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

Рамп-схемы разделения секрета

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Дусалиева Тахира Ахатовича

Научный руководитель		
к. ф.-м. н., доцент	___________	В. Е. Новиков
	19.01.2026 г.	
Заведующий кафедрой		М. Б.
д. ф.-м. н., профессор	___________	Абросимов
	19.01.2026 г.	

Саратов 2026

ВВЕДЕНИЕ

Проблема безопасного и надёжного хранения конфиденциальной информации, такой как криптографические ключи, биометрические данные или государственные секреты, остаётся одной из фундаментальных задач криптографии на протяжении десятилетий. Традиционный подход с хранением секрета в единственном месте создаёт критическую уязвимость – «единую точку отказа», компрометация которой ведёт к полной потере защищаемых данных. Исторически предпринимались попытки решения через механические аналогии, однако они приводили к комбинаторному взрыву сложности, делающему их непригодными на практике.

Решением стали пороговые схемы разделения секрета, обеспечивающие совершенную секретность и устранение комбинаторного взрыва сложности. Однако на практике требование совершенной безопасности часто вступает в конфликт с требованиями к вычислительной и хранимой избыточности, особенно при работе с большими объемами данных. В связи с этим в последние десятилетия значительный интерес вызвали рамп-схемы, предлагающие управляемый компромисс между уровнем защищённости и эффективностью.

Актуальность и новизна работы обусловлена растущей потребностью в практичных криптографических примитивах для распределённого хранения больших данных (например, ключевых материалов, биометрических шаблонов, конфиденциальных документов). Рамп-схемы, предлагая настраиваемый баланс между безопасностью и производительностью, представляют собой перспективное направление развития криптографии. В данной работе проводится систематический анализ и реализация линейных рамп-схем на основе классических конструкций Шамира и Блэкли, что позволяет не только углубить теоретическое понимание их свойств, но и оценить их практическую применимость.

Данная работа опирается на фундаментальные результаты Шамира [2] и Блэкли [3], а также на последующие исследования в области рамп-схем, в частности, работы Блэкли и Медоуза [4] и унифицированный алгебраический подход Котари [6]. Практическая часть работы развивает идеи, изложенные в учебных пособиях [5] и руководствах по реализации [8].

Целью работы является систематическое исследование, формализация и практическая реализация рамп-схем разделения секрета на базе классических конструкций Шамира и Блэкли.

Для достижения поставленной цели решаются следующие задачи:

1. Провести анализ классических пороговых схем разделения секрета и выявить их ограничения.

2. Исследовать теоретические основы (d, k, n) рамп-схем.

3. Исследовать жёсткие линейные рамп-схемы разделения секрета на базе конструкций Шамира и Блэкли.

4. Разработать программный пакет на языке Python, с помощью которого можно провести протокол разделения секрета на основе рамп-схемы исследуемых рамп-схем на языке Python с веб-интерфейсом для наглядной демонстрации их работы.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 57 страниц, из них 49 страниц – основное содержание, включая 20 рисунков и 1 таблицу, список использованных источников из 10 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 рассматривается фундаментальная проблема разделения секрета и пороговые (k, n) схемы, в частности схемы Шамира и Блэкли, которые служат основой для развития более общей концепции – (d, k, n) рамп-схем разделения секрета.

Пусть имеются несколько участников схемы, между которыми требуется разделить некоторый секрет s, и некоторый доверенный участник T, называемый *дилером*, который разделяет s на *множество долей секрета* $S = \{s_1, \dots, s_n\}$ размерности n. Назовём *порогом* натуральное число k, не большее чем n (т.е. $1 \leq k \leq n$). Каждый участник получает от дилера некоторое число долей s_i, которые неизвестны остальным участникам.

Определение 1.1. Система называется (k, n) пороговой схемой разделения секрета, если выполнены следующие условия [5]:

- *условие корректности:* секрет s легко может быть вычислен по произвольному k-элементному подмножеству множества S;
- *условие совершенности:* секрет s нельзя вычислить ни по какому $(k-1)$-элементному подмножеству множества S.

Замечание 1.1. Стоит отметить, что условие совершенности подразумевает также, что любое $(k-1)$-элементное подмножество множества S, не должно раскрывать абсолютно ничего о секрете. Более очевидно это описывается через функцию энтропии в труде Котари:

- *условие корректности:* $H\left(s \middle| s_{i_1}, s_{i_2}, \dots, s_{i_k}\right) = 0$;
- *условие совершенности*: $H(s) = H\left(s \middle| s_{i_1}, s_{i_2}, \dots, s_{i_{k-1}}\right)$.

Раздел 2 посвящён формализации их ключевого свойства – относительной по Шеннону секретности, отличающей эти схемы от классических пороговых. В нём вводится и обобщается математическое определение рамп-схемы.

Основное соображение безопасности в линейной пороговой схемы – это «всё или ничего», то есть совершенная по Шеннону секретность, а именно никакой объём знаний о долях ниже порогового значения k не позволяет байесовскому противнику уточнить априорную догадку относительно защищаемого секрета.

Основное соображение безопасности в (d, k, n) рамп-схеме – это *относительная по Шеннону секретность*. При этом каждая доля частично сокращает пространство возможных секретов, однако внутри оставшегося подпространства априорные предположения противника не могут быть скорректированы – распределение вероятностей для допустимых значений секрета остаётся равномерным.

Определение 2.1. (d, k, n) рамп-схемы, где $1 \leq d \leq k \leq n$, определяются следующим образом. Пусть V – пространство *сокрытия* и W – пространство *секретов* таких, что

$$\frac{\log|V|}{\log|W|} = \frac{k}{d}.$$

Пусть $\varphi: V \to W$ – сюрьективное отображение, то есть такое отображение, что для $\forall w \in W\ \exists v \in V$ такой, что $\varphi(v) = w$. Мы будем называть φ *раскрывающим отображением.* Для заданного секрета w в W мы выбираем точку $y \in \varphi^{-1}(w)$, называемую *точкой сокрытия*. С этой точкой y мы связываем набор из n долей

$$\{Y(1), Y(2), \dots, Y(n)\},$$

где каждая доля $Y(i)$ является подпространством V таким, что

a) пересечение $\cap$ любых k долей равно $\{y\}$;
b) существует целое число λ, зависящее от d и k, такое, что
   i) $1 \leq \lambda \leq k$;
   ii) ограничение φ на объединение λ долей является сюрьективным;
   iii) знание о $w = \varphi(y)$ возрастает некоторым регулярным образом с получением каждой новой доли после λ долей.

В разделе 3 изложен основной результат работы: рассмотрены жесткие линейные рамп-схемы разделения секрета, а также разработан программный пакет, с помощью которого возможна корректная работа со схемами.

В подразделе 3.1 приведено описание генерации публичных параметров, алгоритмов разделения и восстановления для рамп-схемы разделения секрета Шамира.

Генерация публичных параметров схемы:

Пусть F_p – конечное поле, где p – некоторое простое число, $d, k, n \in \mathbb{N}/\{0\}$ – параметры схемы, причём $d \leq k \leq n$ и $n + d < p$. Случайным образом выбираются попарно различные $q_1, \dots, q_n \in F_p/\{0\}$ и $g_1, \dots, g_d \in F_p/\{0\}$.

Обозначим пространство сокрытия $V = F_p^k$ и пространство секретов $W = F_p^d$ и линейное отображение $\varphi: V \to W$, заданное матрицей Вандермонда $G_{d\times k}$ составленной из $g_1, \dots, g_d$, $\varphi(\bar{v}) = G_{d\times k} \cdot \bar{v}^T$, где $\bar{v} \in V$.

Алгоритм разделения:

Вход: секретный вектор $\bar{w} = (w_1, \dots, w_d) \in W$.

Выход: набор из n долей $\{c_1, \dots, c_n\}$, где $\forall c_i \in F_p$, для $i = \overline{1, n}$.

Шаг 1. Дилер выбирает точку сокрытия $\bar{y} = (a_0, \dots, a_{k-1}) \in V$, где $a_d, \dots, a_{k-1}$ выбираются случайно, такую что $L(\bar{g}_i) = w_i$, где $\bar{g}_i = (1, g_i, g_i^2, \dots, g_i^{k-1})$, $L(\bar{v}) = \langle \bar{y}, \bar{v} \rangle$ – линейный функционал. В контексте многочленов, дилер должен выбрать точку сокрытия такую, что

$$\begin{cases} a_0 + a_1 g_1 + a_2 g_1^2 + \dots + a_d g_1^d = w_1 - \sum_{t=d}^{k-1} a_t g_1^t \\ a_0 + a_1 g_2 + a_2 g_2^2 + \dots + a_d g_2^d = w_2 - \sum_{t=d}^{k-1} a_t g_2^t \\ \vdots \\ a_0 + a_1 g_d + a_2 g_d^2 + \dots + a_d g_d^d = w_d - \sum_{t=d}^{k-1} a_t g_d^t \end{cases}.$$

Шаг 2. Для всех $i = \overline{1, n}$ дилер вычисляет смещения $c_i = L(\bar{q}_i) = \langle \bar{y}, \bar{q}_i \rangle$, где $\bar{q}_i = (1, q_i, q_i^2, \dots, q_i^{k-1})$.

Шаг 3. Дилер раздаёт c_i держателям долей и удаляет закрытые данные, а именно точку сокрытия $\bar{y}$ и секретный вектор $\bar{w}$.

Временная сложность $O(d^2 + nk)$.

Алгоритм восстановления:

Вход: набор долей $\{c_1, \dots, c_z\}$, где $1 \le z \le n$.

Выход: секретный вектор $\bar{w} = (w_1, \dots, w_d) \in W$ или сообщение об ошибке восстановления.

Шаг 1. При наличии $z \ge k$ долей участники вычисляют систему линейных уравнений для неизвестной точки сокрытия $\bar{y}$.

$$\begin{cases} \langle \bar{y}, \bar{q}_1 \rangle = c_1 \\ \vdots \\ \langle \bar{y}, \bar{q}_z \rangle = c_z \end{cases},$$

или в контексте многочленов решить

$$\begin{cases} a_0 + a_1 q_1 + a_2 q_1^2 + \dots + a_{k-1} q_1^{k-1} = c_1 \\ \vdots \\ a_0 + a_1 q_1 + a_2 q_1^2 + \dots + a_{k-1} q_1^{k-1} = c_2 \end{cases}.$$

Так как векторы $\bar{q}_i$ линейно независимы, система имеет единственное решение. В контексте многочленов решить систему, согласно предложению 1.1, можно с помощью интерполяции полиномов. Вернуть $\varphi(\bar{y}) = G_{d\times k} \cdot \bar{y}^T = \bar{w}$.

Шаг 2. При наличии $z < k$ долей, участники не смогут восстановить секрет ни коим образом. Вернуть сообщение об ошибке восстановления.

Временная сложность $O(k^2 + dk)$.

В подразделе 3.2 приведено описание генерации публичных параметров, алгоритмов разделения и восстановления для рамп-схемы разделения секрета Блэкли.

Протокол рамп-схемы разделения секрета Блэкли:

Генерация публичных параметров:

Пусть F_p – конечное поле, где p – некоторое простое число, $d, k, n \in \mathbb{N}/\{0\}$ – параметры схемы, причём $d \le k \le n$. Выбираются $n + d$ векторов $\{\bar{g}_1, \dots, \bar{g}_d, \bar{q}_1, \dots, \bar{q}_n\} \in F_p^k$, такие, что любые k из них линейно независимы.

Обозначим пространство сокрытия $V = F_p^k$ и пространство секретов $W = F_p^d$ и линейное отображение $\varphi: V \to W$, которое задаётся как $\varphi(\bar{v}) = (\langle \bar{v}, \bar{g}_1 \rangle, \dots, \langle \bar{v}, \bar{g}_d \rangle)$.

Алгоритм разделения:

Вход: секретный вектор $\bar{w} = (w_1, \dots, w_d) \in W$.

Выход: набор из n долей $\{c_1, \dots, c_n\}$, где $\forall c_i \in F_p$, для $i = \overline{1, n}$.

Шаг 1. Дилер выбирает точку сокрытия $\bar{y} = (\bar{a}_1, \dots, \bar{a}_k) \in V$, такую что выполняется

$$\varphi(y) = w.$$

Шаг 2. Для $i = \overline{1, n}$ дилер вычисляет смещения $c_i = \langle \bar{y}, \bar{q}_i \rangle$.

Шаг 3. Дилер раздает доли c_i участникам схемы и удаляет закрытые данные, а именно точку сокрытия $\bar{y}$ и секретный вектор $\bar{w}$.

Временная сложность $O(dk + nk)$.

Алгоритм восстановления:

Вход: набор долей $\{c_1, \dots, c_z\}$, где $1 \le z \le n$.

Выход: секретный вектор $\bar{w} = (w_1, \dots, w_d) \in W$ или сообщение об ошибке восстановления.

Шаг 1. Если $z \ge k$ участники решают систему линейных уравнений относительно неизвестного $\bar{y}$

$$\begin{cases} \langle \bar{y}, \bar{q}_1 \rangle = c_1 \\ \quad\vdots \\ \langle \bar{y}, \bar{q}_z \rangle = c_z \end{cases}.$$

Поскольку любые k векторов $\bar{q}_i$ линейно независимы, система имеет единственное решение $\bar{y}$. Вернуть $\varphi(\bar{y}) = (\langle \bar{y}, \bar{g}_1 \rangle, \dots, \langle \bar{y}, \bar{g}_d \rangle) = \bar{w}$.

Шаг 2. Если $z < k$ вернуть сообщение об ошибке восстановления.

Временная сложность $O(k^3 + dk)$.

В подразделе 3.3 описан программный пакет «Ramp Sharing» на языке Python. Его архитектура обеспечивает выполнение основных этапов работы жёстких линейных рамп-схем: генерацию публичных параметров, разделение секретов на доли и восстановление секретов из долей.

Программный пакет состоит из 2 частей:

1. Ядро, содержащее всю необходимую алгебраическую логику и реализации рамп-схем.

2. Пользовательское веб-приложение с интерфейсом (webUI), обеспечивающее удобную работу со схемами через браузер.

Экспериментальная проверка подтвердила корректность функционирования пакета на всех этапах обработки данных в рамках жёстких линейных рамп-схем.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы проведено комплексное исследование рамп-схем разделения секрета – криптографических примитивов, представляющих собой обобщение классических пороговых схем. Основным результатом является преодоление ключевого ограничения пороговых схем – низкой эффективности при работе с большими объёмами данных – за счёт контролируемого компромисса между совершенной секретностью и ресурсными затратами.

На основе анализа классических схем Шамира и Блэкли подтверждено, что их свойство совершенной секретности по Шеннону ведёт к k-кратному росту объёма обрабатываемых данных на этапе восстановления, что становится критичным при высоких порогах k и больших секретах.

Исследована теоретическая модель (d, k, n) рамп-схем. Показано, что введение параметра d позволяет кодировать несколько независимых секретов в одной схеме. Доказано, что безопасность таких схем характеризуется понятием относительной секретности по Шеннону, при которой информация о секрете раскрывается постепенно по мере накопления долей, от полной неопределённости до полного восстановления.

В рамках унифицированного алгебраического подхода Котари дано строгое описание и доказаны свойства безопасности жёстких линейных рамп-схем на базе конструкций Шамира и Блэкли. Ключевым преимуществом жёстких схем является фиксация публичных параметров (направляющих векторов), что позволяет хранить и передавать только скалярные смещения, значительно экономя ресурсы.

Разработан программный пакет на языке Python, включающий:

- Библиотеку с реализацией алгебры конечных полей и трёх вариантов рамп-схем.

- Веб-приложение с графическим интерфейсом, обеспечивающее интуитивно понятное выполнение всех этапов работы схемы: генерацию параметров, разделение секрета и его восстановление.

Экспериментальная проверка на тестовых данных подтвердила полную корректность реализаций: исходные данные однозначно восстанавливаются при предъявлении не менее k долей, соответствующей схеме; при предъявлении меньшего числа долей восстановление невозможно. Программный пакет служит наглядным инструментом для изучения и демонстрации свойств рамп-схем.

Все поставленные задачи решены в полном объёме. Проведён теоретический анализ, дано формальное обоснование, разработана и протестирована практическая реализация.

Рамп-схемы демонстрируют значительный выигрыш в эффективности по сравнению с классическими пороговыми схемами. Так, для параметров (d, k, n) общий объём хранимых долей и данных, требуемых для восстановления, уменьшается примерно в d раз по сравнению с $(1, k, n)$ пороговой схемой. Реализованные жёсткие схемы минимизируют накладные расходы на передачу и хранение долей. Таким образом, работа вносит вклад в развитие практико-ориентированных криптографических методов, предлагая сбалансированное решение для современных задач защиты информации.

Теоретические результаты и строгие формулировки могут быть использованы в учебном процессе при изучении современных криптографических протоколов. Разработанный программный комплекс готов к использованию как демонстрационный и исследовательский инструмент для анализа параметров и свойств рамп-схем. Архитектура и алгоритмы реализации могут служить основой для построения реальных систем распределённого безопасного хранения данных в условиях, где абсолютная совершенная секретность избыточна, а на первый план выходят требования к эффективности и управляемому уровню риска.