МЕТОД ПОСТРОЕНИЯ ПОСТКВАНТОВЫХ АЛГОРИТМОВ ЭЦП С ДВУМЯ СКРЫТЫМИ ГРУППАМИ

Петренко А. С.[1]

DOI: 10.21681/2311-3456-2025-2-52-63

Цель работы: *разработать и теоретически обосновать метод построения постквантовых алгоритмов электронной цифровой подписи (ЭЦП) на базе конечных некоммутативных ассоциативных алгебр. При этом необходимо достичь усиленной рандомизации подписи, компактных размеров ключей и высокой производительности.*

Метод исследования: *алгебраическое моделирование некоммутативных структур и компьютерная проверка ассоциативности таблиц умножения (ТУБВ), математическое моделирование процесса подписи и вероятностная оценка криптостойкости при массовом сборе подписей, методы эволюционного поиска, численные эксперименты с генерацией одноразовых экспонент b,n через хаотические отображения и тестирование полученного криптопримитива.*

Результаты исследования: *создан базовый криптопримитив, обеспечивающий двойную рандомизацию подписи за счёт двух специальных векторов, принадлежащих собственным коммутативным подалгебрам. Каждая подпись формируется с использованием одноразовых экспонент, которые вычисляются с использованием хаотических отображений и существенно затрудняют статистический криптоанализ даже при массовом сборе подписей. Дополнительные маскирующие векторы скрывают прямое произведение степенных элементов, что не позволяет злоумышленнику получить упрощённую систему уравнений. Для повышения производительности структуры умножения была реализована процедура автоматизированного «прореживания» таблиц, благодаря которой уменьшилось число ненулевых структурных констант и сократилось время вычислений. Применение эволюционного алгоритма позволило быстрее отбирать подходящие таблицы умножения базисных векторов. Экспериментальный анализ в различных режимах подтверждает экспоненциальную сложность атак при корректном выборе параметров модуля и начальных условий для хаотического генератора. Продемонстрирована возможность реализации алгоритма на средних аппаратных ресурсах.*

Научная новизна: *разработан метод проектирования постквантовых алгоритмов электронной цифровой подписи на основе конечных некоммутативных ассоциативных алгебр с двумя скрытыми группами, позволящий создавать постквантовые схемы электронной цифровой подписи, криптографически стойкие к атакам злоумышленников с применением квантового компьютера.*

Ключевые слова: *постквантовая криптография, некоммутативные ассоциативные алгебры, двойная рандомизация подписи, хаотические отображения, эволюционные алгоритмы, скрытые коммутативные группы, квантовая устойчивость, цифровая подпись, алгебраическая структура, генерирование ключей.*

Введение

Современные схемы с открытым ключом (RSA, ElGamal, ECDSA) уязвимы перед квантовыми вычислителями из-за эффективных квантовых алгоритмов (Шора, Гровера). По этой причине научное сообщество активно разрабатывает постквантовые криптосистемы на решётках, кодах, изогенных кривых и других математических платформах. Однако такие подходы зачастую требуют увеличения размеров ключей и/или существенных вычислительных ресурсов. Одним из перспективных направлений считается использование конечных некоммутативных ассоциативных алгебр, позволяющих реализовать криптопримитивы с более компактными ключами и усиленной рандомизацией [1–9].

Для повышения криптоустойчивости в контексте квантовых угроз [10–13], а также снижения требований к аппаратным ресурсам, в работе предлагается новый метод построения постквантовых алгоритмов ЭЦП на базе КНАА. Данная схема цифровой подписи использует две скрытые коммутативные подалгебры и хаотические отображения для генерации одноразовых экспонент, что значительно повышает криптостойкость. Также эволюционные алгоритмы (ЭА) позволяют адаптивно искать параметры алгебры, избегая полного перебора.

Постановка задачи

В рамках настоящей работы решается задача повышения криптостойкости и производительности постквантовых алгоритмов электронной цифровой подписи (ЭЦП). Для этого необходимо:

1. Использовать четырехмерные (и потенциально более высокоразмерные) КНАА как математическую платформу.
2. Использовать механизмы двух скрытых коммутативных групп [14], отвечающих за рандомизацию подписи.

1 Петренко Алексей Сергеевич, аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, Россия, младший научный сотрудник Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

3. Разработать и систематизировать метод построения криптопримитивов, включающий расширяющие базовый криптопримитив подходы:
   - применение хаотических отображений при генерации параметров;
   - адаптивный выбор структуры и ключевых параметров на основе эволюционных алгоритмов.

Следует особо отметить, что результаты, полученные при решении задачи 3, непосредственно применяются к задачам 1 и 2. В частности, механизм хаотической генерации параметров и адаптивный подбор структуры позволяют обеспечить требуемое ускорение вычислений в рамках решения первой задачи, а также усиленную рандомизацию цифровой подписи в рамках решения второй задачи.

Обобщая описанное выше, цель работы – разработка и обоснование нового метода построения постквантовых алгоритмов ЭЦП, обеспечивающего усиленную рандомизацию, приемлемые размеры ключей и высокую скорость вычислений.

1. Задание конечных некоммутативных ассоциативных алгебр

Конечная некоммутативная ассоциативная алгебра (КНАА) размерности m над $GF(p)$ представляет собой m-мерное векторное пространство с операцией умножения, дистрибутивной относительно сложения. Пусть $e_0, e_1,\ldots, e_{m-1}$ - фиксированный базис. Любой элемент (вектор) $V = (v_0, v_1,\ldots, v_{m-1})$ можно представить как $V = (v_0e_0 + v_1e_1 + \cdots + v_{m-1}e_{m-1})$, где $v_i \in GF(p)$. Умножение векторов задается по правилу:

$$e_i \cdot e_j = \sum_{k=0}^{m-1} \lambda_{i,j}^{k}\, e_k, \qquad (1)$$

и линейно продолжается на все пространство. Коэффициенты $\lambda_{i,j}^{k}$ называют структурными константами. Для криптографического применения важны:

1. Ассоциативность, выражающаяся в выполнении $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ для любых A, B, C;
2. Наличие глобальной единицы E, такой что $E \cdot V = V \cdot E = V$;
3. Некоммутативность, затрудняющая решение возникающих при атаках уравнений.

На практике применяют «прореженные» ТУБВ, когда многие $\lambda_{i,j}^{k}$ равны нулю, что ускоряет умножение в большой размерности m. Например, в четырёхмерном случае отдельные произведения $e_i \times e_j$ обнуляются, а при подходящем выборе λ сохраняется единица E. Такие структуры можно достраивать поэтапно, периодически проверяя ассоциативность, именно это позволяет генерировать новые эффективные и не ресурсоёмкие ТУБВ [15].

Секретный набор структурных констант

Чтобы «спрятать» внутреннюю логику алгебры, часть $\lambda_{i,j}^{k}$ модифицируют случайными δ сдвигами. После каждой модификации выполняют автоматическую проверку ассоциативности. Если всё корректно, итоговая таблица Λ_{secret} фиксируется в качестве основного секрета, неизвестного внешнему наблюдателю. В таком варианте атакующему сложно восстановить полную схему умножения, даже видя результаты произведений.

Использование двух скрытых коммутативных групп

Для усиления рандомизации подписи выбирают два специальных вектора P и H в алгебре, каждый из которых порождает свою коммутативную подалгебру. Пусть P^b и H^n, где b и n являются целыми экспонентами. При построении подписи элементы P^b и H^n комбинируют с маскирующими векторами D, F. Поскольку P и H лежат в разных коммутативных подалгебрах, но в целом алгебра остаётся некоммутативной, атакующему вычислительно сложно (или вычислительно невозможно) свести результат произведений к тривиальному выражению.

Необходимыми компонентами для криптопримитива на КНАА являются:

1. Генерация базовой ТУБВ и проверка ассоциативности;
2. Секретная «донастройка» $\lambda_{i,j}^{k}$, формирующая уникальную Λ_{secret};
3. Выбор двух векторов P, H и масок D, F.

Данная схема задаёт основу для построения подписи, сохраняющей компактность ключей и усложняющей решение нелинейных систем уравнений, особенно при подключении хаотических механизмов и адаптивного перебора параметров, которые будут рассмотрены далее.

Утверждение 1. Об экспоненциальной сложности схемы в условиях квантовых атак

Вскрытие алгоритма на основе конечных некоммутативных ассоциативных алгебр с двумя скрытыми группами имеет экспоненциальную сложность, и квантовый компьютер не дает выигрыша в решении этой задачи.

Доказательство

Рассмотрим криптосистему, основанную на КНАА с двумя скрытыми коммутативными группами. Первоочередная задача, стоящая перед атакующим, состоит в восстановлении скрытых экспонент b и n, которые используются для формирования подписи.

В данной системе скрытые экспоненты b и n используются для построения произведений вида P^b и H^n, где P и H – векторы, порождающие скрытые коммутативные группы. Каждая экспонента может быть представлена как число в пространстве размерности m, что означает, что возможное количество решений для каждого параметра экспоненты – 2^m,

и система уравнений становится экспоненциальной по сложности. Добавление маскирующих векторов D и F, усложняющих прямой анализ, дополнительно увеличивает сложность задачи, однако базовая сложность решения нелинейных уравнений остаётся экспоненциальной, как указано выше, поэтому данным увеличением сложности можно пренебречь как менее значащим в контексте анализа сложности задачи восстановления скрытых экспонент.

Задача восстановления скрытых экспонент b и n сводится к решению системы степенных уравнений, которая требует экспоненциального времени от числа скрытых переменных k и размерности алгебры m, тогда как формула сложности решения такой системы имеет вид:

$$C(k,m,N) \sim O(2^{k \cdot m}), \quad (2)$$

где N – количество наблюдений или же уже известных подписей.

Квантовые алгоритмы, вроде алгоритма Шора, способны решать задачи факторизации и дискретного логарифма за полиномиальное время, однако они не применимы к решению нелинейных систем уравнений в некоммутативных структурах, таких как КНАА. Алгоритм Гровера может ускорить поиск в базе данных за квадратичное время, но в случае многомерных задач с нелинейными уравнениями даже квадратичное ускорение не позволяет значительно снизить экспоненциальную сложность задачи. Как известно на сегодняшний день, квантовый компьютер не имеет известных алгоритмов, которые могут решить задачу восстановления скрытых экспонент b и n за полиномиальное время, несмотря на возможное увеличение их вычислительных мощностей в обозримом будущем.

Подводя итог, сложность восстановления скрытых параметров в рассматриваемой криптосистеме остаётся экспоненциальной от количества скрытых переменных k и размерности пространства m и квантовые алгоритмы не дают какого-либо значимого выигрыша в решении таких задач. Это подтверждает, что алгоритм на основе КНАА с двумя скрытыми группами является квантовоустойчивым. ч.т.д.

2. Базовый криптопримитив на базе КНАА

В данном разделе описывается процесс построения базового постквантового криптопримитива на основе КНАА и параллельно приводятся три основных алгоритма в формате пошагового описания.

Постановка задачи

В общем виде задачу можно сформулировать следующим образом:

- Построить некоммутативную алгебру размерности m над полем $GF(p)$, где будет удобно выполнять операции умножения и возведения в степень;
- Убедиться, что в этой алгебре существуют две «большие» коммутативные группы (скрытые подкольца), порождаемые векторами P и H;
- Использовать эти два генератора для рандомизации подписи (например, P^b, H^n) и маскировать результат слева/справа другими секретными векторами;
- Использовать адаптивный выбор структуры $\lambda_{i,j}^k$, хаотические отображения для экспонент и другие дополняющие базовый криптопримитив подходы.

Ассоциативность

Чтобы алгебра была ассоциативной, требуется $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ для любых A, B, C. Это накладывает огромное количество (до m^4) условий на λ. В рассматриваемом примере предлагается случайно генерировать и затем проверять ассоциативность, отбрасывая неудачные варианты автоматически.

Наличие глобальной единицы

Зачастую необходимо иметь вектор E (единицу), удовлетворяя $E \cdot V = V \cdot E = V$ для всех V. При случайном заполнении λ найти E не всегда тривиально. Но для демонстрации можно либо искусственно строить ТУБВ, либо проверять существование E перебором.

Считается, что атакующий не может из большого числа σ извлечь (b, n), либо раскрыть Λ_{secret} из-за использования некоммутативной структуры и наличии маскирующих множителей. При этом важно, чтобы каждое новое подписание генерировало уникальные b, n.

Теоретическое обобщение алгоритмов

В представленных трех алгоритмах изложена полная схема формирования и использования КНАА для построения базовой постквантовой подписи. Их логика выглядит следующим образом:

Алгоритм 1 (Генерация базовой структуры КНАА) создаёт ТУБВ размерности m над $GF(p)$ с «прореженными» $\lambda_{i,j}^k$. Проверяется ассоциативность, при успехе получается корректная некоммутативная алгебра (схема 1).

Алгоритм 2 (Персонализация КНАА и выбор скрытых векторов) на базе ТУБВ из Алгоритма 1 вносит секретные поправки, сохраняя ассоциативность и скрывая точные детали умножения. Здесь же подбираются векторы P и H для двойной рандомизации и маскирующие множители D, F. Результатом становится уникальная КНАА для каждого нового использования (схема 2).

Алгоритм 3 (Постквантовый ЭЦП на КНАА) объединяет генерацию ключей, подписывание и проверку (схемы 3):

1. Закрытый ключ включает Λ_{secret} и векторы (P, H, D, F);
2. Открытый ключ содержит лишь данные, нужные для проверки в КНАА, но не раскрывает полных $\lambda_{i,j}^k$;

Алгоритм 1. Генерация базовой структуры КНАА

1. Инициализация.
   - Задать m (размерность) и простое p.
   - Пусть Λ – трёхмерный массив размером $(m \times m \times m)$, где $\Lambda[i][j][k] = \lambda_{i,j}^{k}$,. Это означает, что при умножении $e_i \times e_j$ результатом является $\sum_k \lambda_{i,j}^{k} e_k$.
2. Случайное заполнение.
   - Для каждой пары (i, j) с вероятностью около 50–80 % устанавливать $1 - N$ ненулевых констант $\lambda_{i,j}^{k}$.
   - Остальные $\lambda_{i,j}^{k} = 0$ (прореживание).
3. Проверка ассоциативности.
   - Для всех u, v, w в $\{0,\ldots,m-1\}$ проверить $(e_u \cdot e_v) \cdot e_w = e_u \cdot (e_v \cdot e_w)$.
   - Если условие не выполнено, перегенерировать часть констант.
4. Поиск единицы.
   - Проверить, существует ли вектор E такой, что $E \cdot V = V \cdot E = V$ для всех V. Если да – алгебра унитальна, если нет – может быть выбрана неунитальная КНАА или выполняться дополнительный поиск.
5. Выход.
   - При успешной проверке ассоциативности возвращается Λ и, при необходимости, найденный E.

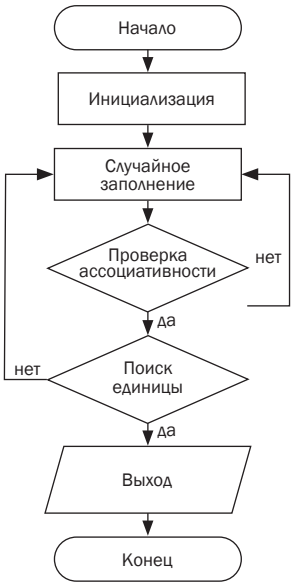

Схема 1. Генерация базовой структуры КНАА

Алгоритм 2. Персонализация КНАА и выбор скрытых векторов

1. Входные данные.
   - Исходная ТУББ Λ из Алгоритма 1, удовлетворяющая ассоциативности.
   - Параметры m, p.
   - Случайный $secretParam$ необходимой длины (128–256 бит).
2. Формирование Λ_{secret}.
   - Определить набор мелких сдвигов или модификаций, вычисленные на основе $secretParam$.
   - Для отдельных (i,j,k) обновить $\lambda_{i,j}^{k} \leftarrow \lambda_{i,j}^{k} + \delta_{i,j,k} \pmod p$.
   - Повторно проверить ассоциативность. Если нарушено, либо откатить изменения, либо генерировать другую последовательность δ.
3. Выбор векторов P, H.
   - Подобрать два вектора $P, H \in GF(p)$, такие что они порождают большие коммутативные подалгебры.
   - Убедиться, что P и H не коммутируют между собой.
4. Маскирующие векторы D, F.
   - При необходимости сгенерировать дополнительные векторы D и F, которые умножаются слева и справа от подписи.
5. Выход.
   - Возвращаем Λ_{secret}, а также набор (P, H, D, F), вся совокупность вышеуказанного теперь является секретными данными для схемы ЭЦП.

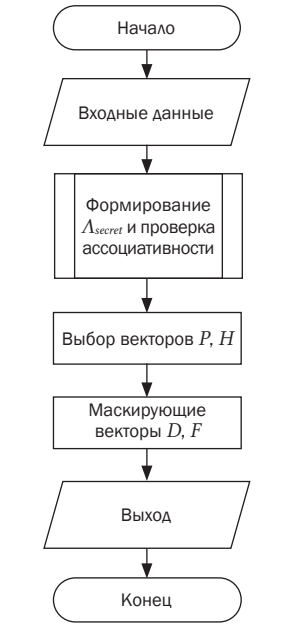

Схема 2. Персонализация КНАА и выбор скрытых векторов

Алгоритм 3. Алгоритм электронной подписи на КНАА

1. Генерация ключей
   - Закрытый ключ хранит полную таблицу Λ_{secret} или способ вычислять произведения, а также секретные векторы P, H, D, F.
   - Открытый ключ может содержать минимальный набор данных, позволяющий проверяющему умножать элементы в КНАА, при необходимости, дополнительные публичные параметры, к примеру, размерность m, модуль p, описания структуры.

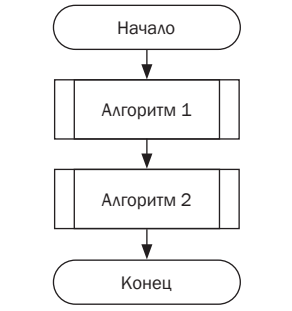

Схема 3. Генерация ключей

2. Подписание
   - Пусть имеется сообщение M. При необходимости вычислить его хеш $H(M)$. Сгенерировать случайные числа b и n заранее обозначенным образом, желательно с достаточно высокой энтропией.
   - Вычислить в КНАА значения $X = P^b$ и $Y = H^n$.
   - Построить подпись S следующим образом: $S = D \cdot X \cdot Y \cdot F$, где D и F – маскирующие элементы, затрудняющие выделение X и Y.
   - Сформировать выходную подпись σ, которая может содержать сам вектор S в зашифрованном или сжатом виде, а также возможные дополнительные метаданные для восстановления подписи.

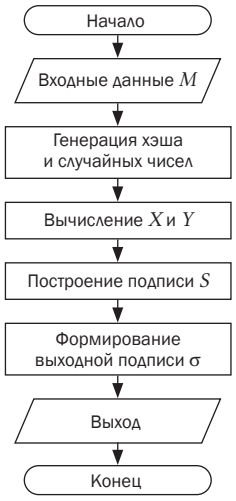

Схема 4. Подписание

3. Проверка
   - Проверяющий получает σ и M. При необходимости, имеет доступ к $H(M)$.
   - На основе публичных данных открытого ключа и публичной процедуры умножения в КНАА проверяет, что S соответствует ожидаемому уравнению.
   - Если сравнение проходит успешно, подпись считается валидной, в противном случае отклоняется.

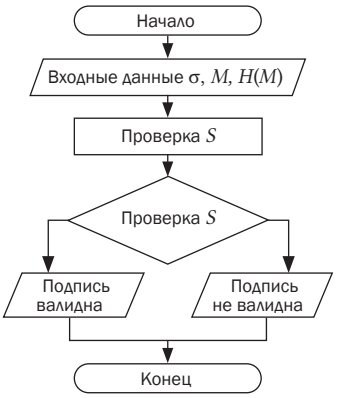

Схема 3. Проверка

3. При подписании генерируются случайные (b, n), вычисляются P^b, H^n, а итоговое $D \cdot (P^b) \cdot (H^n) \cdot F$ становится подписью;
4. Верификация использует публичную процедуру умножения и не позволяет восстановить Λ_{secret}.

Преимущества рассматриваемого базового криптопримитива

В рамках предложенного алгоритма электронной подписи (ЭЦП), построенного на некоммутативных ассоциативных алгебрах (КНАА), можно выделить несколько ключевых преимуществ:

1. **Некоммутативность и маскирование через две скрытые группы.**

Используются два вектора P и H, каждый из которых лежит в своём коммутативном подкольце, но в целом вся алгебра остаётся некоммутативной. Это затрудняет решение возникающих уравнений при попытке раскрыть (b, n). Маскирующие множители D, F скрывают прямое произведение $(P^b) \cdot (H^n)$, из-за чего злоумышленник не видит чистые степенные элементы и не может упростить выражение до хорошо изученных форм.

2. **Двойная усиленная рандомизация.**

В момент подписания выбираются две одноразовых экспоненты b и n, что даёт более высокий уровень «шума» по сравнению со схемами, использующими одну экспоненту. Это особенно важно при наличии большого числа известных подписей, поскольку такая конструкция усложняет попытки построения системы уравнений для криптоанализа [16].

3. **Компактность и вариативность ключей.**

При грамотном выборе структуры Λ можно достичь достаточно компактного представления открытых ключей. При этом не требуется экспоненциальное увеличение параметров, как в некоторых решеточных или кодовых схемах.

4. **Высокая производительность умножения.**

«Прореженные» ТУБВ позволяют ускорять умножение в КНАА, снижая число ненулевых $\lambda_{i,j}^k$. Возведение в степень реализуется достаточно быстро, если заранее оптимизировать ТУБВ.

5. **Сложность обратной задачи в некоммутативной алгебре.**

Известные на сегодняшний день атаки, включая квантовые алгоритмы Шора и Гровера, не дают

полиномиального решения для систем нелинейных уравнений в некоммутативных структурах. Таким образом, при корректном выборе параметров p, размерности m и наличии аппаратной защиты схема считается квантовоустойчивой [17].

Совокупность этих преимуществ делает ЭЦП на КНАА привлекательной для сред, где важны как производительность, так и высокий уровень стойкости, включая стойкость к потенциальным квантовым атакам.

3. Использование хаотических отображений для усиленной рандомизации

Одноразовые экспоненты (b, n), используемые при формировании подписи, можно получать через стандартный генератор случайных чисел (ГСЧ) [18]. Однако добавление хаотического отображения даёт дополнительный уровень непредсказуемости, т.к. оно порождает последовательности, крайне чувствительные к начальным условиям и параметрам. В результате злоумышленнику труднее обнаружить закономерности даже при накоплении большого числа подписей.

Пример логистического отображения

Одним из классических примеров является логистическая карта $x_{k+1} = rx_k(1 - x_k)$, при $r > 3{,}57$ возникает хаотический режим, в котором даже малая погрешность в x_0 приводит к экспоненциальному расхождению траекторий $\{x_k\}$.

Генерация экспонент

1. Инициализация: фиксируется (r, x_0) в секрете;
2. Итерация: перед каждым подписанием несколько раз вычисляем $x \leftarrow r \times x \times (1 - x)$, обновляя x на каждом шаге;
3. Преобразование: пусть x – результат после L итераций. Далее: $realValue = |x| mod\ 1$, таким образом берем дробную часть при необходимости, если x может выйти за 0...1. $tmp = [realValue \times 2^k]$, получаем k-битовую величину.
4. Сжатие по $mod\ p$: $b = tmp\ mod\ p$;
5. Использование: полученные b, n подставляем в P^b и H^n (см. Алгоритм 3), формируя подпись.

Утверждение 2. Хаотическое распределение значений экспонент b и n.

Пусть:

1. $GF(p)$ – поле характеристики q, где q – простое число.
2. Логистическое отображение задаётся как $x_k + 1 = rx_k(1 - x_k)$, $r \approx 4$, $x_0 \in (0, 1)$.
3. Начальное x_0 специально выбирается так, чтобы не попасть в какие-либо небольшие периодические окна, т. е. динамика $\{x_k\}$ остаётся хаотической в смысле эргодичности.

Определим, что при каждом k, $b_k = [x_k \cdot 2^K]\ mod\ q$, где K – достаточно большое целое число, задающее точность дискретизации в виде числа бит после двоичной запятой. Тогда при достаточно большом K величины $b_k \in \{0, \ldots, q-1\}$ распределяются практически равномерно, а вероятность коллизии $b_i = b_j$ при $i \neq j$ стремится к $1/q$. При этом $\{b_k\}$ приобретают свойства, близкие к истинной равномерной случайности, если отсутствует детерминированный доступ к x_0 и r.

Доказательство

На отрезке [0,1] при $r \approx 4$ логистическое отображение $x_k + 1 = rx_k(1 - x_k)$ обычно демонстрирует сложную, хаотическую динамику, за исключением особых значений x_0, ведущих к малым периодам. Из классической теории динамических систем (с учётом работ М. Фейгенбаума, Я. Синая и др.) известно, что для почти всех $x_0 \in (0,1)$ при r близком к 4 итерации $\{x_k\}$ образуют квазиэргодическую последовательность, не застревающую в периодиках.

Чтобы вывести равномерность по $GF(q)$, расщепим $[0,1)$ на q равных интервалов:

$$I_j = [j / q, (j + 1)/q), j = 0, \ldots, q - 1. \quad (3)$$

Если $x_k \in I_j$, можно сделать вывод, что дробная часть $x_k \cdot 2^K$ попадает в интервал, соответствующий j. Тогда $[x_k \cdot 2^K]\ mod\ q = j$.

В силу теории хаоса, последовательность $\{x_k\}$ распределена по $[0,1)$ приблизительно равномерно, если x_0 не порождён бифуркацией или периодической траекторией. Это означает, что для достаточно большого N, доля индексов $k \leq N$, при которых $x_k \in I_j$, сходится к $1/q$. Таким образом, $Pr[b_k = j] \approx 1/q$.

Событие $b_i = b_j$ для $i \neq j$ слабо коррелировано при истинно хаотическом режиме – фактически $\{b_k\}$ имитируют независимые равномерные выборы в $\{0, \ldots, q - 1\}$. Тогда $Pr[b_i = b_j] = 1/q$.

При росте K повышается точность набора $[x_k \cdot 2^K]$. Если K недостаточно велико, возможны «округлительные» ошибки, создающие преференции для некоторых остатков $mod\ q$. Но при $K \longrightarrow \infty$ доля таких ошибок становится незначительной. В частности, если K достаточно, x_k распознаётся почти непрерывно.

При этом:

1. Если x_0 – рациональное число с невысокой степенью в знаменателе, логистическая карта иногда входит в малый период, что нарушает квазиравномерность.
2. Если r не близко к 4, возможна другая, не хаотическая, картина, которую мы в данном контексте не рассматриваем.

Как видно, при типичных хаотических (r, x_0) и достаточно большом K значения $b_k = [x_k \cdot 2^K]\ mod\ q$ распределяются практически равномерно, а вероятность совпадения двух разных $b_i \neq b_j \approx 1/q$.

Это удостоверяет, что хаотический ГСЧ из Алгоритма 5 является статистически надёжным источником случайности в $GF(q)$. ч. т. д.

Результаты и выводы

Утверждение 2 подтверждает теоретические основания для использования логистического генератора в качестве хаотического ГСЧ, подаваемого на вход схемы подписи/шифрования. При нерегулярном x_0 и достаточном K образуемая последовательность $\{b_k\}$ в $GF(q)$ не несёт закономерных паттернов, способных облегчить криптоанализ, что существенно повышает уровень криптостойкости.

Хаотический слой усложняет попытки «подобрать» (b, n), даже если часть открытых данных известна. Следует отметить, что при вещественном логистическом отображении важно избегать так называемых периодических окон, а начальные параметры r, x_0 должны быть высокой точности и храниться в секрете. Таким образом, добавление хаоса повышает уровень рандомизации, делая схему на КНАА ещё более устойчивой к широкому спектру атак. Однако при этом становятся актуальными дополнительные исследования, лежащие вне темы данной работы, касательно практической целесообразности внедрения данного подхода в промышленные реализации схемы ЭЦП ввиду ограниченности вычислительных ресурсов и необходимой скорости работы таких реализаций.

4. Адаптивный подбор параметров КНАА

Даже при «прореженном» заполнении таблицы умножения Λ число вариантов при определенных условиях может оставаться достаточно большим [19]. Ручной перебор недостаточно удобен для повсеместного использования и не гарантирует оптимального баланса между скоростью умножения, ассоциативностью и размером ключей. Поэтому становится актуальным применение эволюционных алгоритмов (ЭА), которые по «поколениям» улучшат структуру Λ, не нарушая ассоциативности.

Эволюционная оптимизация

Обозначим каждую «особь» в ЭА как набор $\lambda_{i,j}^{k}$, после чего выполняются следующие шаги:

- формируется популяция предварительно проверенных на ассоциативность таблиц Λ;
- лучшим особям по совокупному показателю качества (fitness) даётся приоритет;
- специальный кроссовер комбинирует элементы таблиц-родителей, чтобы получить так называемых потомков, добавляя их в популяцию;
- в случайном порядке определяются мутации, которые вносят мелкие изменения δ в новые ТУББ. При этом если ассоциативность портится, особь удаляется;
- итерации (поколения) повторяют, пока не найдётся набор наилучших таблиц согласно установленному Pareto-оптимуму.

Результат и применение

Подводя итог описанному выше, ЭА помогает быстро находить подходящие структуры, решая при этом многокритериальную задачу согласно запросам пользователей. При этом возможно добавлять в функцию приспособленности (fitness) критериев вроде количества ненулевых λ, порядков подалгебр и т.д. Итоговые ТУББ остаются некоммутативными и достаточно сложными для криптоанализа, поскольку злоумышленник не знает $\lambda_{i,j}^{k}$. Адаптивный подбор параметров КНАА на базе эволюционных алгоритмов позволяет получать более эффективные (по конкретному показателю) конфигурации ТУББ для постквантовой подписи. При этом, аналогично с применением хаотических отображений, для данного подхода необходимы дополнительные исследования, подтверждающие или же опровергающие практическую целесообразность внедрения подхода в промышленные реализации.

5. Анализ результатов экспериментов и модель угроз

В данном разделе приводится итоговое исследование, проведенное на базе улучшенного ЭА поиска ассоциативных ТУББ для некоммутативных алгебр. В отличие от предыдущих версий, здесь увеличена размерность с $m = 4$ до $m = 8$, что делает структуру умножения существенно сложнее и позволяет сформировать большее семейство потенциальных криптопримитивов. Также реализованы предопределенные (precomputed) таблицы с различными вариантами вспомогательных предопределённых алгебр с циклическими свойствами, что дает широкий спектр исходных точек для ЭА и гарантирует ассоциативность стартовых решений. На основе полученных результатов формируются графики и итоговые ТУББ, отражающие эффективность и устойчивость предлагаемых подходов.

Общая характеристика экспериментов

Для ускорения вычислений и лучшей демонстрации возможностей был применен ряд усовершенствований. Для ускорения операций умножения и ассоциативных проверок применялась библиотека NumPy, что существенно ускорило вычисления. Для ускорения поиска ассоциативных структур мы использовали небольшое множество заранее подготовленных (precomputed) таблиц, что уменьшало число «плохих» кандидатов.

В ЭА в качестве эволюционирующих объектов выступали 8-мерные таблицы размером 8×8, в которых каждая ячейка является 8-мерным вектором. Инициализация осуществлялась случайной выборкой из заранее заготовленных структур. Затем применялись

специальные операции изоморфного кроссовера и мутации, которые перестраивали таблицы, причем каждое изменение потенциально могло нарушить ассоциативность, а все некорректные потомки отсекались. Для управления сложностью устанавливались параметры: объем популяции $POP\_SIZE = 20$ и количество поколений $GENERATIONS = 50$. Итогом работы стало получение лучшей ТУБВ, максимально повышающей значения фитнеса (fitness) – показателя, учитывающего быстродействие умножения, суммарные координаты векторов и критерий разнообразия.

Общие результаты также были проанализированы графически (Рис. 1, 2):

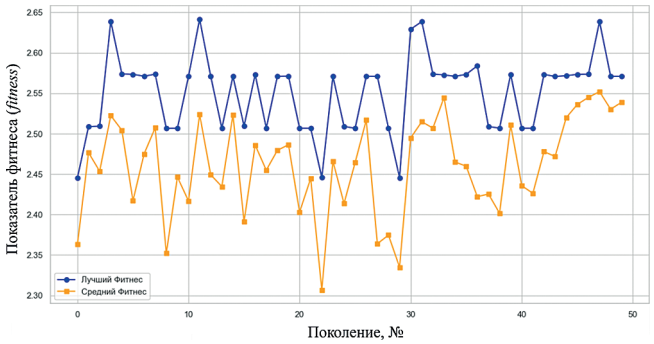

Рис. 1. Динамика лучшего и среднего фитнеса по поколениям

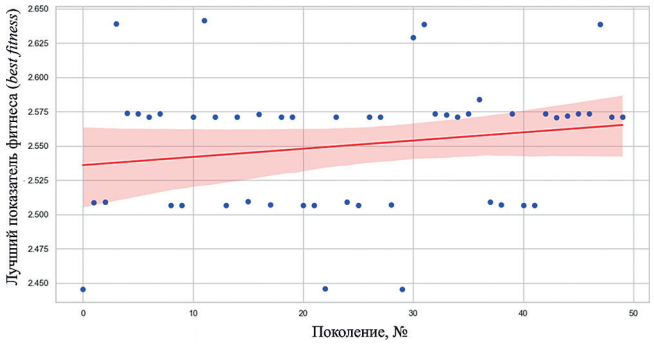

Рис. 2. Тренд-линия для лучшего фитнеса за поколение

Модель атак и теоретические аспекты

Совокупность методов, которыми может пользоваться злоумышленник, может быть рассмотрена как с классической, так и с квантовой точки зрения. Ниже кратко излагаются три наиболее актуальных направления для криптопримитивов на базе некоммутативных ассоциативных алгебр [20].

Прямая атака на секретные параметры

Наиболее очевидная угроза — попытка раскрыть ТУБВ или маскирующие векторы (D, F, P, H), достаточные для подделки подписи. Злоумышленник, как правило, стремится свести анализ к решению системы степенных уравнений в $GF(p)$. Такая система типично включает координаты векторов $(P^b,\ H^n)$, а также неизвестные (b, n, k, t). С ростом числа наблюдений растет число уравнений, однако некоммутативность, совмещенная с маскирующими множителями, многократно усложняет задачу. Практические эксперименты и теоретические результаты подтверждают экспоненциальную сложность подобных систем. Также немаловажно, что подмешивание хаотического генератора для случайных степеней (b, n) затрудняет любой подобный подход к криптоанализу.

Атака на основе множества известных подписей

Злоумышленник может накапливать набор σ_i подписей разных сообщений. Считая, что каждая подпись добавляет уравнения, связывающие (D, F) и случайные (b, n), атакующий рассчитывает, что итоговая система уравнений станет переопределенной, что позволит найти уникальное решение или значительно сократить пространство возможных решений. Тем не менее использование схемы с двумя скрытыми группами (P, H) и хаотическим выбором (b, n) приводит к тому, что данная возможность практически не просматривается. Для каждого экземпляра подписи возникает избыточное число степенных неизвестных, а система остается неразрешимой в пределах доступных ресурсов.

Квантовые атаки (Гровера, Шора)

Классические системы на дискретном логарифме или факторизации разрушаются алгоритмом Шора на квантовом компьютере в полиномиальное время. Однако для некоммутативных нелинейных задач пока не существует известных квантовых алгоритмов, способных решать их за полиномиальное время. Алгоритм Гровера дает квадратичное ускорение полного перебора, но при экспоненциальном характере проблемы такое ускорение не делает задачу потенциально выполнимой. Следовательно, при выборе $p \approx 2^{128} - 2^{256}$ и должном уровне энтропии хаотического генератора рассматриваемые криптопримитивы сохраняют постквантовую устойчивость.

Подводя итог вышеописанному, даже совокупность таких атак пока что не дает злоумышленнику эффективного пути к взлому системы. Тем не менее все сценарии требуют выбора больших p, обеспечения истинно случайных (b, n) и предотвращения утечек через аппаратные уязвимости и/или побочные каналы.

Модель угроз

Важно отметить, что безопасность любой криптосистемы определяется не только теоретической стойкостью, но и реалистичностью векторов атак и предположений о противнике. В контексте описанной схемы на КНАА, можно выделить несколько независимых направлений возможных угроз [10].

В первую очередь, сохраняется упомянутый выше риск компрометации самой математической структуры. Злоумышленник, располагающий большими вычислительными ресурсами, может попытаться решить системы нелинейных уравнений, извлекая секретные векторы или координаты (P^b, H^n). Хаотическое либо адаптивное изменение степеней (b, n), а также наличие разных скрытых групп (P, H) усложняют формализацию такой системы. В отличие от классических атак, к примеру на дискретный логарифм, здесь нет привычных методов, вроде алгоритма Полларда или BKW, т.к. некоммутативность и нелинейность сводят их преимущество на нет.

Во-вторых, угроза может исходить от попыток нарушить целостность или непредсказуемость хаотического генератора, генерирующего (b, n, k, t). Если злоумышленник подменит исходные параметры (r, x) или вычислит их, то сможет предсказывать генерацию секретных экспонент. Подобная ситуация уже возникала в атаках на линейные конгруэнтные генераторы, где небольшой объем псевдослучайных данных позволял вычислить весь механизм генерации.

Еще один класс угроз — атаки на реализацию в виде подмены кода библиотеки умножения, чтения кэш-паттернов или вредоносного внедрения в программный модуль, перехват значений (P^b, H^n) при выносе их из доверенной среды. История взломов RSA/ECC, где теоретически стойкие алгоритмы оказывались уязвимы в практических реализациях, подтверждают серьезность данного риска. Для минимизации таких атак предполагается хранение всех внутренних параметров $(\Lambda(D, F))$ и генератора хаотического состояния изолированно в выделенной доверенной среде (TEE). Однако и TEE может иметь недокументированные уязвимости, что требует более подробного изучения.

Наличие двух скрытых групп и хаотического генератора действительно усложняет чисто математический анализ, однако лишь при условии целостности реализации, корректного выбора больших p и затруднения каких-либо обходных путей для злоумышленника. В совокупности такая модель угроз показывает, что при соблюдении всех мер безопасности схема сохраняет высокий уровень стойкости даже при атаках с использованием ранее неизвестных квантовых алгоритмов.

Результаты экспериментов

Для демонстрации эффективности ЭА и полученного набора 8 мерных таблиц было проведено многократное тестирование программы при размере популяции $POP\_SIZE = 20$ и количестве поколений $GENERATIONS = 50$. В каждом запуске использовалось $DESIRED\_COUNT = 20$ заранее подготовленных ТУБВ, каждая из которых удовлетворяла ассоциативности в 8-мерном пространстве. Как показали многочисленные итерации экспериментальной программы:

- Большинство предопределенных таблиц, прошедших ассоциативность, имели стартовый фитнес порядка 2×10^7. При этом к пятидесятому поколению нередко достигались показатели $\sim 2{,}5 \times 10^7$ или выше;
- Периодические сообщения программы о недостатке новых особей в поколении свидетельствовали о том, что изоморфные кроссовер и мутация достаточно часто ломали ассоциативность, и часть потомков отсеивалась. Но общий тренд фитнеса оставался положительным (Рис. 3);
- Итоговая наилучшая таблица обычно имела заметный отрыв в скорости умножения и отвечала всем обязательным требованиям. Подписи, созданные на базе такой таблицы, корректно верифицировались;
- При некоторых запусках итоговый фитнес мог быть ниже, если исходная совокупность таблиц была менее оптимальна, однако наличие 20 заранее подготовленных структур существенно снижало риск «зацикливания» алгоритма в начальной фазе (Рис. 4).

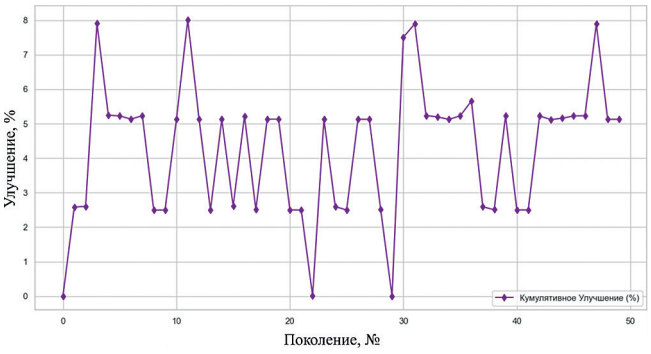

Рис. 3. Кумулятивное улучшение лучшего фитнеса

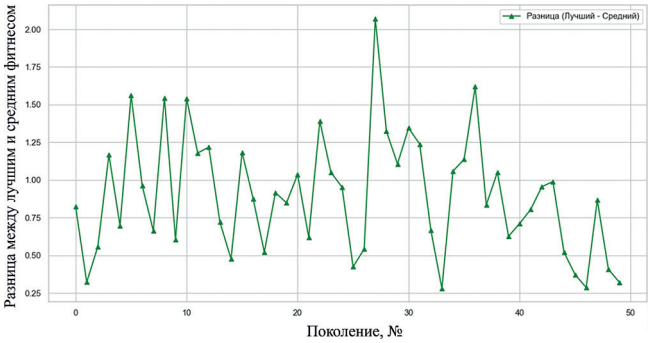

Рис. 4. Разница между лучшим и средним фитнесом по поколениям

Выводы по разделу и дальнейшее развитие

Проведённые эксперименты подтвердили, что эволюционная оптимизация ТУБВ с увеличением размерности до $m = 8$ помогает находить ассоциативные структуры, ускоряющие умножение и не увеличи-

вающие размер ключей. Модель угроз показывает, что использование двух скрытых групп P, H, хаотического выбора (b, n) и маскирующих векторов D, F делает атаки на схему ЭЦП достаточно затруднительными, включая атаки с использованием квантовых алгоритмов Шора и Гровера. При этом остаются риски неалгебраических методов взлома, вроде атак по побочным каналам или компрометации TEE, требующие аппаратных мер.

В перспективе целесообразно:

1. Расширить стартовые таблицы (precomputed) для ещё более быстрого нахождения подходящих вариантов ТУББВ;
2. Усовершенствовать критерии фитнеса, учитывая реальное время подписи, верификации, а также критерий сходства ТУББВ;
3. Рассмотреть поля большего порядка (128–256 бит) с аппаратным ускорением умножения;
4. Проанализировать методы защиты от побочных каналов и взлома генератора (b, n) на уровне выполнения в выделенной доверенной среды.

В целом эксперименты и рассмотренная модель угроз показывают, что при корректном выполнении всех рекомендаций представленный метод построения постквантовых алгоритмов ЭЦП может служить надежной основой для схем электронных подписей в условиях интенсивно развивающихся технологий, включая квантовые вычислители. Отметим, что в рамках данной работы мы ограничиваемся методологией и демонстрационными примерами, приведённые же алгоритмы дают общую концепцию построения криптопримитивов на КНАА, однако для практического протокола и последующей промышленной реализации необходима детальная спецификация формата подписей, процедуры верификации и т.д.

Заключение

В ходе работы был разработан метод построения постквантовых алгоритмов ЭЦП, опирающийся на КНАА. Было показано, что сочетание двойной рандомизации и хаотической генерации одноразовых экспонент (b,n) обеспечивает усиленную криптостойкость к большому количеству атак, и, в частности, к квантовым атакам, поскольку известные алгоритмы (Шора, Гровера) не дают полиномиального решения нелинейных систем в некоммутативном пространстве (Утверждение 1). Реализован ЭА для адаптивного подбора ТУББВ, упрощающий поиск подходящих структур. Проведённая экспериментальная проверка подтверждает эффективность предлагаемой схемы при определенных параметрах, при этом целесообразны дальнейшие исследования с целью выбора оптимальной конфигурации схемы ЭЦП в зависимости от наличия «дополняющих» подходов в условиях ограниченности вычислительных ресурсов.

Научная и практическая значимость состоит в том, что полученные алгоритмы, подходы и методики могут быть включены в дальнейшую разработку отечественных постквантовых систем электронной подписи и шифрования. Практическая достоверность решений подтверждена серией экспериментов, в которых формировались уникальные КНАА-структуры и моделировался процесс подписания при различных параметрах. Важным шагом на пути к формированию нового стандарта ЭЦП является подтверждение безопасности и производительности предложенной схемы через дополнительные исследования и практические испытания, что позволит реализовать предлагаемую схему ЭЦП на практике и обеспечить надежную защиту информации в условиях современных и будущих угроз.

Научный руководитель – Молдовян Николай Андреевич, доктор технических наук, профессор, главный научный сотрудник Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 6603837461. E-mail: moldovan.NA@talantiuspeh.ru

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение №23-03 от 27.09.2024 г.)

Литература

1. Молдовян Н.А., Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6. С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
2. Moldovyan N.A., Moldovyan A.A. P:ost-quantum signature algorithms with a hidden group and doubled verification equation // Information and Control Systems. 2023. No. 3. P. 59–69. DOI: 10.31799/1684-8853-2023-3-59-69.

3. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. No. 3 (103). P. 80–89. DOI: 10.56415/basm.y2023.i3.p80.
4. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova, 2024. V. 32. No. 1(94). P. 46–60. DOI: 10.56415/csjm.v32.04.
5. Молдовян Н.А., Молдовян А.А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.
6. Moldovyan D.N., Moldovyan N.A. Structure of a 4-dimensional algebra and generating parameters of the hidden logarithm problem // Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2022. Т. 18. Вып. 2. С. 209–217. DOI: 10.21638/11701/spbu10.2022.202.
7. Молдовян Д.Н., Молдовян А.А., Костина А.А. Алгебраические алгоритмы ЭЦП с полной рандомизацией подписи // Вопросы кибербезопасности. 2024. № 2(60). С. 93–100. DOI: 10.21681/2311-3456-2024-2-93-100.
8. Ding J., Petzoldt A., Schmidt D.S. Oil and Vinegar. In: Multivariate Public Key Cryptosystems // Advances in Information Security. Springer, New York, NY. 2020. V. 80. P. 89–151. DOI: 10.1007/978-1-0716-0987-3_5.
9. Cartor R., Cartor M., Lewis M., Smith-Tone D. Recent advances in Rainbow Signature Schemes. In: Cheon J.H., Johansson T. (eds) Post-Quantum Cryptography // Lecture Notes in Computer Science. 2022. P. 170–184. DOI: 10.1007/978-3-031-17234-2_9.
10. Petrenko A.S., Petrenko S.S., Makoveichuk K.A., Olifirov A.V. Security Threat Model Based on Analysis of Foreign National Quantum Programs // CEUR Workshop Proceedings. DLT 2021. 2021. P. 11–25.
11. Petrenko A.S., Petrenko S.A. Basic Algorithms Quantum Cryptanalysis // Вопросы кибербезопасности. 2023. No. 1 (53). P. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115.
12. Alexey Petrenko. Applied Quantum Cryptanalysis (scientific monograph). River Publishers, 2023. 222 pp. DOI: 10.1201/9781003392873.
13. Петренко А.С. Квантово-устойчивый блокчейн: как обеспечить безопасность блокчейн-экосистем и платформ в условиях атак с использованием квантового компьютера: – Санкт-Петербург: Питер, 2023. – 318 с.; ISBN 978-5-4461-2357-5
14. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. No. 2(86). P. 206–226.
15. Moldovyan A.A., Moldovyan D.N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023. Vol. 31. No. 1(91). P. 111–124. DOI: 10.56415/csjm.v31.06.
16. Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 185–248. DOI: 10.1007/978-1-0716-0987-3_8.
17. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2023. No. 17(2). Pp.210–226. DOI: 10.1049/ise2.12092.
18. Молдовян Д.Н., Костина А.А. Способ усиления рандомизации подписи в алгоритмах ЭЦП на некоммутативных алгебрах // Вопросы кибербезопасности. 2024. № 4(62). С. 71–81. DOI: 10.21681/2311-3456-2024-4-71-81.
19. Moldovyan D.N., Moldovyan N.A., Moldovyan A.A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022. Vol. 30. No. 1. P. 133–140. DOI: 10.56415/qrs.v30.11.
20. Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow. In: Cheon J.H., Johansson T. (eds) Post-Quantum Cryptography // Lecture Notes in Computer Science. 2022. V. 13512. P. 170–184. Springer, Cham. DOI: 10.1007/978-3-031-17234-2_9.

METHOD FOR CONSTRUCTING POST-QUANTUM ALGORITHMS OF EDS WITH TWO HIDDEN GROUPS

Petrenko A.S.[2]

Keywords: *post-quantum cryptography, noncommutative associative algebras, double randomization of signatures, chaotic maps, evolutionary algorithms, hidden commutative groups, quantum stability, digital signature, algebraic structure, key generation.*

Purpose of work *is to develop and substantiate a method for constructing post-quantum EDS algorithms based on finite noncommutative associative algebras, which provides enhanced signature randomization due to double groups and chaotic mappings, compact key sizes and high performance, as well as automated evolutionary design of the multiplication table structure.*

Research methods: *algebraic modeling of noncommutative structures and computer verification of the associativity of multiplication tables, mathematical modeling of the signature process and probabilistic assessment of cryptographic strength during mass signature collection, evolutionary search methods (evolutionary algorithms, crossover and mutation) for adaptive optimization of the structure of Λ, numerical experiments with the generation of one-time exponentials b, n through logistic mapping and testing of the received cryptoprimitive based on Python and the NumPy library.*

Research results: *a basic cryptographic asset has been formed that supports double randomization of the signature. It is shown that the chaotic generation of exponents (b,n) significantly complicates statistical cryptanalysis, even with mass collection of signatures. An adaptive evolutionary algorithm has been developed that allows for the orderly selection*

2 Alexei S. Petrenko, Ph.D. student of Saint Petersburg State Electrotechnical University «LETI», St. Petersburg, Russia, junior researcher of Scientific Center of Information Technologies and Artificial Intelligence of Sirius University of Science and Technology, Sirius Federal Territory, Russia. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

of the best tables without losing associativity. An experimental analysis was carried out, as a result of which the exponential complexity of attacks was confirmed with the correct choice of parameters, and the results of implementing the scheme on average hardware resources were demonstrated.

The scientific novelty: *a combination of noncommutative algebras with a double group and a chaotic generator is proposed, which increases the level of signature randomization. For the first time, the evolutionary search for table parameters was systematically applied to the task of constructing post-quantum EDS algorithms, which ensures associativity, speed, and theoretical cryptographic stability of the generated tables. The fundamental stability of such a scheme to quantum attacks is shown due to the lack of known polynomial algorithms for solving nonlinear systems in a noncommutative structure.*

The results were obtained *with the financial support of the project «Technologies for countering previously unknown quantum cyber threats», implemented within the framework of the state program of the «Sirius» Federal Territory «Scientific and technological development of the «Sirius» Federal Territory (Agreement No. 23-03 dated September 27, 2024).*

References

1. Moldovjan N.A., Petrenko A.S. Algebraicheskij algoritm JeCP s dvumja skrytymi gruppami // Voprosy kiberbezopasnosti. 2024. № 6. S. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
2. Moldovyan N.A., Moldovyan A.A. P:ost-quantum signature algorithms with a hidden group and doubled verification equation // Information and Control Systems. 2023. No. 3. P. 59–69. DOI: 10.31799/1684-8853-2023-3-59-69.
3. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. No. 3 (103). P. 80–89. DOI: 10.56415/basm.y2023.i3.p80.
4. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova, 2024. V. 32. No. 1(94). P. 46–60. DOI: 10.56415/csjm.v32.04.
5. Moldovjan N.A., Moldovjan A.A. Algoritmy JeCP na konechnyh nekommutativnyh algebrah nad poljami harakteristiki dva // Voprosy kiberbezopasnosti. 2022. № 3(49). S. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.
6. Moldovyan D.N., Moldovyan N.A. Structure of a 4-dimensional algebra and generating parameters of the hidden logarithm problem // Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2022. T. 18. Vyp. 2. S. 209–217. DOI: 10.21638/11701/spbu10.2022.202.
7. Moldovjan D.N., Moldovjan A.A., Kostina A.A. Algebraicheskie algoritmy JeCP s polnoj randomizaciej podpisi // Voprosy kiberbezopasnosti. 2024. № 2(60). S. 93–100. DOI: 10.21681/2311-3456-2024-2-93-100.
8. Ding J., Petzoldt A., Schmidt D.S. Oil and Vinegar. In: Multivariate Public Key Cryptosystems // Advances in Information Security. Springer, New York, NY. 2020. V. 80. P. 89–151. DOI: 10.1007/978-1-0716-0987-3_5.
9. Cartor R., Cartor M., Lewis M., Smith-Tone D. Recent advances in Rainbow Signature Schemes. In: Cheon J.H., Johansson T. (eds) Post-Quantum Cryptography // Lecture Notes in Computer Science. 2022. P. 170–184. DOI: 10.1007/978-3-031-17234-2_9.
10. Petrenko A.S., Petrenko S.S., Makoveichuk K.A., Olifirov A.V. Security Threat Model Based on Analysis of Foreign National Quantum Programs // CEUR Workshop Proceedings. DLT 2021. 2021. P. 11–25.
11. Petrenko A.S., Petrenko S.A. Basic Algorithms Quantum Cryptanalysis // Voprosy kiberbezopasnosti. 2023. No. 1 (53). P. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115.
12. Alexey Petrenko. Applied Quantum Cryptanalysis (scientific monograph). River Publishers, 2023. 222 pp. DOI: 10.1201/9781003392873.
13. Petrenko A.S. Kvantovo-ustojchivyj blokchejn: kak obespechit' bezopasnost' blokchejn-jekosistem i platform v uslovijah atak s ispol'zovaniem kvantovogo komp'jutera: – Sankt-Peterburg: Piter, 2023. – 318 s.; ISBN 978-5-4461-2357-5
14. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. No. 2(86). P. 206–226.
15. Moldovyan A.A., Moldovyan D.N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023. Vol. 31. No. 1(91). P. 111–124. DOI: 10.56415/csjm.v31.06.
16. Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 185–248. DOI: 10.1007/978-1-0716-0987-3_8.
17. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2023. No. 17(2). Rr.210-226. DOI: 10.1049/ise2.12092.
18. Moldovjan D.N., Kostina A.A. Sposob usilenija randomizacii podpisi v algoritmah JeCP na nekommutativnyh algebrah // Voprosy kiberbezopasnosti. 2024. № 4(62). S. 71–81. DOI: 10.21681/2311-3456-2024-4-71-81.
19. Moldovyan D.N., Moldovyan N.A., Moldovyan A.A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022. Vol. 30. No. 1. P. 133–140. DOI: 10.56415/qrs.v30.11.
20. Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow. In: Cheon J.H., Johansson T. (eds) Post-Quantum Cryptography // Lecture Notes in Computer Science. 2022. V. 13512. P. 170–184. Springer, Cham. DOI: 10.1007/978-3-031-17234-2_9.