ПАРАМЕТРИЗАЦИЯ ПОСТКВАНТОВОЙ ЭЛЕКТРОННОЙ ПОДПИСИ КНАА-2-ЭЦП

Петренко А. С.[1]

DOI: 10.21681/2311-3456-2025-5-88-95

Цель работы: *формализовать выбор параметров и определение требований к КНАА-2-ЭЦП, обеспечивающих постквантовую устойчивость (не ниже 2^{200} для Cat 3 и 2^{256} для Cat 5) при сокращении длины подписи до 112 байт (Cat 3) и 128 байт (Cat 5).*

Метод исследования: *обоснование соответствия КНАА-2-ЭЦП нормативам FIPS 204/205/206, SP 800-57-1 Rev.5, ISO/IEC 14888-4:2024 и ГОСТ Р 34.10-2018 с точным определением форматов ASN.1/DER и OID, разработка двух наборов параметров для категорий стойкости 3 и 5 по шкале NIST, задание количественных целевых показателей, формулирование обязательных требований к реализации, в частности константного времени, корректной рандомизации и контрмер.*

Результаты исследования: *установлены два набора параметров, обеспечивающие стойкость $\geq 2^{200}$ (Cat 3) и $\geq 2^{256}$ (Cat 5) и компактность ключей и подписей, определены требования к размеру ключей и подписи, заданы метрики производительности и безопасности, установлены критерии проверки корректности реализации без полного цикла ACVP, регламентированы форматы и процедуры валидации, определены контрмеры против побочных атак и требования к постоянному времени выполнения.*

Научная и практическая значимость *результатов статьи заключается в том, что найденные параметры, требования и профили использования впервые демонстрирует реализацию усиленной рандомизации подписи без удвоения проверочного уравнения, обеспечивая компактность ключей и подписей при сохранении высокой стойкости к квантовым атакам и к атакам по побочным каналам. Это позволяет значительно снизить объем транзакционных данных и требования к пропускной способности сетей и хранилищ, что критически важно для масштабируемых блокчейн-систем, аппаратных криптопроцессоров и энергоэффективных IoT-устройств.*

Ключевые слова: *конечная некоммутативная ассоциативная алгебра; форматы ASN.1/DER; категории стойкости NIST; константное время выполнения; рандомизация подписи; контрмеры безопасности; постквантовая электронная подпись.*

Введение. Рекомендации нормативных документов

Структурно выбор параметров и определение требований основываются на шести документах, напрямую определяющих современные требования к постквантовым электронным подписям и их валидации. Первые три – это стандарты Национального института стандартов и технологий США, целиком посвящённые подписи. Так, FIPS 204 описывает решётчатую схему ML DSA (прежнее название Dilithium) и задаёт образцовую структуру постквантового стандарта от административных пунктов до приложений с контрольными примерами [1]. FIPS 205 регламентирует хэш подпись без сохранения состояния SLH DSA (производную от SPHINCS+) [2]. FIPS 206, находящийся на завершающем этапе утверждения, посвящён подписи FN DSA (Falcon) и примечателен минимальным из финалистов NIST объёмом подписи в 666 байт [3].

Также немаловажно рассмотреть NIST SP 800 57 1 (в 5 редакции), в котором введена шкала категорий криптографической стойкости и приведено сопоставление этих категорий с длинами симметричных ключей [4]. На основании этого документа в текущей статье определены два уровня безопасности – категория 3 ($\approx 2^{200}$ операций перебора) и категория 5 ($\approx 2^{256}$).

Международный стандарт ISO/IEC 14888 4 (2024 г.) посвящён хэш подписям с сохранением состояния [5], его ценность для данной работы состоит в едином формате представления открытых ключей и подписей на языке ASN.1. Формат основывается на структурах SEQUENCE, где модуль p и базисные векторы кодируются как INTEGER и OCTET STRING соответственно, аналогично разделу A.1 FIPS 204. КНАА-2 ЭЦП оформлена в том же формате ASN.1 с кодированием DER (Distinguished Encoding Rules, канонические двоичные правила кодирования ASN.1), что обеспечивает легкое внедрение в существующие инфраструктуры открытых ключей [6].

Дополнительно целесообразно ориентироваться на ГОСТ Р 34.10-2018 «Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки электронной подписи». Хотя данный стандарт и регламентирует классическую подпись на эллиптических кривых,

1 Петренко Алексей Сергеевич, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E mail: a.petrenko1999@rambler.ru

он подробно описывает форматы представления ключей и подписей, процедуры одиночного контрольного примера (KAT), отрицательного теста и парной согласованности ключа. Наконец, ГОСТ 19.105 78 и ГОСТ 19.301 79 определяют требования к оформлению программной документации и методик испытаний.

Перечисленные документы в совокупности образуют достаточную нормативную базу для валидации постквантовой электронной подписи КНАА-2-ЭЦП [7]. Они определяют диапазоны параметров, форму представления результатов и минимальный набор контрольных испытаний, благодаря чему характеристики КНАА-2 ЭЦП можно прямо сопоставлять с утверждёнными и проектируемыми постквантовыми стандартами ЭЦП [8-11].

В статье используются следующие обозначения:

- σ – электронная подпись (результат алгоритма Sign);
- pk / sk – открытый и секретный ключ соответственно;
- v – вектор фиксатор (компонента подписи);
- r, s – скалярные компоненты подписи;
- p – модуль конечного поля $GF(p)$;
- mul – одна операция умножения в $GF(p)$ с последующей редукцией по модулю p.

Применяемые наборы параметров

Используются две целевые категории, определённые руководством NIST SP 800 57 1: категория 3 и категория 5. Категория 3 сопоставима с полной подборкой, требующей порядка 2^{200} элементарных операций, что эквивалентно симметричному ключу длиной не менее 192 бит. Категория 5 соответствует трудоёмкости 2^{256} и соответствует уровню безопасности симметричного ключа длиной 256 бит, тем самым обеспечивая максимально возможный запас прочности в открытой публикации NIST. Ниже в таблице 1 приведено краткое соответствие между категориями, минимальными длинами симметричных ключей и наиболее близкими параметрами уже утверждённых NIST схем подписей (σ – обозначение результирующей электронной подписи).

Таблица 1.

Сопоставление категорий стойкости NIST, эквивалентных симметричных ключей и размеров подписей ML DSA и SLH DSA

Категория NIST	Симметричный ключ (экв.)	Подпись FIPS 204 (ML DSA)	Подпись FIPS 205 (SLH DSA)
3	≥ 192 бит	ML DSA 65 (кат. 3): $\sigma \approx 3{,}23$ КБ	SPHINCS+ 192s: $\sigma \approx 15{,}9$ КБ
5	≥ 256 бит	ML DSA 87 (кат. 5): $\sigma \approx 4{,}52$ КБ	SPHINCS+ 256s: $\sigma \approx 29{,}1$ КБ

Переход от теоретических категорий к конкретным параметрам схемы КНАА-2 ЭЦП основан на следующем результате. Задача восстановления секретного вектора сводится к решению уравнения высокой степени в конечной ассоциативной алгебре, а её сложность оценивается снизу сведением к задаче поиска короткого вектора (SVP) размерности 4. Для параметров, приведённых далее, эта сложность не меньше 2^{200} и 2^{256} операций соответственно, что надёжно покрывает требования двух выбранных категорий.

Практически же категории разделяют области применения, так уровень 3 достаточен для массовых транзакций и пользовательских электронных удостоверений с жизненным циклом до 15 лет, когда как уровень 5 предназначен для долгосрочного нотариального хранения, критических государственных регистров и инфраструктур, рассчитанных на горизонты более тридцати лет. В обеих ситуациях сокращение подписи до 112–128 байт позволяет не менять форматы блоков и сохранять пропускную способность систем даже при полном переходе на постквантовую криптографию.

В данной статье в качестве объектов сравнения используются стандартизованные или находящиеся в финальной стадии стандартизации алгоритмы постквантовой ЭЦП (Dilithium, Falcon, SPHINCS+), а также разработанная схема на основе КНАА. При этом схемы XMSS и LMS, равно как и отечественные ЭЦП (Шиповник, Крыжовник и Гиперикум), в сравнительный анализ не включены ввиду отсутствия их формализованной стандартизации, ограниченности распространённых реализаций и других прикладных барьеров.

Для каждой из двух целевых категорий стойкости установлены конкретные величины открытого ключа, подписи, секретного ключа и трудоёмкости операций подписи и проверки. Таблица 2 сводит полученные значения. При этом mul – это одна операция умножения в поле $GF(p)$ с редукцией по модулю p. Число mul (напр. 9 200 при Verify) показывает трудоёмкость независимо от платформы.

Данные в таблице являются нормативной «верхней границей», реализация же, предъявляемая к испытаниям, должна удовлетворять указанным размерам и не выходить за пределы трудоёмкости операций.

Определяющим конкурентным параметром КНАА-2 ЭЦП является объём результирующей подписи σ. Для выбранных наборов параметров (табл. 1) длина подписи равна 112 байт в категории 3 и 128 байт в категории 5. Ниже в таблице 3 приведено сравнение с действующими и проектируемыми постквантовыми стандартами (данные взяты из текстов FIPS и технических отчётов NIST).

DOI: 10.21681/2311-3456-2025-5-88-95

Таблица 2.

Основные параметры KHAA 2 ЭЦП и трудоёмкость операций для категорий 3 и 5

Показатель	Категория 3	Категория 5
Модуль поля p (двоичных разрядов)	64 бит (реком. $p = 2^{64} - 59$)	128 бит (реком. $p = 2^{128} - 159$)
Размер открытого ключа pk	512 байт (прототип)	704 байт (прототип)
Размер подписи σ	112 байт (прототип)	128 байт (прототип)
Размер секретного ключа sk	640 байт	768 байт
Операций умножения $GF(p)$ при Sign (процедуре подписи)	6 600 mul	6 530 mul
Операций умножения $GF(p)$ при Verify (процедуре проверки)	9 200 mul	9 200 mul

Таблица 3.

Длины подписей постквантовых схем

Алгоритм (категория стойкости)	Длина подписи, байт
KNAA-2 ЭЦП Cat 3	112
KNAA-2 ЭЦП Cat 5	128
FN DSA (Falcon 512, Cat 1)	666
FN DSA (Falcon 1024, Cat 5)	1 280
ML DSA (Dilithium 44, Cat 3)	2 420
ML DSA (Dilithium 87, Cat 5)	4 595
SLH DSA (SPHINCS+ 128s)	7 856
SLH DSA (SPHINCS+ 256s)	41 472

Сокращение подписи до сотен байт имеет два практических следствия. Во-первых, объём блока в распределённом реестре не увеличивается при переходе на постквантовую криптографию, что позволяет сохранять прежний уровень пропускной способности сети и прежнюю стоимость транзакций. Во-вторых, сужается полоса пропускания каналов связи и объём долговременного хранилища: при средней нагрузке 10 000 транзакций в минуту годовой выигрыш объёма относительно схемы Falcon 1024 составляет порядка 10 ТБ.

Показатель длины подписи выбран ключевым критерием эффективности, а следовательно любые оптимизации реализации не должны приводить к увеличению значения σ выше норм, зафиксированных в таблице 2.

Выбор числовых параметров KHAA-2 ЭЦП осуществлялся исходя из достаточной криптографической стойкости и технологической реализуемости на массовых аппаратных платформах.

С точки зрения стойкости фиксированы два предельных модуля поля: $p_{64} = 2^{64} - 59$ для категории 3 и $p_{128} = 2^{128} - 159$ для категории 5. Оба значения являются простыми и удовлетворяют условию $r = p^2 + p + 1$ – простое, что обеспечивает отсутствие малых множителей в порядке мультипликативной подгруппы и равномерное распределение коэффициентов векторов. При таких модулях плотность перебора возможных значений вектора фиксатора превышает 2^{200} и 2^{256} соответственно, что надёжно перекрывает минимальные требования категорий стойкости.

Вторым ограничением служит норма секретных векторов. Для категории 3 установлено значение $\|s\| \le 2^{31}$, при этом среднее число ненулевых коэффициентов в процедуре поиска короткого вектора не превышает 72, а полный перебор оказывается эквивалентным 2^{200} шагам. Для категории 5 норма сокращена до $\|s\| \le 2^{17}$, при расширении поля до 128 бит, что увеличивает сопротивляемость атаке перебора коэффициентов до уровня 2^{256}.

Операционное ограничение связано с возможностями современных 64 и 128 битовых процессоров, так умножение координат модуля p_{64} выполняется одной инструкцией, а умножение по p_{128} – двумя последовательными операциям $mul\ lo$ / $mul\ hi$ без привлечения арифметики с плавающей запятой. $mul\ lo$ / mul hi это пара 64 битных инструкций, которые по очереди выдают младшие и старшие 64 бита из 128 битного произведения двух слов. На x86 64 это MUL (низ) и MULH (верх), а на ARM – UMULH для старшей части. В схеме категории 5 одна операция умножения $GF(p)$ реализуется именно этой парой – сначала $mul\ lo$, затем $mul\ hi$, после чего выполняется редукция по модулю p. Тем самым достигается заявленное число умножений (6 600 / 9 200), а время проверки подписи ориентировочно 0,5 μs (микросекунд) на ядро 3 ГГц (при компилируемой реализации).

Наконец, размеры открытого и секретного ключей (512/704 байт и 640/768 байт в зависимости

от категории) выбраны так, чтобы полностью помещаться в память типового защищённого микроконтроллера и в регистр хранилища аппаратного модуля HSM без фрагментации. В совокупности предложенные параметры гарантируют необходимый уровень стойкости и соответствуют практическим ограничениям вычислительных и коммуникационных ресурсов.

Требования безопасности

Корректная реализация КНАА-2 ЭЦП должна обеспечивать постоянное (равномерное) время выполнения всех операций формирования и проверки подписи. Продолжительность вычислений не может зависеть от содержимого секретных данных, иначе возникает возможность побочных атак по времени или по электромагнитному излучению. Настоящее требование согласуется с разделом 9 стандартов FIPS 204 и FIPS 205, где прямо предписывается исключать любые условные переходы (ветвление) кода, условно связанные с закрытой информацией.

В практическом исполнении это означает следующее. Все арифметические действия над элементами поля $GF(p)$ – умножения, возведения в степень, сложения и вычитания – выполняются по фиксированному числу машинных инструкций, а использование таблиц переходов, где адрес ячейки определяется секретным индексом, не допускается. Переходы между функциями и выбор алгоритмических ветвей разрешается основывать лишь на открытых параметрах, известных ещё до начала криптографического процесса, таких как размер модуля p, категория стойкости или вариант компиляции.

Равномерность времени при этом оценивается экспериментально, на серии из десяти тысяч однотипных тестовых примеров измеряется медиана длительности цикла «подпись – проверка». Разброс между минимальным и максимальным значениями не должен превышать одного процента от медианы. Измерения могут проводиться как средствами программного профилирования (например, perf stat с подсчётом тактов), так и аппаратным методом – прямым наблюдением сигнала питания с временным разрешением не хуже одной наносекунды. При превышении указанного порога реализация считается не отвечающей требованиям и подлежит доработке.

Следует отметить, что алгоритм КНАА-2 ЭЦП требует случайных данных только при генерации секретных ключей, они же создаются на базе логистического хаотического отображения:

$$x_{\ell+1} = r\, x_\ell\, (1 - x_\ell), \quad 3{,}999 \le r \le 4, \quad 0 < x_0 < 1.$$

При указанном значении параметра r траектория отображения демонстрирует режим полностью развитого хаоса ($r \approx 4$): малейшие изменения начального условия x_0 приводят к непредсказуемому расхождению последовательностей. Числовые выходы x_ℓ после преобразования в двоичную форму (берутся младшие 32 бита каждого результата умножения) служат источником случайности для детерминированного генератора псевдослучайных чисел (DRBG), реализованного по рекомендациям ГОСТ Р 50.1.111-2016 и NIST SP 800-90A Rev.1 (DRBG). DRBG реализован как Hash_DRBG на SHA 256 (NIST SP 800 90A Rev.1) vtnjlb100] и, альтернативно, как ГОСТ-совместимый генератор на хэше «Стрибог-256» (ГОСТ Р 34.11-2012). В реализации выбирается один из механизмов, но тесты качества (NIST STS, автотест DRBG) выполняются для выбранного варианта.

Процедура инициализации включает три шага.

1. Из встроенного стохастического генератора TRNG (True Random Number Generator) [12] считывается 256 битовое начальное значение (seed), которое интерпретируется как вещественное x_0 в интервале (0,1).
2. Логистическое отображение выполняется в 1024 итерациях (1000 начальных + 24 для выборки), чтобы исключить корреляцию с x_0. Результаты x_{1000}, … , x_{1023} переводятся в 32 битовые слова и подаются на вход DRBG.
3. DRBG выдаёт требуемый объём случайных байтов для наполнения секретных векторов схемы.

Качество полученного потока проверяют по трём критериям:

- прохождение стандартного статистического набора NIST STS с p-value (уровень значимости) каждой процедуры не ниже 0,01;
- отсутствие значимых автокорреляций на интервале до 128 символов (показатель взаимной корреляции не выше 0,05);
- положительный результат встроенного автотеста DRBG при каждом запуске.

Совместное использование трёх источников неопределённости в виде аппаратного TRNG, хаотического логистического отображения и крипто-стойкого DRBG способно обеспечить непрерывность случайного потока и исключает предсказуемость секретных параметров генерации ключей.

OID-идентификация и форматы ASN.1

Идентификаторы объектов.

Организации разработчику выделяется номер <OrgID> в ветви 1.3.6.1.4.1. Для схемы КНАА-2 ЭЦП резервируются два объекта (формальный синтаксис ASN.1) (см. вставку 1).

Все целые поля записываются без знака, в формате big endian. Эти структуры можно прямо вкладывать в сертификат X.509 (стандартный контейнер открытого ключа (RFC 5280)) [13], контейнер CMS (Cryptographic Message Syntax, формат электронных подписей и зашифрованных сообщений (RFC 5652))

```
knaadsaCat3OID  OBJECT IDENTIFIER ::=   { iso(1) org(3) dod(6) internet(1)
                                        private(4) enterprise(1)
                                        <OrgID> 1 }
knaadsaCat5OID  OBJECT IDENTIFIER ::=   { iso(1) org(3) dod(6) internet(1)
                                        private(4) enterprise(1)
                                        <OrgID> 2 }
Первый обозначает параметры категории стойкости 3, второй параметры категории 5.
Форматы данных (формальный синтаксис ASN.1).
KNAADSA-Types DEFINITIONS ::= BEGIN
KnaadsaPublicKey ::= SEQUENCE {
       modulus       INTEGER,             -- простое p (64 или 128 бит)
       basis         OCTET STRING         -- 4×4 коэффициентов (32 байта)
}
KnaadsaPrivateKey ::= SEQUENCE {
       publicPart  KnaadsaPublicKey,
       seed          OCTET STRING,        -- начальное x0 логистического отображения
       secretVecs    OCTET STRING         -- s1 || s2 (по 4 элемента)
}
KnaadsaSignature ::= SEQUENCE {
       vVector       OCTET STRING,        -- вектор-фиксатор (32 байта)
       rScalar       INTEGER,
       sScalar       INTEGER
}
END
```

Вставка 1

[14] или объект PKCS #11 (запись ключа или подписи внутри аппаратного токена HSM), для этого достаточно указать OID knaadsaCat3OID либо knaadsaCat5OID.

Профили применения алгоритма

Для различных эксплуатационных сценариев задаются три профиля, различающиеся только внешними параметрами вызовов и способом упаковки данных, внутренняя математика алгоритма при этом остаётся неизменной.

Профиль P-SINGLE (одиночная подпись транзакции).

Используется в клиентских приложениях и лёгких кошельках. На вход функции подписи передаются сообщение M произвольной длины и секретный ключ категории 3 или 5. Полученная подпись добавляется непосредственно в поле транзакции (приведено в виде псевдокода):

```
function sign_single(sk, M):
        (v, r, s) ← Sign(M, sk)
        return (v, r, s)
```

Вставка 2

Верификация выполняется узлами сети, открытый ключ хранится в структуре аккаунта.

Профиль P-AGG (агрегированная подпись узлов валидаторов).

Предназначен для протоколов консенсуса, где множество валидаторов подтверждает один блок. Подписи формируются независимо, затем компонента v агрегируется путём поэлементного умножения, после чего совместно вычисляется скаляр r_{sum}. Это позволяет держать размер агрегированной подписи фиксированным в виде трех элементов, независимо от количества участников (приведено в виде псевдокода):

```
function aggregate_signatures (list_of_
signatures):
    v_prod ← 1
    r_sum  ← 0
    s_sum  ← 0
    for (v, r, s) in list_of_signatures:
        v_prod ← v_prod * v
        r_sum  ← r_sum  + r
        s_sum  ← s_sum  + s
    return (v_prod, r_sum mod p, s_sum mod p)
```

Вставка 3

Корректность проверяется единожды для объединённой тройки.

Профиль P-PRECOMP (предкомпилированная проверка в виртуальной машине). Используется в исполнителях смарт контрактов. Функция проверки переносится во встроенный модуль виртуальной машины (EVM core) как предкомпилированный контракт (precompile) для ускорения. Формат вызова (приведен в виде псевдокода):

```
precompile id = 0xD3...
input  = pk ‖ v ‖ r ‖ s ‖ hash(M)
output = 0x01 (valid) | 0x00 (invalid)
```

Вставка 4

Газ (gas) – расчётная единица, которой EVM-совместимые сети измеряют стоимость вычислений, так каждая операция интерпретатора имеет фиксированную цену в газ, а плата пользователя равна произведению объёма газ на текущую цену токена. Для предкомпилированной проверки КНАА-2-ЭЦП (идентификатор 0xD3) принимается тариф: 8 000 газ базово + 3 газ за каждые 100 операций mul в $GF(p)$. Для 9 200 mul это 35 600 газ. Тариф выбран по аналогии с EIP 198 (modexp) и существующими предкомпиляциями EVM. Такое соотношение стандартной и переменной частей делает новую проверку сопоставимой по стоимости с уже существующими криптографическими предкомпилированными контрактами и упрощает экономическую модель смарт-контрактов.

Особенности реализации КНАА-2 ЭЦП

Также для корректной реализации важны следующие контрмеры, представленные на рисунке 1:

1. Постоянное время (Timing SAF).
   - Единственный путь исполнения, отсутствие if/else, зависящих от секретных значений.
   - Таблицы допускаются только с фиксированным, независящим от секрета индексом, перебор осуществляется по всем элементам, если требуется выбор.
   - Допустимое расхождение полного цикла «подпись → проверка» не более ±1 % от медианы по 10 000 измерений (измеряется утилитой perf stat -e cycles с подсчётом тактов процессора).
2. Маскирование секретных векторов (Add Mask).
   - Перед вычислением формируется 256 битная маска m через DRBG.
   - Вектор фиксатор и скаляры обновляются $v \leftarrow v + m$, $r \leftarrow r + m \pmod p$.
   - Маска уничтожается вызовом explicit_bzero (или эквивалентной функцией безопасного обнуления памяти) сразу после шага, без задержки хранения в ОЗУ.
3. Контроль диапазона (Range Check).
   - Каждая координата после операции проверяется на условие $0 \le x_i < p$.
   - Нарушение диапазона интерпретируется как возможный сбой питания или же как лазерная инъекция, в таком случае реализация обнуляет ключи и выходит в аварийный режим.
4. Лимит использования ключа (Key Reuse Cap).
   - Категория 3: максимум 10 000 подписей на пару pk,sk.
   - Категория 5: максимум 100 000 подписей.
   - Таймер повторной функции генерации ключей (keygen) ведётся в неизменяемой памяти, при достижении порога ключ помечается недействительным, генерируется новый с обновлённым начальным значением (seed) из TRNG.
   - Реализации на интерпретируемых языках (Python, JavaScript) допустимы в лабораторной фазе, но на промышленном этапе должны заменяться компилируемым модулем, чтобы выдержать лимиты времени проверки (< 10 μs на Cat 5)

Перечисленные меры реализуются на уровне библиотечного кода и не влияют на размеры подписи или ключей, обеспечивая защиту от побочных временных, корреляционных и сбойных атак при сохранении целевых показателей производительности.

Заключение

В работе сформулированы и достигнуты основные цели по параметризации и валидации постквантовой электронной подписи КНАА-2-ЭЦП. Выбраны и обоснованы два набора параметров для категорий стойкости 3 и 5 по шкале NIST, обеспечивающие требуемый запас криптографической стойкости. Достигнуты целевые показатели эффективности, длина подписи ≤ 112 байт (Cat 3) и ≤ 128 байт (Cat 5) при числе операций проверки ≤ 9 200 mul и времени Verify ≤ 0,5 мкс в компилируемой реализации.

Установлены строгие требования к реализации, включая постоянное время исполнения, корректное

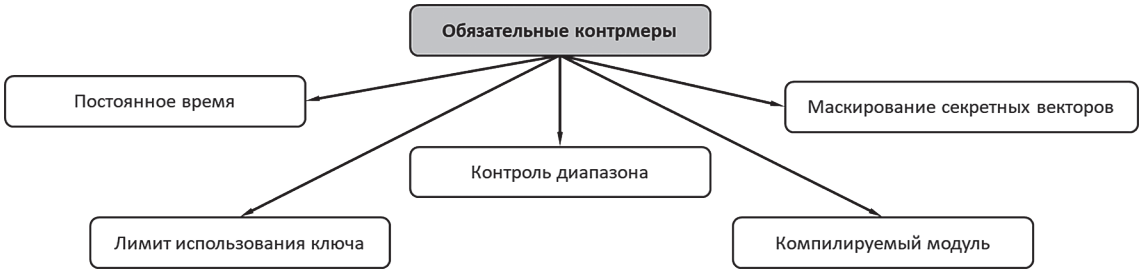

Рис.1. Обязательные контрмеры при программной реализации

использование DRBG и обязательные контрмеры. Что в свою очередь гарантирует устойчивость к атакам по побочным каналам без ухудшения целевых характеристик производительности.

Определены форматы данных ASN.1/DER с соответствующими OID идентификаторами и профили применения алгоритма для различных сценариев использования в блокчейн-сетях, HSM и IoT-устройствах. Полученные результаты создают основу для тематических испытаний и исследований КНАА-2-ЭЦП и его практического внедрения в квантово-устойчивые криптографические системы в дальнейшем.

Исследование выполнено за счет гранта Российского научного фонда № 24-41-04006.
https://rscf.ru/project/24-41-04006/

Литература

1. FIPS PUB 204. Module-Lattice-Based Digital Signature Algorithm (ML-DSA). – Gaithersburg, MD: National Institute of Standards and Technology, 2024. – 65 p. – DOI: 10.6028/NIST.FIPS.204.
2. FIPS PUB 205. Stateless Hash-Based Digital Signature Algorithm (SLH-DSA). – Gaithersburg, MD: National Institute of Standards and Technology, 2024. – 76 p. – DOI: 10.6028/NIST.FIPS.205.
3. FIPS PUB 206. Falcon Digital Signature Algorithm. – Gaithersburg, MD: National Institute of Standards and Technology, 2025. – 72 p.
4. Barker E., Chen L., Roginsky A., Mani A., Smid M., Polk T. Recommendation for Key Management, Part 1: General (Revision 5). – NIST Special Publication SP 800-57 Part 1 Rev.5. – Gaithersburg, MD: National Institute of Standards and Technology, 2020. – DOI:10.6028/NIST.SP.800-57pt1r5.
5. ISO/IEC 14888-4:2024. Information security – Cryptographic techniques – Digital signatures with appendix – Part 4: Stateful hash-based mechanisms. – Geneva: ISO/IEC, 2024.
6. ITU-T Recommendation X.680 (08/2021). Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. — Geneva: ITU-T, 2021.
7. Молдовян Н. А., Петренко А. С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6(64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
8. Markov, A. S., Varenitca, V. V., Arustamyan, S. S. Topical issues in the implementation of secure software development processes. (2023). In the collection: Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance. IPSQDA-2023. P. 48–53.
9. Балябин А. А., Петренко С. А. Модель блокчейн-платформы с кибериммунитетом в условиях квантовых атак // Вопросы кибербезопасности. 2025. № 3(67). С. 72–82. DOI: 10.21681/2311-3456-2025-3-72-82.
10. Петренко А. С., Петренко С. А. Основные алгоритмы квантового криптоанализа // Вопросы кибербезопасности. 2023. № 1(53). С. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115.
11. Petrenko, A. S. Applied Quantum Cryptanalysis (scientific monograph). (2023). River Publishers. 256 p. ISBN 9788770227933. DOI: 10.1201/9781003392873.
12. NIST CSRC. Automated Cryptographic Validation Testing System (ACVTS) [Электронный ресурс]. — Gaithersburg, MD: National Institute of Standards and Technology, 2020–2025. – URL: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/how-to-access-acvts (дата обращения: 22.09.2025).
13. Housley R., Fluhrer S., Kampanakis P., Westerbaan B. Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS). – RFC 9814. – IETF, July 2025. – DOI:10.17487/RFC9814.
14. Housley R. Update to the Cryptographic Message Syntax (CMS) for Algorithm Identifier Protection. – RFC 8933. – IETF, October 2020. – DOI:10.17487/RFC8933.

PARAMETERIZATION OF THE POST-QUANTUM ELECTRONIC SIGNATURE KNAA-2-EDS

Petrenko A. S.[2]

Keywords: *finite noncommutative associative algebra; ASN.1/DER formats; NIST persistence categories; constant runtime; signature randomization; security countermeasures; post-quantum electronic signature.*

Purpose of work *to formalize the choice of parameters and the definition of requirements for the KNAA-2-EDS, ensuring post-quantum stability (at least 2200 for Cat 3 and 2256 for Cat 5) while reducing the signature length to 112 bytes (Cat 3) and 128 bytes (Cat 5).*

Research methods: *substantiation of compliance of KNAA-2-EDS with FIPS 204/205/206, SP 800-57-1 Rev.5, ISO/IEC 14888-4:2024 and GOST R 34.10-2018 standards with precise definition of ASN.1/DER and OID formats, development of two sets of parameters for resistance categories 3 and 5 on the NIST scale, setting quantitative targets, formulation of mandatory implementation requirements, in particular constant time, correct randomization and countermeasures.*

2 Alexey S. Petrenko, Junior Researcher, Laboratory of Computer Security Problems , St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

Results of the study: *two sets of parameters have been established to ensure the durability of* $\geq 2^{200}$ *(Cat 3) and* $\geq 2^{256}$ *(Cat 5) and the compactness of keys and signatures, requirements for the size of keys and signatures have been defined, performance and security metrics have been set, criteria for verifying the correctness of implementation without a full ACVP cycle have been established, formats and validation procedures have been regulated, countermeasures against side attacks and constant execution time requirements are defined.*

Practical relevance: *The result of the article is that the found parameters, requirements and usage profiles demonstrate for the first time the implementation of enhanced signature randomization without doubling the verification equation, ensuring the compactness of keys and signatures while maintaining high resistance to quantum attacks and side-channel attacks. This significantly reduces the amount of transactional data and bandwidth requirements for networks and storage, which is critical for scalable blockchain systems, hardware cryptoprocessors, and energy-efficient IoT devices.*

References

1. FIPS PUB 204. Module-Lattice-Based Digital Signature Algorithm (ML-DSA). – Gaithersburg, MD: National Institute of Standards and Technology, 2024. – 65 p. – DOI:10.6028/NIST.FIPS.204.
2. FIPS PUB 205. Stateless Hash-Based Digital Signature Algorithm (SLH-DSA). – Gaithersburg, MD: National Institute of Standards and Technology, 2024. – 76 p. – DOI:10.6028/NIST.FIPS.205.
3. FIPS PUB 206. Falcon Digital Signature Algorithm. – Gaithersburg, MD: National Institute of Standards and Technology, 2025. – 72 p.
4. Barker E., Chen L., Roginsky A., Mani A., Smid M., Polk T. Recommendation for Key Management, Part 1: General (Revision 5). – NIST Special Publication SP 800-57 Part 1 Rev. 5. – Gaithersburg, MD: National Institute of Standards and Technology, 2020. – DOI:10.6028/NIST.SP.800-57pt1r5.
5. ISO/IEC 14888-4:2024. Information security – Cryptographic techniques – Digital signatures with appendix – Part 4: Stateful hash-based mechanisms. – Geneva: ISO/IEC, 2024.
6. ITU-T Recommendation X.680 (08/2021). Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. – Geneva: ITU-T, 2021.
7. Moldovyan, N. A., Petrenko, A. S. Algebraic signature algorithm with two hidden groups (2024), Voprosy kiberbezopasnosti [Cibersecurity issues], no. 6(64), pp. 98–107, 2024. DOI: 10.21681/2311-3456-2024-6-98-107.
8. Markov, A. S., Varenitca, V. V., Arustamyan, S. S. Topical issues in the implementation of secure software development processes. (2023). In the collection: Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance. IPSQDA-2023. P. 48–53.
9. Balyabin, A. A., Petrenko, S. A. Model of a blockchain platform with cyber-immunity under quantum attacks. (2025). Question Kiberbezopasnosti [Cybersecurity issues]. No. 3(67). P. 72–82. DOI: 10.21681/2311-3456-2025-3-72-82 (Russian Text).
10. Petrenko, A. S., Petrenko, S. A. Basic Algorithms Quantum Cryptanalysis. (2023). Question Kiberbezopasnosti [Cybersecurity issue]. No.1(53), pp. 100–115. DOI:10.21681/2311-3456-2023-1-100-115 (Russian Text).
11. Petrenko, A. S. Applied Quantum Cryptanalysis (scientific monograph). (2023). River Publishers. 256p. ISBN9788770227933. DOI:10.1201/9781003392873.
12. NIST CSRC. Automated Cryptographic Validation Testing System (ACVTS) [Electronic resource]. – Gaithersburg, MD: National Institute of Standards and Technology, 2020–2025. – URL: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/how-to-access-acvts (access date: 09/22/2025).
13. Housley R., Fluhrer S., Kampanakis P., Westerbaan B. Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS). – RFC 9814. – IETF, July 2025. – DOI:10.17487/RFC9814.
14. Housley R. Update to the Cryptographic Message Syntax (CMS) for Algorithm Identifier Protection. – RFC 8933. – IETF, October 2020. – DOI:10.17487/RFC8933.