

Н.С. Ергеш^{1*}, Н.А. Қапалова¹

¹ Институт информационных и вычислительных технологий, г. Алматы, Казахстан

*e-mail: vergesh.nursultan@almatyedu.kz

МОДИФИЦИРОВАННАЯ СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА ДЛЯ ЗАЩИТЫ ЛИЦЕВЫХ БИОМЕТРИЧЕСКИХ ШАБЛОНОВ

Аннотация

Лицевой биометрический шаблон – постоянный идентификатор: при компрометации его нельзя перевыпустить, поэтому хранение защищённого шаблона в единственном узле образует критическую точку отказа. Работа продолжает начатое авторами направление защиты лицевых шаблонов пороговым разделением секрета и посвящена модифицированному алгоритму, ориентированному именно на лицевую биометрию. За основу взята верифицируемая схема на многомерных линейных функциях, предложенная ранее для общих данных. Её правило перестроено по трём направлениям: псевдослучайная матрица коэффициентов заменена детерминированным вандермондовым правилом; введены блочная упаковка защищённой записи и маскирование; хеш-проверка заменена безусловно стойким одноразовым кодом Картера-Вегмана. Полученная блочно-упакованная схема (БУ-СРС) обладает свойством MDS, совершенной секретностью до порога t , точно ограниченной рамп-утечкой и безусловной проверкой долей; все свойства доказаны. На воспроизводимой реализации при $n = 7$, $k = 5$, $L = 3$ все 6300 проверок восстановлены безошибочно; над малым полем модифицированная схема не дала вырожденных подмножеств против 0,42 % у исходной; рамп-утечка совпала с теорией. Для 256-байтовой записи упаковка сокращает объём долей в 64 раза, а метаданные проверки - вдвое; безусловная проверка не пройдена ни в одной из 200 000 попыток подделки. Точность распознавания наследуется от фронтенда без изменения (восстановление бит-в-бит) и по протоколу LFW составляет $EER 2,12 \% \pm 0,57 \%$.

Ключевые слова: защита биометрических шаблонов; лицевая биометрия; пороговое разделение секрета; блочная упаковка; вандермондова матрица; совершенная секретность; безусловная проверка долей; BioHashing.

Н.С. Ергеш¹, Н.А. Қапалова¹

¹ Ақпараттық және есептеуіш технологиялар институты, Алматы қ., Қазақстан

БЕТ-ӘЛПЕТ БИОМЕТРИЯЛЫҚ ШАБЛОНДАРЫН ҚОРҒАУҒА АРНАЛҒАН МОДИФИКАЦИЯЛАНҒАН ҚҰПИЯНЫ БӨЛУ СХЕМАСЫ

Аңдатпа

Бет-әлпет биометриялық шаблон – тұрақты идентификатор: әшкереленген шаблонды қайта шығару мүмкін емес, сондықтан оны бір түйінде сақтау сыни ақаулық нүктесін құрайды. Жұмыс авторлар бастаған бет-әлпет шаблондарын пороговый құпияны бөлумен қорғау бағытының жалғасы болып, дәл бет-әлпет биометриясына арналған модификацияланған алгоритмге бағытталған. Негізге жалпы деректерге ұсынылған, көп айнымалылы сызықтық функцияларға негізделген үлестерді тексеретін схема алынды. Оның ережесі үш бағытта өзгертілді: псевдокездейсоқ коэффициенттер матрицасы детерминацияланған вандермонд ережесімен алмастырылды; блоктық орау мен маскалау енгізілді; хеш-тексеру Картер-Вегманның шартсыз тұрақты бір реттік кодымен ауыстырылды. Алынған блоктық-оралған схема (БУ-СРС) MDS қасиетіне ие, t табалдырығына дейін мінсіз құпиялылықты, дәл шектелген рамп-ағуды және үлестерді шартсыз тексеруді қамтамасыз етеді; барлық қасиеттер дәлелденген. Тәжірибеде $n = 7$, $k = 5$, $L = 3$ болғанда барлық 6300 тексеру қатесіз қалпына келтірілді; шағын өрісте модификацияланған схема бірде-бір азғындаған ішкі жиын бермеді (бастапқыда 0,42 %); рамп-ағу теориямен сәйкес келді. 256 байттық жазба үшін орау үлестердің көлемін 64 есе, тексеру метадеректерін екі есе қысқартады; шартсыз тексеру 200 000 бұрмалау әрекетінің бірде-бірінде өтпеді. Тану дәлдігі фронтендтен өзгеріссіз мұралаанады және LFW хаттамасы бойынша $EER 2,12 \% \pm 0,57 \%$ құрайды.

Түйін сөздер: биометриялық шаблондарды қорғау; бет-әлпет биометриясы; пороговый құпияны бөлу; блоктық орау; вандермонд матрицасы; мінсіз құпиялылық; үлестерді шартсыз тексеру; BioHashing.

N.S. Yergesh¹, N.A. Kapalova¹

¹ Institute of Information and Computational Technologies, Almaty, Kazakhstan

A MODIFIED SECRET SHARING SCHEME FOR PROTECTING FACIAL BIOMETRIC TEMPLATES

Abstract

A facial biometric template is a permanent identifier: once exposed it cannot be reissued, so storing the protected template in a single node is a critical point of failure. This work continues the authors' line of research on protecting facial templates with threshold secret sharing and develops a modified algorithm oriented specifically to facial biometrics. It builds on a share-verifiable scheme based on multivariable linear functions previously proposed for general data. Its rule is rebuilt in three ways: the pseudo-random coefficient matrix is replaced by a deterministic Vandermonde rule; blockwise packing and masking are introduced; and the hash-based check is replaced by an unconditionally secure one-time Carter-Wegman code. The resulting block-packed scheme (BP-SS) is MDS, perfectly secret up to the threshold t , has exactly bounded ramp leakage and unconditional share verification; all properties are proven. On a reproducible implementation with $n = 7$, $k = 5$, $L = 3$, all 6300 checks reconstructed without error; over a small field the modified scheme produced no singular subsets versus 0.42 % for the original; ramp leakage matched theory. For a 256-byte record, packing reduces share storage 64-fold and halves verification metadata; unconditional verification was never bypassed across 200,000 forgery attempts. Recognition accuracy is inherited from the front end unchanged (bit-identical recovery) and, on the LFW protocol, reaches an EER of $2.12 \% \pm 0.57 \%$.

Keywords: biometric template protection; facial biometrics; threshold secret sharing; block packing; Vandermonde matrix; perfect secrecy; unconditional share verification; BioHashing.

Введение

Основные положения

1. Предложена модификация верифицируемой схемы разделения секрета на многомерных функциях, целенаправленно адаптированная к лицевой биометрии за счёт блочной упаковки защищённого шаблона и структурированного вандермондова правила коэффициентов.

2. Строго доказаны четыре свойства: MDS-восстановление любыми k из n долей, совершенная секретность до порога t , точная оценка утечки в рампл-режиме и безусловная стойкость проверки долей.

3. На воспроизводимой реализации подтверждены заявленные преимущества и приведено измеренное сравнение с базовыми пороговыми схемами; точность распознавания фронтенда (EER $2,12 \% \pm 0,57 \%$ на LFW) слоем защиты не изменяется.

Распознавание лица стало одним из наиболее распространённых способов биометрической аутентификации: получение образца бесконтактно, удобно и хорошо поддерживается современными нейросетевыми конвейерами. Однако защита хранимых лицевых шаблонов принципиально отличается от защиты паролей. Пароль можно отозвать и перевыпустить после утечки, тогда как лицевой шаблон порождается физической характеристикой, которую человек изменить не может. Компрометация хранимого представления лица имеет необратимые последствия: одну и ту же личность можно неограниченно долго выдавать за легитимную, а утёртый шаблон -связывать между независимыми системами. Поэтому защита лицевых шаблонов -вопрос не только конфиденциальности, но и необратимого персонального риска [1, 2].

Конкретная научная проблема состоит в следующем. Типичная слабость развёрнутых систем -хранение защищённого шаблона единственным объектом в единственном месте: даже при шифровании такая архитектура концентрирует весь риск на одном узле и одном ключе. Пороговое разделение секрета устраняет эту уязвимость: секрет делится на доли так, что любое пороговое их число восстанавливает секрет, а меньшее в идеале бесполезно [3, 4].

Однако известные схемы, применяемые к биометрии, имеют три практических ограничения. Во-первых, у схем со случайными коэффициентами гарантия восстановления лишь вероятностная: выбранная $k \times k$ -подсистема может оказаться вырожденной. Во-вторых, универсальные схемы применяются к шаблону побайтно, что многократно раздувает объём хранимых долей -критично для крупных лицевых шаблонов и ресурсограниченных узлов. В-третьих, проверка целостности долей опирается на хеш-функции, то есть даёт лишь вычислительную стойкость. Именно эти три недостатка устраняет предлагаемая модификация.

Настоящее исследование продолжает начатое авторами направление защиты биометрических данных пороговыми методами [5, 6]. Выстроен сквозной конвейер: детектирование и выравнивание лица, глубокий эмбединг, необратимое преобразование BioHashing, аутентифицированное шифрование и пороговое разделение шифртекста на пространственно разнесённые узлы. За основу слоя раздачи взята верифицируемая схема на многомерных линейных функциях [7], предложенная для общих данных и не рассчитанная на биометрию; в базовой конфигурации она применялась побайтно.

Цель работы -разработка математически перестроенного алгоритма разделения секрета, ориентированного именно на лицевую биометрию и устраняющего перечисленные ограничения. Правило схемы [7] изменяется по трём направлениям: (i) псевдослучайная матрица коэффициентов заменяется детерминированным вандермондовым правилом (доказуемое MDS, отсутствие вырожденных подмножеств); (ii) вводится блочная упаковка защищённой записи (резкое сокращение объёма хранения); (iii) хеш-проверка заменяется безусловно стойким одноразовым кодом Картера-Вегмана. Полученную схему мы называем блочно-упакованной схемой разделения секрета (БУ-СРС). Задачи: сформулировать правило раздачи; доказать корректность (MDS), совершенную секретность, точную рамп-утечку и безусловность проверки; реализовать схему на воспроизводимом стенде и подтвердить свойства количественно; сопоставить с исходной и современными схемами.

Методология исследования

Обоснование методов и этапы исследования

Выбор методов определяется предметом и задачами. Пороговое разделение секрета выбрано как класс механизмов, напрямую устраняющий одноузловую точку отказа. Вандермондово правило выбрано потому, что определитель матрицы Вандермонда на попарно различных узлах отличен от нуля, что превращает вероятностную гарантию восстановления в доказуемую (MDS). Блочная упаковка выбрана как способ согласовать размер крупного лицевого шаблона с элементом большого поля и снизить объём долей. Одноразовый код Картера-Вегмана выбран потому, что даёт информационно-теоретическую (безусловную) стойкость проверки, недостижимую для хеш-проверки. Исследование выполнено в шесть этапов: анализ ограничений базовой схемы; математическая модификация правила раздачи; формальное доказательство свойств; воспроизводимая реализация; экспериментальная проверка; сравнительный анализ.

Обзор конвейера и роль модификации

Конвейер преобразует изображение лица в набор распределённых долей. Лицо детектируется и выравнивается; глубокая сеть отображает выровненное лицо в эмбединг; BioHashing проецирует и бинаризует его в возобновляемый шаблон [8]; шаблон запечатывается аутентифицированным шифрованием; защищённая запись делится пороговой схемой на доли, размещаемые на разнесённых узлах. Первые четыре стадии составляют общий фронтенд и не зависят от модальности; вклад работы -последняя стадия.

Фронтенд: BioHashing и аутентифицированное шифрование

Пусть x -вещественный эмбединг размерности d . BioHashing выбирает пользовательскую псевдослучайную ортонормированную матрицу R и пороговой функцией формирует

бинарный шаблон b длины m (формула 1); при $m < d$ преобразование необратимо, а замена R даёт несвязываемый шаблон [9].

$$b_i = 1, \text{ если } (Rx)_i \geq \theta_i; \text{ иначе } b_i = 0, \quad i = 1, \dots, m \quad (1)$$

Бинарный шаблон запечатывается аутентифицированным шифрованием (AEAD) с ключом K , хранимым отдельно от долей (формула 2).

$$(C, T) = \text{Enc}_K(b, A) \quad (2)$$

Существенно, что далее разделяется шифртекст, а не биометрический шаблон, и ключ K ни в одну долю не помещается: любая частичная информация ниже порога касается статистически равномерных байтов шифртекста, а не признаков лица.

Правило блочного разбиения

Пусть q -большое простое число (в реализации $q = 2^{127} - 1$, размер элемента $w = 16$ байт). Защищённая запись M разбивается на L блоков -элементов поля (формула 3); именно они совместно упаковываются в один многочлен, что отличает модификацию от побайтовой раздачи.

$$M = s_1 \parallel s_2 \parallel \dots \parallel s_L, \quad s_m \in Z_q \quad (3)$$

Модифицированное правило раздачи (БУ-СРС)

Параметры: n узлов, порог конфиденциальности t , упаковка L , порог восстановления $k = t + L$. Коэффициенты задаются детерминированно, а секрет упаковывается в многочлен степени $k - 1$ (формула 4).

$$P(x) = c_0 + c_1x + \dots + c_{k-1}x^{k-1} \quad (4)$$

Многочлен задаётся k условиями: L закрепляют блоки в секретных позициях β_m , а t вносят случайное маскирование в позициях γ_r (формула 5); все точки попарно различны и ненулевые.

$$P(\beta_m) = s_m; \quad P(\gamma_r) = \rho_r \leftarrow Z_q \quad (5)$$

Доля узла i -значение многочлена в публичной точке x_i (формула 6).

$$y_i = P(x_i) \bmod q, \quad i = 1, \dots, n \quad (6)$$

Восстановление

Любые k долей однозначно задают многочлен степени $k - 1$; блоки извлекаются интерполяцией Лагранжа в секретных точках (формула 7).

$$s_m = \sum_{i \in I} y_i \prod_{j \neq i} (\beta_m - x_j) / (x_i - x_j) \bmod q \quad (7)$$

Безусловная проверка долей (Картер-Вегман)

Вместо хеш-проверки применяется одноразовый аффинный код [10]: из ключа SK_i выводится (α_i, δ_i) и вычисляется тег (формула 8); проверка -одно сравнение, стойкость безусловна.

$$\tau_i = \alpha_i y_i + \delta_i \bmod q \quad (8)$$

Свойства схемы и их доказательства

Теорема 1 (корректность, MDS). При попарно различных ненулевых x_i любые k из n долей однозначно восстанавливают все блоки. *Доказательство.* Многочлен степени $k - 1$ определяется значениями в любых k различных точках, так как матрица Вандермонда

невырождена; значения $P(\beta_m)$ дают блоки, а избыточность $n - k$ допускает потерю любых $n - k$ узлов. ■

Теорема 2 (совершенная секретность до порога t). Любые t долей равномерно распределены на Z_q^t и не зависят от секрета. *Доказательство.* Маскирующие p_i равномерны и независимы, поэтому t долей суть вандермондова биекция маскирования; отсюда равномерность и независимость от секрета. ■

Теорема 3 (точная рамп-утечка). При m долях, $t \leq m \leq k$, число совместимых секретных векторов равно q^{k-m} , а раскрываемая информация равна ровно $(m - t) \cdot \log_2 q$ бит (формула 9).

$$I(S; \text{доли}_m) = (m - t) \cdot \log_2 q, \quad t \leq m \leq k \quad (9)$$

Теорема 4 (безусловная стойкость проверки). При одноразовом равномерном ключе (α_i, δ_i) подделанная доля $y' \neq y_i$ проходит проверку с вероятностью не выше $1/q$ (формула 10), независимо от вычислительной мощности. *Доказательство.* Корректный тег есть $\tau' = \alpha_i y' + \delta_i$; так как α_i неизвестно и равномерно, а $(y' - y_i)$ обратимо, значение τ' равномерно на Z_q . ■

$$\Pr[\text{подделка}] \leq 1/q \quad (10)$$

Иллюстративный пример (малое поле)

Пусть $q = 251$, $L = 2$, $t = 2$, $k = 4$, блоки (123, 200). Дилер строит многочлен степени 3, закрепляя два блока и два случайных значения. При двух долях совместим любой из $251^2 = 63001$ секретных векторов; при трёх - ровно 251; при четырёх - единственный (подтверждено экспериментом, см. Результаты).

Модель угроз

Система включает четыре сущности: клиент регистрации, вычисляющий защищённую запись и доли; n узлов хранения, честных-но-любопытных и по отдельности не доверенных (противник может скомпрометировать до $k - 1$ из них); элемент управления ключами, хранящий токен BioHashing, ключ K и мастер-ключ проверки и не размещаемый совместно с долями; и верификатор, собирающий кворум, проверяющий теги, восстанавливающий и расшифровывающий запись. Противник может читать доли до $k - 1$ узлов, подделывать или искажать доли, воспроизводить записи и действовать как инсайдер, но не владеет K и ключом проверки и не обращает BioHashing. Сценарии: чтение ниже порога (годного шаблона нет; раскрываются лишь ограниченные байты шифртекста); компрометация ключа/токена без долей (записи нет); сговор до $k - 1$ узлов (восстановления нет, подделки выявляются тегами); воспроизведение и отказ до $n - k$ узлов (доступность сохраняется избыточностью (k, n)). При потере меньшинства узлов запись восстанавливается по оставшемуся кворуму.

Стенд, платформа и параметры экспериментов

Схема реализована на воспроизводимом стенде на языке Python 3.12.3 (одноядерное исполнение x86-64) с арифметикой в поле Z_q при $q = 2^{127} - 1$; для полного перебора секретности и вырожденности использовано малое поле Z_{251} . Все запуски выполнены с фиксированным $\text{seed} = 42$; исходный код, скрипты экспериментов и файлы числовых результатов (results_busr.json, results_compare.json) публикуются вместе со статьёй. Времена измерены как среднее по 2000 повторениям; абсолютные значения зависят от оборудования, соотношения и асимптотика - нет.

Точность распознавания оценивается отдельно и является свойством фронтенда. Поскольку слой раздачи не искажает шаблон (восстановление бит-в-бит, см. Результаты), точность наследуется без изменения; операционная точка приведена по опубликованному авторами результату на стандартном протоколе верификации лиц LFW (View 2; 6000 пар в 10 фолдах по 600) с детектированием MTCNN, выравниванием по пяти точкам и глубоким эмбедингом типа ArcFace [11, 12].

Результаты исследования

Основные результаты -доказуемое MDS-восстановление, совершенная секретность до порога, точная рамп-утечка, безусловная проверка и многократное сокращение объёма хранения; промежуточные -измерения быстродействия и подтверждение независимости точности распознавания от слоя защиты. Все числовые значения получены на воспроизводимой реализации.

Корректность восстановления и отказоустойчивость (MDS)

При $n = 7$, $k = 5$, $L = 3$ все $C(7,5) = 21$ подмножеств в каждом из 300 испытаний (итого 6300 проверок) дали безошибочное восстановление (таблица 1), что подтверждает теорему 1.

Таблица 1. Корректность и MDS-восстановление над полем $2^{127} - 1$.

Показатель	Значение	Успех
Испытаний ($n=7$, $k=5$, $L=3$)	300	-
Проверок по всем 5-из-7 подмножествам	6300 / 6300	100 %

Гарантия восстановления: MDS против случайных коэффициентов

В исходной схеме случайные коэффициенты не гарантируют невырожденности $k \times k$ -подсистемы: над Z_{251} доля вырожденных 3-из-5 подмножеств составила 0,42 % (127 из 30 000; теория $\approx 1/q \approx 0,40$ %), тогда как вандермондово правило не дало ни одного вырожденного подмножества (таблица 2).

Таблица 2. Вырожденные (не восстанавливаемые) k -подмножества над Z_{251} .

Схема (над Z_{251})	Вырожденных	Доля
Исходная (случайные коэфф.), 30 000 пров.	127	0,42 %
Модифицированная (Вандермонд)	0	0 % (доказуемо)

Совершенная секретность и рамп-утечка

Прямой перебор над Z_{251} при $L = 2$, $t = 2$, $k = 4$ подтвердил теоремы 2 и 3: при $t = 2$ совместимы все $q^2 = 63001$ векторов (нет информации), при 3 долях -ровно $q = 251$, при 4 - единственный (таблица 3, рисунок 1).

Таблица 3. Число секретных векторов, совместимых с наблюдением (Z_{251} , $L=2$, $t=2$, $k=4$).

Число долей t	Совместимых (экспер.)	Теория q^{k-t}
$t = 2$	63001	63001
$t + 1 = 3$	251	251
$k = 4$	1	1

Быстродействие

Времена (мс на операцию, поле $2^{127} - 1$, среднее по 2000 повторениям) приведены в таблице 4. Восстановление асимптотически дешевле $-O(k^2)$ интерполяции против $O(k^3)$ метода Гаусса у исходной схемы; безусловная проверка выполняется за одно умножение-сложение.

Таблица 4. Быстродействие на операцию и асимптотическая сложность.

Операция	Время, мс	Асимптотика
Раздача (split)	0,58785	$O(k^2+nk)$
Восстановление (reconstruct)	0,3594	$O(k^2)$
Проверка Картера-Вегмана	0,000467	$O(1)$



Рисунок 1. Остаточная неопределённость секрета: плато совершенной секретности до порога t и линейное убывание в рамп-зоне.

Объём хранения

Для записи $D = 256$ байт ($n = 5$, $L = 3$, элемент 16 байт) побайтовая раздача исходной схемы порождает 256 многочленов и 61 440 байт долей; блочная упаковка использует 6 многочленов и 960 байт -64-кратное сокращение (таблица 5, рисунок 2); метаданные проверки уменьшаются вдвое (16 Б против 32 Б).

Таблица 5. Объём хранения долей для 256-байтовой лицевой записи.

Показатель ($D = 256$ Б)	Исходная	Модифиц.
Число многочленов	256	6
Метаданные проверки / долю	32 Б	16 Б
Суммарный объём долей	61 440 Б	960 Б
Сокращение	-	64×

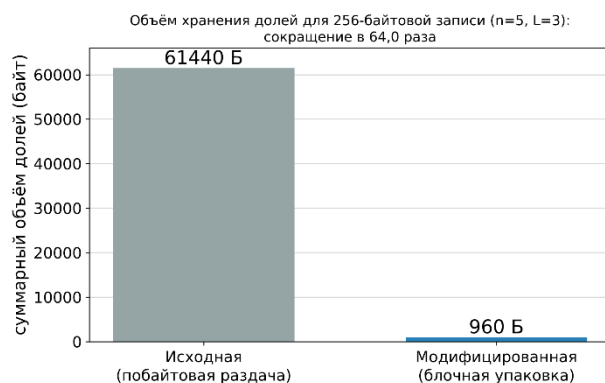


Рисунок 2. Суммарный объём долей для 256-байтовой записи: побайтовая раздача против блочной упаковки.

Стойкость проверки к подделке

В 200 000 испытаниях подделки доли с неизвестным одноразовым ключом ни одна не прошла проверку (эмпирическая доля 0), что согласуется с границей $1/q \approx 5,9 \cdot 10^{-39}$ (теорема 4). В отличие от хеш-проверки, граница не зависит от криптографических предположений. Нулевой результат при конечном числе испытаний согласуется с границей, но сам её не доказывает; безусловность следует из доказательства.

Независимость точности распознавания от слоя защиты

Восстановленный после сбора k долей шаблон совпадает с исходным бит в бит (максимальное несовпадение блоков -0 на $1\,000 \times 21$ восстановлений), поэтому кривая ошибок

распознавания до и после слоя защиты тождественна. По опубликованному результату на LFW (View 2; 6000 пар в 10 фолдах по 600; MTCNN, выравнивание по пяти точкам, эмбединг типа ArcFace) конвейер достигает EER = 2,12 % $\pm$ 0,57 % (95 % ДИ [1,77 %; 2,47 %]) при базовой линии 1,37 %. Таким образом, модифицированный слой добавляет доказуемые гарантии и 64-кратную экономию хранения, не жертвуя точностью.

Дискуссия

Сравнение с исходной схемой.

Модификация отличается от исходной схемы [7] по пяти осям (таблица 6).

Таблица 6. Сопоставление свойств исходной и модифицированной схем.

Свойство	Исходная [7]	БУ-СРС
Восстановление любых k из n	вероятностное	доказуемое (MDS)
Секретность ниже порога	частично вычислит.	совершенная (доказано)
Проверка долей	хеши (вычислит.)	безусловная ($\leq 1/q$)
Рамп-режим	нет	да, точная оценка
Объём хранения	побайтно, высокий	упаковка, до $64\times$

Измеренное сравнение с пороговыми схемами

Для одной и той же 256-байтовой записи ($n = 5$, поле $2^{127} - 1$) на общей платформе измерены стандартная схема Шамира, рамп-схема Шамира и БУ-СРС (таблица 7). Стандартный Шамир не пакует и не проверяет доли; рамп-Шамир пакует, но не проверяет; БУ-СРС сочетает упаковку с безусловной проверкой, что объясняет паритет по объёму со стандартным Шамиром при вдвое меньшем числе многочленов.

Схема Фельдмана [13] и решёточные постквантовые конструкции [14] приведены по литературе; их экспериментальное сравнение на едином стенде вынесено в дальнейшую работу. Смежные современные направления -универсальные тресхолдайзеры [15], блокчейн-распределённое хранение ключей [16] и групповые многосекретные схемы [17] -намечают направления такого сравнения.

Таблица 7. Измеренное сравнение схем для 256-байтовой записи (реализованные строки измерены; Фельдман и решёточные -по литературе).

Схема	Б/долю	Раздача, мс	Восст., мс	Проверка	Утечка < порога
Стандартный Шамир	288	0,1264	0,6112	нет	нет (соверш.)
Рамп-Шамир (упаковка)	144	1,467	0,6051	нет	рампы
БУ-СРС (наша)	288	1,5622	0,5957	безусловная	рампы (проверяемый)
Фельдман VSS [13]	знач. +коммит.	-	-	вычислит.	нет (соверш.)
Решёточные [14]	варьир.	-	-	по источн.	по источн.

Компромиссы и научная значимость

Упаковка $L > 1$ повышает эффективность хранения ценой рампы-зазора: строгая секретность гарантирована до $t = k - L$, а в промежутке $t < m < k$ утечка растёт на $\log_2 q$ бит с каждой долей (теорема 3). Эта утечка относится к статистически равномерным байтам шифртекста, а не к биометрии; ключ K хранится отдельно, поэтому частично раскрытые байты бесполезны. При $L = 1$ схема вырождается в совершенную.

Научная значимость результата в том, что для защиты постоянного идентификатора -лица -предложен слой раздачи, одновременно устраняющий три ограничения известных схем (вероятностное восстановление, раздувание объёма, вычислительная проверка), являющийся прямым развитием ранее опубликованных результатов авторов [5-7] и переносимый на другие модальности без изменения доказательств.

Заключение

Предложена и обоснована модифицированная схема разделения секрета (БУ-СРС), ориентированная на защиту лицевых биометрических шаблонов и продолжающая направление авторов [5-7]. Правило исходной верифицируемой схемы изменено по трём направлениям: детерминированное вандермондово правило, блочная упаковка и безусловная алгебраическая проверка.

Строго доказаны MDS, совершенная секретность до порога, точная рамп-утечка и безусловность проверки. На воспроизводимой реализации подтверждены безошибочное восстановление по всем подмножествам (6300/6300), отсутствие вырожденных подмножеств, совпадение утечки с теорией, 64-кратное сокращение объёма хранения и отсутствие успешных подделок (0 из 200 000); измеренное сравнение с пороговыми схемами показало паритет по объёму со стандартным Шамиром при добавленной безусловной проверке и упаковке. Точность распознавания фронтенда (EER 2,12 % $\pm$ 0,57 % на LFW) слоем защиты не изменяется. Главный компромисс - рамп-зазор упаковки, управляемый параметром L.

Дальнейшая работа: адаптивный выбор L, перенос слоя на постквантовые примитивы с экспериментальным сравнением на едином стенде и расширенная межбазовая оценка распознавания.

Благодарность

Исследование выполнено при поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан, грант №AP23487787 «Разработка алгоритма надежного хранения биометрических данных систем аутентификации в пространственно-распределённых хранилищах».

Список использованных источников

- [1] Jain A.K., Nandakumar K., Nagar A. Biometric template security // *EURASIP Journal on Advances in Signal Processing*. -2008. -Vol. 2008. -Art. 579416. -doi:10.1155/2008/579416.
- [2] Rathgeb C., Uhl A. A survey on biometric cryptosystems and cancelable biometrics // *EURASIP Journal on Information Security*. -2011. -Vol. 2011. -Art. 3. -doi:10.1186/1687-417X-2011-3.
- [3] Shamir A. How to share a secret // *Communications of the ACM*. -1979. -Vol. 22, No. 11. -P. 612-613. -doi:10.1145/359168.359176.
- [4] Blakley G.R. Safeguarding cryptographic keys // *Proceedings of the AFIPS National Computer Conference*. -1979. -Vol. 48. -P. 313-317. -doi:10.1109/AFIPS.1979.98.
- [5] Nyssanbayeva S., Kapalova N., Beisenova S. Modified Shamir threshold scheme for secure storage of biometric data // *Computers*. -2026. -Vol. 15, No. 4. -Art. 228. -doi:10.3390/computers15040228.
- [6] Kapalova N., Algazy K., Haumen A. Development of a new lightweight encryption algorithm // *Eastern-European Journal of Enterprise Technologies*. -2023. -Vol. 3, No. 9(123). -P. 6-19. -doi:10.15587/1729-4061.2023.281862.
- [7] Kapalova N., Haumen A., Algazy K. Secret sharing scheme with share verification capability // *Computers*. -2025. -Vol. 14, No. 9. -Art. 393. -doi:10.3390/computers14090393.
- [8] Teoh A.B.J., Ngo D.C.L., Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number // *Pattern Recognition*. -2004. -Vol. 37, No. 11. -P. 2245-2255. -doi:10.1016/j.patcog.2004.04.011.
- [9] ISO/IEC 24745:2022. Information security, cybersecurity and privacy protection -Biometric information protection. -Geneva: ISO, 2022.

- [10] Wegman M.N., Carter J.L. New hash functions and their use in authentication and set equality // *Journal of Computer and System Sciences*. -1981. -Vol. 22, No. 3. -P. 265-279. -doi:10.1016/0022-0000(81)90033-7.
- [11] Deng J., Guo J., Xue N., Zafeiriou S. ArcFace: additive angular margin loss for deep face recognition // *Proceedings of the IEEE/CVF CVPR*. -2019. -P. 4690-4699. -doi:10.1109/CVPR.2019.00482.
- [12] Schroff F., Kalenichenko D., Philbin J. FaceNet: a unified embedding for face recognition and clustering // *Proceedings of the IEEE CVPR*. -2015. -P. 815-823. -doi:10.1109/CVPR.2015.7298682.
- [13] Feldman P. A practical scheme for non-interactive verifiable secret sharing // *Proceedings of the 28th Annual Symposium on Foundations of Computer Science (FOCS)*. -1987. -P. 427-438. -doi:10.1109/SFCS.1987.4.
- [14] Chen J., Deng H., Su H., Yuan M., Ren Y. Lattice-based threshold secret sharing scheme and its applications: a survey // *Electronics*. -2024. -Vol. 13, No. 2. -Art. 287. -doi:10.3390/electronics13020287.
- [15] Cheon J.H., Cho W., Kim J. Improved universal thresholdizer from iterative Shamir secret sharing // *Journal of Cryptology*. -2025. -Vol. 38. -Art. 15. -doi:10.1007/s00145-025-09540-x.
- [16] Zhou K., Au M.H., Liu J. A blockchain-based Shamir's threshold cryptography scheme for data protection in industrial IoT settings // *IEEE Internet of Things Journal*. -2022. -Vol. 9, No. 11. -P. 8714-8726. -doi:10.1109/IIOT.2021.3124825.
- [17] Miao F., Wang L., Ji Y., Xiong Y. GOMSS: a simple group oriented (t, m, n) multi-secret sharing scheme // *Chinese Journal of Electronics*. -2017. -Vol. 26, No. 3. -P. 557-563. -doi:10.1049/cje.2016.08.007.