ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056.52

АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА ДЛЯ РЕЗЕРВНОГО ХРАНЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Статья поступила в редакцию 31.03.2019, в окончательной варианте – 17.04.2019.

Носиров Зафаржон Амрулоевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

магистрант, ORCID https://orcid.org/0000-0001-6858-1241, https://elibrary.ru/author_profile.asp?authorid=964195, e-mail: nosirovzafar@outlook.com

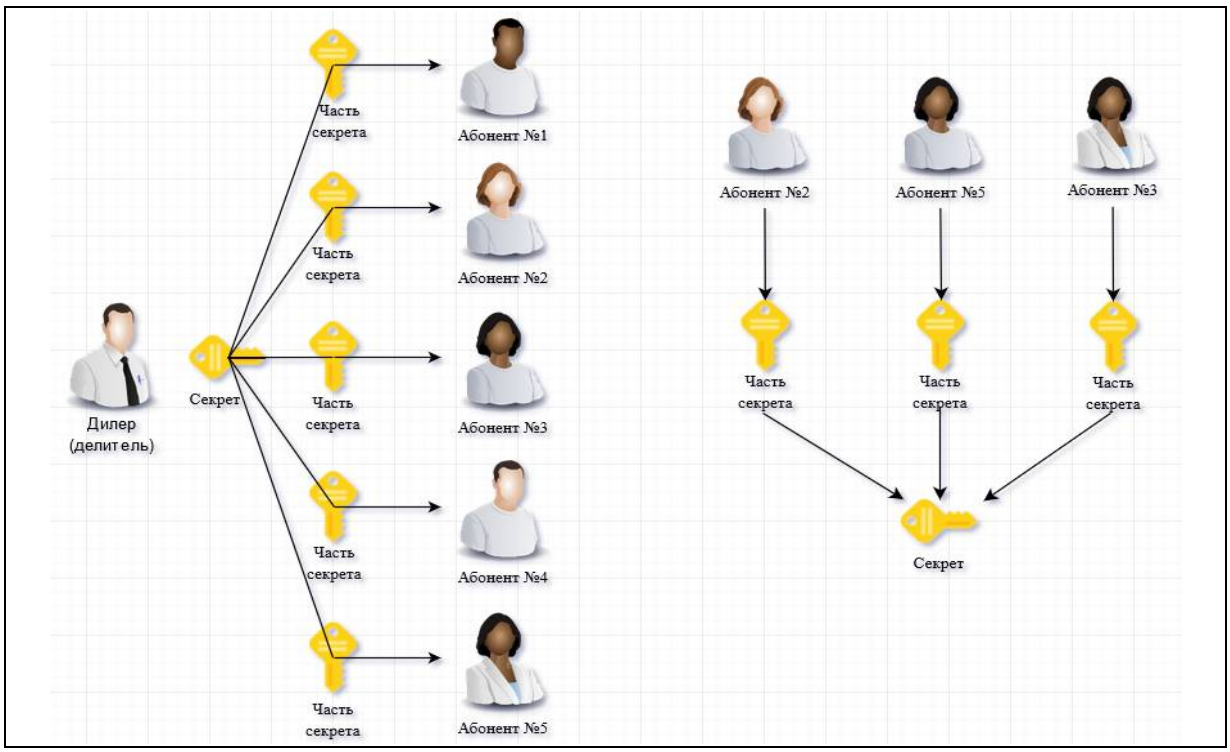
Щербинина Оксана Владимировна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

кандидат технических наук, доцент, https://elibrary.ru/author_items.asp?authorid=159547, e-mail: oksana@asu.edu.ru

В современных информационных системах организаций хранится и обрабатывается большой объем данных, защита которых предусматривает использование ключевой информации. В большинстве случаев в роли ключевой информации выступают различные пароли административного доступа, пин-коды и т.д. В случае их потери доступ к информационным системам может быть утрачен. Поэтому задачи безопасного хранения/восстановления ключевой информации являются актуальными. В статье рассмотрены основные способы решения проблем, связанных с утратой ключевой информации и ее востановлением: резервное копирование и хранение копий в различных местах; доверительное хранение ключевой информации несколькими абонентами; использование протоколов криптографического разделения секрета. Выявлено, что наиболее эффективным решением рассматриваемой проблемы является применение протоколов криптографического разделения секрета. Рассмотрены современные виды компьютерных атак на данные протоколы. Также проанализированы пороговые схемы разделения секрета, которые являются основой протоколов криптографического разделения секрета. Анализ пороговых схем проведен на основе таких параметров: совершенность, идеальность, ресурсоемкость, оценка сложности вычисления алгоритма. Выявлено, что пороговая схема Шамира является совершенной, идеальной и менее ресурсоемкой по сравнению с другими вариантами. Поэтому она может быть рекомендована как предпочтительный вариант решения задач хранения и восстановления ключевой информации.

Ключевые слова: схемы разделения секрета, разделение ключей, пороговые схемы разделения секрета, ключевая информация, восстановление ключевой информации, схема Шамира

Графическая аннотация (Graphical annotation)



ANALYSIS OF CRYPTOGRAPHIC SECRET SHARING SCHEMES FOR BACKING UP KEY INFORMATION

The article was received by editorial board on 31.03.2019, in the final version – 17.04.2019.

Nosirov Zafarzhon A., Astrakhan State University, 20a Tatishev St., Astrakhan, 414056, Russian Federation, undergraduate student, ORCID https://orcid.org/0000-0001-6858-1241, https://elibrary.ru/author_profile.asp?authorid=964195, e-mail: nosirovzafar@outlook.com

Shcherbinina Oksana V., Astrakhan State University, 20a Tatishev St., Astrakhan, 414056, Russian Federation,

Cand. Sci. (Engineering), Assistant Professor, https://elibrary.ru/author_items.asp?authorid=159547, e-mail: oksana@asu.edu.ru

Modern information systems of organizations store and process a large amount of data, which protection involves the used key information. In most cases, different passwords, PIN codes, etc., are used as key information. If they are lost, access to information systems may be lost. Therefore, the tasks of safe storage/recovery are relevant. The article describes the main ways to solve problems related to the loss key information: backup and storage copies in various places; confidential storage of key information by several subscribers; use cryptographic secret sharing protocols. It was revealed that the most effective solution to the problem under consideration is the use of cryptographic secret sharing protocols. Considered modern types of computer attacks on these protocols. Also analyzed threshold secret sharing schemes, which are the basis of cryptographic secret sharing protocols. The analysis of threshold schemes was carried out on the basis parameters as: perfect, ideal, resource-intensive, and an estimate of the complexity algorithm. It is revealed that the threshold scheme of Shamir is perfect, ideal and less resource-intensive in comparison with other options.

Keywords: secret sharing schemes, keys sharing, threshold secret sharing schemes, key information, backing up key information, Shamir's scheme

Введение. Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Она является системообразующим фактором жизни, активно влияющим на состояние безопасности различных направлений деятельности организаций и физических лиц. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности (ИБ), и в дальнейшем эта зависимость будет только возрастать [10]. Поэтому вопросы, связанные с методами (технологиями) защиты информации, являются чрезвычайно важными для обеспечения безопасного цифрового пространства. Зачастую такие вопросы приводят к сложным задачам разграничения коллективного доступа к информационным ресурсам.

Практически во всех современных информационных системах организаций хранится и обрабатывается большой объем данных, защита которых предусматривает использование ключевой информации (КИ). Чаще всего ключевой информацией являются секретные ключи для административного доступа, пароли, кодовые слова, секрет и т.д. При этом КИ обеспечивает конфиденциальность данных, и в случае ее утраты доступ к информационным системам может быть утрачен. Исходя из этого, возникает необходимость в обеспечении одного из основных сервисов ИБ – «доступности» – при утере КИ. Поэтому основной целью данной статьи является комплексный анализ вопросов, связанных с обеспечением безопасного хранения КИ и ее восстановления при необходимости.

Общая характеристика предметной области. Существуют различные способы решения рассматриваемой в статье проблемы (обеспечения возможностей восстановления КИ с соблюдением необходимых норм ИБ): резервное копирование ключевой информации и хранение копий в различных местах; доверительная передача КИ несколькими абонентами; использование протоколов криптографического разделения секрета (ПКРС). Однако каждый из этих способов имеет определенные недостатки. В работе [25] было проведено их сравнение, результаты которого представлены в таблице 1.

Таблица 1 – Сравнительный анализ способов резервного хранения КИ

Параметр	Использование резервного копирования	Доверие ключевой информации нескольким абонентам	Использование протоколов криптографического разделения секрета
Простота	+	+	–
Надёжность	+	–	+
Безотказность	–	–	+
Секретность	–	–	+

На основе анализа данных из таблицы 1 видно, что наиболее эффективным способом обеспечения доступности и конфиденциальности информации в случае утраты КИ является использование ПКРС, которые применяются для распределенного хранения данных.

Для понимания принципа работы ПКРС рассмотрим демонстрационный пример использования протоколов разделения секрета. Допустим, администратору ИБ какой-либо информационной системы (ИС) необходимо разделить КИ, состоящую из двенадцати символов, между четырьмя сотрудниками. Это необходимо для того, чтобы в случае отсутствия администратора ИБ по тем или иным причинам, сотрудники смогли оперативно получить доступ к ИС и провести необходимые неотложные операции. В данном случае администратор ИБ является диллером (делителем), а сотрудники – хранителями. Для того чтобы раздать каждому хранителю часть КИ, диллер делит КИ на количество хранителей. В нашем случае каждый сотрудник получит по четыре символа из КИ и номер позиции (группы символов), где должна располагаться эта часть. Зная номера позиций для частей КИ и содержания «фрагментов КИ», хранители, собравшись вместе, смогут полностью восстановить секрет при отсутствии дилера.

Представим числовой пример для описанной технологии (подхода). Пусть секретом является последовательность символов z@far2190429. Разделение секрета: 1-му сотруднику символы «429» и позиция № 4; 2-му сотруднику символы «ar2» и вторую позицию для группы символов; 3-му сотруднику символы «z@f» и позиция № 1; 4-му сотруднику символы «190» и позиция № 3.

Существенным недостатком данного подхода является то, что части секрета хранятся сотрудниками в открытом виде. Данный факт существенно влияет на уровень конфиденциальности информации.

В связи с этим недостатком рассмотренная технология разделения секрета практически не применяется для «рабочих» целей. Ее усовершенствование в принципе возможно, например, путем использования криптографических преобразований. Такая технология получила название ПКРС.

Однако в связи с бурным развитием информационных технологий ПКРС стали менее безопасными, так как появились новые виды компьютерных атак, направленных на взлом указанных протоколов [1]. В частности, это связано с тем, что, согласно результатам анализа, проведенного компанией Positive Technologies, при хранении паролей в информационных системах в большинстве случаев не используются защитные механизмы для их локального хранения/восстановления [25]. Поэтому можно утверждать, что анализ ПКРС с целью их совершенствования является весьма актуальной задачей.

Сравнительный анализ пороговых схем разделения секрета. В основе любого криптографического протокола лежит набор определенных правил, регламентирующих использование криптографического преобразования и алгоритмов в информационных процессах. В основе ПКРС может лежать алгоритм пороговой схемы разделения секрета (СРС).

Для использования пороговых СРС формируются группы участников, которые используются для хранения «частей» секрета. Пороговые СРС позволяют распределить секрет между абонентами (участниками) групп таким образом, чтобы легитимные абоненты могли однозначно восстановить секрет, а нелегетимные – не получали никакой дополнительной (по отношению к уже имеющейся) априорной информации о возможном содержании секрета [9].

В типичных случаях ПКРС включают в себя две основные фазы [12].

1. Разделение секрета – фаза раздачи, в рамках которой дилер (делитель), знающий секрет M, генерирует n долей $c_1, c_2, ..., c_n$ секрета и выдает каждому участнику его долю по защищенному каналу связи. Раздача организовывается таким образом, чтобы легитимные абоненты только при совместных действиях могли восстановить секрет, а нелегетимные – не могли.

2. Восстановление секрета – фаза, при которой легитимные абоненты могут объединить свои доли секретов и получить секрет. В большинстве рассматриваемых далее алгоритмов требуется обязательное участие в востановлении всех легитимных абонентов, между которыми была распределена «секретная» информация.

На рисунке приведена пороговая схема разделения секрета.

В ходе исследования были рассмотрены следующие пороговые СРС:

- СРС Шамира [26];
- СРС Блэкли [19];
- СРС, основанная на эллиптической кривой [7];
- СРС Карнина – Грина – Хеллмана [23];
- СРС Асмута – Блума [22].

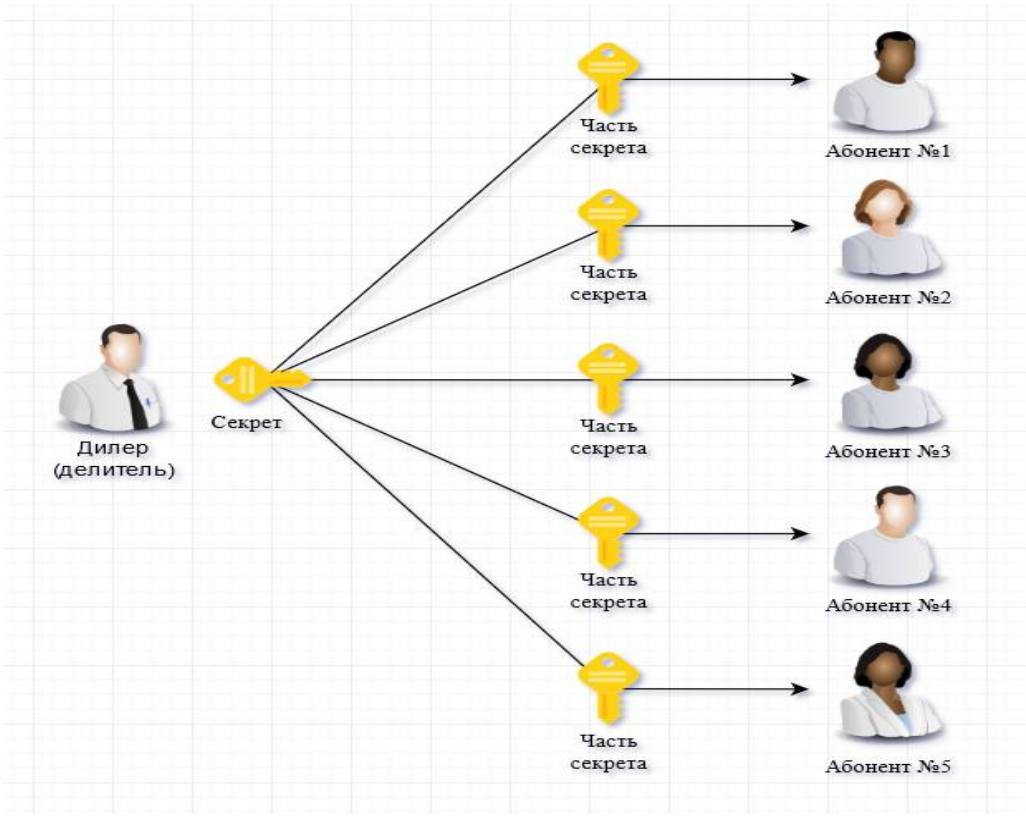


Рисунок – Схема классического протокола разделения секрета

С целью выявления наиболее эффективного ПКРС было решено провести их сравнительный анализ по следующим основным параметрам, вляющим на уровень безопасности использования алгоритмов:

1) сложность вычислений. Оценка сложности алгоритма складывается из оценок, получаемых на фазе разделения и восстановления секрета;

2) ресурсоемкость вычислений (количество памяти, используемой на этапах разделения и восстановления секрета);

3) совершенность (СРС является совершенной, если любое количество нелегитимных пользователей не может извлечь никакой информации о секрете) [14];

4) идеальность (СРС является идеальной, если размер доли секрета равен размеру самого секрета) [16].

В настоящей работе используются следующие обозначения:

- k – минимальное количество легитимных абонентов, необходимых для восстановления секрета;
- n – число долей, на которое делится секрет;
- p – большое простое число;
- Z_p – размерность простого модуля кольца целых чисел;
- M – секрет (ключевая информация).

Схема разделения секрета Шамира. Пороговая схема Шамира (k, n) построена вокруг концепции полиномиальной интерполяции [15]. Если необходимо разделить секрет таким образом, чтобы восстановить его могли только k абонентов, то нужно «спрятать» его в формулу многочлена степени (k-1). Восстанавливается этот многочлен по k точкам [3]. Проведем анализ сложности вычислений.

Фаза разделения секрета.

Шаг 1. На данном шаге выбирается случайное простое число p. Проверка числа на простоту является ресурсоемким процессом и существенно влияет на общую оценку сложности алгоритма. Оценка данного шага зависит от используемого алгоритма проверки числа на простоту. Для проверки простоты случайно выбранного числа использовался вероятностный тест Бейли – Померанца – Селфриджа – Уогстаффа [6]. Сложность этого шага равна $O(1)$ – усредненному значению взятому из работы [7].

Шаг 2. На данном шаге алгоритма для построения полинома над полем

Z_p выбирается ($k-1$) коэффициентов. Оценка сложности шага равна $O(k)$.

Шаг 3. Количество итераций для вычисления теней равна n, каждая итерация включает вложенный цикл, проходящий по ($k-1$) координатам. Общая оценка данного шага равна $O(k \cdot n)$ [17].

Шаг 4. Сложность данного шага зависит от количества участников, в нашем случае она равна n. За время $O(n)$ участникам раздаются доли секрета.

Так как $k < n < k$, то оценка сложности вычислений для разделения секрета составит $O(k \cdot n)$.

Фаза восстановления секрета. Процесс восстановления секрета осуществляется путем построения интерполяционного полинома Лагранжа. Общая оценка сложности алгоритма составляет $O(k \cdot n)+O(k^2)$ [4].

Анализ ресурсоемкости вычислений. Необходимое количество памяти оперативного запоминающего устройства для хранения долей секрета равно величине $n \cdot |m| + O(|m|)$, где $|m|$ – максимальная длина секрета M. Для разделения/восстановления секрета, при $n = k = 64$ понадобится около 8192 байт оперативной памяти.

Совершенность/идеальность. Схема Шамира является совершенной и идеальной. Идеальность следует из того, что размер секрета равен размеру p, как и размер доли секрета, полагающейся каждому участнику. Предположим, что секрет в схеме Шамира восстанавливается путем решения системы линейных уравнений. Нелегетимные абоненты должны составить систему из менее чем k уравнений с k неизвестными. Решением такой системы является множество точек, лежащих на гиперплоскости в k-мерном пространстве, а значит, никакое значение секрета не может быть отвергнуто как невозможное [5]. Следовательно, схема Шамира является совершенной.

Схема разделения секрета Блэкли. Схема Блэкли или векторная СРС основана на использовании точек многомерного пространства [20]. Любые две или более некомпланарных плоскостей пересекаются в пространстве и одна из координат точки пересечения является секретом. Если секрет закодировать как несколько координат точки, то уже по одной гиперплоскости можно будет получить какую-то информацию о секрете, то есть о взаимозависимости координат точки пересечения [18]. Проведем анализ сложности вычислений.

Фаза разделения секрета.

Шаг 1. Как и в схеме Шамира, оценка сложности данного шага зависит от алгоритма проверки простоты числа и составит $O(1)$.

Шаг 2. Сложность данного шага при выборе $(k–1)$ чисел составит $O(k)$.

Шаг 3. Для каждого из n участников определяется коэффициент d_i, и на каждой итерации необходим набор из k случайно сгенерированных чисел. Оценка вычислительной сложности шага составит $O(k \cdot n)$.

Шаг 4. Как и в схеме Шамира, для разделения долей секрета n участникам потребуется n итераций. За время $O(n)$ участникам раздаются доли секрета.

Фаза восстановления. Задача восстановления секрета реализуется путем решения систем линейных уравнений. Эффективным вариантом такого решения является использование метода Крамера, так как секретом является первая координата точки, полученная в результате решения [11].

Для восстановления секрета необходимо вычислить два определителя матриц с размерностью $k \times \cdot k$. Определители матриц определяются на основе метода Гаусса, и оценка сложности составляет $O(k^3)$ [4].

Общая оценка вычислительной сложности схемы Блэкли составляет $O(k \cdot n)+O(k^3)$.

Анализ ресурсоемкости вычислений. Число байт оперативной памяти, необходимой для разделения секрета на доли, оценивается величиной $n \times k \times |m|$. Для операций разделения/восстановления секрета при $n = k = 64$ понадобится около 266 Кбайт оперативной памяти.

Совершенность/идеальность. Так как размер каждой доли секрета в k раз превосходит размер секрета, то схема Блэкли не может быть идеальной. Однако она является совершенной, поскольку решением системы $(k–1)$ линейных сравнений с k неизвестными является множество решений, лежащих на гиперплоскости в k-мерном пространстве. Это означает, что секрет M может принимать любое значение из множества возможных секретов.

Схема разделения секрета, основанная на эллиптической кривой. Разделение секрета на эллиптической кривой происходит по алгоритму из [13], описанному ниже. Выполним анализ сложности вычислений.

Фаза разделения.

Шаг 1. Дилер выбирает эллиптическую кривую EC с необходимым количеством точек (не менее n). Каждому из участников СРС (в том числе хранителю секрета) ставится в соответствие точка на эллиптической кривой, включая «бесконечно удаленную».

Шаг 2. На этом шаге дилер выбирает многочлен степени n на этой кривой. Коэффициенты данного многочлена известны только ему. Точка на эллиптической кривой, которая обозначает участника – хранителя секрета, известна всем.

Шаг 3. Дилер подставляет координаты этой точки в выбранный им многочлен, вычисляет значение секрета.

Шаг 4. Для того чтобы каждому участнику раздать свою долю секрета, дилер подставляет координаты точки участника в многочлен, получая долю секрета для него. В итоге участник имеет точку на эллиптической кривой (ID) и долю секрета ($Secret$).

Общая оценка вычислительной сложности фазы разделения секрета в схемах, основанных на эллиптических кривых, составляет $O(k \cdot n)$.

Фаза восстановления. Для восстановления секрета нескольким участникам необходимо объединиться, чтобы восстановить коэффициенты выбранного дилером многочлена. Математически это сводится к решению некоторой системы уравнений. Участники, составляющие разрешенную коалицию, получают искомый многочлен. В него они подставляют координаты точки, обозначающей секрет. В итоге они получают секрет, который сформировал дилер. Оценка сложности вычислений фазы восстановления секрета в данной схеме равна $O(k^2)$.

Анализ ресурсоемкости вычислений. Так как объем оперативной памяти точки на эллиптической кривой не превышает объем, необходимый для хранения самого секрета, то схема наследует ресурсоемкость схемы Шамира [8]. Для восстановления секрета понадобится около 25 Кбайт памяти.

Совершенность/идеальность. Схемы, основанные на эллиптических кривых, являются совершенными, так как в предъявляемых нелегитимными пользователями долях секрета не может содержаться в совокупности никакой информации о секрете. Однако они не являются идеальными, так как размер каждой доли секрета в k раз превосходит размер секрета.

Схема разделения секрета Карнина – Грина – Хеллмана. Данная схема основана на решении систем алгебраических уравнений [20]. Проведем анализ сложности вычислений.

Фаза разделения. Для разделения секрета между n различными сторонами (участниками группы) так, чтобы минимум k сторон могли его восстановить, выбирается $(n+1)$ векторов V_i размерности k, также необходимо, чтобы ранг любой матрицы, составленной из k данных векторов, был равен k. Вектор V_0 известен всем участникам [11]. Секретом является скалярное произведение (u, V_0), где u – это набор векторов, а долями являются скалярные произведения (u, V_i). Сложность этапа разделения секрета на n частей равна $O(n)$.

Фаза восстановления. Для восстановления секрета по известным долям решается система из k уравнений для нахождения вектора u. Сложность данного этапа будет равна $O(k^3)$.

Анализ ресурсоемкости вычислений. Так как секрет представляется в виде матричного произведения 2-х векторов, то объем оперативной памяти для хранения координат векторов равен 64 байта. Для разделения секрета на доли при $n = 64$ понадобится $(2 \times \cdot n+1) \cdot 64 = 8256$ байт оперативной памяти.

Для восстановления секрета необходимо решить систему линейных алгебраических уравнений. Наилучшим вариантом для целочисленной арифметики является метод Крамера. Для вычисления значения необходимо вывить $(k+1)$ определителей матриц с размерностью $k \times k$. В итоге для восстановления секрета понадобится 8320 байт оперативной памяти.

Совершенность/идеальность. Схема Карнина – Грина – Хеллмана является совершенной, так как секрет M может принимать любое значение из множества возможных секретов. Однако она, так же как и схема, основанная на эллиптических кривых, не является идеальной, так как размер каждой доли секрета в k раз превосходит размер самого секрета.

Схема разделения секрета Асмута – Блума. Схема Асмута – Блума – пороговая схема разделения секрета, построенная с использованием простых чисел [16]. Позволяет разделить секрет между n сторонами таким образом, что его смогут восстановить любые k участников. Выполним анализ сложности вычислений.

Фаза разделения.

Шаг 1. Для (k, n) пороговой схемы выбирается простое число p.

Шаг 2. Затем выбираются числа, меньшие p – $d_1, d_2, \ldots, d_n$, для которых выполняются условия Асмута – Блума.

Оценка сложности вычислений фазы разделения секрета равна $O(n)$.

Фаза восстановления. Восстановить секрет возможно, объединив любые k теней (долей секрета), используя китайскую теорему об остатках, но это невозможно с помощью любых $(k-1)$ теней [21]. Оценка сложности вычислений фазы восстановления секрета равна $O(k^2)$.

Анализ ресурсоемкости вычислений. Каждое простое число d_i занимает объем оперативной памяти, равный 100 байт. Затем для проверки условий нахождения d_i потребуется $2 \times k \times |d_i|$ памяти, т.е. примерно 12,8 Кбайт. Для хранения в памяти одной доли секрета при $p = 28$ байт, $k = 64$ байт потребуется $|p|+|d_i|+|k_i|$ – это приблизительно 192 байта. В итоге для разделения секрета понадобится 57 кбайт оперативной памяти. Для восстановления секрета понадобится около 320 байт.

Совершенность/идеальность. Схема Асмута – Блума является совершенной потому, что секрет M может принимать любое значение из множества возможных секретов. Но она также не является идеальной, поскольку размер каждой доли секрета в k раз превосходит размер самого секрета.

До этого момента в статье были проанализированы пороговые СРС с точки зрения ресурсоемкости и сложности вычислений. Также важно рассмотреть виды атак на данные схемы, так как в связи с научно-техническим прогрессом нарушители изобретают (применяют) все более изощренные виды атак.

Виды атак на пороговые схемы разделения секрета. Компьютерная атака на пороговые СРС возможна, если в число k участников разделения секрета проник нарушитель.

У нарушителя имеется масса потенциальных возможностей обойти пороговую схему. Отметим, в частности, следующее [17].

1. Нарушитель может использовать неверную часть секрета (например, произвольное число) специально – тогда группа не сможет восстановить секрет. Однако установить, кто именно предъявил неверную часть, будет невозможно.

2. Нарушитель может спровоцировать начало процедуры разделения секрета, если ему удастся сойти за «своего». Тогда он сможет получить доли секрета остальных участников.

3) В $(k; n)$ пороговой схеме нарушитель может притвориться $(k+1)$ участником. Так как k участников будет достаточно для восстановления секрета, то нарушитель может предъявить в качестве своей доли секрета произвольную последовательность символов.

При этом нарушитель сможет узнать части секрета остальных легитимных абонентов, а затем воссоздать секрет полностью. Это является следствием неидеальности некоторых СРС.

Также существуют угрозы компьютерных атак на СРС по внешним каналам, когда нарушитель пытается извлечь полезную информацию из времени выполнения, кэширования, из сбоев приложения и т.д. Возможность проведения таких атак обычно связана с ошибками, допущенными при разработке программного обеспечения [2].

Обсуждение результатов. Результаты проведенного исследования показали, что применение ПКРС является наиболее эффективным способом хранения/восстановления ключевой информации. Также выявлено, что ПКРС подвержены современным видам компьютерных атак, которые значительно влияют на уровень информационной безопасности.

В таблице 2 показана сводка результатов сравнительного анализа пороговых схем разделения секрета.

Таблица 2 – Результаты сравнительного анализа пороговых СРС

Пороговая схема	Совершенность	Идеальность	Ресурсоемкость (Кбайт)	Оценка сложности
Схема Шамира	+	+	8	$O(n\cdot k)+O(k^2)$
Схема Блэкли	+	–	266	$O(n\cdot k)+O(k^3)$
Схема, основанная на эллиптической кривой	+	–	25	$O(n\cdot k)+O(k^2)$
Схема Карнина – Грина – Хеллмана	+	–	8,1	$O(n)+O(k^3)$
Схема Асмута – Блума	+	–	57	$O(n)+O(k^2)$

Из таблицы 2 можно сделать вывод, что схема Шамира обладает свойствами совершенности и идеальности, она также является менее ресурсоемкой по сравнению с другими схемами. По сложности вычислений схема Шамира уступает схеме Асмута – Блума. Однако приемущество по другим параметрам в данном случае является решающим.

Вывод. Результаты сравнительного анализа пороговых СРС свидетельствуют о том, что по комплексу показателей СРС Шамира является наиболее эффективной по сравнению с остальными. Поэтому данную схему целесообразно использовать как основу для последующей разработки защищенного ПКРС.

Библиографический список

1. Алферов А. П. Основы криптографии : учебное пособие / А. П. Алферов и др. – 3-е изд., испр. и доп. – Москва : Гелиос АРВ, 2005. – 480 с.

2. Аббасов А. Э. Оценка качества программного обеспечения для современных систем обработки информации / А. Э. Аббасов, Т. Э. Аббасов // Информационно-технологический вестник. – 2015. – Т. 5, № 3. – С. 15–27.

3. Алексейчук А. Н. Совершенные схемы разделения секрета и конечные универсальные алгебры / А. Н. Алексейчук // Анализ и обработка данных. – 2005.

4. Ващенко Г. В. Вычислительная математика. Основы алгебраической и тригонометрической интерполяции / Г. В. Ващенко // Современные проблемы науки и образования. – 2009. – № 1. – С. 54–55.

5. Лавриненко А. Н. Некоторые элементы концепции активной безопасности в современной криптографии / А. Н. Лавриненко, Н. И. Червяков // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. – 2014. – Т. 30, № 8-1 (179).

6. Мельман В. С. Методы анализа тестов простоты числа / В. С. Мельман, Ю. В. Шабля, Д. В. Кручинин // Электронные средства и системы управления. – 2016. – № 1-2. – С. 54–55.

7. Медведев Н. В. Почти пороговые схемы разделения секрета на эллиптических кривых / Н. В. Медведев, С. С. Титов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2011. – № 1 (23). – С. 91–95.

8. Молдовян А. А. Протоколы с нулевым разглашением секрета и обоснование безопасности схем цифровой подписи / А. А. Молдовян и др. // Вопросы защиты информации. – 2011. – № 4. – С. 6–11.

9. Могилевская Н. С. Пороговое разделение файлов на основе битовых масок: идея и возможное применение / Н. С. Могилевская, Р. В. Кульбикаян, Л. А. Журавлёв // Вестник Донского государственного технического университета. – 2011. – Т. 11, № 10. – С. 1749–1754.

10. Президент РФ. Стратегия национальной безопасности Российской Федерации. – Москва : Проспект, 2016. – 120 с.

11. Пьянов С. М. Сравнительный анализ стойкости некоторых классов схем разделения секрета / С. М. Пьянов // Магистерская диссертация по программе «Математическое и программное обеспечение защиты информации». – Москва : МГУ им. Ломоносова, 2013. – 67 с.

12. Петров А. Компьютерная безопасность. Криптографические методы защиты / А. Петров. – Москва : Litres, 2017. –140 с.

13. Пискова А. В. Разработка алгоритма электронной цифровой подписи, основанного на задачах факторизации и дискретного логарифмирования на эллиптических кривых / А. В. Пискова, А. Г. Коробейников // Сборник трудов IV Всероссийского конгресса молодых ученых. – Санкт-Петербург : Университет ИТМО, 2015. – С. 322–326.

14. Парватов Н. Г. Совершенные схемы разделения секрета / Н. Г. Парватов // Прикладная дискретная математика. – 2008. – № 2 (2). – С. 41–47.

15. Червяков Н. И. Новый метод порогового разделения секрета, основанный на системе остаточных классов / Н. И. Червяков, М. А. Дерябин // Информационные технологии. – 2016. – Т. 22, № 3. – С. 211–219.

16. Шенец Н. Н. Об идеальных модулярных схемах разделения секрета в кольцах многочленов от нескольких переменных / Н. Н. Шенец. – 2011. – Режим доступа: http://elib.bsu.by/handle/123456789/9565, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 20.03.2019).

17. Шнайер Б. Практическая криптография / Б. Шнайер, Н. Фергюсон – Москва : Диалектика, 2005. – 480 с.

18. Шарый С. П. Курс вычислительных методов / С. П. Шарый. – Новосибирск : Новосиб. гос. ун-т, 2012. – 420 с.

19. Bozkurt I. N. Threshold cryptography based on blakely secret sharing / I. N. Bozkurt , G. Selcuk // Information Sciences. – 2008. – P. 1–4.

20. Blakley G. R. Safeguarding cryptographic keys / G. R. Blakley et al. // Proceedings of the national computer conference. – 1979. – Vol. 48. – P. 313–317.

21. Dingyi P. Chinese remainder theorem: applications in computing, coding, cryptography / P. Dingyi, S. Arto, D. Cunsheng. – World Scientific, 1996.

22. Ito M. Secret sharing scheme realizing general access structure / M. Ito , A. Saito , T. Nishizeki // Electronics and Communications in Japan (Part III: Fundamental Electronic Science). – 1989. – Vol. 72, № 9. – P. 56–64.

23. Karnin E. On secret sharing systems / E. Karnin, J. Greene, M. Hellman // IEEE Transactions on Information Theory. – 1983. – Т. 29, № 1. – P. 35–41.

24. Kiparisova A. I. Providing access to information systems of higher education in the case of loss of key information / A. I. Kiparisova , I. M. Azhmuhamedov // Международный научно-исследовательский журнал. – 2016. – № 2-2 (44).

25. Positive Research. Актуальные киберугрозы: II квартал 2018 года // Positive Research Center. – 10.09.2018. – Режим доступа: http://blog.ptsecurity.ru/2018/09/cyberthreats-II-quarter-2018.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 20.03.2019).

26. Stadler M. Publicly verifiable secret sharing / M. Stadler // International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 1996. – P. 190–199.

References

1. Alferov A. P. et al. *Osnovy kriptografii : uchebnoe posobie* [Basics of cryptography : Tutorial]. 3-rd ed., rev. and add. Moscow, Gelios ARV Publ., 2005. 480 p.

2. Abbasov A. E., Abbasov T. E. Otsenka kachestva programmnogo obespecheniya dlya sovremennykh sistem obrabotki informatsii [Evaluation of software quality for modern information processing systems]. *Informatsionno-tekhnologicheskiy vestnik* [Information Technology Bulletin], 2015, vol. 5, no. 3, pp. 15–27.

3. Alekseychuk A. N. Sovershennye skhemy razdeleniya sekreta i konechnye universalnye algebry [Perfect secret separation schemes and finite universal algebras]. *Analiz i obrabotka dannykh* [Data Analysis and Processing], 2005.

4. Vashchenko G. V. Vychislitelnaya matematika. Osnovy algebraicheskoy i trigonometricheskoy interpolyatsii [Computational Mathematics. Basics of algebraic and trigonometric interpolation]. *Sovremennye problemy nauki i obrazovaniya* [Modern problems of Science and Education], 2009, no. 1, pp. 54–55.

5. Lavrinenko A. N., Chervyakov N. I. Nekotorye elementy kontseptsii aktivnoy bezopasnosti v sovremennoy kriptografii [Some elements of the concept of active security in modern cryptography]. *Nauchnye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika* [Scientific News of Belgorod State University. Series: Economy. Computer science], 2014, vol. 30, no. 8-1 (179).

6. Melman V. S., Shablya Yu. V., Kruchinin D. V. Metody analiza testov prostoty chisla [Methods for analyzing simplicity test numbers]. *Elektronnye sredstva i sistemy upravleniya* [Electronic Tools and Control Systems], 2016, no. 1-2, pp. 54–55.

7. Medvedev N. V., Titov S. S. Pochti porogovye skhemy razdeleniya sekreta na ellipticheskikh krivykh [Almost threshold secret separation schemes on elliptic curves]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of Tomsk State University of Control Systems and Radioelectronics], 2011, no. 1 (23).

8. Moldovyan A. A. et al. Protokoly s nulevym razglasheniem sekreta i obosnovanie bezopasnosti skhem tsifrovoy podpisi [Protocols with zero disclosure of the secret and the justification of the security of digital signature schemes]. *Voprosy zashhity informatsii* [Information Security Issues], 2011, no. 4, pp. 6–11.

9. Mogilevskaya N. S., Kulbikayan R. V., Zhuravlev L. A. Porogovoe razdelenie faylov na osnove bitovykh masok: ideya i vozmozhnoe primenenie [Threshold file sharing based on bit-masks: idea and possible use]. *Vestnik Donskogo gosudarstvennogo tekhnicheskogo universiteta* [Bullettin of the Don State Technical University], 2011, vol. 11, no. 10.

10. *Prezident RF. Strategiya natsionalnoy bezopasnosti Rossiyskoy Federatsii* [President of the Russin Federation. National Security Strategy of the Russian Federation]. Moscow, Prospekt Publ., 2016.

11. Pyanov S. M. Sravnitelnyy analiz stoykosti nekotorykh klassov skhem razdeleniya sekreta [Comparative analysis of the resistance of some classes of secret separation schemes]. *Magisterskaya dissertatsiya po programme «Matematicheskoe i programmnoe obespechenie zashchity informatsii»* [Master's thesis in the program «Mathematical and software information protection»], 2013. 67 p.

12. Petrov A. *Kompyuternaya bezopasnost. Kriptograficheskie metody zashchity* [Computer security. Cryptographic methods of protection]. Moscow, Litres Publ., 2017. 114 p.

13. Piskova A. V., Korobeynikov A. G. Razrabotka algoritma elektronnoy tsifrovoy podpisi, osnovannogo na zadachakh faktorizatsii i diskretnogo logarifmirovaniya na ellipticheskikh krivykh [Development of an electronic digital signature algorithm based on the problems of factorization and discrete logarithmization on elliptic curves]. *Sbornik trudov IV Vserossiyskogo kongressa molodykh uchenykh* [Proceedings of the IV All-Russian Congress of Young Scientists]. St. Petersburg, ITMO University Publ., 2015, pp. 322–326.

14. Parvatov N. G. Sovershennye skhemy razdeleniya sekreta [Perfect secret sharing schemes]. *Prikladnaya diskretnaya matematika* [Applied Discrete Mathematics], 2008, no. 2 (2), pp. 41–47.

15. Chervyakov N. I., Deryabin M. A. Novyy metod porogovogo razdeleniya sekreta, osnovannyy na sisteme ostatochnykh klassov [New method of threshold secret separation, based on the system of residual classes]. *Informatsionnye tekhnologii* [Information Technologies], 2016, vol. 22, no. 3, pp. 211–219.

16. Shenets N. N. Ob idealnykh modulyarnykh skhemakh razdeleniya sekreta v koltsakh mnogochlenov ot neskolkikh peremennykh [On the ideal modular secret separation schemes in polynomial rings of several variables], 2011. Available at: http://elib.bsu.by/handle/123456789/9565 (accessed 20.03.2019).

17. Shnayer B., Fergyuson N. *Prakticheskaya kriptografiya* [Practical cryptography]. Moscow, Dialektika, 2005. 480 p.

18. Sharyy S. P. *Kurs vychislitelnykh metodov* [The course of computational methods]. Novosibirsk, Novosibirsk State University Publ., 2012.

19. Bozkurt I. N., Selcuk G. Threshold cryptography based on blakely secret sharing. *Information Sciences*, 2008, pp. 1–4.

20. Blakley G. R. et al. Safeguarding cryptographic keys. *Proceedings of the national computer conference*, 1979, vol. 48, pp. 313–317.

21. Dingyi P., Arto S., Cunsheng D. *Chinese remainder theorem: applications in computing, coding, cryptography*. World Scientific, 1996.

22. Ito M., Saito A., Nishizeki T. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 1989, vol. 72, no. 9, pp. 56–64.

23. Karnin E., Greene J., Hellman M. On secret sharing systems. *IEEE Transactions on Information Theory*, 1983, vol. 29, no. 1, pp. 35–41.

24. Kiparisova A. I., Azhmuhamedov I. M. Providing access to information systems of higher education in the case of loss of key information. *Mezhdunarodnyy nauchno-issledovatelskiy zhurnal* [International Research Journal], 2016, no. 2-2 (44).

25. Positive Research. Aktualnye kiberugrozy: II kvartal 2018 goda [Current cyber threats: II quarter of 2018]. *Positive Research Center*. 10.09.2018. Available at: http://blog.ptsecurity.ru/2018/09/cyberthreats-II-quarter-2018.html (accessed 20.03.2019).

26. Stadler M. Publicly verifiable secret sharing. *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1996, pp. 190–199.