МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Пороговая схема разделения мультисекрета

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Цыпина Андрея Алексеевича

Научный руководитель
к. ф.-м. н., доцент _____ В. Е. Новиков
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

В информационных системах защита важной информации, в частности, такой как криптографические ключи, коды доступа или уникальные биометрические данные, является задачей первостепенной важности. Традиционный подход к хранению подобной информации подразумевает ее концентрацию в одном хранилище. Такой метод, несмотря на свою простоту, создает фундаментальную уязвимость, известную как единая точка отказа. Компрометация или физическое уничтожение этого единственного хранилища приводит к безвозвратной потере секрета или его попаданию в руки злоумышленника, что в обоих случаях является нежелательным событием.

Простое дублирование секрета на нескольких носителях не решает проблему кардинально, а лишь увеличивает "поверхность атаки" — теперь для компрометации достаточно получить доступ к любой из копий. С другой стороны, утрата даже одной из копий может быть некритичной, но управление согласованностью и безопасностью множества идентичных копий порождает новые сложности.

Схемы разделения секрета были предложены как элегантное и математически строгое решение этой дилеммы. Впервые независимо разработанные Ади Шамиром[1] и Джорджем Блэкли[2] в 1979 году, эти схемы предлагают метод распределения секрета среди группы участников таким образом, чтобы только авторизованные подмножества (коалиции) этой группы могли его восстановить.

Пусть S — это секрет, некоторое конечное сообщение. Схема разделения секрета — это метод, позволяющий дилеру разделить секрет S на n долей, которые распределяются между некоторым числом участников, так чтобы схема удовлетворяла двум фундаментальным свойствам:

[1] Shamir, A. How to Share a Secret / A. Shamir // Communications of the ACM. — 1979. — Vol. 22, No. 11. — P. 612–613.
[2] Blakley, G. R. Safeguarding Cryptographic Keys / G. R. Blakley // Proceedings of the National Computer Conference. — 1979. — Vol. 48. — P. 313–317.

1) любая авторизованная коалиция участников может объединить свои доли для однозначного восстановления секрета S;

2) любая неавторизованная коалиция участников не может получить никакой информации о секрете S из своих долей.

Основное назначение схем разделения секрета заключается в распределении доверия и повышении отказоустойчивости[3,4,5]. Вместо того чтобы полагаться на надежность одного хранителя или одной системы хранения, ответственность распределяется между несколькими участниками. Это позволяет системе выдерживать как отказы (случайную утерю долей), так и компрометацию (утечку долей к злоумышленнику) определенного числа участников без ущерба для безопасности или доступности секрета.

Наиболее известным и широко применяемым классом являются (k, n)-пороговые схемы, где $1 \leq k \leq n$. В такой схеме любая группа, предоставляющая k и более долей является авторизованной, в противном случае группа не является авторизованной. Параметр k называется порогом.

Формально, пусть Γ — это множество всех авторизованных подмножеств участников (так называемая структура доступа)[6]. Для (k, n)-пороговой схемы структура доступа определяется как:

$\Gamma = \{A \subseteq \mathcal{P} \mid |A| \geq k\}$, где $|A|$ – число долей группы участников A, $\mathcal{P}$ – множество участников.

В рамках такой схемы достигаются две ключевые цели:

1) секрет может быть восстановлен даже при утере до $(n - k)$ долей;

2) злоумышленник, собравший до $(k - 1)$ долей, не получает никакой информации о секрете.

---

[3] Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер ; пер. с англ. — Москва : Триумф, 2002. — 816 с.

[4] Beimel, A. Secret-Sharing Schemes: A Survey / A. Beimel // Coding and Cryptology (IWCC 2011) : Lecture Notes in Computer Science. — Springer, 2011. — Vol. 6639. — P. 11–46.

[5] Menezes, A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. — Boca Raton : CRC Press, 1996. — 816 p.

[6] Benaloh, J. Generalized Secret Sharing and Monotone Functions / J. Benaloh, J. Leichter // Advances in Cryptology — CRYPTO ’88 : Proceedings : Lecture Notes in Computer Science. — Springer, 1990. — Vol. 403. — P. 27–35.

Введем обозначения: $\mathcal{S}$ – множество всех возможных секретов, $S, S' \in \mathcal{S}$, $\{s_i\}$ – доли секрета S', $A \subseteq \mathcal{P}$ – некоторая группа участников. Если доля $\{s_i\}$ достается участнику из группы A, то обозначаем $\{s_i\} \in A$. Схема разделения секрета называется совершенной, если для любой неавторизованной коалиции $A \notin \Gamma$ условная вероятность получения конкретного значения секрета S' при наличии их долей $\{s_i\}$ равна априорной вероятности этого значения[7]:

$$\forall A \notin \Gamma, \forall \{s_i\} \in A, \forall S' \in \mathcal{S}: P(S = S' \mid \{s_i\} \in A) = P(S = S')$$

Это означает, что знание долей неавторизованной группой не дает абсолютно никакой новой информации о секрете. Схема Шамира, основанная на интерполяции полиномов над конечным полем, является классическим примером совершенной пороговой схемы.

Схемы разделения секрета находят применение во множестве задач. В частности:

1) управление криптографическими ключами — защита мастер-ключей, корневых сертификатов и ключей шифрования баз данных; доступ к ключу требует кворума администраторов, что позволяет исключить доверие к одному лицу;

2) пороговая криптография — распределённое выполнение операций расшифрования или цифровой подписи, когда ни один участник в одиночку не может выполнить криптографическую операцию;

3) безопасные многопартийные вычисления — совместная обработка конфиденциальных входных данных несколькими организациями без их раскрытия друг другу;

4) распределённое хранение данных — повышение надёжности и конфиденциальности в облачных хранилищах за счёт разнесения долей по различным серверам и провайдерам.

[7] Stinson, D. R. Cryptography : Theory and Practice / D. R. Stinson, M. B. Paterson. — 4th ed. — Boca Raton : Chapman and Hall/CRC, 2018. — 598 p.

Во многих практических сценариях требуется работать не с одним секретом, а с целым набором взаимосвязанных секретов: несколькими ключами, параметрами протокола, фрагментами конфигурации и т.п. Наивный подход — запускать пороговую схему отдельно для каждого секрета — приводит к линейному росту объёма данных и усложняет управление долями. Более эффективным решением являются пороговые схемы разделения мультисекрета, в которых в рамках одной конструкции одновременно разделяется набор $s_1, \dots, s_m$, причём каждый секрет может быть восстановлен независимо, при участии не менее чем t доверенных лиц, и раскрытие одного секрета не даёт информации о остальных.

Актуальность темы данной работы обусловлена тем, что пороговые схемы разделения мультисекрета позволяют более эффективно и гибко организовать распределённое хранение и использование ключевой информации по сравнению с независимым применением классической схемы Шамира для каждого секрета.

Объектом исследования в работе являются пороговые схемы разделения секрета.

Предметом исследования — пороговая схема разделения мультисекрета, основанная на многочлене от двух переменных над конечным полем, и методы её алгоритмической и программной реализации для экспериментальной проверки.

Целью дипломной работы является исследование пороговой схемы разделения мультисекрета, основанной на многочлене от двух переменных над конечным полем, и разработка программного прототипа для проверки корректности и оценки практических характеристик схемы.

Для достижения поставленной цели в работе решаются следующие задачи:

1) изучить теоретические основы конечных групп, колец и полей, а также полиномов над конечными полями, необходимые для понимания схем разделения секрета;

2) рассмотреть классические схемы разделения секрета, проанализировать их свойства и ограничения;

3) изучить пороговую схему разделения мультисекрета на основе многочлена от двух переменных и формулы Лагранжа;

4) разработать алгоритмы генерации долей и восстановления мультисекрета, определить требования к выбору параметров схемы и реализовать их в виде программного прототипа;

5) оценить влияние параметров схемы на объём данных и точность восстановления секрета.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 64 страницы, из них 40 страниц – основное содержание, включая 14 рисунков и 2 таблицы, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 «Теоретические основы схем разделения секрета» изложены математические понятия, необходимые для описания и реализации пороговых схем разделения секрета и их обобщения на случай нескольких секретов. В подразделе 1.1 приведены основные определения теории конечных групп, используемые далее при рассмотрении алгебраических структур с обратимыми операциями. В подразделе 1.2 рассматриваются конечные кольца и конечные поля, вводится поле $GF(q)$ и поясняется практический смысл выбора простого модуля q при реализации вычислений, а также необходимость корректного выполнения операций деления как умножения на обратный элемент. В подразделе 1.3 рассматриваются многочлены над конечными полями и формулируются результаты об интерполяции многочленов по заданным значениям, включая интерполяцию Лагранжа, используемую при восстановлении секрета в пороговых схемах. Отдельно обсуждаются многочлены от двух переменных и возможность построения бивариантной функции по набору «срезов», что является теоретической основой дальнейшей мультисекретной конструкции.

Введённый математический аппарат (конечные поля, обратимые операции и интерполяция многочленов) задаёт основу для строгого описания классических пороговых схем и позволяет перейти к построению мультисекретной схемы на базе многочлена двух переменных.

В разделе 2 «Классические схемы разделения секретов» рассмотрены основные подходы к пороговому разделению секрета и их ключевые идеи. В подразделе 2.1 описана векторная схема Блэкли с геометрической интерпретацией долей и восстановлением секрета по пересечению гиперплоскостей. В подразделе 2.2 рассмотрена схема Асмута–Блума, основанная на модулярной арифметике и восстановлении по системе сравнений. В подразделе 2.3 рассмотрена схема Миньотта, в которой пороговое свойство

обеспечивается выбором модулей и применением китайской теоремы об остатках. В подразделе 2.4 описана схема Карнина–Грина–Хеллмана и подчёркнуты общие принципы порогового построения: использование случайности и невозможность гарантированного восстановления при недостаточном числе долей. В подразделе 2.5 подробно рассмотрена схема Шамира, где доли формируются как значения многочлена над конечным полем, а восстановление секрета осуществляется интерполяцией Лагранжа при наличии не менее t долей. Показано, что именно полиномиальный подход является наиболее удобной базой для обобщения на случай нескольких секретов.

Классические схемы демонстрируют разные способы реализации порогового свойства, однако наиболее универсальным для дальнейших обобщений является полиномиальный подход, в котором восстановление естественно сводится к интерполяции над конечным полем.

В разделе 3 «Пороговая схема разделения мультисекрета» изложен основной результат работы — протокол разделения и восстановления нескольких секретов в рамках одной пороговой конструкции, а также программная реализация данного протокола. В подразделе 3.1 описана схема, в которой одновременно разделяется набор секретов $s_1, \dots, s_m$ и обеспечивается их независимое восстановление при участии не менее чем t долей.

Следующий протокол реализует пороговую схему разделения мультисекрета:

Генерация параметров схемы.

q – большое простое число. Задается n – количество долей, t – пороговое значение.

Выбираются различные ненулевые элементы $\alpha_1, \dots, \alpha_n \in GF(q)$ – метки долей, и пусть также выбраны попарно различные ненулевые $\beta_1, \dots, \beta_m \in GF(q)$ – метки секретов.

Разделение мультисекрета.

Дилер обладает набором секретов $s_1, \dots, s_m \in GF(q)$. Для каждого s_i дилер случайным образом выбирает коэффициенты $a_{i1}, \dots, a_{it-1} \in GF(q)$ и формируются многочлены

$$L_i(y) = s_i + a_{i1}y + a_{i2}y^2 + \cdots + a_{it-1}y^{t-1}, i = 1, \dots m.$$

По набору этих многочленов строится единственный многочлен от двух переменных $F(x, y) \in GF(q)[x, y]$, степени не выше $t-1$ по каждой переменной, для которого выполняется условие:

$$F(\beta_i, y) = L_i(y), i = 1, \dots m.$$

Многочлен строится следующим образом:

$$F(x, y) = \sum_{i=1}^{m} l_i(x) * L_i(y), \text{где } l_i(x) = \frac{\prod_{j \neq i} x - \beta_j}{\prod_{j \neq i} \beta_i - \beta_j}. \qquad (1)$$

Покажем, что при этом будет выполняться следующие равенства: $s_1 = F(\beta_1, 0), \dots, s_m = F(\beta_m, 0)$.

Отметим свойство базиса Лагранжа для метки произвольного секрета s_k:

$$l_i(\beta_k) = \begin{cases} 1, & \text{если } k = i \\ 0, & \text{если } k \neq i \end{cases}.$$

Подставим в (1) $x = \beta_k, y = 0$:

$$F(\beta_k, 0) = \sum_{i=1}^{m} l_i(\beta_k) * L_i(0).$$

По вышеназванному свойству базиса Лагранжа все множители $l_i(\beta_k)$ равны нулю, кроме случая $i = k$.

$$F(\beta_k, 0) = \sum_{i=1}^{t} \begin{cases} 1 * L_k(0), & \text{если } k = i \\ 0 * L_i(0), & \text{если } k \neq i \end{cases} = L_k(0).$$

По построению $L_k(0) = s_k$.

Для каждого участника дилер вычисляет:

$$f_i(x) = F(x, \alpha_i)$$

и передает ему долю – $(\alpha_i, f_i(x), q, \beta_1, \dots, \beta_m)$.

Этап восстановления мультисекрета.

Допустим, группа собрала t долей и решила восстановить секрет s_r из набора секретов.

Каждый участник вычисляет $z_i = f_i(\beta_r) = F(\beta_r, \alpha_i) = L_r(\alpha_i)$.

1. Участники обмениваются (или передают реконструктору) своими параметрами (α_i, z_i).
2. После обмена значениями z_i секрет s_r восстанавливается по формуле интерполяции Лагранжа:

$$L_r(0) = s_r = \sum_{1 \le i \le t} z_i * \prod_{1 \le k \le t, k \ne i} \frac{\alpha_k}{\alpha_k - \alpha_i}.$$

Полученное значение s_r является исходным секретом.

В подразделе 3.2 описан программный прототип на языке Python, реализующий генерацию долей, получение индивидуальных долей для выбранного секрета и восстановление секрета из порогового набора долей.

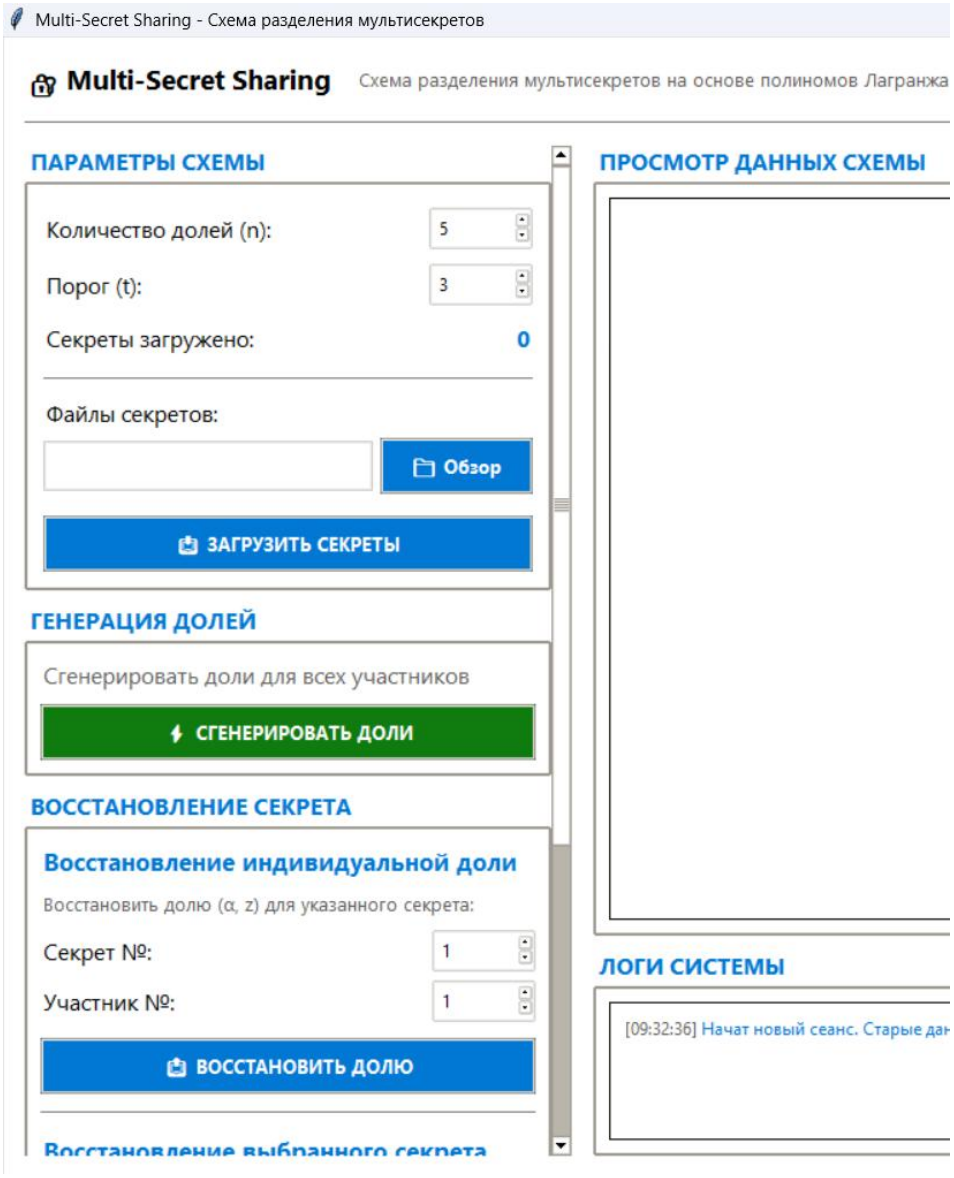

Рисунок 1 – Основное окно программы

Приводятся результаты экспериментальной проверки: демонстрируется корректное восстановление при достаточном числе долей и некорректный результат при попытке восстановления при числе долей меньше порога.

ЗАКЛЮЧЕНИЕ

В данной работе была рассмотрена и реализована пороговая схема разделения мультисекрета, основанная на алгебраических свойствах конечных полей. На теоретическом уровне были последовательно введены необходимые понятия теории групп и полей, описаны классические схемы разделения секрета и показано, как данные идеи обобщаются на случай нескольких секретов с использованием многочлена от двух переменных. Изучение схемы Шамира сыграло ключевую роль, позволив понять основной смысл работы: принцип кодирования секрета в коэффициенты полинома, пороговое восстановление с помощью интерполяции Лагранжа и фундаментальное значение выбора конечного поля для обеспечения безопасности и корректности.

Практическим результатом работы стала реализация программного прототипа, позволяющего выполнять генерацию долей и восстановление мультисекрета, а также проводить тестирование корректности протокола при различных параметрах и наборах долей. Реализация может использоваться как основа для дальнейших исследований и развития прикладных решений распределённого хранения секретов.