УДК 004.75

Н. И. Червяков, д-р техн. наук, проф., зав. каф., e-mail: k-fmf-primath@stavsu.ru,
М. А. Дерябин, аспирант, мл. науч. сотр., e-mail: maxim.deryabin@gmail.com
ФГАОУ ВПО Северо-Кавказский федеральный университет, г. Ставрополь

Новый метод порогового разделения секрета, основанный на системе остаточных классов

Рассмотрены основные принципы построения схем разделения секрета на основе системы остаточных классов. На основе анализа абсолютной и вычислительной стойкости известных модулярных схем предложен новый подход к построению вычислительно-стойкой схемы разделения секрета, основанный на переводе секрета в систему остаточных классов. Его основной особенностью является малый размер долей секрета относительно размера разделяемой информации, что позволяет эффективно хранить и передавать информацию. Проведенный в работе анализ показал, что при выборе в качестве системы компактных последовательностей взаимно простых чисел вычислительная стойкость предлагаемой схемы приближается к вычислительной стойкости схемы Асмута—Блума.

Ключевые слова: *пороговые схемы разделения секрета, Китайская теорема об остатках, система остаточных классов, совершенные схемы*

Введение

Схемы разделения секрета (СРС) представляют собой протоколы распределения некоторой секретной информации (секрета) среди группы участников, каждый из которых получает свою долю секрета. При этом восстановление секрета возможно лишь в случае объединения долей секрета некоторой коалиции участников. Такую коалицию называют разрешенной коалицией. Использование СРС позволяет надежно скрыть информацию, распределив ее, например, в различные не связанные друг с другом хранилища. Одним из самых распространенных видов СРС являются пороговые схемы. В данных схемах секрет, разделенный среди n участников, восстановить могут только k и более участников, где порог k является важным параметром схемы и $2 < k \leqslant n$. Среди таких схем одной из самых известных является схема Шамира [1], получившая широкое распространение благодаря доказанной высокой стойкости.

Широко известны также СРС, основанные на Китайской теореме об остатках. Данные схемы базируются на модулярном представлении числа — в виде набора остатков от деления на заранее подобранные взаимно простые числа. Китайская теорема об остатках [2] позволяет восстанавливать позиционное значение на основе модулярного представления, обеспечивая алгоритмическую основу для восстановления секрета. К схемам такого типа относятся схемы Асмута—Блума [3] и Миньотта [4].

Однако важным вопросом при исследовании СРС является стойкость предложенного метода, которая понимается как вероятность восстановления секрета для неразрешенной коалиции участников. Понятие стойкости здесь используется с точки зрения устойчивости схемы к атакам различного рода. Основным видом атак в области пороговых СРС является попытка восстановления секрета группой участников, число которых не превышает заданный "порог" схемы. Для схем, основанных на Китайской теореме об остатках, важным результатом является введенная в работе [5] асимптотическая совершенность СРС. В асимптотически совершенной СРС количество получаемой информации при объединении долей секрета неразрешенной коалицией стремится к нулю при правильном выборе параметров схемы, основным из которых является набор модулей системы остаточных классов. В работах [5 и 6] показана асимптотическая совершенность схемы Асмута—Блума при достаточно близком расположении оснований системы. Однако описание схемы не будет полным без анализа ее вычислительной стойкости.

Важным свойством любой информационной системы является ее эффективность, которая полностью зависит от поставленных перед ней задач. Параметрами эффективности в данном контексте выступают скорость и точность системы, а также затрачиваемые ресурсы. Задачей проектировщиков является разработка системы таким образом, чтобы требуемая точность работы была достигаема за наименьшее время и с наименьшими затратами. Для СРС можно выделить два основных направления их применения. Первым является хранение или передача ключей, информации небольшого размера. В данном случае создаваемая система нечувствительна к ресурсам, а обеспечение стойкости является приоритетной задачей. Вторым направлением является потоковая передача информации и ее хранение, которые ограничены в плане ресурсов. Так как в данном случае количество обрабатываемой информации намного выше, то важными параметрами информационной системы для такого

случая являются скорость обработки и объем выходных данных. В первом случае для конкретного объема информации необходимо использовать совершенную СРС. При этом вероятность потери ключа будет равна вероятности его подбора. Во втором случае абсолютной безопасностью можно пренебречь в пользу скорости и повышения объема обрабатываемой информации. Основную роль здесь играет доказанная вычислительная стойкость используемой схемы. Вычислительная стойкость характеризуется сложностью раскрытия секрета, неразрешенной коалицией участников и оценивается вычислительной сложностью полного перебора элементов данного множества. Стойкость такого рода отражает стойкость схемы при практической реализации.

СРС находят дальнейшее развитие при реализации множественных схем разделения секрета [7], взвешенных схем [8] и верифицируемых схем [9]. Однако подробный анализ вычислительной стойкости данных схем ранее не проводили. В связи с этим чаще всего на практике используют вычислительно неэффективную схему Асмута—Блума, которая доказано является асимптотически совершенной [5, 6].

В данной работе предлагается новый подход к разделению секрета, основанный на переводе позиционного секрета в систему остаточных классов (СОК). Отличительной особенностью данного подхода является ориентация на эффективность схемы в условиях разделения большого объема информации. В разделе 1 приведены общие понятия, касающиеся СОК и СРС на ее основе. Кроме того, в нем более детально обсуждается вопрос об абсолютной и относительной стойкости схемы. В разделе 2 предложена новая схема разделения секрета на основе использования СОК и проведено исследование стойкости данной схемы при практической реализации в сравнении с классическими пороговыми схемами на СОК — схемами Асмута—Блума и Миньотта.

1. Схемы разделения секрета с использованием СОК и их свойства

Пусть каждый участник схемы имеет уникальный номер или идентификатор, все множество которых назовем универсальным множеством номеров и обозначим U (в простейшем случае $U = \{1, 2, ..., n\}$, где n — число участников схемы). Множество номеров разрешенной коалиции назовем разрешенным подмножеством множества U и обозначим I. Вместе с тем, неразрешенным подмножеством будем называть подмножество $\tilde{I}$ номеров участников любой коалиции, не имеющей права восстанавливать секрет. Областью определения секрета S при этом будем называть множество, объединяющее все возможные значения секрета s.

Система остаточных классов представляет собой одну из самых распространенных непозиционных систем счисления. Каждая конкретная СОК определяется системой взаимно простых оснований $\{p_1, p_2, ..., p_n\}$ и диапазоном представления $P = \prod_{i=1}^{n} p_i$. Позиционное число X такое, что $0 \leqslant X < P$, в этой системе представляется в виде кортежа из n чисел $(x_1, x_2, ..., x_n)$, полученных по формуле

$$x_i = X \bmod p_i,\ i = 1, 2, ..., n.$$

СОК имеет множество приложений, среди которых можно отметить ускорение операций за счет параллельной реализации базовых арифметических операций, контроль целостности информации, цифровая обработка сигналов. Хорошо разработанные методы обратного перевода чисел из СОК в позиционную систему вместе с эффективной реализацией вычисления остатка от деления делают данную систему подходящей для использования в качестве основы СРС [10—12].

В основе модулярного исчисления лежит Китайская теорема об остатках, согласно которой число X, $0 \leqslant X < P$, представленное остатками $(x_1, x_2, ..., x_n)$ в системе модулей $\{p_1, p_2, ..., p_n\}$, можно единственным образом вычислить по формуле

$$X = \left| \sum_{i=1}^{n} \left| P_i^{-1} \right|_{p_i} P_i x_i \right|_P,$$

где $P_i = \frac{P}{p_i}$, $\left| P_i^{-1} \right|_{p_i}$ — мультипликативная инверсия P_i по модулю p_i для $i = 1, 2, ..., n$.

Рассмотрим далее две СРС, основанные на СОК. На этапе генерирования параметров в схеме Асмута—Блума вначале выбирается число p_0, которое определяет множество всех возможных секретов. Произвольный секрет s следует выбирать так, что $s \in Z_{p_0}$. Далее система оснований $p_1 < p_2 < ... < p_k < p_{k+1} < ... < p_n$ подбирается так, что

$$\prod_{i=1}^{k} p_i > p_0 \prod_{i=0}^{k-2} p_{n-i},$$

последнее неравенство принято называть условием Асмута—Блума. На этапе разделения секрета генерируется случайное число r такое, что $s' = s + rp_0 < \prod_{i=1}^{k} p_i$. Секрет s такой, что делится таким образом, что $s_i = s' \bmod p_i$ есть доля секрета для каждого участника с номером i, где $i = 1, 2, ..., n$. В данном методе любое разрешенное множество участников с номерами из I может единственным образом восстановить секрет; при этом $|I| = m \geqslant k$. Вначале с помощью Ки-

тайской теоремы об остатках вычисляется позиционное число x на основе модулярного представления $(s_{i_1}, s_{i_2}, ..., s_{i_m})$ в СОК с основаниями $p_{i_1}, p_{i_2}, ..., p_{i_m}$, где $i_j \in I$ для всех $j = 1, 2, ..., m$. Исходный секрет восстанавливается как остаток от деления числа x на p_0: $s = x \bmod p_0$.

Для обсуждения вопроса стойкости схемы Асмута—Блума рассмотрим случай, когда объединены доли некоторой неразрешенной коалиции участников с номерами из $\tilde{I}$. Тогда $|\tilde{I}| \leqslant k - 1$, пусть $P = \prod_{i=1}^{k} p_i$ и $\tilde{P} = \prod_{i \in \tilde{I}} p_i$. Все, что будет известно в таком случае — это число $\tilde{s} = s' \bmod \tilde{P}$. Так как по условию Асмута—Блума $P/\tilde{P} > p_0$ и $(\tilde{P}, p_0) = 1$, то набор чисел $\tilde{s}$, таких что $\tilde{s} \equiv s' \bmod \tilde{P}$ и $\tilde{s} < P$, покрывает все классы вычетов по модулю m_0. Таким образом, как показано в работе [3], коалиция, объединяющая менее k долей секрета, не получает никакой полезной информации о секрете, что говорит о стойкости схемы. Однако серьезным ее недостатком является увеличение размера долей секрета относительно размера самого секрета, что приводит к существенному избытку выходной информации. Данного недостатка лишена следующая пороговая схема разделения секрета — (k, n)-пороговая схема Миньотта.

В схеме Миньотта система оснований $p_1 < p_2 < ... ... < p_k < p_{k+1} < ... < p_n$ подбирается как последовательность Миньотта, числа в которой удовлетворяют неравенству

$$\alpha = \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i = \beta.$$

Для достижения стойкости секрет s выбирается. При этом для произвольного секрета s из промежутка (α, β) числа $s_i = s \bmod p_i$ есть доли секрета для каждого участника с номером i, где $i = 1, 2, ..., n$. Восстановить секрет может любое разрешенное множество участников с номерами I, при этом $|I| = m \geqslant k$, секрет s вычисляется с использованием Китайской теоремы об остатках на основе числа $(s_{i_1}, s_{i_2}, ..., s_{i_m})$, представленного в СОК с основаниями $p_{i_1}, p_{i_2}, ..., p_{i_m}$, где $i_j \in I$ для всех $j = 1, 2, ..., m$.

Для того чтобы обеспечить достаточный уровень стойкости схемы необходимо использовать последовательности Миньотта с большим значением $\frac{\beta - \alpha}{\beta}$ [4]. Как показано в работе [6], схема Миньотта не является стойкой в абсолютном смысле, однако она нашла большое применение на практике за счет уменьшения объема выходных данных.

Ниже рассмотрим понятия, играющие важную роль в теории абсолютной стойкости схемы. Основываясь на данном аппарате, можно оценить энтропию для схем разделения секрета. Информационную энтропию в условии отсутствия информации о долях секрета обозначим как $H(s \in S)$, где s есть секрет, распределенный в области определения секрета S. В данном случае энтропия максимальна, так как рассматривается только общедоступная информация. Энтропию секрета при условии, что известны доли секрета от участников, чьи номера принадлежат некоторому множеству $I \subseteq U$, обозначим как $H(s \in S \mid s_i : i \in I)$. В случае, если I представляет собой множество номеров разрешенного подмножества участников, то $H(s \in S \mid s_i : i \in I) = 0$, так как в данном случае секрет должен быть правильно восстановлен. Для обратного случая, в котором объединяется неразрешенное множество участников, важно добиться максимума условной энтропии. Данное условие приводит к формулировке условия совершенности схемы на основе вероятностного подхода. При этом важнейшим понятием теории СРС является убыль неопределенности схемы, под которой понимается величина

$$\Delta(s_i : i \in I) = H(s \in S) - H(s \in S | s_i : i \in I).$$

Убыль неопределенности в случае, если I является множеством номеров разрешенного подмножества участников, равна безусловной энтропии области определения секрета: $\Delta(s_i : i \in I) = H(s \in S)$. Пусть теперь множество участников является неразрешенным. СРС является *совершенной*, если для всех неразрешенных подмножеств участников с номерами $\tilde{I}$ следует

$$\Delta(s_i : i \in \tilde{I}) = 0.$$

Однако как было отмечено ранее, для анализа стойкости СРС, основанных на СОК, было введено дополнительное понятие, позволяющее исследовать свойства СРС данного типа общепринятыми методами [5]. Поэтому в данном случае было введено понятие *асимптотически совершенной СРС*. Схема является асимптотически совершенной, если для всех неразрешенных подмножеств участников с номерами $\tilde{I}$ и для любого $\varepsilon > 0$ существует такое p, что при условии выбора на этапе генерации параметров СРС системы оснований $p_0 < p_1 < ... < p_n$ так, что $p_i > p$ $(i = 0, 1, ..., n)$ для нее следует

$$\Delta(s_i : i \in \tilde{I}) < \varepsilon.$$

Открытым остается вопрос о том, как именно необходимо подбирать параметры СРС на СОК, чтобы она обладала свойством асимптотической совершенности. В работе [5] показана асимптотическая совершенность схемы Асмута—Блума при

использовании "достаточно близко расположенных" взаимно простых чисел в качестве системы оснований СОК. В работе [6] в качестве системы модулей предлагается использовать так называемые компактные последовательности взаимно простых чисел.

Согласно [6] последовательность $p_0 < p_1 < ... < p_n$ называется компактной последовательностью взаимно простых чисел с начальным значением p_0, если $p_n < p_0 + p_0^{\theta}$ для некоторого действительного числа $\theta \in (0, 1)$.

Рассмотрим структуру компактной последовательности на конкретном примере. Пусть $p_0 = 20$. Возьмем несколько взаимно простых с ним чисел: $p_1 = 21$, $p_2 = 29$ и $p_3 = 43$. Вычислим полученное значение θ исходя из условия $p_n = p_0 + p_0^{\theta}$. Тогда $\theta = \log p_0(p_n - p_0)$ и в нашем случае $\theta \approx 1{,}015$. Очевидно, что выбранная последовательность 20, 21, 29, 43 компактной не является. Заменим в ней число $p_3 = 43$ на $p_3 = 31$. Для полученной последовательности 20, 21, 29, 31 значение $\theta = 0{,}756$, откуда следует, что она является компактной.

Компактные последовательности взаимно простых чисел играют важную роль в исследовании стойкости СРС. Использование данных последовательностей в качестве системы оснований СОК позволяет строить эффективные и стойкие схемы, что обусловлено близостью чисел на числовой прямой. В работе [6] показано, что схема Асмута—Блума является асимптотически совершенной при использовании компактной последовательности в качестве системы оснований СОК. Стоит отметить, что схема Миньотта асимптотически совершенной не является. Однако исследование стойкости не будет полным без анализа вычислительной стойкости методов. В дальнейшем будем полагать, что в качестве системы оснований использована именно компактная последовательность взаимно простых чисел.

Обратимся далее к понятию вычислительной стойкости схемы. Пусть в некоторый момент времени некоторому аналитику удалось собрать доли неразрешенного подмножества участников с номерами $\tilde{I}$ для некоторой конкретной СРС. Задача аналитика в таком случае состоит в том, чтобы восстановить секрет на основе имеющихся данных. В реальной ситуации множество S можно разделить на два подмножества. Первое подмножество S_1 будет состоять из всех вариантов секрета, которые не подходят на роль секрета при известных данных. Второе подмножество S_2 будет содержать все оставшиеся возможные варианты секрета. Например, если в схеме Миньотта известна доля секрета s_j для модуля p_j, $0 \leqslant j \leqslant n$, то секрет обязательно должен удовлетворять условию: $s \equiv s_j \bmod p_j$. Следовательно, в данном случае $S_1 = \{s : s \in S \wedge s \not\equiv s_j \bmod p_j\}$ и $S_2 = \{s : s \in S \wedge s \equiv s_j \bmod p_j\}$. Отметим, что в случае, если СРС совершенна, то для нее $S_1 = \varnothing$ и $S_2 = S$.

Таким образом, для того чтобы найти исходный секрет, необходимо перебрать все варианты, входящие в S_2, и стойкость схемы зависит от мощности этого множества и от вычислительной сложности полного перебора. Необходимо генерировать параметры схемы так, чтобы аналитик не смог с использованием современных вычислительных ресурсов подобрать секрет за приемлемое время. Схему, отвечающую данным условиям, будем называть *вычислительно стойкой*.

В качестве меры вычислительной стойкости примем мощность множества S_2: $f(\tilde{I}) = |S_2|$. Для схемы Асмута—Блума, принимая в расчет ее асимптотическую совершенность и условие Асмута—Блума, $f(\tilde{I}) = |S| = |Z_{p_0}| = p_0$ для любого $\tilde{I}$.

Легко видеть, что не все абсолютно стойкие схемы являются вычислительно стойкими, но вместе с тем вычислительно стойкие схемы не всегда совершенны. Наиболее важной в практическом смысле является именно вычислительная стойкость.

В данном пункте нами введены основные понятия, используемые при построении СРС, основанных на СОК. Рассмотрены наиболее известные СРС на СОК — схема Асмута—Блума и схема Миньотта. Приведены основные подходы, применяемые для анализа стойкости СРС и их расширение для СРС на СОК. Далее рассматривается предлагаемая схема, основанная на использовании СОК, обладающая похожей стойкостью, по способная разделять секрет гораздо большего размера.

2. Предлагаемая схема разделения секрета, основанная на использовании СОК

В схемах Асмута—Блума и Миньотта на область секрета S накладываются существенные ограничения. В первом случае она равна Z_{p_0}, во втором случае существенно усекается за счет исключения из диапазона достаточно большого промежутка чисел. Рассмотрим теперь схему разделения секрета, основанную на простом переводе секрета из области $S = [0, P)$ в избыточную систему остаточных классов с основаниями $p_1, p_2, ..., p_n$. Базовым преимуществом данной схемы является существенная экономия объема информации при ее передаче и хранении. Однако предлагаемая схема, очевидно, не является совершенной, так как при условии раскрытия части долей секрета энтропия существенно уменьшается.

Предлагаемая (k, n)-пороговая схема разделения секрета, основанная на использовани СОК.

Генерация параметров. Подбирается компактная последовательность взаимно простых чисел $p_1 < p_2 < ... < p_k < p_{k+1} < ... < p_n$, при этом $p_n < p_1 + p_1^{\theta}$, где $\theta \in (0, 1)$; секрет s выбирается из промежутка $(0, P)$,

где P представляет собой рабочий диапазон СОК и определяется согласно выражению

$$P = \prod_{i=1}^{k} p_i,$$

доли секрета s_i имеют множества представления Z_{p_i} для участника с номером i, где $i = 1, 2, ..., n$.

Разделение секрета. Доли секрета s вычисляются так, что $s_i = s \bmod p_i$ есть доля секрета для каждого участника с номером i, где $i = 1, 2, ..., n$.

Восстановление секрета. Любое разрешенное множество участников с номерами I может единственным образом восстановить секрет, при этом $|I| = m \geqslant k$; секрет s вычисляется с использованием Китайской теоремы об остатках на основе числа $(s_{i_1}, s_{i_2}, ..., s_{i_m})$, представленного в СОК с основаниями $p_{i_1}, p_{i_2}, ..., p_{i_m}$, где $i_j \in I$ для всех $j = 1, 2, ..., m$.

Рассмотрим далее основные свойства предлагаемой схемы. Ключевой характеристикой схемы является ее вычислительная стойкость, которая напрямую зависит от значений используемых оснований. Следующее утверждение позволяет установить нижнюю границу для выбора оснований.

Утверждение 1. В предлагаемой схеме для любого неразрешенного подмножества участников с номерами $\tilde{I}$ следует, что $P > \tilde{P} = \prod_{i \in \tilde{I}} p_i$ при $p_1 > 2^{k-1}$.

Доказательство. Используя тот факт, что в пороговых СРС максимальным неразрешенным подмножеством является подмножество с номерами n, $n - 1$, ..., $n - k + 2$ и учитывая определение компактных последовательностей, получим

$$\tilde{P} < \prod_{i=0}^{k-2} p_{n-i} < (p_1 + p_1^{\theta})^{k-1} =$$

$$= p_1^{k-1}(1 + p_1^{\theta-1})^{k-1} < p_1^{k-1} 2^{k-1}.$$

Вместе с тем $P > p_1^k$. Отсюда

$$\frac{P}{\tilde{P}} > \frac{p_1^k}{p_1^{k-1} 2^{k-1}} = \frac{p_1}{2^{k-1}}.$$

Для соблюдения условия $P > \tilde{P}$ необходимо выполнение неравенства $P/\tilde{P} > 1$. Данное неравенство обязательно будет выполнено в случае, если выполнится неравенство $\frac{p_1}{2^{k-1}} > 1$, или, что равносильно, $p_1 > 2^{k-1}$. *Утверждение доказано.*

Иными словами, предлагаемая схема применима при выборе модуля p_1 на этапе генерирования параметров таким, что $p_1 > 2^{k-1}$.

Утверждение 2. Для предлагаемой схемы при объединении долей неразрешенного подмножества участников с номерами $\tilde{I}$ мощность множества перебора определяется выражением

$$f(\tilde{I}) = \left\lfloor \frac{P}{\tilde{\tilde{P}}} \right\rfloor,$$

где $\tilde{\tilde{P}} = \prod_{i \in \tilde{I}} p_i$.

Доказательство. Так как доли участников с номерами, принадлежащими $\tilde{I}$, известны, то на основе СОК, основаниями которой являются все числа p_{i_j} такие, что $i_j \in \tilde{I}$, можно восстановить число $\tilde{s} \equiv s \bmod \tilde{P}$. На основе последнего сравнения $s = a\tilde{P} + \tilde{s}$. Единственным неизвестным параметром секрета остается a. Именно множество всех возможных чисел a необходимо перебирать. Однако s определено в СОК с диапазоном P, следовательно, $0 \leqslant a\tilde{P} + \tilde{s} < P$, откуда

$$-\frac{\tilde{s}}{\tilde{\tilde{P}}} \leqslant a < \frac{P - \tilde{s}}{\tilde{\tilde{P}}}.$$

Принимая во внимание, что число s, а вместе с ним и число a, является целым неотрицательным числом, и так как $\tilde{s} < \tilde{\tilde{P}}$, получим

$$0 = \left\lceil -\frac{\tilde{s}}{\tilde{\tilde{P}}} \right\rceil \leqslant a \leqslant \left\lfloor \frac{P - \tilde{s}}{\tilde{\tilde{P}}} \right\rfloor = \left\lfloor \frac{P}{\tilde{\tilde{P}}} \right\rfloor.$$

То есть число a лежит в промежутке $\left[0, \left\lfloor \frac{P}{\tilde{\tilde{P}}} \right\rfloor\right]$, мощность которого равна

$$f(\tilde{I}) = \left\lfloor \frac{P}{\tilde{\tilde{P}}} \right\rfloor + 1.$$

Утверждение доказано.

Исследуем далее вопрос о том, как связаны мощности множеств перебора схемы Асмута—Блума и предлагаемой схемы при одинаковом выборе параметров СОК. Пусть схема Асмута—Блума определяется набором оснований $p_0 < p_1 < p_2 < ... < p_k < p_{k+1} < ... < p_n$. Для обеспечения асимптотической идеальности СРС Асмута—Блума потребуем, чтобы данная последовательность была компактной с начальным значением p_0, или $p_n < p_0 + p_0^{\theta}$ для $\theta \in (0, 1)$. При этом последовательность $p_1 < ... < p_n$ будет компактной с начальным значением p_1. Данную СОК будем использовать в качестве основы для предлагаемой СРС.

Мощность множества перебора Асмута—Блума константна и равна p_0. Обозначим $f(\tilde{I})$ мощность

множества перебора предлагаемой схемы. Значение $f(\tilde{I})$ можно получить из утверждения 2:

$$f(\tilde{I}) = \left\lfloor \frac{P}{\tilde{P}} \right\rfloor + 1.$$

Пусть далее $\tilde{I}_{\max}$ есть множество номеров неразрешенного подмножества с наибольшим диапазоном. Тогда, как было сказано ранее,

$$\tilde{P}_{\max} = \prod_{i=0}^{k-2} p_{n-i}.$$

Установим связь между значением $f(\tilde{I}_{\max})$ и k. Построим две СРС, в одной из которых возьмем в качестве порога k, в другой — $n - k + 1$. При этом положим, что $2 \leqslant k \leqslant \left\lfloor \frac{n}{2} \right\rfloor$. Рассчитаем $f(\tilde{I}_{\max})$ для второй СРС:

$$\frac{\prod_{i=1}^{n-k+1} p_i}{\prod_{i=0}^{n-k-1} p_{n-i}} = \frac{p_1 p_2 \cdots p_k p_{k+1} \cdots p_{n-k+1}}{p_{k+1} p_{k+2} \cdots p_{n-k+1} p_{n-k+2} \cdots p_n} =$$

$$= \frac{p_1 p_2 \cdots p_k}{p_{n-k+2} \cdots p_n} = \frac{\prod_{i=1}^{k} p_i}{\prod_{i=0}^{k-2} p_{n-i}}.$$

Выражение справа представляет собой значение $f(\tilde{I}_{\max})$ для первой СРС. Следовательно, значения $f(\tilde{I}_{\max})$ симметричны по k относительно значения $\left\lfloor \frac{n}{2} \right\rfloor$. Пусть теперь $2 \leqslant k < \left\lfloor \frac{n}{2} \right\rfloor$ и $k_1 = k + 1$. Пусть значение f_{k_1} равно значению $f(\tilde{I}_{\max})$ для СРС с порогом k_1. Оценим величину f_{k_1}:

$$f_{k_1} = \frac{\prod_{i=1}^{k_1} p_i}{\prod_{i=0}^{k_1-2} p_{n-i}} = \frac{\prod_{i=1}^{k+1} p_i}{\prod_{i=0}^{k-1} p_{n-i}} =$$

$$= \frac{p_{n-k+2}}{p_{k+1}} \frac{\prod_{i=1}^{k} p_i}{\prod_{i=0}^{k-2} p_{n-i}} = \frac{p_{n-k+2}}{p_{k+1}} f_k,$$

где f_k представляет собой значение $f(\tilde{I}_{\max})$ для СРС с порогом k. Так как $2 \leqslant k < \left\lfloor \frac{n}{2} \right\rfloor$, то $n - k + 2 > \left\lfloor \frac{n}{2} \right\rfloor$, следовательно, $n - k + 2 > k + 1$, учитывая ограничения, накладываемые на модули СОК, получим, что $p_{n-k+2} > p_{k+1}$, следовательно, $\frac{p_{n-k+2}}{p_{k+1}} > 1$. Учитывая сделанные ранее рассуждения, получим, что $f_{k_1} < f_k$. Иными словами, наихудшим случаем, в котором $f(\tilde{I}_{\max})$ принимает наименьшее значение, является случай $k = \left\lfloor \frac{n}{2} \right\rfloor$. Ввиду симметричности $f(\tilde{I}_{\max})$ относительно данного значения целесообразно рассматривать k в границах $\left[2, \frac{n}{2}\right]$, так как для промежутка $\left[\frac{n}{2}, n-1\right]$ рассуждения ведутся похожим образом. Особым случаем является СРС, в которой $k = n$. Для такой СРС $f(\tilde{I}_{\max}) = p_1$.

Докажем далее ряд важных утверждений, позволяющих достаточно точно оценить величину $f(\tilde{I}_{\max})$.

Утверждение 3. Для любой последовательности $p_1 < p_2 < \ldots < p_n$ следует, что

$$\frac{P}{\tilde{P}_{\max}} \leqslant p_1. \qquad (1)$$

Доказательство. Рассматривая $\tilde{P}_{\max}$, заметим, что так как последовательность p_i возрастает, то $p_k \leqslant p_n$, $p_{k-1} \leqslant p_{n-1}$, ..., $p_2 \leqslant p_{n-k+2}$. При этом равенства $p_i = p_{n-i+2}$, $i = 2, 3, \ldots, k$, достигаются только при $k = n$. Это означает, что

$$P' = \prod_{i=2}^{k} p_i \leqslant \tilde{P}_{\max}.$$

Так как $P = p_1 P'$, то $\frac{P}{\tilde{P}_{\max}} \leqslant p_1$. *Утверждение доказано.*

Выражение (1) показывает верхнюю границу для $f(\tilde{I}_{\max})$. Для оценки нижней границы $f(\tilde{I}_{\max})$ докажем следующее утверждение.

Утверждение 4. Для любой последовательности $p_1 < p_2 < \ldots < p_n$, такой, что $p_n < p_1 + p_1^{\theta}$, $0 < \theta < 1$, и любого k, такого, что $2 \leqslant k < \left\lfloor \frac{n}{2} \right\rfloor$, следует, что

$$\frac{P}{p_i \tilde{P}_{\max}} > \left(\frac{1}{1 + p_1^{\theta - 1}} \right)^{k-1}. \qquad (2)$$

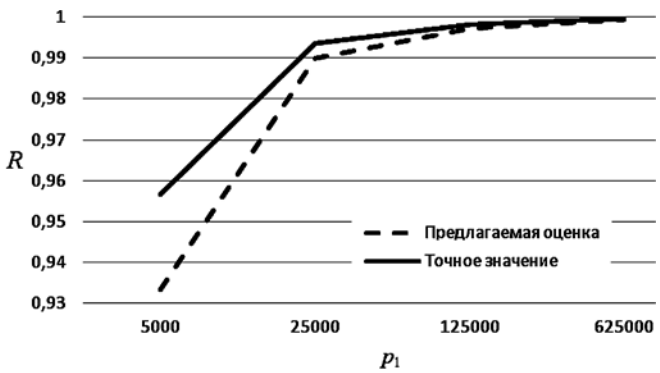
Доказательство. Так как последовательность компактна с начальным значением p_1, то $\tilde{P}_{\max} < (p_1 + p_1^{\theta})^{k-1}$. Вместе с тем, так как последовательность возрастает, то $P > p_1^k$. Следовательно

$$\frac{P}{\tilde{P}_{\max}} > \frac{p_1^k}{(p_1 + p_1^{\theta})^{k-1}} = p_1\left(\frac{p_1}{p_1 + p_1^{\theta}}\right)^{k-1} = p_1\left(\frac{1}{1 + p_1^{\theta-1}}\right)^{k-1},$$

откуда следует неравенство (2).

Утверждение доказано.

Основываясь на утверждениях 3 и 4, можно достаточно точно определить границы для величины $\frac{P}{\tilde{P}_{\max}}$, которые напрямую зависят от значения p_1. Рассмотрим далее конкретный пример, позволяющий увидеть, как быстро величина $\frac{P}{\tilde{P}_{\max}}$ сходится к p_1. На рисунке изображен график изменения величины $R = \frac{P}{p_1 \tilde{P}_{\max}}$ при выборе в качестве системы оснований СОК минимальных компактных последовательностей для различных значений p_1. Из графика видно, что при увеличении p_1 значение R приближается к 1 и, следовательно, $\frac{P}{\tilde{P}_{\max}}$ приближается к p_1. При этом предлагаемая оценка (2) позволяет оцепить величину R снизу. Утверждения 3 и 4 позволяют оценить степень близости $\frac{P}{\tilde{P}_{\max}}$ к p_1 в зависимости от заданных p_1, θ, k и n до этапа генерирования самой последовательности.



Оценка величины $R = \frac{P}{p_1 \tilde{P}_{\max}}$ в зависимости от значения p_1 при $n = 15$, $k = 7$

Доказанное утверждение 4 имеет важное значение для оценки вычислительной стойкости рассматриваемых пороговых схем. При фиксированных θ и k значение $\frac{P}{\tilde{P}_{\max}}$ находится в следующих границах:

$$p_1\left(\frac{1}{1 + p_1^{\theta-1}}\right)^{k-1} 1 < \frac{P}{\tilde{P}_{\max}} \leqslant p_1. \quad (3)$$

При этом легко показать, что для фиксированных $0 < \theta < 1$ и $2 \leqslant k \leqslant n$

$$\lim_{p_1 \to \infty}\left(\frac{1}{1 + p_1^{\theta-1}}\right)^{k-1} = 1 \text{ и } \frac{1}{1 + p_1^{\theta-1}} < 1.$$

Следовательно

$$\left(\frac{1}{1 + p_1^{\theta-1}}\right)^{k-1} = (1 - \varepsilon),$$

где $0 < \varepsilon < 1$. Причем, чем больше p_1, тем ближе ε к 0. Тогда из неравенства (3) следует

$$p_1(1 - \varepsilon) < \frac{P}{\tilde{P}_{\max}} \leqslant p_1.$$

На основании данного выражения можно получить следующую оценку для $f(\tilde{I}_{\max})$:

$$p_1 - [\varepsilon p_1] < f(\tilde{I}_{\max}) - 1 \leqslant p_1. \quad (4)$$

Последнее неравенство позволяет определить степень близости величины $f(\tilde{I}_{\max})$ к p_1 без генерации самой последовательности. Так как $p_1 > p_0$, то за счет всех ограничений, накладываемых на $\frac{P}{\tilde{P}_{\max}}$, получим, что с возрастанием числа p_0 мощность множества перебора предлагаемой схемы $f(\tilde{I}_{\max})$ будет приближаться к числу p_1. Можно сделать вывод, что мощность множества перебора для предлагаемой схемы разделения секрета при выборе достаточно больших модулей эквивалентна мощности множества перебора схемы Асмута— Блума, которая равна p_0.

Сопоставим теперь предлагаемую схему со схемой Миньотта. Базовым конструктивным требованием схемы Миньотта является включение секрета s в промежуток $\left(\alpha = \prod_{i=0}^{k-2} p_{n-i}, \beta = \prod_{i=1}^{k} p_i\right)$. Доказанные ранее утверждения относительно значения мно-

жества перебора предлагаемой схемы позволяют отойти от данного правила в пользу увеличения общего диапазона представления секрета. Основываясь на предположении равномерного распределения секрета в промежутке [0, P), компактности множества $p_0 < p_1 < ... < p_n$ и достаточно большом значении p_0, легко показать, что вероятность попадания секрета в промежуток [0, α) приближается к вероятности "угадать" произвольный секрет в схеме Асмута—Блума. Отметим, что в используемых обозначениях $\alpha = \widetilde{P}_{\max}$ и $\beta = P$. Действительно, область определения секрета в схеме Асмута—Блума равна Z_{p_0} и определяется значением p_0. При равномерном распределении секрета на данном множестве вероятность выбора произвольного секрета равна $1/p_0$. Вместе с тем, вероятность попадания числа в промежуток [0, α) = [0, $\widetilde{P}_{\max}$) равна $\frac{|[0, P_{\max})|}{|[0, P)|} = \frac{\widetilde{P}_{\max}}{P}$. Но согласно утверждению 3, при достаточно большом p_0 величина $\frac{P}{\widetilde{P}_{\max}}$ эквивалентна величине p_0.

Отсюда следует, что выбор параметров, определяющих предлагаемую СРС, позволяет уйти от ограничений, накладываемых на параметры схемы Миньотта. Равномерность распределения секрета может быть достигнута за счет предварительного шифрования информации. Рассмотрим далее примеры генерации параметров предлагаемой СРС на основе использования СОК.

Пример. Пусть $p_1 = 1024$, $n = 10$ и $k = 5$ и требуется, чтобы отклонение от мощности перебора Асмута—Блума не превышало 10 %. Определим, каким должно быть θ в данном случае. Согласно оценкам (3) и (4) получим

$$\theta < \log_{p_1}\left(\frac{1}{\sqrt[k-1]{1-\varepsilon}} - 1\right) + 1,$$

где ε есть требуемое отклонение. В нашем случае $\varepsilon = 0{,}05$. Подставив в формулу имеющиеся данные, получим $\theta < 0{,}477$. Следовательно, числа последовательности, обеспечивающей требуемую мощность множества перебора, должны попадать в промежуток [1024, 1051). Для данной СРС $f(\widetilde{I}_{\max}) > 921$. *Конец примера.*

Стоит отметить, что доказательство возможности генерирования компактных последовательностей на основе заданного начального значения является довольно сложной теоретико-числовой задачей. При этом, чем меньше у числа p_1 уникальных делителей, тем выгоднее его использовать в качестве основы для такой последовательности, так как при этом снижается количество чисел в промежутке от p_1 до $2p_1$, невзаимно простых с p_1. Генерирование компактных последовательностей есть предмет дальнейших исследований. На данный момент можно ограничиться лишь практическими рекомендациями, заключающимися в выборе в качестве p_1 числа достаточно большой величины и с наименьшим количеством делителей.

В данном пункте рассмотрена предлагаемая схема разделения секрета, основанная на использовании СОК. Утверждения 1—5 позволяют оценить качества каждой конкретной СРС. Во-первых, согласно утверждению 1, $p_1 > 2^{k-1}$. Таким образом, зафиксирована граница, начиная с которой, необходимо генерировать последовательность оснований. Отметим, что p_1 должно быть существенно больше числа 2^{k-1} для обеспечения максимальной вычислительной стойкости. Во-вторых, важным параметром схемы является величина θ, определяющая компактную последовательность. Чем ближе θ к нулю, тем лучше свойства СРС в плане вычислительной стойкости, что следует из утверждения 4 и неравенства (3).

Заключение

Важным свойством схемы является минимальная избыточность информации в процессе разделения секрета. Для СРС Асмута—Блума количество информации, получаемой в результате вычисления долей секрета, существенно превосходит количество информации, которое несет в себе сам секрет. Вместе с тем, предлагаемая схема способна разделить секрет величины P, при этом области определения долей секрета в свою очередь равны p_i для участника с номером i. Очевидно, что каждый участник получает доли гораздо меньшего размера, чем исходный секрет, в отличие от СРС Асмута—Блума. Оценка (4) позволяет сделать вывод, что при одинаковом выборе параметров СОК для предложенной схемы и схемы Асмута—Блума, их вычислительная стойкость совпадает. Важными условиями для генерирования системы оснований СОК являются выбор p_1 так, что $p_1 > 2^{k-1}$, и выбор θ как можно ближе к 0. Наиболее подходящим применением предложенной СРС является использование ее для хранения или передачи больших объемов информации, так как она ориентирована на многократное использование выбранных параметров. Одним из перспективных направлений будущей работы является разработка вычислительно эффективного метода генерирования набора оснований СОК по заранее заданным p_1, θ и k.

Работа выполнена при поддержке базовой части государственного задания СКФУ №2563.

Список литературы

1. **Shamir A.** How to share a secret // Communications of the ACM. 1979. N. 22 (11). P. 612—613.

2. **Червяков Н. И., Галушкин А. И., Евдокимов А. А., Лавриненко А. В., Лавриненко И. Н.** Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. 280 с.

3. **Asmuth C. A., Bloom J.** A Modular Approach to Key Safeguarding // IEEE Transactions on Information Theory. 1983. 29 (2). P. 208—210.

4. **Mignotte M.** How to Share a Secret // Lecture Notes in Computer Science. 1983. Vol. 149. P. 371—375.

5. **Quisquater M., Preneel B., Vandewalle J.** On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem. // Lecture Notes in Computer Science. 2002. Vol. 2274. P. 199—210.

6. **Barzu M., Tiplea F. L., Dragan C. C.** Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes // Information Sciences. 2013. N. 240. P. 161—172.

7. **Hsu C.-F., Harn L.** Multipartite Secret Sharing Based on CRT // Wireless Personal Communications. 2014. Vol. 78 (1). P. 271—282.

8. **Harn L., Fuyou M.** Weighted secret sharing based on the Chinese remainder theorem // International Journal of Network Security. 2007. Vol. 16 (6). P. 420—426.

9. **Liu Y., Harn L., Chang C.-C.** A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets // International Journal of Communication Systems. 2014. N. 28 (7). P. 1282—1292.

10. **Червяков Н. И.** Ускоренный алгоритм определения позиционных характеристик и его нейросетевая реализация // Нейрокомпьютеры: разработка, применение. 2001. № 10. С. 19—21.

11. **Червяков Н. И., Бабенко М. Г., Ляхов П. А., Лавриненко И. Н.** Эффективный алгоритм точного определения универсальной позиционной характеристики модулярных чисел и его применение для вычисления основных проблемных операций в системе остаточных классов // Инфокоммуникационные технологии. 2014. Т. 12. № 1. С. 4—18.

12. **Chervyakov N. I., Averbukh V. M., Babenko M. G., Lyakhov P. A., Gladkov A. V., Gapochkin A. V.** Approximate method of implementation non-modular operations in the residue number system // Fundamental research. 2012. N. 6. P. 189—193.

N. I. Chervyakov, Professor, Chief of Department
of Applied Mathematics and Mathematical Modeling, k-fmf-primath@stavsu.ru,
M. A. Deryabin, Postgraduate Student, Junior Researcher
of Department of Organization of Scientific Research, maxim.deryabin@gmail.com
North Caucasus Federal University, Stavropol

New Method of Threshold Secret Sharing Based on Residue Number System

This paper researches basic principle of constructing secret sharing schemes based on residue number system (RNS). Perfect and computational secrecy analysis of existing secret sharing schemes based on RNS is followed by a new approach to constructing a secret sharing scheme based on conversion of the secret to RNS. The main feature of the proposed method is the fact that the size of each share is small relatively to the size of the secret. Mentioned above feature results in effective data storage and transfer. Performed analysis has shown that using compact sequences of co-prime numbers as moduli set leads to computational secrecy of proposed scheme being close to the computational secrecy of Asmuth—Bloom scheme.

Keywords: *threshold secret sharing schemes, Chinese reminder theorem, residue number system, perfect schemes*

References

1. **Shamir A.** How to share a secrety, *Communications of the ACM*, 1979, no. 22 (11), pp. 612—613.

2. **Chervyakov N. I., Galushkin A. I., Evdokimov A. A., Lavrinenko A. V., Lavrinenko I. N.** *Primenenie iskusstvennyh nejronnyh setej i sistemy ostatochnyh klassov v kriptografii*, Moscow, Fizimatlit, 2012. 280 p.

3. **Asmuth C. A., Bloom J.** A Modular Approach to Key Safeguarding, *IEEE Transactions on Information Theory*, 1983, 29 (2), pp. 208—210.

4. **Mignotte M.** How to Share a Secret, *Lecture Notes in Computer Science*, 1983, vol. 149, pp. 371—375.

5. **Quisquater M., Preneel B., Vandewalle J.** On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem, *Lecture Notes in Computer Science*, 2002, vol. 2274, pp. 199—210.

6. **Barzu M., Tiplea F. L., Dragan C. C.** Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes, *Information Sciences*, 2013, no. 240, pp. 161—172.

7. **Hsu C.-F., Harn L.** Multipartite Secret Sharing Based on CRT, *Wireless Personal Communications*, 2014, vol. 78 (1), pp. 271—282.

8. **Harn L., Fuyou M.** Weighted secret sharing based on the Chinese remainder theorem, *International Journal of Network Security*, 2007, vol. 16 (6), pp. 420— 426.

9. **Liu Y., Harn L., Chang C.-C.** A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets, *International Journal of Communication Systems*, 2014, 28 (7), pp. 1282—1292.

10. **Chervyakov N. I.** Uskorennyj algoritm opredelenija pozicionnyh harakteristik i ego nejrosetevaja realizacija, *Nejrokomp'jutery: razrabotka, primenenie*, 2001, no. 10, pp. 19—21.

11. **Chervjakov N. I., Babenko M. G., Ljahov P. A., Lavrinenko I. N.** Jeffektivnyj algoritm tochnogo opredelenija universal'noj pozicionnoj harakteristiki moduljarnyh chisel i ego primenenie dlja vychislenija osnovnyh problemnyh operacij v sisteme ostatochnyh klassov, *Infokommunikacionnye tehnologii*, 2014, vol. 12, no. 1, pp. 4—18.

12. **Chervyakov N. I., Averbukh V. M., Babenko M. G., Lyakhov P. A., Gladkov A. V., Gapochkin A. V.** Approximate method of implementation non-modular operations in the residue number system, *Fundamental research*, 2012, no. 6, pp. 189—193.