно решение $x \in \mathbf{Z}[i]$ системы сравнений (7), используя известные алгоритмы [9, 12];

2) найти элемент $x_A \in X_A$, удовлетворяющий условию (8), разделив x на m_A с остатком в кольце $\mathbf{Z}[i]$;

3) положить $s^{(0)} = \mathrm{Re}(x_A)$.

Оценки криптографической стойкости предложенной схемы разделения секрета

Пусть теперь $A \subseteq P$ — произвольная коалиция участников СРС $\Sigma(m_1, m_2, ..., m_n)$ такая, что $|A| \le k-1$. Для указанных выше $s^{(0)}$ и $(c_1, ..., c_n)$ обозначим S_A множество всех элементов $s_0 \in S_0$, каждому из которых соответствует набор проекций $(c_i : i \in A)$. Более точно: множество S_A состоит из всех элементов $s_0 \in S_0$, для которых существует элемент $s_1 \in \mathbf{Z}$ такой, что $s \overset{\text{def}}{=} s_0 + s_1 i \in S$, и c_i является остатком от деления s на m_i для всех $i \in A$.

Оценим значения параметров $\tau_A = |S_A|$, $I_A = -\log\frac{|S_A|}{|S_0|}$, первый из которых равен числу опробований, производимых участниками коалиции A для нахождения секретного ключа $s^{(0)}$ по имеющимся у них проекциям, а второй — «комбинаторному» количеству информации ([13], стр. 215), содержащейся в наборе проекций $(c_i : i \in A)$ о ключе $s^{(0)}$.

Рассмотрим множество $R_A = \{r \in \mathbf{Z}[i] : x_A + rm_A \in S\}$ и определим отображение $\varphi_A : R_A \to S_A$, полагая $\varphi_A(r) = \mathrm{Re}(x_A + rm_A)$, $r \in R_A$. Согласно определению множества S_A, отображение φ_A сюръективно и, поскольку $|R_A| = \sum_{s_0 \in S_A} |\varphi_A^{-1}(s_0)| \le |S_A| \max_{s_0 \in S_A} |\varphi_A^{-1}(s_0)|$, то

$$|S_A| \ge \frac{|R_A|}{\mu_A}, \tag{11}$$

где

$$\mu_A \overset{\text{def}}{=} \max_{S_0 \in S_A} \left| \varphi_A^{-1}(s_0) \right|. \tag{12}$$

Убедимся в справедливости следующих неравенств:

$$|R_A| \geq \frac{\pi(M_2 - M_1)}{4N(m_A)} - \pi(1+\sqrt{2})\frac{\sqrt{M_2}+\sqrt{M_1}}{\sqrt{N(m_A)}}, \tag{13}$$

$$\mu_A \leq \frac{2\sqrt{M_2}}{N(m_A)} + 1. \tag{14}$$

Для доказательства формулы (13) заметим, что в силу определения множества R_A справедливы следующие соотношения:

$$r \in R_A \Leftrightarrow \frac{1}{4}M_1 \leq N(x_A + rm_A) < \frac{1}{4}M_2 \Leftrightarrow \frac{M_1}{4N(m_A)} \leq N(\frac{x_A}{m_A} + r) < \frac{M_2}{4N(m_A)} \Leftrightarrow$$
$$\Leftrightarrow \frac{\sqrt{M_1}}{2|m_A|} \leq \left| \frac{x_A}{m_A} + r \right| < \frac{\sqrt{M_2}}{2|m_A|}.$$

Отсюда, используя неравенства (8), получим, что

$$R_A \supseteq \{r \in \mathbf{Z}[i] : \frac{\sqrt{M_1}}{2|m_A|} + \frac{1}{\sqrt{2}} \leq |r| < \frac{\sqrt{M_2}}{2|m_A|} - \frac{1}{\sqrt{2}}\} \supseteq \{r \in \mathbf{Z}[i] : \frac{\sqrt{M_1}}{2|m_A|} + 1 < |r| \leq \frac{\sqrt{M_2}}{2|m_A|} - 1\}.$$

Следовательно, справедливо неравенство

$$R_A \geq \rho((\frac{\sqrt{M_2}}{2|m_A|} - 1)^2) - \rho((\frac{\sqrt{M_1}}{2|m_A|} + 1)^2), \tag{15}$$

где функция ρ определена перед формулировкой леммы 3. Заметим теперь, что на основании неравенства $|m_A| \leq \sqrt{M_1}$, вытекающего из первого соотношения (2), и условия (в) справедлива оценка $(\frac{\sqrt{M_2}}{2|m_A|} - 1)^2 > 2$. Таким образом, согласно формуле (15) и утверждению леммы 3, имеет место неравенство $|R_A| \geq \pi(\frac{\sqrt{M_2}}{2|m_A|} - 1 - \sqrt{2})^2 - \pi(\frac{\sqrt{M_1}}{2|m_A|} + 1 + \sqrt{2})^2$, совпадающее с формулой (13). Итак, неравенство (13) доказано.

Убедимся в справедливости формулы (14). Зафиксируем элементы $s_0 \in S_A$ и $r \in \varphi_A^{-1}(s_0)$. Заметим, что для доказательства формулы (14) достаточно установить справедливость следующего утверждения: для любого $r' \in \varphi_A^{-1}(s_0)$ существуют элементы $\alpha \in Z$, $m \in \mathbf{Z}[i]$ такие, что:

$$r' = r + \alpha m, \tag{16}$$

$$N(m) = N(m_A), \tag{17}$$

$$|\alpha| < \frac{\sqrt{M_2}}{N(m_A)}. \tag{18}$$

Действительно, при выполнении указанного утверждения мощность множества $\varphi_A^{-1}(s_0)$ не превосходит количества целых точек α в интервале $(-\frac{\sqrt{M_2}}{N(m_A)}, \frac{\sqrt{M_2}}{N(m_A)})$, которое, в свою очередь, не превышает $\frac{2\sqrt{M_2}}{N(m_A)} + 1$.

Итак, пусть $r' \in \varphi_A^{-1}(s_0)$. Обозначим $r = r_1 + r_2 i$, $r' = r_1' + r_2' i$, $m_A = m_1 + m_2 i$,

$$s = x_A + r m_A = s_0 + s_1 i, \tag{19}$$

$$s' = x_A + r' m_A = s_0 + s_1' i. \tag{20}$$

Отметим, что, поскольку s, $s' \in S$, то

$$\frac{1}{2}\sqrt{M_1} \le |s| < \frac{1}{2}\sqrt{M_2}, \ \frac{1}{2}\sqrt{M_1} \le |s'| < \frac{1}{2}\sqrt{M_2}. \tag{21}$$

Кроме того, на основании условий (а), (б) и утверждения леммы 2 справедливо равенство $(m_1, m_2) = 1$.

Из формул (19), (20) следует:

$$s_0 = \mathrm{Re}(x_A) + \mathrm{Re}(r m_A) = r_1 m_1 - r_2 m_2, \tag{22}$$

$$s_0 = \mathrm{Re}(x_A) + \mathrm{Re}(r' m_A) = r_1' m_1 - r_2' m_2. \tag{23}$$

Вычитая равенство (23) из равенства (22), получим, что $0 = (r_1 - r_1')m_1 - (r_2 - r_2')m_2$, откуда в силу взаимной простоты чисел m_1 и m_2 следует, что существует элемент $\alpha \in Z$ такой, что

$$r_1' = r_1 + \alpha m_2,\ r_2' = r_2 + \alpha m_1. \tag{24}$$

Положим $m = m_2 + im_1$. Тогда на основании соотношений (24) выполняются равенства (16), (17). Далее, в силу соотношений (17), (19) и (20) $s - s' = (r - r')m_A = -\alpha m m_A$; следовательно, $|s - s'| = |\alpha|\, N(m_A)$. Наконец, в силу неравенств (21)

$$|s - s'| \le |s| + |s'| < \sqrt{M_2},$$

откуда вытекает неравенство (18). Таким образом, сформулированное выше утверждение, а вместе с ним и формула (14), доказаны.

Докажем теперь следующую теорему, устанавливающую оценки криптографической стойкости описанной выше схемы разделения секрета.

Теорема. Пусть $A \subseteq P$ — произвольная коалиция участников СРС $\Sigma(m_1, m_2, ..., m_n)$ такая, что $|A| \le k - 1$. Тогда, каким бы ни был секретный ключ $s^{(0)} \in S_0$, для его восстановления по набору проекций $(c_i : i \in A)$ участникам коалиции A потребуется выполнить не менее

$$\tau_A = |S_A| \ge \frac{\pi M_2}{4(M_1 + 2\sqrt{M_2})} - 1 - \pi\sqrt[4]{M_2} \tag{25}$$

опробований элементов множества S_0. При этом количество информации относительно ключа $s^{(0)}$, содержащейся в наборе $(c_i : i \in A)$, удовлетворяет неравенству:

$$I_A \le -\log\left(\frac{\pi\sqrt{M_2}}{4M_1}\left(\frac{1}{1 + \frac{2\sqrt{M_2}}{M_1}}\right) - \frac{1}{\sqrt{M_2}} - \frac{\pi}{\sqrt[4]{M_2}}\right). \tag{26}$$

Доказательство. На основании формул (11), (13) и (14)

$$\begin{aligned} |S_A| \ge \frac{|R_A|}{\mu_A} \ge \frac{\pi(M_2 - M_1)}{4N(m_A)} \cdot \frac{N(m_A)}{N(m_A) + 2\sqrt{M_2}} - \\ - \pi(1 + \sqrt{2})\frac{\sqrt{M_2} + \sqrt{M_1}}{\sqrt{N(m_A)}} \cdot \frac{N(m_A)}{N(m_A) + 2\sqrt{M_2}}. \end{aligned} \tag{27}$$

Поскольку $N(m_A) \le M_1$, то первое слагаемое в правой части неравенства (27) больше либо равно $\frac{\pi(M_2 - M_1)}{4(M_1 + 2\sqrt{M_2})} \ge \frac{\pi M_2}{4(M_1 + 2\sqrt{M_2})} - 1$. Следовательно, для доказательства неравенства (25) достаточно показать, что:

$$(1+\sqrt{2})\frac{\sqrt{M_2}+\sqrt{M_1}}{\sqrt{N(m_A)}} \cdot \frac{N(m_A)}{N(m_A)+2\sqrt{M_2}} \le \sqrt[4]{M_2}\ . \qquad (28)$$

Заметим, что выражение в левой части неравенства (28) равно

$$(1+\sqrt{2})(\sqrt{M_2}+\sqrt{M_1})\frac{1}{\sqrt{N(m_A)}+\frac{2\sqrt{M_2}}{\sqrt{N(m_A)}}} \le \frac{(1+\sqrt{2})(\sqrt{M_2}+\sqrt{M_1})}{2\sqrt{2}\sqrt[4]{M_2}},$$

поскольку $u + v \ge 2\sqrt{uv}$ для любых $u, v > 0$. Далее, используя неравенство $M_1 < \frac{1}{36} M_2$, получим

$$\frac{1+\sqrt{2}}{2\sqrt{2}}\left(\frac{\sqrt{M_2}+\sqrt{M_1}}{\sqrt[4]{M_2}}\right) \le \frac{1+\sqrt{2}}{2\sqrt{2}} \cdot \frac{7}{6}\sqrt[4]{M_2} < \sqrt[4]{M_2},$$

откуда и следует справедливость неравенства (28).

Итак, формула (25) доказана. Справедливость неравенства (26) следует непосредственно из оценок (25) и (6). Теорема доказана.

Сравнительный анализ стойкости модулярных схем разделения секрета над кольцами целых и гауссовых целых чисел соответственно

Рассмотрим модулярную СРС $\Sigma^{(0)}(m'_1, m'_2, \ldots, m'_n)$ над кольцом $\mathbf{Z}$, соответствующую последовательности натуральных чисел $m'_1, m'_2, \ldots, m'_n$, удовлетворяющих условию

$$M'_1 \overset{\text{def}}{=} \max_{\substack{A \subset P: \\ |A|=k-1}} m'_A \ < \ M'_2 \overset{\text{def}}{=} \min_{\substack{A \subset P: \\ |A|=k}} m'_A, \qquad (29)$$

где $m'_A = \prod_{i \in A} m'_i$, $A \subseteq P$. Указанная СРС является (k,n)-пороговой схемой разделения секрета для множества секретных ключей $S'_0 = \{s'_0 \in \mathbf{Z} : M'_1 < s'_0 < M'_2\}$ [1]. Справедливо равенство

$$\left|S_0'\right| = M_2' - M_1' - 1. \tag{30}$$

Пусть $A \subseteq P$ — коалиция участников СРС $\Sigma^{(0)}(m_1', m_2', \ldots, m_n')$ такая, что $\left|A\right| \le k-1$. Тогда для параметров τ_A' и I_A', которые определяются аналогично введенным выше параметрам τ_A и I_A соответственно, справедливы следующие оценки:

$$\frac{M_2' - M_1'}{M_1'} - 1 \le \frac{M_2' - M_1'}{m_A'} - 1 \le \tau_A' \le \frac{M_2' - M_1'}{m_A'} + 1, \tag{31}$$

$$\log m_A' + \log\left(\frac{M_2' - M_1' - 1}{M_2'}\right) \le I_A' \le \log M_1' + \log\left(\frac{M_2' - M_1' - 1}{M_2' - 2M_1'}\right). \tag{32}$$

Далее ограничимся рассмотрением коалиций $A \subseteq P$, удовлетворяющих условию $m_A' = M_1'$. В этом случае при больших значениях M_1' и M_2' справедливы следующие (приближенные) равенства:

$$\tau_A' = \frac{M_2' - M_1'}{M_1'}, \tag{33}$$

$$I_A' = \log M_1'. \tag{34}$$

Сравним значения параметров (33) и (34) с оценками (25) и (26) соответственно. Предположим, что СРС $\Sigma(m_1, m_2, \ldots, m_n)$ и $\Sigma^{(0)}(m_1', m_2', \ldots, m_n')$ удовлетворяют следующему условию:

$$m_i' = N(m_i),\ i \in \overline{1,n}. \tag{35}$$

В этом случае $m_A' = N(m_A)$ для любого $A \subseteq P$; в частности, $M_1 = M_1'$, $M_2 = M_2'$. Заметим, что при выполнении условия (35) множества ключей в рассматриваемых схемах разделения секрета имеют различные мощности:

$$\left|S_0\right| = \sqrt{M_2},\ \left|S_0'\right| = M_2 - M_1 \tag{36}$$

(равенства (36) являются приближенными, см. формулы (6) и (30)). Поэтому корректное сравнение стойкости указанных СРС предполагает использование параметров I_A, I_A'.

Пусть $M_1,\ M_2 \to \infty$ так, что

$$\frac{M_2^{3/4}}{M_1} \to \infty,\ \frac{\sqrt{M_2}}{M_1} \to 0. \tag{37}$$

Тогда на основании формул (26) и (34) справедливо следующее неравенство:

$$I'_A - I_A \geq \log\left(\frac{\pi}{4}\sqrt{M_2}\right) + o(1), \tag{38}$$

где $o(1) \to 0$ при $M_1,\ M_2 \to \infty$. Это означает, что количество информации о секретном ключе, содержащейся в проекциях участников запрещенной коалиции A СРС $\Sigma(m_1, m_2, ..., m_n)$, примерно на $\log\left(\frac{\pi}{4}\sqrt{M_2}\right)$ бит меньше, чем количество информации о ключе, содержащейся в проекциях участников такой же коалиции СРС $\Sigma^{(0)}(m'_1, m'_2, ..., m'_n)$. Аналогичный результат, свидетельствующий о более высокой стойкости предложенной СРС по сравнению с модулярной схемой разделения секрета [1], получается и в том случае, когда мощности множеств ключей в обеих СРС (практически) совпадают.

Приведем конкретный пример, иллюстрирующий последнее утверждение. Пусть $P = \{1, 2, 3, 4\}$, $k = 2$, $m'_1 = 5 = 2^2 + 1$, $m'_2 = 10 = 3^2 + 1$, $m'_3 = 13 = 2^2 + 3^2$, $m'_4 = 17 = 4^2 + 1$ и m_1, m_2, m_3, m_4 — целые гауссовы числа с нормами m'_1, m'_2, m'_3, m'_4 соответственно (например, можно положить $m_1 = 2 + i$, $m_2 = 3 + i$, $m_3 = 2 + 3i$, $m_4 = 4 + i$). Для любого $i \in \overline{1,4}$ зададим последовательности чисел

$$m_{i,t} = m_i^t,\ m'_{i,t} = (m'_i)^t,\ t = 1, 2, ... \tag{39}$$

Отметим, что для любого натурального t числа $m_{1,t}$, $m_{2,t}$, $m_{3,t}$ и $m_{4,t}$ удовлетворяют сформулированным выше условиям (а) и (б).

Обозначим:

$$M_{1,t} = \max_{\substack{A \subset P: \\ |A|=1}} (m'_A)^t,\ M_{2,t} = \min_{\substack{A \subset P: \\ |A|=2}} (m'_A)^t. \tag{40}$$

Тогда

$$M_{1,t} = 17^t,\ M_{2,t} = 50^t,\ t = 1, 2, ... \tag{41}$$

Отметим также, что $\frac{M_{2,t}^{3/4}}{M_{1,t}} = \left(\frac{50\sqrt{50}}{289}\right)^{t/2} \to \infty$, $\frac{M_{2,t}^{1/2}}{M_{1,t}} = \left(\frac{50}{289}\right)^{t/2} \to 0$, $t \to \infty$ (см. формулы (37)).

Пусть теперь $t = 80$. Рассмотрим $(2,4)$-пороговые модулярные схемы разделения секрета, первая из которых (над кольцом $\mathbf{Z}$) определяется последовательностью целых чисел

$$m'_{1,40} = 5^{40},\ m'_{2,40} = 10^{40},\ m'_{3,40} = 13^{40},\ m'_{4,40} = 17^{40}, \tag{42}$$

вторая (над кольцом $\mathbf{Z}[i]$) — последовательностью гауссовых целых чисел

$$m_{2,80} = (3+i)^{80}, m_{3,80} = (2+3i)^{80}, m_{4,80} = (4+i)^{80}. \tag{43}$$

Подчеркнем, что числа (43) удовлетворяют сформулированным выше условиям (а), (б) и (в).

Сравним значения параметров, характеризующих стойкость СРС, построенных на основе последовательностей (42) и (43) соответственно.

Согласно равенствам (36), (41), мощности множеств ключей в рассматриваемых СРС равны соответственно $|S'_0| = M_{2,40} - M_{1,40} = 50^{40} - 17^{40}$ и $|S_0| = \sqrt{M_{2,80}} = 50^{40}$. Отметим, что $50^{40}(1-3^{-40}) < |S'_0| < 50^{40}$, так, что соотношение $|S'_0| \cdot |S_0|^{-1}$ практически равно 1. Далее, на основании равенства (33) число ключей, которые потребуется перебрать одному из участников СРС над кольцом $\mathbf{Z}$, равно:

$$\tau'_A = \frac{M_{2,40} - M_{1,40}}{M_{1,40}} = \left(\frac{50}{17}\right)^{40} - 1 \approx 1{,}19 \cdot 2^{62}. \tag{44}$$

При этом согласно неравенству (25), число ключей, которые необходимо перебрать любому участнику СРС над кольцом $\mathbf{Z}[i]$, равно:

$$\tau_A \geq \frac{\pi}{4}\left(\frac{50}{17}\right)^{80}\left(\frac{1}{1+2\left(\frac{50}{289}\right)^{40}}\right) - 1 - \pi \cdot 50^{20} > \frac{\pi}{4}\left(\frac{50}{17}\right)^{80}(1-2^{-8}) - 1 \approx \frac{\pi}{4} \cdot 2^{124} - 1. \tag{45}$$

Итак, сравнивая выражения (44) и (45), заключаем, что вычислительная стойкость СРС, соответствующей системе гауссовых целых чисел (43), примерно в 2^{62} раз выше вычислительной стойкости СРС, соответствующей системе целых чисел (42), при (практически) одинаковых мощностях множеств секретных ключей в обеих схемах.

В заключение отметим, что предложенную конструкцию СРС $\Sigma(m_1, m_2, \ldots, m_n)$ нетрудно модифицировать таким образом, чтобы получить схемы разделения секрета над кольцом $\mathbf{Z}[i]$, аналогичные целочисленным модулярным СРС, описанным в [2–4]. Стойкость указанных модифицированных схем раз-

деления секрета можно оценить, проведя рассуждения, аналогичные изложенным выше при доказательстве соотношений (25), (26).

1. *Mignotte M.* How to Share a Secret // Advances in Cryptology — EUROCRYPT'82, Proceedings. — Springer Verlag, 1983. — P. 371–375.

2. *Asmuth C.*, *Bloom J.* A modular Approach to Key Safeguarding // IEEE Trans. on Inform. Th. — 1983. — IT-29. — P. 208–210.

3. *Goldreich O.*, *Ron D.*, *Sudan D.* Chinese Remainder with Errors // IEEE Trans. on Inform. Th. — 2000. — IT-46. — P. 1330–1338.

4. *Quisquater M.*, *Preneel B.*, *Vanderwalle J.* On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem // Public Key Cryptography — PKC'02, Proceedings. — Springer Verlag, 2002. — P. 199 – 210.

5. *Ifrene S.* General Secret Sharing Based on the Chinese Remainder Theorem // http://eprint.iacr.org/2006/166.

6. *Shamir A.* How to Share a Secret // Comm. ACM. — 1979. — Vol. 22, N 1. — P. 612–613.

7. *Синьков М.В.*, *Бояринова Ю.Е.*, *Калиновский Я.А.*, *Трубников П.В.* Развитие задачи разделения секрета // Реєстрація, зберігання і оброб. даних. — 2003. — Т. 5, № 4. — С. 90–96.

8. *Галибус Т.Н.*, *Матвеев Г.В.* Особенности модулярного разделения секрета // www.cryptography.ru/db/20.02.2004.

9. *Бояринова Ю.Е.*, *Одарич Я.В.* Восстановление информации в задаче разделения секрета для гиперкомплексных числовых систем 2-го порядка с помощью алгоритма Евклида // Реєстрація, зберігання і оброб. даних. — 2005. — Т. 7, № 1. — С. 103–114.

10. *Айерлэнд К.*, *Роузен М.* Классическое введение в современную теорию чисел / Пер. с англ. — М.: Мир, 1987. — 416 с.

11. *Чандрасекхаран К.* Введение в аналитическую теорию чисел / Пер. с англ. — М.: Мир, 1974. — 188 с.

12. *Ноден П.*, *Китте К.* Алгебраическая алгоритмика / Пер. с франц. — М.: Мир, 1999. — 720 с.

13. *Колмогоров А.Н.* Теория информации и теория алгоритмов. — М.: Наука, 1987. — 304 с.

Поступила в редакцию 01.03.2007