УДК 003.26
doi:10.31799/1684-8853-2025-6-51-63
EDN: AEXSDC

Научные статьи
Articles

Применение метода компактного описания подстановки для модификации схемы цифровой подписи на основе протокола аутентификации Штерна

И. С. Ниткин[а,б], *аспирант, orcid.org/0000-0001-5240-1744, exebopen@gmail.com*
[а]*Университет ИТМО, Кронверкский пр., 49, Санкт-Петербург, 197101, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *схема аутентификации без разглашения Штерна — один из востребованных протоколов для построения схемы цифровой подписи на основе корректирующих кодов. Важным недостатком формирования схемы подписи на основе таких протоколов является значительный размер подписи.* ***Цель:*** *разработать оптимизированную по памяти версию квантово-устойчивой схемы электронную подпись, основанную на схеме Штерна.* ***Результаты:*** *исследована схема подписи на основе протокола аутентификации Штерна, размеры блоков элементов структуры подписи, взаимосвязь размеров блоков со значениями открытых параметров схемы подписи. Сделан вывод, что наибольший объем памяти необходим для хранения значений случайных подстановок. Выполнена оценка криптостойкости схемы подписи на основе протокола аутентификации Штерна с использованием модели наилучшей известной атаки. Разработан метод компактного описания подстановки с использованием информационного вектора, который применен для модификации схемы подписи на основе протокола аутентификации Штерна. Выполнена оценка уровня криптографической стойкости в модели наилучшей известной атаки модифицированной схемы подписи на основе протокола аутентификации Штерна. Проведено теоретическое и экспериментальное сравнение функциональных характеристик схемы цифровой подписи на основе протокола аутентификации Штерна и ее модифицированной версии. Предложенная модификация позволяет значительно снизить размеры подписи, при этом, с учетом выбранной модели оценки, общий уровень криптографической стойкости схемы подписи не снижается.* ***Практическая значимость:*** *полученные в рамках исследования результаты могут быть использованы для оптимизации по памяти схем подписи на основе других протоколов аутентификации без разглашения на основе корректирующих кодов, а также для разработки других методов оптимизации по памяти схемы цифровой подписи на основе протокола аутентификации Штерна.*

Ключевые слова *— постквантовая криптография, криптография на основе корректирующих кодов, электронная подпись, схема цифровой подписи, схема Штерна.*

Для цитирования: Ниткин И. С. Применение метода компактного описания подстановки для модификации схемы цифровой подписи на основе протокола аутентификации Штерна. *Информационно-управляющие системы*, 2025, № 6, с. 51–63. doi:10.31799/1684-8853-2025-6-51-63, EDN: AEXSDC

For citation: Nitkin I. S. Permutation compact description method and its application for Stern-based digital signature modification. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 6, pp. 51–63 (In Russian). doi:10.31799/1684-8853-2025-6-51-63, EDN: AEXSDC

Введение

Постквантовая криптография представляет собой раздел криптографии, который изучает алгоритмы и протоколы, устойчивые к атакам при помощи квантового компьютера (квантово-устойчивые криптографические схемы) [1].

Квантовый алгоритм Шора позволяет за полиномиальное время решать задачи факторизации целого числа и дискретного логарифмирования [2]. Вычислительная сложность описанных задач лежит в основе стойкости криптографических систем, как соответствующих общемировым стандартам (RSA, DSA, ECDSA и т.п.), так и описанных в стандартах Российской Федерации [3]. Таким образом, при использовании алгоритма Шора теоретически могут быть осуществлены успешные атаки на большинство существующих на данный момент систем защиты информации.

Для практической реализации таких атак необходим криптографически-релевантный квантовый компьютер (CRQC), который в настоящее время не может быть реализован технологически. Несмотря на то, что технологии квантовых вычислений развиваются стремительно, исследователи утверждают, что появления CRQC по самым оптимистичным оценкам можно ожидать не ранее 2030 г.

При этом специфика применения криптографических средств в системах защиты информации требует разработки и внедрения квантово-устойчивых криптографических схем, не дожидаясь момента появления CRQC. Применение асимметричных алгоритмов шифрования дает возможность злоумышленнику осуществить сбор зашифрованной информации в ожидании появления технологий, позволяющих выполнить быстрое дешифрование без знания секрет-

ных ключей. Поэтому некоторые категории информации, для которых необходимо обеспечение конфиденциальности на длительные сроки, являются потенциально уязвимыми [4].

Аналогично, квантово-устойчивые схемы подписи должны внедряться заблаговременно, потому что появление CRQC потребует не только единовременного внедрения устойчивых алгоритмов в информационные системы, но и обновления долговременных подписей доверенных удостоверяющих центров, дистрибутивов и т.п., что не представляется возможным на практике.

Национальный институт стандартов и технологий США проводит конкурсные исследования на выработку стандартов квантово-устойчивых криптографических схем [4, 5]. По итогам конкурса [4] среди прочих для стандартизации была выбрана схема выработки общего секретного ключа на основе квазициклических кодов [6].

В рамках рабочей группы Технического комитета по стандартизации «Криптографическая защита информации» Росстандарта (ТК 26) также проводятся исследования в этом направлении. Одним из объектов исследования является схема цифровой подписи на основе схемы Штерна, получившая название «Шиповник» (https://kryptonite.ru/articles/how-eds-will-change-in-the-post-quantum-era/). Стойкость данной схемы основана на NP-полной задаче синдромного декодирования произвольного линейного кода [7].

Использование в качестве криптографического примитива корректирующих кодов является одним из основных подходов при построении квантово-устойчивых криптографических схем [8]. Значимым преимуществом такого подхода является возможность обеспечения стойкости криптографической схемы на уровне сложности решения NP-полной задачи синдромного декодирования. Кроме того, корректирующие коды являются одним из наиболее исследованных постквантовых криптографических примитивов.

Первая криптосистема на основе корректирующих кодов была предложена Робертом МакЭлисом в 1978 г. [9]. В 2001 г. Николас Куртуа, Матье Финиаз и Николас Сандрие предложили схему подписи на основе криптосистемы МакЭлиса [10]. Главными недостатками данной схемы являются необходимость многократно повторять алгоритм выработки подписи, а также значительные размеры ключевой пары. Кроме этого, стойкость данной схемы подписи строится на предположении, что поиск порождающего многочлена и вектора локаторов для кода Гоппы по проверочной матрице является вычислительно сложной задачей. Несмотря на многолетние безуспешные попытки опровергнуть это утверждение, на сегодня вычислительная сложность данной задачи не формализована в контексте классов сложности вычислительных задач.

Другим вариантом построения схемы подписи на основе корректирующих кодов является использование протоколов аутентификации без разглашения. Для NP-полной задачи синдромного декодирования произвольного линейного двоичного кода такая схема аутентификации была предложена Жаком Штерном [11] в 1993 г. В качестве развития идей Штерна были предложены другие схемы аутентификации без разглашения на основе произвольных линейных кодов [12–19].

На основе протокола аутентификации без разглашения может быть разработана схема подписи при помощи преобразования Фиата — Шамира [20]. В частности, на основе протокола CROSS ID [15, 16] разработана схема подписи [21], которая прошла отбор первого раунда [22] конкурса [5].

На основе схемы Штерна также разработана квантово-устойчивая схема электронной подписи [23]. Одним из важных недостатков данной схемы является значительный размер формируемой подписи, что определяется необходимостью многократно повторять процедуру аутентификации без разглашения. Кроме того, необходимость проверки веса Хэмминга секретного ключа без разглашения его значения требует хранения в составе подписи произвольных подстановок. Для одной такой подстановки необходимо хранить в памяти вектор значений от 1 до n, где n — это длина подстановки.

В рамках настоящего исследования предложен метод компактного описания подстановки с помощью информационного вектора параметризуемой длины. С использованием данного метода предложена модифицированная схема подписи на основе протокола аутентификации Штерна, позволяющая оптимизировать объем памяти, необходимый для хранения подписи.

Схема подписи на основе протокола аутентификации Штерна

Схема аутентификации Штерна

Протокол аутентификации без разглашения позволяет доказать знание некоторого «секрета» (например, секретного ключа), не раскрывая при этом его значение. Схема Штерна [11] — протокол аутентификации без разглашения, стойкость которого основана на NP-полной задаче синдромного декодирования.

Принцип работы схемы заключается в обмене сообщениями между доказывающим и проверяющим по открытому каналу.

Открытые параметры схемы Штерна:

— значения n, k;

— функция хеширования $h(x)$: $x \to \{0, 1\}^l$;

— проверочная матрица $\mathbf{H}^{n\times k}$ произвольного двоичного линейного кода;

— значение $\mathbf{y} = \mathbf{H}\mathbf{s}^{\mathrm{T}}$, где $\mathbf{s}$ — двоичный вектор длины n заданного веса Хэмминга ω, $\mathrm{wt}(\mathbf{s}) = \omega$.

В качестве секретного ключа в схеме Штерна рассматривается двоичный вектор $\mathbf{s}$ заданного веса ω.

Процесс аутентификации происходит следующим образом.

Шаг 1. Доказывающий выбирает произвольный вектор $\mathbf{u} \in \{0, 1\}^n$ и произвольную подстановку $\sigma \in S_n$, где S_n — симметрическая группа степени n. На основе выбранных значений доказывающий вычисляет значения обязательств $c_0 = h(\sigma \mid \mathbf{H}\mathbf{u}^{\mathrm{T}})$, $c_1 = h(\sigma(\mathbf{u}))$, $c_2 = h(\sigma(\mathbf{u} \oplus \mathbf{s}))$ и передает их проверяющему.

Шаг 2. Проверяющий отправляет доказывающему случайное значение запроса $b \in \{0, 1, 2\}$.

Шаг 3. В зависимости от полученного значения b доказывающий отправляет проверяющему значения ответов r:

если $b = 0$, $r = \sigma \mid \mathbf{u}$;

если $b = 1$, $r = \sigma \mid \mathbf{u} \oplus \mathbf{s}$;

если $b = 2$, $r = \sigma(\mathbf{u}) \mid \sigma(\mathbf{s})$.

Шаг 4. Проверяющий выполняет проверки:

если $b = 0$:

$$c_0 \overset{?}{=} h\left(\sigma \mid \mathbf{H}\mathbf{u}^{\mathrm{T}}\right),\ c_1 \overset{?}{=} h\left(\sigma(\mathbf{u})\right);$$

если $b = 1$:

$$c_0 \overset{?}{=} h\left(\sigma \mid \mathbf{H}(\mathbf{u} \oplus \mathbf{s})^{\mathrm{T}} \oplus \mathbf{y}\right),\ c_2 \overset{?}{=} h\left(\sigma(\mathbf{u} \oplus \mathbf{s})\right);$$

если $b = 2$:

$$c_1 \overset{?}{=} h\left(\sigma(\mathbf{u})\right),\ c_2 \overset{?}{=} h\left(\sigma(\mathbf{u} \oplus \mathbf{s})\right),\ \mathrm{wt}\left(\sigma(\mathbf{s})\right) \overset{?}{=} \omega.$$

Шаги 1–4 повторяются δ раз, где δ — заданный параметр стойкости.

Если все проверки пройдены успешно, знание значения секретного ключа считается подтвержденным.

Вероятность принятия доказательства проверяющей стороной в одном раунде при условии, что доказывающий не обладает знанием значения секрета, составляет 2/3. Если отбросить одно из возможных значений запроса b, знание секрета не является необходимым для выработки обязательства, которое будет принято проверяющей стороной.

Если $b \neq 1$, то злонамеренный доказывающий вместо вектора $\mathbf{s}$ при формировании обязательств c_0, c_1, c_2 использует произвольный вектор $\mathbf{t}_1$: $\mathrm{wt}(\mathbf{t}_1) = \omega$.

Если $b \neq 2$, при формировании обязательств вместо $\mathbf{s}$ используется вектор $\mathbf{t}_2$: $\mathbf{y} = \mathbf{H}\mathbf{t}_2^{\mathrm{T}}$.

Если $b \neq 0$, вместо $\mathbf{s}$ используется вектор $\mathbf{t}_1$, а $c_0 = h(\sigma \mid \mathbf{H}(\mathbf{u} \oplus \mathbf{t}_1)^{\mathrm{T}} \oplus \mathbf{y})$.

Преобразование Фиата — Шамира [20] позволяет на основе протоколов аутентификации без разглашения формировать схемы подписи. В том числе на основе схемы Штерна предложена схема подписи [23].

Схема цифровой подписи не может быть реализована в интерактивном виде, поэтому вместо генерации случайного значения b оно вычисляется при помощи троичной хеш-функции $f(x)$: $x \to \{0, 1, 2\}^{\delta}$.

При формировании подписи в первую очередь вычисляется δ наборов обязательств по схеме Штерна ($c = c_0 \mid \ldots \mid c_{\delta-1}$). После этого сформированные обязательства вместе с подписываемым сообщением подаются на вход троичной хеш-функции $f(x)$, и на основе полученного значения вектора вызовов ($b = f(c \mid m) = b_0 \mid \ldots \mid b_{\delta-1}$) формируется блок ответов ($r = r_0 \mid \ldots \mid r_{\delta-1}$) в соответствии со схемой Штерна. Значение подписи представляет собой конкатенацию блоков c и r ($Sig = c \mid r$).

При проверке подписи в первую очередь вычисляется значение вектора вызовов, после чего осуществляется δ проверок обязательств по схеме Штерна. Подпись принимается, если все проверки пройдены успешно.

Подробное описание схемы цифровой подписи на основе протокола аутентификации Штерна (СП СШ) представлено в [23].

Исследование размеров блоков подписи на основе схемы Штерна

Для достижения цели оптимизации по памяти подписи, основанной на схеме Штерна, проведена оценка размеров блоков структуры подписи исходя из значений открытых параметров схемы подписи:

— размер блока c_i равен $3l$ бит, где l — битовая длина значения хеш-функции $h(x)$;

— размер блока r_i зависит от значения b_i. Если $b_i \in \{0, 1\}$, размер блока r_i составляет $n + n \cdot \log_2 n$ бит. При $b_i = 2$ размер блока r_i составляет $2n$ бит.

Конкретные значения системных параметров для СП СШ подбираются из соображений необходимости обеспечения криптографической стойкости [24]. В рамках исследования рассматриваются два набора значений системных параметров схемы подписи на основе схемы Штерна, которые приводятся в научных источниках. В ч. 1 табл. 1 представлены значения системных параметров из указанных наборов.

Для набора № 1 [25] значение l не приведено в источнике, поэтому $l = 112$ (с точностью до одного байта) вычислено пропорционально значению n на основе значений набора № 2 [23].

Размеры элементов структуры СП СШ для исследуемых наборов конкретных значений си-

■ ***Таблица 1.*** Системные параметры и характеристики схемы цифровой подписи на основе протокола аутентификации Штерна

■ ***Table 1.*** Stern-based digital signature open parameters and characteristics

Значение	Формула	Набор № 1	Набор № 2
Часть 1. Значения системных параметров			
n	–	620	2896
k	–	310	1448
ω	–	68	318
δ	–	137	137
l	–	(112)	512
Часть 2. Размеры блоков формируемой подписи			
$\lvert c_i \rvert$	$3l$	336 бит	1536 бит
$\lvert r_{i,\mathbf{u}} \rvert$	$2n$	1240 бит	5792 бит
$\lvert r_{i,\sigma} \rvert$	$n + n \cdot \log_2 n$	6820 бит	37648 бит
$\lvert c \rvert$	$\delta \cdot \lvert c_i \rvert$	5,62 Кбайт	25,69 Кбайт
$\lvert r \rvert$	$\delta \cdot \lvert r_{i,\sigma} \rvert$	114,06 Кбайт	629,61 Кбайт
$\lvert Sig \rvert$	$\lvert c \rvert + \lvert r \rvert$	119,67 Кбайт	655,30 Кбайт
Часть 3. Оценка уровня криптографической стойкости			
λ_δ	$-\log_2\left(\frac{2}{3}\right)^\delta$	80 бит	80 бит
λ_{HC}	$\frac{l}{2}$	56 бит	256 бит
$\lambda_{\mathbf{s}}$	$\log_2\binom{n}{\omega}$	305 бит	1440 бит
λ_{SD}	$0{,}0885 \cdot n$	54 бита	256 бит
$\lambda_{\mathbf{u}}$	n	620 бит	2896 бит
λ_σ	$\log_2\binom{n}{\omega}$	305 бит	1440 бит
λ	$\min(\lambda_\delta, \lambda_{HC}, \lambda_{\mathbf{s}}, \lambda_{SD}, \lambda_{\mathbf{u}}, \lambda_\sigma)$	54 бита	80 бит

стемных параметров представлены в ч. 2 табл. 1. Наибольший объем памяти в структуре СП СШ, значительно превосходящий объем памяти, требуемый для других значений в составе подписи, необходим для хранения случайных подстановок.

В табл. 1, 2 использованы следующие обозначения:

– $\lvert c_i \rvert$ – размер блока c_i;
– $\lvert r_{i,\mathbf{u}} \rvert$ – размер блока r_i при условии $b_i = 2$;
– $\lvert r_{i,\sigma} \rvert$ – размер блока r_i при условии $b_i \in \{0, 1\}$;
– $\lvert c \rvert$ – размер блока c;
– $\lvert r \rvert$ – размер блока r;
– $\lvert Sig \rvert$ – размер формируемой подписи;
– λ_δ – уровень криптостойкости при атаке на подделку подписи;
– λ_{HC} – уровень криптостойкости при атаках, основанных на поиске коллизии хеш-функции;
– $\lambda_{\mathbf{s}}$ – уровень криптостойкости при атаке перебора возможных значений секретного ключа;
– λ_{SD} – уровень криптостойкости при атаке с использованием декодирования по информационным совокупностям;
– $\lambda_{\mathbf{u}}$ – уровень криптостойкости при атаке перебора возможных значений $\mathbf{u}_i$;
– λ_σ – уровень криптостойкости при подборе значения $\mathbf{s}$ по известному значению $\sigma_i(\mathbf{s})$;
– λ – общий уровень криптостойкости схемы подписи.

Оценка уровня криптографической стойкости схемы цифровой подписи на основе протокола аутентификации Штерна

В рамках настоящего исследования для оценки криптографической стойкости применяется *модель наилучшей известной атаки*, в которой в качестве показателя избран уровень криптографической стойкости, измеренный в битах. В качестве общего уровня стойкости криптографической схемы принимается наименьшее значение среди оценок уровня криптографической стойкости для атак на исследуемую схему.

При проведении оценки криптографической стойкости СП СШ рассматриваются атаки с использованием детерминированной машины Тьюринга. В рамках настоящего исследования оценка уровня криптографической стойкости СП СШ при атаках с использованием квантового компьютера не проводилась. Применение квантового компьютера позволяет получить значительное ускорение при решении проблемы синдромного декодирования [26]. Последние публикации предлагают алгоритмы, которые позволяют декодировать произвольный линейный код за $2^{0{,}0508n}$ вычислительных операций [27]. Кроме того, алгоритм Гровера [28] может обеспечивать квадратичное ускорение перебора.

При проведении оценки криптографической стойкости схемы цифровой подписи на основе протокола аутентификации Штерна рассмотрены атаки на подделку подписи и атаки на раскрытие значения секретного ключа.

При реализации *атаки на подделку подписи* злоумышленник должен предъявить пару (m, Sig) – произвольное сообщение и подпись данного сообщения, выработанную без знания секретного ключа, которая успешно пройдет проверку.

Алгоритм проведения атаки на подделку подписи.

Шаг 1. Сформировать δ наборов обязательств $c = c_0 \mid \ldots \mid c_{\delta-1}$, каждый из которых пройдет проверку по схеме Штерна с вероятностью $\frac{2}{3}$.

Шаг 2. Подобрать такое значение m, при котором набор значений запросов $b_0 \mid \ldots \mid b_{\delta-1} = f(c \mid m)$ совпадет с номерами проверок, прохождение которых заложено для каждого набора обязательств.

Уровень криптостойкости СП СШ при атаке на подделку подписи в данном случае определяется по формуле $\lambda_\delta = -\log_2\left(\frac{2}{3}\right)^\delta$ [бит].

Другие атаки на подделку подписи связаны с поиском коллизии хеш-функции. Лучший алгоритм поиска коллизии хеш-функции основан на парадоксе дней рождения и требует $2^{\frac{l}{2}}$ операций хеширования, следовательно, уровень криптостойкости СП СШ при *атаках, основанных на поиске коллизии хеш-функции*, определяется по формуле $\lambda_{HC} = \frac{l}{2}$ [бит].

Подбор секретного ключа *по публичному ключу и известным параметрам системы* может быть осуществлен либо посредством полного перебора возможных значений секретного ключа, либо посредством решения NP-полной задачи синдромного декодирования произвольного линейного кода.

Уровень криптостойкости при *атаке с использованием перебора возможных значений секретного ключа* определяется исходя из мощности множества допустимых значений секретного ключа, которая вычисляется как число сочетаний из n по ω. Следовательно, уровень криптостойкости при данной атаке определяется по формуле $\lambda_{\mathbf{s}} = \log_2\binom{n}{\omega}$ [бит].

Лучший из известных алгоритмов решения задачи синдромного декодирования основан на декодировании по информационным совокупностям и требует порядка $2^{0{,}0885n}$ битовых операций [29]. Таким образом, уровень криптостойкости при *атаке с использованием декодирования по информационным совокупностям* определяется по формуле $\lambda_{SD} = 0{,}0885n$ [бит].

Важно отметить, что эффективность алгоритмов декодирования по информационным совокупностям постоянно улучшается. Одним из актуальных подходов является сведение данной задачи к вычислительно сложным задачам на алгебраических решетках [30].

Для атак по *подбору значения секретного ключа на основе значений блока r* рассмотрены нижеописанные варианты.

При $b_i = 1$ может быть осуществлен *подбор значения* $\mathbf{s}$ *по известному значению* $\mathbf{u}_i \oplus \mathbf{s}$. Вычислительная сложность такой атаки эквивалентна перебору возможных значений $\mathbf{u}_i$. Уровень криптографической стойкости схемы подписи на основе схемы Штерна при реализации данной атаки определяется по формуле $\lambda_{\mathbf{u}} = n$ [бит].

При $b_i = 2$ может быть осуществлен подбор значения $\mathbf{s}$ по известному значению $\sigma_i(\mathbf{s})$. Для реализации атаки необходимо выполнить проверку:

$$\mathbf{y} \stackrel{?}{=} \mathbf{H}\left(\sigma_s\left(\sigma_i\left(\mathbf{s}\right)\right)\right)^{\mathrm{T}}, \qquad (1)$$

где $\sigma_{\mathbf{s}}$ — случайно выбранная подстановка длины n.

Если проверка пройдена успешно, значение секретного ключа восстановлено. Количество подстановок $\sigma_{\mathbf{s}}$ таких, что $\sigma_{\mathbf{s}}^{-1}\left(\mathbf{s}\right) = \sigma_i\left(\mathbf{s}\right)$, составляет $n!(n-\omega)!$.

Вероятность успешной атаки вычисляется по формуле

$$P_S = \frac{Q_1 Q_0}{Q} = \frac{\omega!(n-\omega)!}{n!} = \binom{n}{\omega}^{-1}, \qquad (2)$$

где Q_1 — количество способов поместить ω единиц двоичного вектора $\mathbf{s}$ на ω позиций; Q_0 — количество способов поместить $n - \omega$ нулей двоичного вектора $\mathbf{s}$ на $n - \omega$ позиций; Q — общее количество возможных подстановок длины n.

Тогда уровень криптографической стойкости при *атаке на подбор значения секретного ключа по известному значению* $\sigma_i(\mathbf{s})$ определяется по формуле

$$\lambda_\sigma = -\log_2 P_S = \log_2\binom{n}{\omega}. \qquad (3)$$

Общий уровень криптографической стойкости СП СШ в рамках модели наилучшей известной атаки вычисляется по формуле

$$\lambda = \min(\lambda_\delta, \lambda_{HC}, \lambda_{\mathbf{s}}, \lambda_{SD}, \lambda_{\mathbf{u}}, \lambda_\sigma). \qquad (4)$$

В части 3 табл. 1 приведены расчеты уровня криптографической стойкости СП СШ при значениях системных параметров из наборов № 1 и 2.

В работе [23] приводится оценка уровня доказуемой криптографической стойкости для набора № 2 значений системных параметров на уровне 70 бит. Данный результат не противоречит значению, полученному в модели наилучшей известной атаки.

Модифицированная схема цифровой подписи на основе протокола аутентификации Штерна

Метод компактного описания подстановки при помощи информационного вектора

Для достижения цели оптимизации по памяти квантово-устойчивой подписи на основе схемы Штерна следует сократить размеры элементов подписи. Установлено, что наибольший объем памяти в структуре подписи необходим для хранения значений случайных подстановок. Для сокращения этого объема разработан метод компактного задания подстановки с использованием регистров сдвига с линейной обратной связью (РСЛОС).

Регистры сдвига с линейной обратной связью применяются для генерации псевдослучайных битовых последовательностей. Один такт работы РСЛОС представляет собой генерацию одного бита выходной последовательности, расчет значения входного бита и обновление состояния регистра.

Последовательность, генерируемая РСЛОС, определяется характеристическим многочленом и начальным состоянием (вектором инициализации). Максимальный период последовательности для регистра сдвига длины L составляет $2^L - 1$ и достигается при условии, что характеристический многочлен РСЛОС является примитивным многочленом поля $GF(2^L)$. В этом случае состояние регистра для каждого такта не повторяется в течение одного периода работы, и РСЛОС принимает все возможные состояния, кроме нулевого.

Таким образом, при помощи РСЛОС может быть сгенерирована подстановка любой длины $N \le 2^L - 1$. Для этого необходимо записывать в вектор, описывающий подстановку, состояния регистра сдвига, не превышающие значения N, в течение одного периода работы в порядке их возникновения. Полученный вектор значений описывает подстановку заданной длины N.

Оптимальным является выбор значения L, рассчитанного по формуле $L = \lfloor \log_2 N \rfloor$.

Если зафиксировать конкретное значение характеристического многочлена в качестве открытого параметра системы, подстановка длины N может быть компактно задана описанным способом при помощи значения вектора инициализации РСЛОС. Количество различных подстановок, которые могут быть заданы таким способом, составляет N.

Для увеличения мощности множества подстановок, которые могут быть заданы компактным способом при помощи РСЛОС, в настоящем исследовании предлагается метод, названный *расширением подстановки*.

Расширение подстановки — это генерация на основе подстановки длины N подстановки длины $N + 1$ путем дополнения значением $N + 1$ вектора, описывающего подстановку длины N. При этом значение $N + 1$ размещается на произвольной позиции от 0 до N с последующим сдвигом на одну позицию всех значений вектора, находящихся на позициях с номерами, не меньше чем у выбранной.

Таким образом, при помощи двух значений (вектора инициализации (от 1 до N) и номера позиции для расширения (от 0 до N)) может быть задана подстановка длины $N + 1$ из множества мощностью $N(N + 1)$.

В рамках исследования введен параметр γ, который называется *степенью расширения подстановки*. Он описывает количество расширений заданной компактным способом с использованием РСЛОС подстановки. С использованием γ-кратного расширения подстановки на основе подстановки длины $n - \gamma$ может быть выработана подстановка длины n. Подстановка длины $n - \gamma$ может быть компактно описана при помощи одного значения. При этом значение вектора инициализации для РСЛОС может быть объединено с вектором значений длины γ, задающим подстановку длины n на основе подстановки длины $n - \gamma$, в единый информационный вектор.

Таким способом может быть сгенерирована подстановка длины n, заданная при помощи $\gamma + 1$ значений.

Пример.

На основе РСЛОС с характеристическим многочленом $p(x) = x^3 + x + 1$ *и вектором инициализации* IV = 4= 100_2 *может быть сгенерирована подстановка длины 5:* (4, 5, 3, 1, 2).

После этого могут быть выполнены четыре расширения полученной подстановки, которые задаются значениями: [2, 1, 0, 6]. *В результате будет получена подстановка длины 9:* (8, 4, 7, 5, 6, 3, 9, 1, 2).

На основе описанных результатов сформулировано понятие информационного вектора подстановки и разработан алгоритм формирования подстановки по информационному вектору подстановки.

Понятие информационного вектора подстановки определено следующим образом: *информационный вектор подстановки длины n со степенью расширения* γ — это вектор длины $\gamma + 1$ следующего вида:

$$\mathbf{v}_{n,\gamma} = \Big[\big[0..(n-\gamma)\big),\ \big[0..(n-\gamma+1)\big),$$
$$\big[0..(n-\gamma+2)\big),\ \ldots,\ \big[0..(n-1)\big),\ \big[0..n\big)\Big],$$

где $[0\ ..\ a)$ — произвольное целое число x: $0 \le x < a$.

Обозначим $V_{n,\gamma}$ множество всех различных векторов $\mathbf{v}_{n,\gamma}$.

Ниже представлен алгоритм формирования вектора подстановки по информационному вектору подстановки.

PERMUTATION($\mathbf{v}_{n,\gamma}$, $p(x)$: $\deg(p(x)) = \lfloor \log_2(n - \gamma) \rfloor$):

Шаг 1. Построить РСЛОС на основе примитивного многочлена $p(x)$;

Шаг 2. Инициализировать РСЛОС значением $\mathbf{v}_{n,\gamma}[0] + 1$;

Шаг 3. Для i от 0 до $2^{\deg(p(x))} - 1$:

3.1. Считать значение регистра t;

3.2. Если $t \le n - \gamma$ — записать t на i-ю позицию вектора *perm*;

3.3. Выполнить один такт работы РСЛОС.

Шаг 4. Для i от 1 до $\gamma + 1$ получить новое значение вектора *perm* следующим образом:

4.1. Добавить $\mathbf{v}_{n,\gamma}[i]$ первых значений вектора *perm*;

4.2. Добавить значение $\text{len}(perm) + 1$;

4.3. Добавить оставшиеся значения вектора функции перестановки *perm*.

Результат: *perm* — подстановка длины n.

При проведении исследования сформулирована и доказана **теорема** о вложении множества информационных векторов подстановок во множество подстановок.

Отображение множества $V_{n,\gamma}$ в множество элементов симметрической группы S_n с функцией отображения **PERMUTATION**($\mathbf{v}_{n,\gamma}$, $p(x)$) инъективно.

Доказательство:

1. Результатом выполнения алгоритма **PERMUTATION**($\mathbf{v}_{n,\gamma}$, $p(x)$) является подстановка.

Работа РСЛОС детерминирована, следовательно, результатом выполнения шага 3 алгоритма является вектор из $n - \gamma$ различных значений от 1 до $n - \gamma$.

Выполнение шага 4 алгоритма представляет собой последовательное дополнение вектора значений, полученного в результате выполнения шага 3, значениями от $n - \gamma + 1$ до n.

Таким образом, результатом работы алгоритма является вектор длины n, содержащий все различные значения от 1 до n, который по определению описывает подстановку длины n.

2. Если $\mathbf{v}_{n,\gamma} \ne \mathbf{v}'_{n,\gamma}$, то **PERMUTATION**($\mathbf{v}_{n,\gamma}$, $p(x)$) $\ne$ $\ne$ **PERMUTATION**($\mathbf{v}'_{n,\gamma}$, $p(x)$).

Назовем i-ядром подстановки порядок следования элементов от 1 до i данной подстановки.

Если $\mathbf{v}_{n,\gamma}[0] \ne \mathbf{v}'_{n,\gamma}[0]$, то подстановки **PERMUTATION**($\mathbf{v}_{n,\gamma}$, $p(x)$), **PERMUTATION**($\mathbf{v}'_{n,\gamma}$, $p(x)$) имеют различные $(n - \gamma)$-ядра.

Если $\mathbf{v}_{n,\gamma}[i] \ne \mathbf{v}'_{n,\gamma}[i]$: $1 \le i \le \gamma + 1$, то при выполнении i-й итерации шага 4 алгоритма будет получен различный результат.

Если i-ядро подстановки **PERMUTATION**($\mathbf{v}_{n,\gamma}$, $p(x)$) не совпадает с i-ядром подстановки **PERMUTATION**($\mathbf{v}'_{n,\gamma}$, $p(x)$), то **PERMUTATION**($\mathbf{v}_{n,\gamma}$, $p(x)$) $\ne$ **PERMUTATION**($\mathbf{v}'_{n,\gamma}$, $p(x)$).

3. Из 1 и 2 следует, что каждому информационному вектору подстановки соответствует подстановка, притом только одна. *Что и требовалось доказать*.

Модифицированная схема цифровой подписи на основе протокола аутентификации Штерна

На основе вышеописанного метода компактного описания подстановки разработана модифицированная схема подписи на основе протокола аутентификации Штерна (МСП СШ). Модификация предлагает генерацию и хранение в составе блока ответов информационных векторов подстановок. Ниже представлено описание данной схемы подписи.

Системные параметры:

— значения n, k;

— значение ω, которое определяет вес Хэмминга секретного ключа;

— двоичная матрица полного ранга $\mathbf{H}^{n \times k}$;

— функция хеширования $h(x)$: $x \to \{0, 1\}^l$;

— значение параметра стойкости δ;

— троичная хеш-функция $f(x)$: $x \to \{0, 1, 2\}^\delta$;

— значение γ, которое определяет степень расширения подстановки;

— примитивный над полем $GF(2)$ многочлен $p(x)$: $\deg(p(x)) = \lfloor \log_2(n - \gamma) \rfloor$.

Ключевая пара:

$sk = \mathbf{s}$: $\{0, 1\}^n$, $\text{wt}(\mathbf{s}) = \omega$;

$pk = \mathbf{y}$: $\mathbf{y} = \mathbf{H}\mathbf{s}^{\text{T}}$.

Алгоритм формирования подписи.

В качестве входных значений передается значение секретного ключа $\mathbf{s}$ и подписываемое сообщение m.

Шаг 1. Повторить δ раз:

1.1. Сгенерировать $\mathbf{u}_i \in \{0, 1\}^n$, $(\mathbf{v}_{n,\gamma})_i \in V_{n,\gamma}$.

1.2. Вычислить $\sigma_i = \mathbf{PERMUTATION}((\mathbf{v}_{n,\gamma})_i, p(x))$.

1.3. Вычислить $c_{0i} = h(\sigma_i \mid \mathbf{H}\mathbf{u}_i^{\text{T}})$.

1.4. Вычислить $c_{1i} = h(\sigma(\mathbf{u}_i))$.

1.5. Вычислить $c_{2i} = h(\sigma(\mathbf{u}_i \oplus \mathbf{s}))$.

1.6. Вычислить $c_i = c_{0i} \mid c_{1i} \mid c_{2i}$.

Шаг 2. Вычислить $c = c_0 \mid \ldots \mid c_{\delta-1}$.

Шаг 3. Вычислить $b = f(c \mid m) = b_0 \mid \ldots \mid b_{\delta-1}$.

Шаг 4. Повторить δ раз:

Для b_i, $(\mathbf{v}_{n,\gamma})_i$, $\mathbf{u}_i$, σ_i вычислить r_i:

если $b_i = 0$, $r_i = \mathbf{u}_i \mid (\mathbf{v}_{n,\gamma})_i$;

если $b_i = 1$, $r_i = \mathbf{u}_i \oplus \mathbf{s} \mid (\mathbf{v}_{n,\gamma})_i$;

если $b_i = 2$, $r_i = \sigma_i(\mathbf{u}_i) \mid \sigma_i(\mathbf{s})$.

Шаг 5. Вычислить $r = r_0 \mid \ldots \mid r_{\delta-1}$.

Шаг 6. Вычислить значение подписи $Sig = c \mid r$.

Алгоритм проверки подписи.

В качестве входных значений передается значение открытого ключа $\mathbf{y}$, сообщение m и значение подписи $Sig = c \mid r$.

Шаг 1. Вычислить значение $b = f(c \mid m) = b_0 \mid \ldots \mid b_{\delta-1}$.

Шаг 2. Для каждого b_i:

Если $b_i = 0$:

– вычислить $\sigma_i = \mathbf{PERMUTATION}((\mathbf{v}_{n,\gamma})_i, p(x))$;

– выполнить проверки

$$\mathbf{c}_{i0} \stackrel{?}{=} h\left(\sigma_i|\mathbf{H}\mathbf{u}_i^{\mathrm{T}}\right),\ c_{i1} \stackrel{?}{=} h\left(\sigma_i\left(\mathbf{u}_i\right)\right).$$

Если $b_i = 1$:

– вычислить $\sigma_i = \mathbf{PERMUTATION}((\mathbf{v}_{n,\gamma})_i, p(x))$;

– выполнить проверки

$$\mathbf{c}_{i0} \stackrel{?}{=} h\left(\sigma_i|\mathbf{H}\left(\mathbf{u}_i \oplus \mathbf{s}\right)^{\mathrm{T}} \oplus \mathbf{y}\right),\ c_{i2} \stackrel{?}{=} h\left(\sigma_i\left(\mathbf{u}_i \oplus \mathbf{s}\right)\right).$$

Если $b_i = 2$, выполнить проверки

$$c_{i1} \stackrel{?}{=} h\left(\sigma_i\left(\mathbf{u}_i\right)\right),\ c_{i2} \stackrel{?}{=} h\left(\sigma_i\left(\mathbf{u}_i \oplus \mathbf{s}\right)\right),\ \mathrm{wt}\left(\sigma(\mathbf{s})\right) \stackrel{?}{=} \omega.$$

Если все проверки пройдены успешно — подпись принимается. Иначе — отклоняется.

Оценка уровня криптографической стойкости модифицированной схемы цифровой подписи на основе протокола аутентификации Штерна

На основе оценки уровня криптографической стойкости СП СШ может быть произведена оценка уровня криптографической стойкости МСП СШ. Произведенная модификация оказывает влияние только на оценку уровня криптографической стойкости при атаке на подбор значения секретного ключа по известному значению $\sigma_i(\mathbf{s})$.

Для уточнения оценки уровня криптографической стойкости МСП СШ относительно уровня оценки криптографической стойкости базовой версии в рамках модели наилучшей известной атаки необходимо рассчитать значения вероятности успешной атаки и уровня криптографической стойкости при атаке на подбор значения секретного ключа по известному значению $\sigma_i(\mathbf{s})$ способом, аналогичным представленному в формулах (2), (3).

Для проведения оценки уровня криптографической стойкости рассматривается выполнение проверки (1) при условии, что $\sigma_{\mathbf{s}} = (\sigma')^{-1}$, где $\sigma' = \mathbf{PERMUTATION}(\mathbf{v}_{n,\gamma}, p(x))$, $\mathbf{v}_{n,\gamma}$ — случайный информационный вектор из множества $V_{n,\gamma}$.

Необходимость вычисления обратной подстановки обусловлена тем, что в отличие от S_n множество подстановок, соответствующих $V_{n,\gamma}$, в общем случае не является группой.

Вероятность успешной атаки не превышает следующего значения:

$$P_{SM} \le \frac{Q_1 Q_0}{Q}, \qquad (5)$$

где Q_1 — количество подстановок, соответствующих $V_{n,\gamma}$, размещающих ω единиц двоичного вектора $\mathbf{s}$ на ω заданных позиций; Q_0 — количество подстановок, соответствующих $V_{n,\gamma}$, размещающих $n - \omega$ нулей двоичного вектора $\mathbf{s}$ на $n - \omega$ заданных позиций; Q — общее количество возможных подстановок, соответствующих $V_{n,\gamma}$.

В числителе дроби (5) вычисляется предельное возможное количество подстановок, соответствующих $V_{n,\gamma}$, которые переводят вектор $\mathbf{s}$ в вектор $\sigma_i(\mathbf{s})$.

Общее количество возможных подстановок по теореме о вложении множества информационных векторов подстановок во множество подстановок вычисляется как мощность множества $V_{n,\gamma}$ по формуле

$$Q = \prod_{j=0}^{\gamma}(n-j) = \frac{n!}{(n-\gamma-1)!}. \qquad (6)$$

Чтобы вычислить значение Q_1 для МСП СШ, необходимо определить значение q_1 как количество единиц в первых $n - \gamma$ разрядах вектора $\mathbf{s}$.

$(n - \gamma)$-ядро подстановки в МСП СШ определяется РСЛОС. В симметрической группе S_n для q_1 значений $(n - \gamma)$-ядра найдутся подстановки, которые соответствуют $q_1!$ различным способам разместить q_1 значений вектора, описывающего функцию перестановки. Для подстановок, которые соответствуют множеству информационных векторов подстановок $V_{n,\gamma}$, необходимо исключить все такие способы, кроме циклических.

Таким образом, количество способов поместить ω единиц двоичного вектора $\mathbf{s}$ на ω позиций для МСП СШ вычисляется по формуле

$$Q_1 = \frac{\omega!}{\frac{q_1!}{q_1}} = \frac{\omega!}{(q_1-1)!}. \qquad (7)$$

Аналогично, при вычислении Q_0 для МСП СШ необходимо определить значение q_0 как количество нулей в первых $n - \gamma$ разрядах вектора $\mathbf{s}$.

Количество нулей в первых $n - \gamma$ разрядах вектора $\mathbf{s}$ вычисляется по формуле $q_0 = n - \gamma - q_1$.

По аналогии с вычислением значения Q_1, количество способов поместить $n - \omega$ нулей двоичного вектора $\mathbf{s}$ на $n - \omega$ позиций для МСП СШ определяется по формуле

$$Q_0 = \frac{(n-\omega)!}{(q_0-1)!} = \frac{(n-\omega)!}{(n-\gamma-q_1-1)!}. \qquad (8)$$

Оценка, вычисляемая по формулам (5)–(8), является завышенной, так как формируется из следующих предположений:

— среди подстановок, соответствующих $V_{n,\gamma}$, найдутся Q_1 способов размещений единиц на

ω произвольных позиций для любого значения вектора **s**;

– среди подстановок, соответствующих $V_{n,\gamma}$, найдутся Q_0 способов размещения нулей вектора **s** для каждого возможного способа размещения единиц.

Вероятность успешной атаки на подбор значения секретного ключа по известному значению $\sigma_i(\mathbf{s})$ для МСП СШ не превышает

$$P_{SM} \le \frac{Q_1 Q_0}{Q} = \frac{\frac{\omega!}{(q_1-1)!}\cdot\frac{(n-\omega)!}{(n-\gamma-q_1-1)!}}{\frac{n!}{(n-\gamma-1)!}} =$$

$$= \frac{\omega!(n-\omega)!(n-\gamma-1)!}{n!(q_1-1)!(n-\gamma-q_1-1)!} =$$

$$= P_S \cdot \frac{(n-\gamma-1)!}{(q_1-1)!(n-\gamma-q_1-1)!},$$

где P_S – вероятность успешной атаки на подбор значения секретного ключа по известному значению $\sigma_i(\mathbf{s})$ для СП СШ, вычисленная по формуле (2).

Тогда уровень криптографической стойкости при атаке на подбор значения секретного ключа по известному значению $\sigma_i(\mathbf{s})$ для МСП СШ определяется по формуле

$$\lambda_\sigma = -\log_2 P_{SM} = \log_2 \frac{n!(q_1-1)!(n-\gamma-q_1-1)!}{\omega!(n-\omega)!(n-\gamma-1)!}. \quad (9)$$

По формуле (9) значение системного параметра γ может быть подобрано исходя из выбранного значения λ_σ.

Общий уровень криптографической стойкости, измеренный в битах, для МСП СШ может быть вычислен по формуле (4).

Сравнительный анализ модифицированной и базовой схем подписи на основе протокола аутентификации Штерна

В ходе исследования был проведен сравнительный анализ функциональных характеристик СП СШ и предложенной модифицированной версии. Под функциональными характеристиками понимается размер формируемой подписи и производительность алгоритмов схемы подписи.

Для выполнения сравнения размера подписи необходимо вычислить размеры блоков структуры МСП СШ и сравнить их с соответствующими значениями для СП СШ, приведенными в табл. 1.

Чтобы вычислить размеры блоков, необходимо определить значения системных параметров для МСП СШ на основе исследуемых наборов значений системных параметров [25, 23]. Для этого по формулам (6)–(9) подобраны наименьшие значения степени расширения подстановки. Эти значения вычислены исходя из требования обеспечения уровня криптографической стойкости при атаке на подбор значения секретного ключа по известному значению $\sigma_i(\mathbf{s})$ не ниже общего уровня криптографической стойкости для каждого набора, представленного в табл. 1.

Для набора № 1 исходя из $\lambda_\sigma = \lambda = 54$ определено значение $\gamma = 268$. Для набора № 2, аналогично, ($\lambda_\sigma = \lambda = 80$) определено значение $\gamma = 478$.

В отличие от СП СШ для модифицированной версии схемы подписи размер блока r_i при $b_i \in \{0, 1\}$ составляет $n + (\gamma + 1) \cdot \log_2 n$ [бит].

Сопоставлены размеры блоков структуры подписи и значения характеристик криптографической стойкости, претерпевшие изменения в результате модификации (см. табл. 2). В графе «Коэффициент» табл. 2 рассчитаны относительные значения показателей, в качестве базовых рассматриваются значения характеристик СП СШ.

Из табл. 2 следует, что разработанная модификация позволяет значительно сократить размеры затронутых модификацией блоков структуры подписи и, как следствие, размеры подписи в целом. Для набора значений системных параметров № 1 в результате модификации размер подписи уменьшился в 1,96 раза, для набора зна-

■ ***Таблица 2.*** Сравнение показателей СП СШ и МСП СШ

■ ***Table 2.*** Basic and modified versions Stern-based digital signature comparison

Показатель	СП СШ	МСП СШ	Коэффициент
Набор № 1			
γ	–	268	–
$\lvert r_i, \sigma\rvert$, бит	6820	**3310**	**0,485**
$\lvert r\rvert$, Кбайт	114,06	**55,36**	**0,485**
$\lvert Sig\rvert$, Кбайт	119,67	**60,97**	**0,510**
λ_σ, бит	305	54	–
λ, бит	54	54	–
Набор № 2			
γ	–	478	–
$\lvert r_i, \sigma\rvert$, бит	37648	**8644**	**0,230**
$\lvert r\rvert$, Кбайт	629,61	**144,56**	**0,230**
$\lvert Sig\rvert$, Кбайт	655,30	**170,25**	**0,260**
λ_σ, бит	1440	80	–
λ, бит	80	80	–

чений системных параметров № 2 — в 3,85 раза соответственно.

При этом предложенная модификация не влияет на общий уровень криптографической стойкости схемы подписи с учетом выбранной модели оценки.

Для сравнения времени выполнения алгоритма формирования подписи и алгоритма проверки подписи выполнена программная реализация СП СШ и МСП СШ. В качестве среды реализации выбрана система компьютерной алгебры SageMath 9.3.

По результатам проведения серии экспериментов для набора значений системных параметров № 1, представленного в табл. 1, наблюдается увеличение времени работы алгоритмов МСП СШ относительно алгоритмов СП СШ: в 1,11 раза для алгоритма формирования подписи и в 1,32 раза — для алгоритма проверки.

Для набора значений системных параметров № 2, представленного в табл. 1, была проведена ограниченная серия экспериментов. В результате модификации для набора № 2 наблюдается увеличение времени работы алгоритма формирования подписи в 1,08 раза, алгоритма проверки подписи — в 1,38 раза.

Заключение

Уменьшение размеров формируемой подписи для модифицированной версии схемы цифровой подписи (в 1,96 раза для набора значений системных параметров, обеспечивающих криптографическую стойкость на уровне 54 бита, в 3,85 раза для криптографической стойкости на уровне 80 бит соответственно) является значимым в контексте недостатков схемы подписи на основе протокола аутентификации Штерна, а также абсолютного значения снижения размеров подписи. При этом снижение производительности алгоритмов схемы подписи не является значимым в связи с особенностями применения схем цифровой подписи в информационных системах. Необходимо отметить, что увеличение времени работы алгоритмов схемы подписи связано с особенностями инструментов программной реализации и использованием высокоуровневого языка программирования. При выполнении программной реализации на языке системного программирования данное отставание может быть нивелировано.

При этом для практического использования предложенной модифицированной версии необходимо определить уровень ее стойкости в модели доказуемой стойкости.

Для дальнейших исследований в рамках предметной области могут быть выбраны следующие направления:

— уточнение оценки уровня криптостойкости модифицированной схемы цифровой подписи на основе протокола аутентификации Штерна (в том числе с использованием модели доказуемой стойкости);

— разработка других методов оптимизации по памяти для схемы подписи на основе протокола аутентификации Штерна;

— применение предложенного метода компактного описания подстановки для оптимизации по памяти схем подписи на основе других протоколов аутентификации без разглашения на основе произвольных линейных кодов.

Финансовая поддержка

Работа выполнена в рамках государственного задания (проект FSER20250003).

Благодарности

Автор выражает благодарность Вадиму Валерьевичу Давыдову, Андрею Андреевичу Голованову и Сергею Валентиновичу Беззатееву за помощь при проведении исследования, Ивану Владимировичу Чижову за предоставленный отзыв на результаты исследования, Юлии Викторовне Ниткиной за помощь при работе с текстом статьи.

Литература

1. **Boudot F., Gaudry P., Guillevic A., Heninger N., Thomé E., Zimmermann P.** The state of the art in integer factoring and breaking public-key cryptography. *IEEE Security & Privacy*, 2022, vol. 20, no. 2, pp. 80–86. doi:10.1109/MSEC.2022.3141512
2. **Shor P. W.** Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.
3. ГОСТ 34.10-2018. *Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи*. М., Стандартинформ, 2018. 21 с.
4. *Post-Quantum Cryptography | CSRC*. https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals (дата обращения: 01.06.2025)
5. *Post-Quantum Cryptography: Additional Digital Signature Schemes | CSRC*. https://csrc.nist.gov/projects/

pqc-dig-sig/standardization/call-for-proposals (дата обращения: 01.06.2025)
6. **Alagic G., Bros M., Ciadoux P., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y.-K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Silberg H., Smith-Tone D., Waller N.** Status report on the fourth round of the NIST post-quantum cryptography standardization process. *NIST IR 8545*, 2025. doi:10.6028/NIST.IR.8545
7. **Chailloux A., Etinski S.** On the (in)security of optimized Stern-like signature schemes. *Designs, Codes and Cryptography*, 2024, no. 92, pp. 803–832. doi:10.1007/s10623-023-01329-y
8. **Weger V., Gassner N., Rosenthal J.** *A Survey on code-based cryptography*. 2022. https://arxiv.org/pdf/2201.07119 (дата обращения: 01.06.2025). doi:10.48550/arXiv.2201.07119
9. **McEliece R. J.** A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report, Jet Propulsion Laboratory, Pasadena*, 1978, pp. 114–116.
10. **Courtois N., Finiasz M., Sendrier N.** How to achieve a McEliece-based digital signature scheme. *Advances in Cryptology — ASIACRYPT 2001*, 2001, pp. 157–174. doi:10.1007/3-540-45682-1_8
11. **Stern J.** A new identification scheme based on syndrome decoding. *Advances in Cryptology — CRYPTO'93*, 1993, pp. 13–21. doi:10.1007/3-540-48329-2_2
12. **Véron P.** Improved identification schemes based on error-correcting codes. *Applicable Algebra in Engineering, Communication and Computing*, 1996, no. 8, pp. 57–69. doi:10.1007/BF01190881
13. **Cayrel P., Véron P., El Y. A. S. M.** A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. *17th International Workshop, SAC 2010*, 2010, pp. 171–186. doi:10.1007/978-3-642-19574-7_12
14. **Jain A., Krenn S., Pietrzak K., Tentes A.** Commitments and efficient zero-knowledge proofs from learning parity with noise. *Advances in Cryptology — ASIACRYPT 2012*, 2012, pp. 663–680. doi:10.1007/978-3-642-34961-4_40
15. **Feneuil T., Joux A., Rivain M.** Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs. *Advances in Cryptology — CRYPTO 2022*, 2022, pp. 541–572. doi:10.1007/978-3-031-15979-4_19
16. **Feneuil T., Joux A., Rivain M.** Shared permutation for syndrome decoding: new zero-knowledge protocol and code-based signature. *Designs, Codes and Cryptography*, 2023, no. 91, pp. 563–608. doi:10.1007/s10623-022-01116-1
17. **Baldi M., Bitzer S., Pavoni A., Santini P., Wachter-Zeh A., Weger V.** Zero knowledge protocols and signatures from the restricted syndrome decoding problem. *14th International Conference on Post-Quantum Cryptography (PQCrypto 2023)*, 2023.
18. **Baldi M., Battaglioni M., Chiaraluce F., Horlemann-Trautmann A.-L., Persichetti E., Santini P., Weger V.** A new path to code-based signatures via identification schemes with restricted errors. *Advances in Mathematics of Communications*, 2025, no. 19(5), pp. 1360–1381. doi:10.3934/amc.2024058
19. **Manganiello F., Slaughter F.** Generic error SDP and generic error CVE. *Code-Based Cryptography — CBCrypto 2023*, 2023, pp. 125–143. doi:10.1007/978-3-031-46495-9_7
20. **Fiat A., Shamir A.** How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology — CRYPTO'86*, 1986, pp. 186–194. doi:10.1007/3-540-47721-7_12
21. **Bidoux L., Gaborit P., Kulkarni M., Mateu V.** Code-based signatures from new proofs of knowledge for the syndrome decoding problem. *Designs, Codes and Cryptography*, 2023, no. 91, pp. 497–544. doi:10.1007/s10623-022-01114-3
22. **Alagic G., Bros M., Ciadoux P., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y.-K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Silberg H., Smith-Tone D., Waller N.** Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process. *NIST IR 8528*, 2024. doi:10.6028/NIST.IR.8528
23. **Vysotskaya V. V., Chizhov I. V.** The security of the code-based signature scheme based on the stern identification protocol. *Прикладная дискретная математика*, 2022, № 57, с. 67–90. doi:10.17223/20710410/57/5
24. **Esser A., Bellini E.** Syndrome decoding estimator. *Public-Key Cryptography — PKC 2022*, 2022, pp. 112–141. doi:10.1007/978-3-030-97121-2_5
25. **Roy P. S., Morozov K., Fukushima K., Kiyomoto S.** Evaluation of code-based signature schemes. *Cryptology ePrint Archive*, 2019. https://eprint.iacr.org/2019/544 (дата обращения: 01.06.2025).
26. **Bernstein D. J.** Grover vs. McEliece. *Post-Quantum Cryptography (PQCrypto 2010)*, 2010, pp. 73–80. doi:10.1007/978-3-642-12929-2
27. **Kirshanova E.** Improved quantum information set decoding. *Post-Quantum Cryptography (PQCrypto 2018)*, 2018, pp. 507–527. doi:10.1007/978-3-319-79063-3_24
28. **Grover L. K.** A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.
29. **Both L., May A.** Decoding linear codes with high error rate and its impact for LPN security. *Post-Quantum Cryptography (PQCrypto 2018)*, 2018, pp. 25–46. doi:10.1007/978-3-319-79063-3_2
30. **Debris-Alazard T., Ducas L.,van Woerden W. P. J.** An algorithmic reduction theory for binary codes: LLL and more. *IEEE Transactions on Information Theory*, 2022, vol. 68, no. 5, pp. 3426–3444. doi:10.1109/TIT.2022.3143620

UDC 003.26
doi:10.31799/1684-8853-2025-6-51-63
EDN: AEXSDC

Permutation compact description method and its application for Stern-based digital signature modification

I. S. Nitkin[a,b], Post-Graduate Student, orcid.org/0000-0001-5240-1744, exebopen@gmail.com
[a]ITMO University, 49, Kronverksky Pr., 197101, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: The Stern authentication scheme is foundational zero-knowledge protocols for constructing quantum-resistant code-based digital signatures. However, the key limitation of this approach is the significant size of the generated signature. **Purpose:** To develop a memory-optimized Stern-based digital signature. **Results:** The study investigates the Stern-based digital signature, analyzing the sizes of its structural elements, and signature system parameters to its block size relation. We conclude that the largest memory consumption is required for storing random permutation values. We perform the cryptographic security analysis using the best-known attack model for Stern-based digital signature. We develop a method of permutation compact description using an information vector and apply it to Stern-based digital signature modification. The cryptographic security of the modified Stern-based digital signature using the same model is evaluated. A theoretical and experimental comparative analysis of the functional characteristics between the original and modified signature schemes demonstrates that the proposed modification significantly reduces generated signature size while maintaining the overall cryptographic strength of the scheme according to the chosen evaluation model. **Practical relevance:** The results can be applied to memory optimization for signature schemes using other code-based zero-knowledge protocols, as well as to the development of further optimization methods for Stern-based digital signatures.

Keywords — post-quantum cryptography, code-based cryptography, digital signature, Stern scheme, Stern-based signature.

For citation: Nitkin I. S. Permutation compact description method and its application for Stern-based digital signature modification. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 6, pp. 51–63 (In Russian). doi:10.31799/1684-8853-2025-6-51-63, EDN: AEXSDC

Financial support
The work was performed within the framework of the state assignment (project FSER-2025-0003).

References

1. Boudot F., Gaudry P., Guillevic A., Heninger N., Thomé E., Zimmermann P. The state of the art in integer factoring and breaking public-key cryptography. *IEEE Security & Privacy*, 2022, vol. 20, no. 2, pp. 80–86. doi:10.1109/MSEC.2022.3141512
2. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS'94)*, 1994, pp. 124–134.
3. State Standard 34.10-2018. *Informatsionnaia tekhnologiia. Kriptograficheskaia zashchita informatsii. Protsessy formirovaniia i proverki elektronnoi tsifrovoi podpisi* [Information technology. Cryptographic data security. Processes of digital signature generation and verification]. Moscow, Standartinform Publ., 2018. 21 p. (In Russian).
4. *Post-Quantum Cryptography | CSRC*. Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals (accessed 1 June 2025)
5. *Post-Quantum Cryptography: Additional Digital Signature Schemes | CSRC*. Available at: https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals (accessed 1 June 2025)
6. Alagic G., Bros M., Ciadoux P., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y.-K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Silberg H., Smith-Tone D., Waller N. Status report on the fourth round of the NIST post-quantum cryptography standardization process. *NIST IR 8545*, 2025. doi.org/10.6028/NIST.IR.8545
7. Chailloux A., Etinski S. On the (in)security of optimized Stern-like signature schemes. *Designs, Codes and Cryptography*, 2024, no. 92, pp. 803–832. doi:10.1007/s10623-023-01329-y
8. Weger V., Gassner N., Rosenthal J. A survey on code-based cryptography, 2022. Available at: https://arxiv.org/pdf/2201.07119 (accessed 1 June 2025). doi:10.48550/arXiv.2201.07119
9. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report, Jet Propulsion Laboratory, Pasadena*, 1978, pp. 114–116.
10. Courtois N., Finiasz M., Sendrier N. How to achieve a McEliece-based digital signature scheme. *Advances in Cryptology — ASIACRYPT 2001*, 2001, pp. 157–174. doi:10.1007/3-540-45682-1_8
11. Stern J. A new identification scheme based on syndrome decoding. *Advances in Cryptology — CRYPTO'93*, 1993, pp. 13–21. doi:10.1007/3-540-48329-2_2
12. Véron P. Improved identification schemes based on error-correcting codes. *Applicable Algebra in Engineering, Communication and Computing*, 1996, no. 8, pp. 57–69. doi:10.1007/BF01190881
13. Cayrel P., Véron P., El Y. A. S. M. A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. *17th International Workshop: Selected Areas in Cryptography — SAC 2010*, 2010, pp. 171–186. doi:10.1007/978-3-642-19574-7_12
14. Jain A., Krenn S., Pietrzak K., Tentes A. Commitments and efficient zero-knowledge proofs from learning parity with noise. *Advances in Cryptology — ASIACRYPT 2012*, 2012, pp. 663–680. doi:10.1007/978-3-642-34961-4_40
15. Feneuil T., Joux A., Rivain M. Shared permutation for syndrome decoding: New zero-knowledge protocol and code-based signature. *Designs, Codes and Cryptography*, 2023, no. 91, pp. 563–608. doi:10.1007/s10623-022-01116-1
16. Feneuil T., Joux A., Rivain M. Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs. *Advances in Cryptology — CRYPTO 2022*, 2022, pp. 541–572. doi:10.1007/978-3-031-15979-4_19
17. Baldi M., Bitzer S., Pavoni A., Santini P., Wachter-Zeh A., Weger V. Zero knowledge protocols and signatures from the restricted syndrome decoding problem. *14th International Conference on Post-Quantum Cryptography — PQCrypto 2023*, 2023.
18. Baldi M., Battaglioni M., Chiaraluce F., Horlemann-Trautmann A.-L., Persichetti E., Santini P., Weger V. A new path to code-based signatures via identification schemes with restricted errors. *Advances in Mathematics of Communications*, 2025, no. 19(5), pp. 1360–1381. doi:10.3934/amc.2024058
19. Manganiello F., Slaughter F. Generic error SDP and generic error CVE. *Code-Based Cryptography — CBCrypto 2023*, 2023, pp. 125–143. doi:10.1007/978-3-031-46495-9_7
20. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology — CRYPTO'86*, 1986, pp. 186–194. doi:10.1007/3-540-47721-7_12
21. Bidoux L., Gaborit P., Kulkarni M., Mateu V. Code-based signatures from new proofs of knowledge for the syn-

drome decoding problem. *Designs, Codes and Cryptography*, 2023, no. 91, pp. 497–544. doi:10.1007/s10623-022-01114-3
22. Alagic G., Bros M., Ciadoux P., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y.-K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Silberg H., Smith-Tone D., Waller N. Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process, *NIST IR 8528*, 2024. doi:10.6028/NIST.IR.8528
23. Vysotskaya V. V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol. *Prikladnaya diskretnaya matematika*, 2022, no. 57, pp. 67–90. doi:10.17223/20710410/57/5
24. Esser A., Bellini E. Syndrome decoding estimator. *Public-Key Cryptography – PKC 2022*, 2022, pp. 112–141. doi:10.1007/978-3-030-97121-2_5
25. Roy P. S., Morozov K., Fukushima K., Kiyomoto S. Evaluation of code-based signature schemes. *Cryptology ePrint Archive*, 2019. Available at: https://eprint.iacr.org/2019/544 (accessed 1 June 2025)
26. Bernstein D. J. Grover vs. McEliece. *Post-Quantum Cryptography – PQCrypto 2010*, 2010, pp. 73–80. doi:10.1007/978-3-642-12929-2_6
27. Kirshanova E. Improved quantum information set decoding. *Post-Quantum Cryptography – PQCrypto 2018*, 2018, pp. 507–527. doi:10.1007/978-3-319-79063-3_24
28. Grover L. K. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.
29. Both L., May A. Decoding linear codes with high error rate and its impact for LPN security. *Post-Quantum Cryptography – PQCrypto 2018*, 2018, pp. 25–46. doi:10.1007/978-3-319-79063-3_2
30. Debris-Alazard T., Ducas L.,van Woerden W. P. J. An algorithmic reduction theory for binary codes: LLL and more. *IEEE Transactions on Information Theory*, 2022, vol. 68, no. 5, pp. 3426–3444. doi:10.1109/TIT.2022.3143620