УДК: 004.056

Артём О. Макаров
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
e-mail: zma.94@mail.ru, https://orcid.org/0000-0002-8574-9621

СХЕМА ПОСТКВАНТОВОЙ АГРЕГИРОВАННОЙ ПОДПИСИ С ЛЕНИВОЙ ПРОВЕРКОЙ НА ОСНОВЕ МНОГОМЕРНЫХ КВАДРАТИЧНЫХ МНОГОЧЛЕНОВ

DOI: http://dx.doi.org/10.26583/bit.2023.3.02

Аннотация. Агрегированные подписи являются частным видом электронных подписей. Они позволяют объединять индивидуальные подписи, полученные различными подписантами для различных сообщений, в единую подпись. Такая подпись обеспечивает аутентичность, целостность и неотказуемость для всех подписанных сообщений. При этом длина полученной агрегированной подписи значительно меньше суммы длин исходных подписей. Последовательные агрегированные подписи – это подтип агрегированных подписей. С их помощью можно объединять индивидуальные подписи только в процессе подписания. Подписи данного типа могут быть использованы во множестве приложений, включая протоколы защищенной маршрутизации, защищенное журналирование, сенсорные сети, инфраструктуру открытых ключей, блокчейн. В данной статье представлена новая схема постквантовой агрегированной подписи с ленивой проверкой. Данная схема позволяет избавиться от необходимости проверки текущей последовательной агрегированной подписи при формировании новой, что расширяет её возможное применение по сравнению с существующими последовательными постквантовыми схемами. В качестве основы предлагаемой схемы подписи используется односторонняя подстановка с секретом HFEv-, являющаяся стойкой к квантовым атакам; а также обобщенная конструкция Гентри, О'Нила и Рейзина для получения ленивой верификации с применением идеального шифра, который может быть реализован с использованием сети Фейстеля и блочного шифра. Для представленной схемы приведены формальные доказательства её стойкости на основе игровой модели Белларе – Рогавея, заключающиеся в сведении стойкости схемы к стойкости односторонней подставки с секретом HFEv-, а также представлен набор параметров схемы для параметров стойкости в 80 и 120 бит.

Ключевые слова: электронная подпись, постквантовая криптография, агрегированная подпись, последовательная агрегированная подпись, ленивая проверка, квадратичные многочлены.
Для цитирования: МАКАРОВ, Артём О. СХЕМА ПОСТКВАНТОВОЙ АГРЕГИРОВАННОЙ ПОДПИСИ С ЛЕНИВОЙ ПРОВЕРКОЙ НА ОСНОВЕ МНОГОМЕРНЫХ КВАДРАТИЧНЫХ МНОГОЧЛЕНОВ. Безопасность информационных технологий, [S.l.], т. 30, № 3, с. 30–50, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1527. DOI: http://dx.doi.org/10.26583/bit.2023.3.02.

Artyom Makarov
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31 Moscow, 115409, Russia
e-mail: zma.94@mail.ru, https://orcid.org/0000-0002-8574-9621

LMQSAS – post-quantum aggregate signature scheme with lazy verification

DOI: http://dx.doi.org/10.26583/bit.2023.3.02

Abstract. Aggregated signatures are a type of digital signatures that allow individual signatures obtained by different signers for different messages to be combined into a single signature that provides authenticity, integrity, and non-repudiation for all signed messages. In this case, the length of the resulting aggregated signature is much less than the sum of the lengths of the individual signatures. Sequential aggregated signatures are a subtype of aggregated signatures and allow individual signatures to be combined only during the signing procedure. Signatures of this type can be used in a variety of applications, including secure routing protocols, secure logging, sensor networks, public key

infrastructure, blockchain. In this paper we present a new post-quantum aggregated signature scheme with lazy verification that eliminates the need for checking the current sequential aggregated signature during the signature process, which expands its possible application as compared to existing sequential post-quantum signature schemes. The proposed signature scheme is based on post-quantum HFEv- one-way trapdoor permutation, which is known to be resistant to quantum attacks; and Unified Framework of Gentry, O'Neill and Reyzin for obtaining lazy verification using an ideal cipher that can be implemented using the Feistel network and a block cipher. For the presented scheme we provide formal proofs of its security using Bellare-Rogaway game model: the security of the scheme was reduced to the security of a HFEv- one-way trapdoor permutation. We also present a set of parameters for the proposed scheme to meet 80 and 120-bit security levels.
Keywords: digital signature, post-quantum cryptography, aggregated signatures, sequential aggregated signatures, lazy verification, multivariate cryptography.
For citation: MAKAROV, Artyom O. Lmqsas - post-quantum aggregate signature scheme with lazy verification. IT Security (Russia), [S.l.], v. 30, n. 3, p. 30–50, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1527. DOI: http://dx.doi.org/10.26583/bit.2023.3.02.

Введение

Большинство асимметричных криптосистем, используемых в существующих информационных системах, основаны на предположении о сложности таких вычислительных задач, как вычисление дискретного логарифма и факторизация больших целых чисел. Несмотря на то, что данные задачи считаются экспоненциально сложными для классических алгоритмов, известно о существовании квантовых алгоритмов, таких как алгоритм Шора [1] и его модификации, позволяющих получать решения данных задач за полиномиальное время. Принимая во внимание текущие успехи в сфере квантовых компьютеров, задача разработки и анализа постквантовых схем, стойких к известным квантовым атакам, становится чрезвычайно актуальной. Для построения постквантовых схем могут быть использованы математические аппараты теории алгебраического кодирования, решёток, хэш-функций, суперсингулярных эллиптических кривых и многомерных квадратичных многочленов.

Особенностью схем на основе квадратичных многочленов является малый размер подписи и высокое быстродействие, что позволяет использовать их во множестве приложений, включая встраиваемые устройства. Криптосистема HFE (Hidden Field Equations) [2] и её вариация HFEv- [3] являются наиболее известными и изученными схемами и служат основой многих схем электронной подписи [4].

Последовательные агрегированные подписи позволяют группе подписантов, использующих различные ключевые пары, подписать различные сообщения единой агрегированной подписью, которая обеспечивает целостность, аутентичность и неотказуемость для всех подписанных сообщений. С целью уменьшения количества хранимой и передаваемой информации подписи данного типа могут применяться во множестве приложений, включая протоколы защищенной маршрутизации, инфраструктуру открытых ключей, защищенное журналирование, сенсорные сети и блокчейн [5]. В отличие от групповых схем подписи, агрегированные подписи формируют подписи для различных сообщений [6], а в отличие от протоколов мультиподписей [7–10] – не требуется взаимодействие между подписантами, кроме, может быть, передачи текущей агрегированной подписи и открытых ключей.

Схемы последовательных агрегированных подписей могут быть построены на основе односторонних подстановок с секретом [11], однако в общем случае требуют проверки текущей агрегированной подписи перед формированием новой подписи, что негативно влияет на быстродействие процедуры подписи. Существует ряд способов [12–14], позволяющих построить так называемые подписи с ленивой проверкой, для

которых отсутствие проверки подписи на этапе её формирования не оказывает негативного влияния на стойкость схемы. Существующие постквантовые схемы агрегированной подписи [15; 16] не обладают свойством ленивой проверки.

Данная статья посвящена построению схемы постквантовой агрегированной подписи на основе многомерных квадратичных многочленов с ленивой проверкой, в частности схема использует HFEv- в качестве односторонней функции с секретом. Для достижения ленивой проверки применяется обобщённая схема Гентри [12] с идеальным шифром, для построения которого используется схема FNR [17] и хэш-функция в модели случайного оракула.

Статья построена следующим образом: в разделе 1 описано построение схем последовательной агрегированной подписи; в разделе 2 приведены основные используемые термины и определения; в разделе 3 представлено формальное описание существующей схемы MQSAS; в разделе 4 доказана формальная стойкость схемы MQSAS; в разделе 5 описан предлагаемый подход к построению схемы последовательной агрегированной подписи с ленивой проверкой на основе схемы MQSAS; в разделе 6 дано описание предлагаемой схемы последовательной агрегированной подписи LMQSAS с ленивой проверкой; в разделе 7 доказана стойкость предлагаемой схемы; в разделе 8 рассматривается вопрос построения идеального шифра для использования в рамках предлагаемой схемы; в разделе 9 рассматриваются предлагаемые параметры схемы; в заключении представлены результаты работы.

1. Последовательные агрегированные подписи

Одним из возможных способов построения схемы агрегированной подписи является построение последовательной агрегированной подписи с использованием односторонней функции с секретом. Например, схема последовательной подписи, полученная Лисянской и др. [11], использует односторонние подстановки с секретом для обеспечения агрегации. Каждый подписант в цепочке складывает по модулю 2 текущую агрегированную подпись с хэш-значением всех подписываемых сообщений в цепочке (включая своё) и всех открытых ключей и вычисляет обратную подстановку с секретом с использованием своего закрытого ключа. Однако для достижения стойкости данной схемы требуется проведение двух дополнительных проверок. Во-первых, следует убедиться, что открытые ключи действительно задают преобразования на основе односторонней подстановки с секретом. Во-вторых, каждому подписанту необходимо проверить текущую агрегированную подпись перед непосредственной процедурой подписи. Эти ограничения ведут к увеличению времени подписания, а также не позволяют добиться ленивой проверки, критичной для производительности в ряде приложений, таких как защищенная маршрутизация [5].

В настоящий момент единственной схемой постквантовой агрегированной подписи на основе квадратичных многочленов является схема MQSAS [15]. Используя её идеи и обобщенную схему Гентри, можно построить новую схему агрегированной подписи с ленивой проверкой.

Для описания формальной модели стойкости введём определение стойкой последовательной агрегированной подписи. Под оракулом, пренебрежимо малой величиной, игрой, экспериментом и преимуществом здесь и далее будем понимать соответствующие термины в игровой модели Белларе – Рогавея [18; 19].

Определение 1 (Пренебрежимо малая величина [18]**).** Величина, заданная функцией $\epsilon(\lambda)$ от некоторого параметра λ, называется пренебрежимо малой, если $\forall c > 0, \exists K > 0: \forall \lambda \geq K\ \epsilon(\lambda) < \lambda^{-c}$.

Определение 2 (PPT алгоритм). PPT алгоритмом назовём недетерминированный алгоритм, время выполнения t которого для некоторого полиноминально ограниченного входа $i(\lambda)$ от параметра λ является полиномиально ограниченным везде, кроме, может быть, конечного числа входных величин, число которых есть пренебрежимо малая величина от размера входного множества алгоритма.

Определение 3 (Стойкая последовательная агрегированная подпись [11]**).** Последовательная агрегированная подпись – тройка алгоритмов *Генерация параметров*, *Агрегированная подпись*, *Агрегированная проверка*: $SAS = (Kg, AggSign, AggVer)$. Алгоритм генерации параметров Kg принимает на вход 1^k для некоторого параметра k и выдаёт ключевую пару (pk_i, sk_i). Алгоритм агрегированной подписи $AggSign$ принимает на вход закрытый ключ sk_i, сообщение m_i, текущую агрегированную подпись σ_{i-1}, список пар «открытый ключ – сообщение» $\big((pk_1, m_1), \dots, (pk_{i-1}, m_{i-1})\big)$ и выдаёт новую агрегированную подпись σ_i. Агрегированная проверка $AggVer$ принимает на вход список пар «открытый ключ – сообщение» $\big((pk_1, m_1), \dots, (pk_i, m_i)\big)$ и агрегированную подпись σ_i и выдаёт результат проверки из множества $\{0,1\}$.

Пусть A – PPT алгоритм в игре против последовательной агрегированной подписи SAS. Эксперимент игры $\mathrm{Exp}_{SAS,A}^{\mathrm{sas-uf}}(k)$ состоит из трех этапов:

инициализация: $(pk, sk) \leftarrow Kg(1^k)$;

атака: выполнение алгоритма $A^{AggSign(sk,*,*,*),pk}$;

подделка подписи: $\big((pk_1, m_1), \dots, (pk_i, m_i), \sigma\big) \leftarrow_R A$, выдаёт 1, если $AggVer\big((pk_1, m_1), \dots, (pk_i, m_i), \sigma\big) = 1$, $pk_{i^*} = pk$ для некоторого $1 \le i^* \le n$, A не делал запросов к оракулу подписи вида $AggSign\Big(sk, m_{i^*}, \big((pk_1, m_1), \dots, (pk_{i^*-1}, m_{i^*-1})\big)\Big)$.

Преимущество противника A в игре против схемы последовательной подписи есть величина

$$\mathrm{Adv}_{SAS,A}^{\mathrm{sas-uf}} = \Pr\big[\mathrm{Exp}_{SAS,A}^{\mathrm{sas-uf}}(k) = 1\big].$$

Схема SAS называется стойкой, если для любого PPT алгоритма противника A величина преимущества $\mathrm{Adv}_{SAS,A}^{\mathrm{sas-uf}}$ в описанной выше игре есть пренебрежимо малая величина.

2. Формальное описание схемы MQSAS

Перейдём к формальному описанию схемы MQSAS, которая будет являться основой схемы с ленивой проверкой.

Генерация параметров. Для каждого пользователя генерируется ключевая пара в соответствии с алгоритмом генерации схемы HFEv-. Пусть H – стойкая к коллизиям хэш-функция. Пусть $n, D, a, v, l \in \mathbb{N}$ – параметры схемы. Пусть K – конечное поле из g элементов. Тогда центральное преобразование F в схеме HFEv- задаётся следующим образом:

$$F: E \times K^v \to E: F(x) = \sum_{0 \le i \le j}^{q^i + q^j \le D} a_{ij} x^{q^i + q^j} + \sum_{i=0}^{q^i \le D} b_i(v_1, \dots, v_v) x^{q^i} + c(v_1, \dots, v_v),$$

где $a_{ij} \in K, b_i: K^v \to E$ – линейная функция, $c: K^v \to E$ – квадратичная функция, E – расширение поля K степени n, Φ – естественный изоморфизм: $\Phi: F^n \to E: \Phi(x_1, \dots, x_n) = \sum_i x_i X^{i-1}, i \in \{1, .., n\}$.

Тогда $F': K^n \to F^n: F' = \Phi^{-1} \circ F \circ \Phi$ — квадратичное отображение, где $\circ$ – операция композиции отображений. Для скрытия структуры F' используются аффинные или

линейные отображения $S: K^n \to K^{n-a}$ и $T: K^{n+v} \to F^{n+v}$ максимального ранга. Также вычисляются значения $P = S \circ F' \circ T$, $id = H(P)$. Открытым ключом является пара $pk = (id, P)$, секретным ключом – тройка отображений $sk = (T, F, S)$.

Агрегированная подпись. Пусть $U = \{u_1, \dots, u_k\}$ – множество пользователей, m_i – сообщение, подписанное пользователем u_i, $pk = \{pk_1, \dots, pk_n\}$ – открытые ключи пользователей U, σ_{i-1} – предыдущее значение агрегированной подписи сообщений $\{m_j \mid 1 \le j < i\}$. Перед формированием подписи пользователь проводит проверку текущей агрегированной подписи σ_{i-1}. Для генерации подписи при $i = 1$ (случай $\sigma_0 = 0$) пользователь производит подпись на основе алгоритма подписи схемы HFEv-. Для $i \in \{1, .., k\}$ подпись разбивается на 2 блока: $\sigma_{i-1} = (S', X')$: $|S'| = n - a$ бит. Затем он использует свой секретный ключ sk_i для вычисления подписи согласно алгоритму подписи схемы Gui [4], для значения хэш-функции $h = H(m_1, \dots, m_i, id_1, \dots, id_i)$. Далее пользователь объединяет полученную подпись $(S_i, X_l, \dots, X_1)$ с агрегированной подписью σ_{i-1} для получения новой агрегированной подписи σ_i: $S^* = S' \oplus S_l, X^* = (X_l, \dots, X_1, X'), \sigma = (S^*, X^*)$. Алгоритм формирования агрегированной подписи представлен на рис. 1 (a).

Агрегированная проверка. Пусть $U = \{u_1, \dots, u_i\}$ – множество пользователей, m_j – сообщение, подписанное пользователем u_j, $pk = \{pk_1, \dots, pk_i\}$ – открытые ключи пользователей U, $pk_j = (P_j, id_j)$, σ – агрегированная подпись сообщений $\{m_j \mid 1 \le j < i\}$. Подпись σ представляется в виде $\sigma = (S', X_{il}, \dots, X_{(i-1)l+1}, X_{(i-1)l}, \dots, X_1)$: $|S'| = n - a$ бит, $|X_j| = a + v$ бит, $j \in \{1, .., il\}$. Дальнейший алгоритм вычисления представлен на рис. 1 (b).

```
if i = 1 then
  S' = 0^(n-a)
  X' ← ∅
else if AggVerify(i − 1, σ_{i−1}, pk_1, …, pk_{i−1}, m_1, …, m_{i−1})
        = TRUE then
  (S', X') ← split(σ_{i−1})
else return ∅
end if
h ← H(m_1, …, m_i, id_1, …, id_i)
for j = 1 to l do
  D_j ← first n − a bits of h
  (S_j, X_j) ← HFEv_{sk_j}^{−1}(D_j)
  h ← H(h)
end for
S' ← S' ⊕ S_l
X' ← (X_l || … || X_1 || X')
σ_i ← (S', X')
return σ_i
```

(a)

```
for j = i to 1 do
  h ← H(m_1, …, m_i, id_1, …, id_j)
  for k = 1 to l do
    D_k ← first n − a bits of h
    h ← H(h)
  end for
  for k = l − 1 to 0 do
    S' = P_j(S' || X_{(j−1)l+k+1}) ⊕ D_{k+1}
  end for
end for
if S' = 0 then
  return TRUE
else
  return FALSE
end if
```

(b)

Рис. 1. Алгоритм формирования (a) и проверки (b) агрегированной электронной подписи схемы MQSAS

Fig. 1. MQSAS Signature (a) and Verification (b) algorithms

Размер агрегированной подписи для k сообщений при параметрах (n, D, a, v, l) составляет $(n - a) + kl(a + v)$ бит.

3. Теоретическая стойкость схемы MQSAS

В [15] представлена краткая идея доказательства стойкости схемы MQSAS, без формального доказательства теорем, в данном разделе приведём доказательство её

стойкости, которое будет полезно при доказательстве стойкости предлагаемой схемы с ленивой проверкой, описанной в следующих разделах.

Предположение 1 (Стойкость односторонней функции HFEv-). Функция HFEv (t, ϵ) – стойкая односторонняя, т.е. для всех PPT противников, имеющих время не более t в игре на стойкость односторонней функции, их преимущество при нахождении прообраза $x \in K^{n+v}$ для данной величины $y \in K^{n-a}$: $y = \mathrm{HFEv}(x)$ $Adv^{ow}_{\mathrm{HFEv}}(A) = \Pr[y \leftarrow_R K^{n-a}, x \leftarrow A \mid \mathrm{HFEv}(x) = y| \leq \epsilon$, для пренебрежимо малой ϵ.

Введём вспомогательное определение.

Определение 4 (Расширяемое отображение на основе функции). Отображение (Π_v, Π_v^{-1}): $\Pi_v^{-1}: S \times X^* \to S \times X^{*+1}$ назовём расширяемым, если оно представимо в виде $\Pi_v^{-1}: (s, x_1, \dots, x_k) \mapsto (s', x_1, \dots, x_k, x')$, где $(s', x') = \Pi^{-1}(s)$ для некоторого отображения (Π, Π^{-1}): $\Pi^{-1}: S \to S \times X$, называемого основой, $X^{*+1} \equiv X^*$ ($+1$ в показателе обозначает, что выходные строки имеют длину на 1 больше, чем входные).

Лемма 1 (Стойкость расширяемой односторонней подстановки с секретом). Пусть (Π, Π^{-1}): $\Pi^{-1}: S \to S \times X$ (t, ϵ) – стойкая односторонняя функция с секретом, являющаяся основой для расширяемого биективного отображения (Π_v, Π_v^{-1}): $\Pi_v^{-1}: S \times X^* \to S \times X^{*+1}$. Тогда (Π_v, Π_v^{-1}) – (t, ϵ) – стойкая односторонняя подстановка с секретом на S.

Доказательство. Докажем сведением от противного. Пусть существует противник, моделируемый эффективным алгоритмом A, в игре против Π_v как стойкой односторонней подстановки. Построим эффективный алгоритм B в игре на стойкость Π как стойкой односторонней функции с секретом.

Алгоритм B устроен следующим образом. Получая от претендента случайную величину $(s'_b, x'_b) \in S \times X^*$, он передаёт её на вход алгоритма A в виде $(s'_b, x'_b || \emptyset) \in S \times X^{*+1}$, где $\emptyset$ – пустая строка.

При обработке запросов к оракулу Π_v^{-1} алгоритм B, получая от алгоритма A запрос к оракулу обратной односторонней подстановки вида (s_a, x_a), отправляет запрос s_a собственному оракулу односторонней функции, получая $s_d = \Pi(s_c, x_c)$, после чего отправляет (s_b, x_d) как ответ на запрос.

При обработке запросов к оракулу Π_v алгоритм B, получая от алгоритма A запрос к оракулу обратной односторонней подстановки вида $(s_c, x_c || x_d)$, отправляет запрос (s_c, x_c) собственному оракулу односторонней функции, получая $(s_b, x_b) = \Pi(s_a)$, после чего отправляет $(s_b, x_b || x_a)$ как ответ на запрос.

В результате алгоритм A выдаёт выход (s''_a, x''_a). Выходом алгоритма B является величина s''_a. Игра на стойкость с использованием алгоритма B представлена на рис. 2.

Алгоритм B является элементарной обёрткой вокруг алгоритма A, прозрачно и детерминировано обрабатывающего все запросы алгоритма A путём внесения детерминированных изменений в сообщения. Выход алгоритма B полностью определяется выходом алгоритма A. Алгоритм B выигрывает в игре против односторонней функции с секретом тогда, и только тогда, когда алгоритм A выдаёт верный прообраз (s''_a, x''_a), переданного ему на этапе инициализации значения $(s'_b, x'_b || \emptyset)$, т.е. тогда и только когда $(s_b, x_b) = \Pi(x''_a)$. Следовательно, $Adv^{ow}_{H_v}(A) = Adv^{ow}_{H}(B)$.

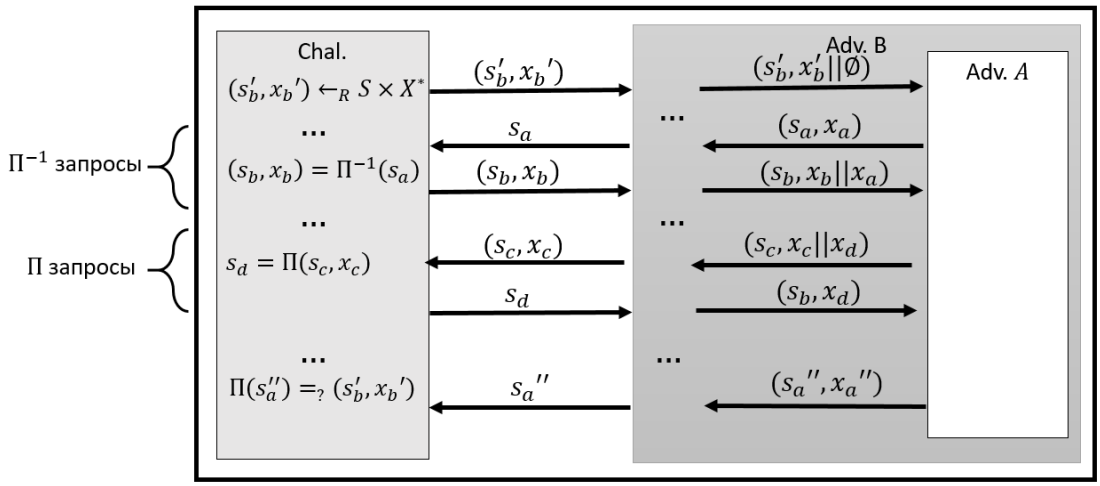

Рис. 2. Алгоритм противника B в игре на стойкость односторонней функции с секретом
Fig. 2. Adversary B algorithm against secure trapdoor permutation

Утверждение 1 (Расширяемость подстановки HFEv −). Функция агрегирования $F: (S_{i-1}, X_{i-1}, \dots, X_1) \mapsto (S_i, X_i X_{i-1}, \dots, X_1)$ на основе HFEv, где $(S_i, X_i) = \mathrm{HFEv}^{-1}(S_{i-1})$, используемая в определении схемы $MQSAS$, является расширяемой подстановкой с основой HFEv^{-1}.

Определение 5 (Итеративная расширяемая подстановка с использованием хэш-функции). Пусть $\Pi_v^{-1}: S \times X^* \to S \times X^{*+1}$ – расширяемое обратимое отображение и представимо в виде $\Pi_v^{-1}: (s, x_1, \dots, x_k) \mapsto (s', x_1, \dots, x_k, x')$, где $(s', x') = \Pi^{-1}(s)$ для некоторой основы $\Pi^{-1}: S \to S \times X$, $X^{*+1} \equiv X^*$. Подстановка ${\Pi^{-1}}_v^l(s, X)$ вычисляется с использованием хэш-функции $H: S \to S$, как указано в алгоритме на рис. 3.

$e: x \mapsto x$
$H^i \leftarrow \underbrace{H \circ H \dots \circ H}_{i}$
$H^0: x \mapsto \emptyset$
$S_v^0 \leftarrow S$
for $i = 1$ **to** l **do**
  $(S_v^i, X) \leftarrow \Pi^{-1}(\mathrm{H}^{i-1}(S) \oplus S_v^{i-1})$
  $X_v^i \leftarrow X || X_v^{i-1}$
end for
return (S_v^i, X_v^i)

Рис. 3. Алгоритм вычисления итеративной расширяемой подстановки на входах (S, X)
Fig. 3. Extendable iterative permutation algorithm on inputs (S, X)

Подстановка $\Pi_v^l(S, X)$ называется итеративной расширяемой подстановкой на S на основе функции П с параметром повторения l.

Лемма 2 (Стойкость итеративной подстановки с использованием хэш-функции). Пусть ${\Pi^{-1}}_v^l(s, X)$ – итеративная подстановка с параметром повторения l на основе (t, ϵ) стойкой односторонней функции с секретом $\Pi^{-1}: S \to S \times X$ (t, ϵ), H – случайный оракул. Тогда Π_v – (t', ϵ') – стойкая односторонняя подстановка с секретом на S, где $t' = t/l$, $\epsilon' = \epsilon^{1/l}$.

Доказательство. Докажем сведением от противного. Пусть существует противник, моделируемый эффективным алгоритмом A, в игре против Π_v^l как стойкой односторонней подстановки. Построим эффективный алгоритм B в игре на стойкость Π как стойкой односторонней функции с секретом. Алгоритм противника B при ответах на запросы в игре против односторонней подстановки с секретом представлен на рис. 4. Частный случай игры при $l = 2$ приведён на рис. 5. В доказательствах используется явная передача значения $H(s_{a0})$ в запросах Π и Π^{-1}. Это необходимо только для построения доказательства. Так как данная подставка будет использоваться в качестве односторонней функции с секретом для построения схем подписи, значение $H(s_{a0})$ будет соответствовать хэш-значению для части подписываемого сообщения, которое в явном виде может быть получено всеми сторонами.

В результате работы алгоритм A выдаёт величину q, равную $\Pi_v^l(s_b')$, с вероятностью ϵ' за время t'. Получая величину q, алгоритм B вычисляет $p_i = \Pi(q)$, $h = H(s'_b), q' = p \oplus h$ и выдаёт q' в качестве результата игры, выигрывая с вероятностью ϵ за время t.

Противник B осуществляет l запросов к оракулу на каждый запрос к оракулу алгоритма A, $t = lt'$. Так как (Π, Π^{-1}) – односторонняя подстановка с секретом, вероятность того, что $q' = \Pi^{-1}(s_b')$ при случайном выборе $s_b{}'$ составляет ϵ. Вероятность того, что при фиксированном $a_{ai}, s_{ci} = \Pi^{-1}(H^i(s_b') \oplus s_{bi})$ составляет ϵ, так как вычисление Π^{-1} выполняется от случайной величины, полученной от случайного оракула H^i, выход которого независим при каждом $i = l..1$. Так как описанные выше события независимы, вероятность осуществления атаки алгоритмом A равно произведению данных вероятностей и $\epsilon = \epsilon'^l$. Итого имеем $t' = t/l\,, \epsilon' = \epsilon^{1/l}$.

Инициализация $s_b{}'$: $H^i \leftarrow \underbrace{H \circ H \ldots \circ H}_{i}$ $H^0 : x \mapsto \emptyset$ $h = H(s_b')$ $(s_b'', x_b'') \leftarrow \Pi^{-1}(h)$ **return** (s_b', x_b'')	Π_l^{-1} *запросы* s_a $s_{a0} \leftarrow s_a$ $x_{a0} \leftarrow \emptyset$ **for** $i = 1$ **to** l **do** $s_{ci} \leftarrow H^{i-1}(s_{a0}) \oplus s_{ai-1}$ $(s_{di}, x_{di}) \leftarrow \Pi^{-1}(s_{ci})$ $s_{ai} \leftarrow s_{di}$ $x_{ai} \leftarrow x_{di} \| x_{ai-1}$ **return** $(s_{al}, x_{al} \| \ldots \| x_{a1}, H(s_{a0}))$
Π_l *запросы* (s_a, x_a) $(s_{al}, x_{al} \| \ldots \| x_{a1}, H(s_{a0})) \leftarrow (s_a, x_a)$ **for** $i = l - 1$ **to** 0 **do** $s_{ci} \leftarrow \Pi(s_{ai+1}, x_{ai+1})$ $s_{di} \leftarrow H^l(s_{a0}) \oplus s_{ci}$ $s_{ai} \leftarrow s_{di}$ **return** (s_{a0})	
Получение ответа $q \leftarrow A$ $(s_{al}, x_{al} \| \ldots \| x_{a1}, H(s_{a0})) \leftarrow (s_a, x_a)$ **for** $i = l - 1$ **to** 0 **do** $s_{ci} \leftarrow \Pi(s_{ai+1}, x_{ai+1})$ $s_{di} \leftarrow H^l(s_{a0}) \oplus s_{ci}$ $s_{ai} \leftarrow s_{di}$ $q' \leftarrow (s_{a1} \oplus h(s_b'), x_{c1})$ **return** q'	

Рис. 4. Алгоритм работы противника B в игре против односторонней подстановки с секретом
Fig. 4. Adversary B algorithm's queries against trapdoor permutation

Теорема 1 (Стойкость схемы MQSAS). Предполагая (t', ϵ') односторонность функции HFEv, последовательная агрегированная подпись MQSAS с параметром l является $(t, q_H, q_S, n, \epsilon)$ стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи, причём для всех t', ϵ':

$$\epsilon \leq (q_S + q_H + 1)\, \epsilon'^{1/l}),$$
$$t \leq t'/l - 4kq_H + 4kq_S + 7k + 1.$$

Доказательство. Докажем сведением от противного. Пусть существует противник, моделируемый эффективным алгоритмом A в игре против схемы агрегированной подписи MQSAS. Тогда существует эффективный алгоритм B, использующий A в игре на стойкость односторонней расширяемой подстановки Π_v, используемой в схеме MQSAS.

Пусть A является $(t, q_H, q_S, n, \epsilon)$ алгоритмом, т.е. выполняется за время не более t, выполняет не более q_H запросов к оракулу хэш-функции, не более q_S запросов к оракулу агрегированной подписи, число пользователей в агрегированной подписи не превосходит n, преимущество в игре не более ϵ.

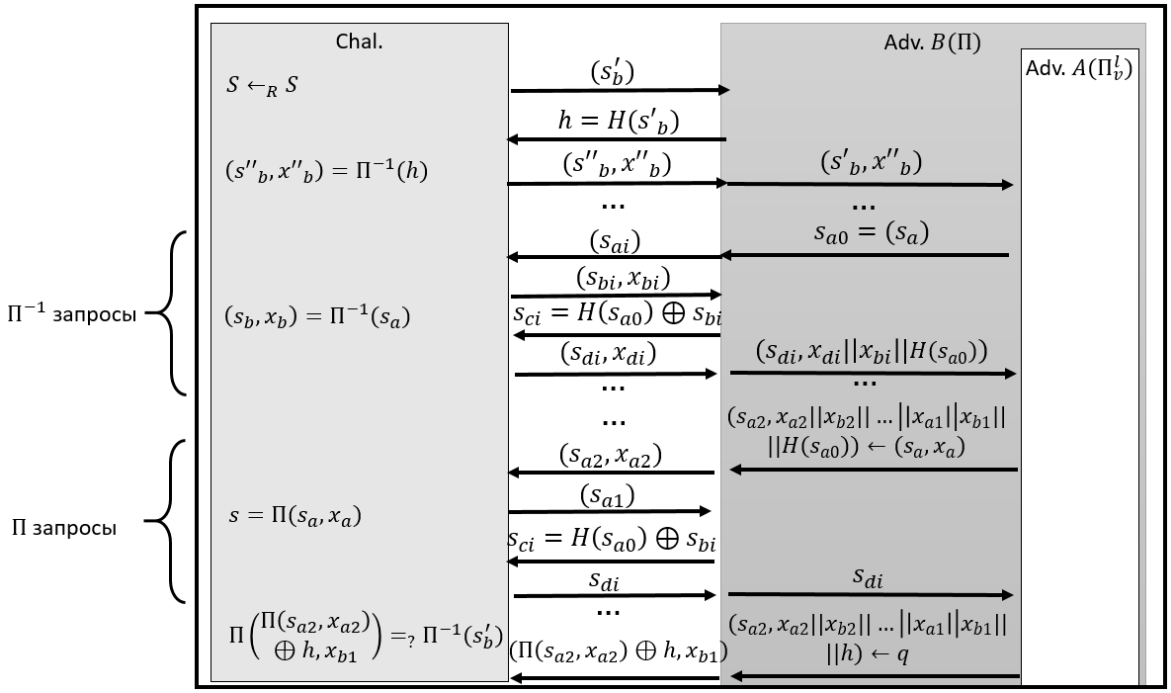

Рис. 5. Игра на стойкость односторонней подстановки с секретом против противника B при $l = 2$
Fig. 5. One-way trapdoor permutation game against Adversary B for $l = 2$

Построим алгоритм противника B способом, аналогичным описанному в [11], как обёртку вокруг алгоритма противника A, отвечающего на запросы хэширования и агрегированной подписи против расширяемой подстановки Π_v. Используя рассуждения, аналогичные первоисточнику, получим, что MQSAS является $(t, q_H, q_S, n, \epsilon)$ стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи при условии (t', ϵ') стойкости односторонней подстановки Π_v.

Так как HFEv является основой расширяемой подстановки Gui = Π_v, заменяя используемую в Gui хэш-функцию H на $H_s^*: H^*(m) = H(m) \oplus s, (H^*)^i(m) = H^{i-1}\big(h^*(m)\big), i = 2..l$, где l – параметр повторения схемы MQSAS, s – параметр H_s^*,

изменяемый на каждой итерации вычисления последовательной подписи и равный предыдущему значению агрегированной подписи, получаем описание схемы, использующей итеративную подстановку с секретом с использованием хэш-функции H. Затем, используя **Утверждение 1**, **Лемму 1** и **Лемму 2,** получаем сведение стойкости Π_v к стойкости HFEv^{-1} как односторонней функции с секретом, что и доказывает теорему.

4. Построение схемы с ленивой проверкой

Существуют способы модификации классической конструкции Лисянской при построении последовательных агрегированных подписей для достижения ленивой проверки. В настоящий момент известны схемы Невена [13], BGR [14] и Гентри [12]. Конструкция Гентри является обобщением и упрощением конструкций Невена и BGP. Конструкция Гентри представлена на рис. 6.

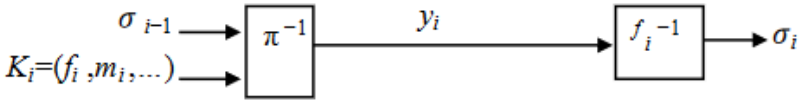

Рис. 6. Схема обобщенной последовательной агрегации Гентри
Fig. 6. Gentry's unified sequential aggregation scheme

Основная идея, лежащая в основе модификации, – применение идеального шифра π, моделируемого стойким алгоритмом блочного шифрования или сетью Фейстеля с использованием случайного оракула, моделируемого стойкой криптографической хэш-функцией. Данный шифр инициализируется ключом на основе односторонних подстановок с секретом $f_1, \dots, f_i$, инициализированных соответствующими открытыми ключами подписантов, и их подписываемыми сообщениями. Опираясь на указанную идею, можно показать стойкость схемы с ленивой проверкой в модели идеального шифра и случайного оракула.

Рассмотрим возможность модификации постквантовой схемы агрегированной электронной подписи MQSAS с целью достижения ленивой проверки с использованием обобщенной схемы агрегации Гентри.

При применении схемы Гентри необходимо использование модели, отличной от односторонней подстановки с секретом, а именно модели односторонней подстановки с секретом без сцеплений (claw-free trapdoor permutation). В то же время схема HFEv- является лишь односторонней функцией с секретом, и использование её в явном виде в схеме Гентри невозможно без адаптации доказательства стойкости.

Прежде чем приступить к описанию предлагаемой схемы и доказательству её стойкости, введём некоторые определения.

Определение 6 (Идеальный шифр [20]**).** Пусть $\pi: \{0,1\}^* \to \{0,1\}^{\geq k} \to \{0,1\}^{\geq k}$. $K \in \{0,1\}^*, \pi_K$ – подстановка на $\{0,1\}^{\geq k}$, π_K^{-1} – обратная ей подстановка. Тогда π – идеальный шифр, если $\forall\, K \in \{0,1\}^*, \forall n \geq k, \pi_K$ – случайная подстановка на $\{0,1\}^n$ и противник имеет доступ к оракулу π_K, $\pi_{K'}$ и $\pi_{K'}^{-1}$ при заданном противником K' на каждом запросе и неизвестном случайном K.

Определение 7 (Стойкая односторонняя подстановка с секретом без сцеплений [21]**).** Пусть F – функция, которая на входе 1^k для некоторого параметра k выдаёт тройку функций (f, g, f^{-1}), определяющих подстановки на некотором множестве $\{0,1\}^k$, где f, g – вычисление подстановки, f^{-1} – вычисление обратной подстановки к f. Пусть A – PPT алгоритм, преимущество в игре которого определяется величиной

$$Adv_F^{cf}(A) = \Pr[f(x) = g(x'): (f, g, f^{-1}) \leftarrow_R F, x \leftarrow_R A^{f,g}].$$

Тогда F – стойкая односторонняя подстановка с секретом, если для всех PPT алгоритмов противников величина Adv_{F}^{cf} – пренебрежимо малая.

Определение 8 (Итеративная расширяемая подстановка с использованием идеального шифра). Пусть $\Pi_v^{-1}: S \times X^* \to S \times X^{*+1}$ – расширяемое обратимое отображение и представимо в виде $\Pi_v^{-1}: (s, x_1, \dots, x_k) \mapsto (s', x_1, \dots, x_k, x')$, где $(s', x') = \Pi^{-1}(s)$ для некоторой основы $\Pi^{-1}: S \to S \times X$, $X^{*+1} \equiv X^*$. Подстановка ${\Pi^{-1}}_v^l(s, X)$ вычисляется с использованием идеального шифра π, как указанно в алгоритме на рис. 7.

Лемма 3 (Стойкость итеративной подстановки с использованием идеального шифра). Пусть ${\Pi^{-1}}_v^l(s, X)$ – итеративная подстановка с параметром повторения l на основе (t, ϵ) стойкой односторонней функции с секретом $\Pi^{-1}: S \to S \times X$ (t, ϵ) с использованием π – идеального шифра. Тогда Π_v – (t', ϵ'), стойкая односторонняя подстановка с секретом на S, где $t' = t/l$, $\epsilon' = \epsilon^{1/l}$.

$e: x \mapsto x$
$S_v^1 \leftarrow S$
for $i = 2$ **to** l **do**
  $(S_v^i, X) \leftarrow \Pi^{-1}\left(\pi^{-1}(S_v^{i-1})\right)$
  $X_v^i \leftarrow X || X_v^{i-1}$
end for
return (S_v^l, X_v^l)

Рис. 7. Алгоритм вычисления итеративной расширяемой подстановки с использованием идеального шифра на входах (S, X)
Fig. 7. Extendable iterative permutation algorithm based on ideal cipher on inputs (S, X)

Доказательство. Для доказательства стойкости конструкции воспользуемся утверждением об эквивалентности моделей идеального шифра и случайного оракула [20], иными словами, возможно заменить вычисление хэш-функции на вычисление идеального шифра. Далее заметим, что для любой инъективной функции $f: T \to T$ и случайного оракула $H: T \to T$ композиция $f \circ H$ является случайным оракулом $f \circ H: T \to T$, так как функция f есть лишь преобразование множества без коллизий. Таким образом, $\Pi^{-1} \circ \pi$ есть случайный оракул. Далее доказательство аналогично доказательству **Леммы 2**, с заменой вычисления $s \oplus H(a)$ на $\pi^{-1}(s)$, где $(s, X) = \Pi^{-1}(a)$.

В результате игры Противник B осуществляет l запросов к оракулу на каждый запрос к оракулу алгоритма A, $t = lt'$. Так как (Π, Π^{-1}) – односторонняя подстановка, вероятность того, что $q' = \Pi^{-1}(s_b')$ при случайном выборе $s_b{}'$ составляет ϵ. Вероятность того, что при фиксированном $a_{ai}, s_{ci} = \Pi^{-1}(\pi^{-1}(s_{bi}))$ составляет ϵ, так как вычисление Π^{-1} выполняется от случайной величины, полученной от случайного оракула π^{-1}, выход которого независим при каждом $i = l..1$, так как s_{bi} – различные результаты вычисления Π^{-1} на различных точках. Так как описанные выше события независимы, вероятность осуществления атаки алгоритмом A равно произведению данных вероятностей и $\epsilon = \epsilon'^l$. Итого имеем $t' = t/l$, $\epsilon' = \epsilon^{1/l}$.

5. Формальное определение схемы LMQSAS

Опишем построение схемы последовательной агрегированной подписи с ленивой проверкой на основе многомерных квадратичных многочленов. В качестве основы конструкции используется обобщённая схема Гентри с рандомизацией. В качестве односторонней функции используется HFEv-. Схема Гентри также требует использования идеального шифра, который может моделироваться стойким блочным шифром или 8-ми раундовой сетью Фейстеля в модели случайного оракула [22]. Вопрос реализации идеального шифра будет рассмотрен более подробно в следующем разделе.

Предлагаемая схема представлена на рис. 8, где $\sigma_i = (S'_i, X'_i)$, π^{-1} – вычисление расшифрования идеального шифра, (PK_i, SK_i) – ключевая пара i – го подписанта, $h_0 = \pi^{-1}_{PK_i||m_i||r_i}(S'_{i-1})$, $q = 1..l$, l – параметр повторения схемы Gui, вычисление отображения HFEv- производится аналогично описанному ранее для схемы MQSAS, пунктирными линиями обозначена однократная передача одного из значения в один из циклов.

Генерация параметров. Пусть K – конечное поле из g элементов, $n, D, a, v, l, \rho \in \mathbb{N}$ – параметры схемы, $U = \{u_1, \dots, u_k\}$ – множество пользователей, H – стойкая к коллизиям хэш-функция. Для каждого пользователя генерируется ключевая пара $(pk = (id, P)$, $sk = (S, F, T))$ в соответствии с алгоритмом *Генерации параметров* схемы MQSAS, как указано в разделе 4. Пусть $\pi: PK \times \{0,1\}^k \to \{0,1\}^k$ – идеальный шифр, где PK – множество открытых ключей.

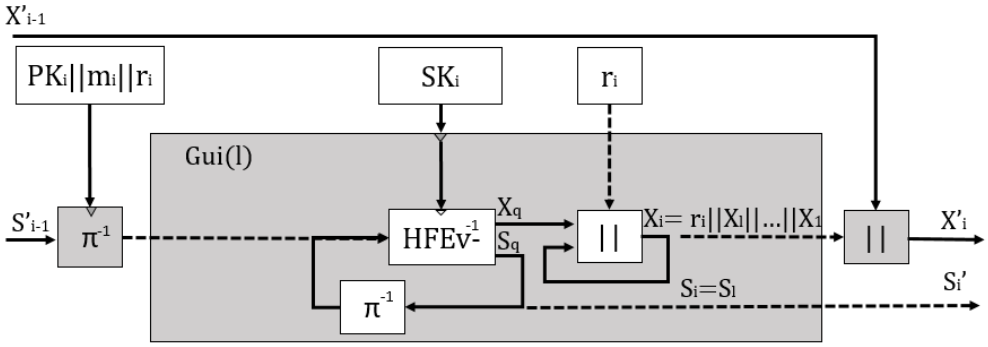

Рис. 8. Вычисление итерации схемы LMQSAS при формировании подписи
Fig. 8. Computation of LMQSAS signature iteration

Агрегированная подпись. Пусть $U = \{u_1, \dots, u_k\}$ – множество пользователей, m_i – сообщение, подписанное пользователем u_i, $pk = \{pk_1, \dots, pk_n\}$ – открытые ключи пользователей U, σ_{i-1} – предыдущее значение агрегированной подписи для сообщений $\{m_j \mid 1 \le j < i\}$. Для генерации подписи при $i = 1$ (случай $\sigma_0 = 0$) пользователь производит подпись на основе алгоритма подписи схемы Gui. Для $i \in \{1, .., k\}$ подпись разбивается на 2 блока: $\sigma_{i-1} = (S', X')$: $|S'| = n - a$ бит. Генерируется случайная равномерно распределённая величина $r_i \leftarrow \{0,1\}^\rho$. Вычисляется $K_i \leftarrow pk_i||m_i||r_i$, $y_i = \pi^{-1}_{K_i}(S')$. Затем пользователь использует свой секретный ключ sk_i для вычисления подписи согласно алгоритму подписи схемы Gui, для значения y_i: $(S, X) = \mathrm{Gui}_{sk}(y_i)$ с параметром повторения l, где в качестве хэш-функции $H(x)$ используется $\pi^{-1}(\mathrm{HFEv}(x))$. Затем он объединяет полученную подпись с агрегированной подписью σ_{i-1} для получения новой агрегированной подписи σ_i: $S^* = S$, $X^* = (r_i||X, X')$, $\sigma = (S^*, X^*)$. Алгоритм формирования агрегированной подписи представлен на рис. 9 (а).

Агрегированная проверка. Пусть $U = \{u_1, \dots, u_i\}$ – множество пользователей, m_i – сообщение, подписанное пользователем u_i, $pk = \{pk_1, \dots, pk_i\}$ – открытые ключи пользователей U, σ_i – агрегированная подпись сообщений $\{m_j \mid 1 \le j < i\}$. Подпись σ представляется в виде $\sigma = (S', r_i, X_{il}, \dots, X_{(i-1)l+1}, r_{i-1}, X_{(i-1)l}, \dots, X_1)$: $|S'| = n - a$ бит, $|X_j| = a + v$ бит, $j \in \{1, .., il\}$, $|r_i| = \rho$ бит. Дальнейший алгоритм вычисления представлен на рис. 9 (b).

```
if i = 1 then
  S' = 0^{n-a}
  X' ← ∅
else (S', X') ← split(σ_{i-1})
end if
r_i ←_R {0,1}^ρ
h = π^{-1}_{PK_i||m_i||r_i}(S')
for j = 1 to l do
  D_j ← first n − a bits of h
  (S_j, X_j) ← HFEv_{sk_j}^{-1}(D_j)
  h ← π^{-1}_{PK_i||m_i||r_i}(S_j)
end for
S' ← S_l
X' ← (r_i||X_l|| ... ||X_1||X')
σ_i ← (S', X')
return σ_i
```

(a)

```
for j = l to 1 do
  h ← S'
  for k = l − 1 to 2 do
    S'_k ← HFEv_{pk_j} − (h, X_{(j-1)l+l+1})
    h ← π_{K_i||m_i||r_i}(S'_k)
  end for
  S' = π_{K_i||m_i||r_i}(h)
end for
if S' = 0 then
  return TRUE
else
  return FALSE
end if
```

(b)

Рис. 9. Алгоритм формирования (a) и проверки (b) агрегированной электронной подписи схемы LMQSAS

Fig. 9. LMQSAS signature (a) and verification (b) algorithms

6. Теоретическая стойкость LMQSAS

Лемма 4 (Стойкость расширяемой односторонней подстановки с секретом без сцеплений). Пусть $\Pi: S \to S \times X$ (t, ϵ) – стойкая односторонняя функция с секретом без сцеплений, являющаяся основой для расширяемого биективного отображения $\Pi_v: S \times X^* \to S \times X^{*+1}$. Тогда Π_v – (t, ϵ), стойкая односторонняя подстановка с секретом без сцеплений на $S \times X^*$.

Доказательство. Доказательство аналогично доказательству **Леммы 1**, с заменой односторонней функции/подстановки с секретом на одностороннюю функцию/подстановку без сцеплений.

Теорема 2 (Стойкость схемы LMQSAS). Предполагая (t, ϵ') стойкость односторонней функции HFEv- при её использовании в итеративной конструкции с использованием идеального шифра с параметром l как стойкой односторонней функции, последовательная агрегированная подпись LMQSAS является $(t, q_H, q_\pi, n, k, \epsilon)$ стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи, причём для всех $t \epsilon k$, где $k = (n - a)$ – размер агрегируемой части агрегированной подписи, $n, D, a, v, l, \rho \in \mathbb{N}$ – параметры схемы:

$$\epsilon(k) \le \frac{q_H 2^{k+r}}{(2^k - q_\pi^2)(2^\rho - q_H^2)} (\epsilon'(k))^{1/l} + q_\pi^2 / 2^k,$$

$$t(k) = t'(k)/l.$$

Идея доказательства. Основная идея для доказательства схемы – использование **Леммы 1**, **Леммы 3** и **Леммы 4** для построения стойкой односторонней подстановки с

секретом на основе односторонней функции с секретом. После чего описанная односторонняя подстановка используется в качестве основы схемы Гентри, аналогично доказанному в теореме 4.3 из [12]. Однако указанная терема доказана в исходной статье авторами для подстановки $(f, f^{-1}): f: \{0,1\}^k \to \{0,1\}^k$ для некоторой фиксированной величины k, имеем функцию $(f, f^{-1}): f^{-1}: \{0,1\}^k \to \{0,1\}^m$, $m > k$, которая является подстановкой на $\{0,1\}^k$, что требует адаптации теоремы. К тому же исходное доказательство строится на модели стойкой односторонней подстановки с секретом без сцеплений, в то время как имеем лишь стойкую одностороннюю подстановку с секретом. При этом используемая подстановка не является гомоморфной или случайно самосводимой (random self-reducible [23]), что иначе позволило бы использовать её для построения функции без сцеплений [24]. Однако возможно применение техники, описанной в [14], позволяющей перейти в доказательстве от односторонних подстановок без сцеплений к стандартным подстановкам, теряя при этом в стойкости лишь кратную величину, равную числу запросов к оракулу подписи.

Прежде чем приступить к доказательству теоремы, докажем вспомогательную Лемму сходимости до 0.

Пусть A — противник в модели идеального шифра π, длина входа и выхода которого задаётся некоторой величиной $k \in \mathbb{N}$, ключ идеального шифра также описывает некоторую функцию $f: \{0,1\}^k \to \{0,1\}^m$, независимую от функции $\pi: f \times \{0,1\}^k \to \{0,1\}^m$. A может оправлять запросы к оракулу π идеального шифра в формате f, y для получения случайной величины $x \in \{0,1\}^m$ и запросы к оракулу π^{-1} в формате f, x для получения $y \in \{0,1\}^k$. Для простоты доказательства примем, что противник не передаёт оракулу дважды одни и те же значения и не запрашивает избыточные значения, которые он уже знает, т.е. не запрашивает $\pi^{-1}[f, x]$, если ранее был запрошен $x = \pi[f, y]$ для одного или нескольких запросов.

Определение 9 (Связность записей [12]**)**. Запись $x_1 = \pi(f_2, y_2)$ называется связанной с записью $x_0 = \pi(f_1, y_1)$, если $f_1(x_1) = y_1$. Альтернативная запись определения: запись $y_2 = \pi^{-1}(f_2, x_1)$ называется связанной с записью $y_1 = \pi^{-1}(f_1, x_0)$, если $x_1 = f^{-1}(y_1)$.

Определение 10 (Цепь [12]**)**. Записи $x_0, \ldots, x_{q-1}$ образуют цепь, если x_i и x_{i+1} связаны для $i = 0, \ldots, q-2$, q называется длиной цепи.

Определение 11 (Цепь к нулю [12]**)**. Цепью к нулю называется запись $x = \pi[f, y]$, если $x = 0^k$, или запись x_q, связанная цепью $x_0, \ldots, x_q$, в которой $x_0 = 0^k$ (т.е. запись связана по цепочке с нулём).

Утверждение 2. Пусть $(f, f^{-1}): f^{-1}: \{0,1\}^k \to \{0,1\}^m$. При случайном выборе $y_1, \ldots, y_q \in \{0,1\}^m$ $Y_{\max}$ — случайная величина, равная размеру прообраза $f^{-1}(y_i)$ по всем $i = 1, .., q$. Тогда $\mathbf{E}[Y_{\max}] = q$

$$E[Y_{\max}] = \sum_{x=0}^{\infty} \Pr[Y_{\max} > x] \le \sum_{x=0}^{\infty} \sum_{i=1}^{q} \Pr[Y_i > x] = \sum_{i=1}^{q} \mathbf{E}[Y_{\mathrm{i}}] = \sum_{i=1}^{q} 1 = q.$$

Определение 12 (Прямой и обратный запрос [12]**)**. Запись $x = \pi[f, y]$ назовём прямым запросом, если она была получена путём обращения к оракулу π, запись $x = \pi[f, y]$ назовём обратным запросом, если она получена путём обращения к оракулу π^{-1}.

Определение 13 (Коллизия цепи [12]**)**. Пусть Coll_1 — событие, при котором прямой запрос $x_i = \pi[f_{i+1}, y_{i+1}]$ связан с некоторым обратным запросом $x_{i-1} = \pi[f_i, y_i]$, Coll_2 —событие, при котором обратный запрос $x_{i-1} = \pi[f_i, y_i]$ связан с некоторым прямым или обратным запросом $x_i = \pi[f_{i+1}, y_{i+1}]$. Пусть $\mathrm{Coll} = \mathrm{Coll}_1 \vee \mathrm{Coll}_2$.

Утверждение 3. При запросе противником A не более q запросов $\Pr[\mathrm{Coll}] < q^2/2^k$.

Доказательство. Пусть после i обратных запросов P_i есть максимальный размер прообраза $f^{-1}(y)$ по всем запросам. Тогда, используя **Утверждение 2,** имеем для прямого запроса $x = \pi[f, y]$:

$$\Pr[x = \pi[f, y] \text{ образует коллизию}] \leq \sum_{j=1}^{\infty} j \Pr[P_i = j]\, 2^{-k} = \mathbf{E}[P_i] 2^{-k} \leq i 2^{-k}.$$

Для обратного запроса $x_{i-1} = \pi[f_i, y_i]$ случайные величины y_i независимы, так как для произвольной записи $x_i = \pi[f_{i+1}, y_{i+1}]$ $f_i(x_i)$ уже задано, до выбора величины y_i. Следовательно, вероятность совпадения $f_i(x_i) = y_i$ есть вероятность совпадения со случайной величиной, и $\Pr[f_i(x_i) = y_i] = 2^{-m} < 2^{-k}$. $\Pr[\mathrm{Coll}] = \Pr[\mathrm{Coll}_1 \vee \mathrm{Coll}_2] \leq q^2/2^k$.

Лемма 5 (Сходимость до нуля при использовании односторонней функции с секретом). Пусть BAD_π — событие, при котором прямой запрос образует цепь к нулю. Тогда для противника A, делающего не более q запросов, $\Pr[\mathrm{BAD}_\pi] \leq q^2/2^k$.

Доказательство. Доказательство аналогично лемме сходимости к нулю из статьи Гентри [12] с использованием доказанных выше утверждений и односторонней функции вместо подстановки.

Теорема 3 (Стойкость ленивой вероятностной схемы Гентри) [12]. Предполагая (t, ϵ') стойкость односторонней подстановки без сцеплений $(f, f^{-1}, g) \leftarrow F(1^k)$ для некоторого параметра k, $\rho = \rho(k)$ как стойкой функции без сцеплений, последовательная агрегированная вероятностная схема Гентри является $(t, q_H, q_\pi, n, k, \epsilon)$ стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи, причём для всех t, ϵ, k:

$$\epsilon(k) \leq \frac{q_H 2^{k+\rho}}{(2^k - q_\pi^2)(2^\rho - q_H^2)} (\epsilon'(k))^{1/l} + q_\pi^2/2^k,$$
$$t(k) = t'(k).$$

Доказательство ***Теоремы 2***. Формальная стойкость полученной схемы может быть показана с использованием теоремы, аналогичной теореме 4.2 из [12], с предположением о стойкости HFEv- как односторонней подстановки с секретом без сцеплений.

Алгоритм B с преимуществом $\epsilon_{cw}{}'$ нахождения сцеплений из **Теоремы 3.3** выше может быть адаптирован (алгоритм B_{ow} с преимуществом ϵ'_{ow}) для построения атаки на одностороннюю подстановку [14]. Заменяя одностороннюю подстановку без сцеплений с секретом (f, f^{-1}, g) на одностороннюю функцию (f, f^{-1}), необходимо симулировать ответы от оракула g в ответе на запросы к случайному оракулу H, не имея доступа к оракулу g. Вместо вычисления y_i с использованием g противник выбирает y_i случайно равновероятно, кроме одного случайного запроса, в котором он выбирает $y_{i=k} = y$. Когда противник получает сцепление (x_j^*, x'_j), $f(x_j^*) = y_i$, тогда с вероятностью $1/q_H$ $y_i = y_k$ (т.е. противник найдёт сцепление именно на той итерации, на которой использовалось значение $y_{i=k} = y$, тем самым найдя прообраз x_j^* для f от y). Так как обработка запросов к оракулу H – единственное место в рамках протокола, в котором используется оракул к g, преимущество противника уменьшается в q_H раз по сравнению с исходным алгоритмом:

$$\epsilon'_{ow} = \epsilon'_{cw}/q_H.$$

Отсюда имеем для односторонней подстановки с секретом:

$$\epsilon_{cw}^{\prime(k)} \geq \frac{(2^k - q_\pi^2)(2^t - q_H^2)}{2^{k+r}} \left(\epsilon^{(k)} - \frac{q_\pi^2}{2^k}\right),$$

$$\epsilon_{ow}'^{(k)} \geq \frac{1}{q_H}\frac{(2^k - q_\pi^2)(2^\rho - q_H^2)}{2^{k+\rho}}\left(\epsilon^{(k)} - \frac{q_\pi^2}{2^k}\right),$$

$$\epsilon(k) \leq \frac{2^{k+\rho}q_H}{(2^k - q_\pi^2)(2^\rho - q_H^2)}\,\epsilon_{ow}'(k) + q_\pi^2/2^k.$$

Далее с помощью **Леммы 1** и **Леммы 3** заменяем одностороннюю подстановку с секретом на расширяемую одностороннюю подстановку Gui с секретом с параметром повторения l на основе односторонней функции с секретом HFEv-. Имеем $\epsilon_{ow}' = (\epsilon'(k))^{1/l}$, отсюда:

$$\epsilon(k) \leq \frac{q_H 2^{k+\rho}}{(2^k - q_\pi^2)(2^\rho - q_H^2)}\,(\epsilon'(k))^{1/l} + q_\pi^2/2^k,$$

$$t(k) = t'(k)/l.$$

7. Реализация идеального шифра

Как упоминалось ранее, предлагаемая схема требует наличия идеального шифра, который обычно реализуется с использованием стойкого блочного шифра. Размер блока блочного шифра должен соответствовать размеру агрегируемой части подписи, размер ключа – размеру сообщения, открытого ключа и используемой случайной величины. Принимая во внимание размер открытого ключа схемы Gui, составляющий порядка десятка килобайт, и размер агрегируемой части подписи – около 100 бит, получаем невозможность использования стандартных блочных шифров в качестве идеального шифра. Таким образом, нужно решить две задачи – получить идеальный шифр, который имеет размер блока, соответствующий размеру агрегируемой части последовательной подписи, а также имеет произвольно большой размер ключа.

Для достижения первой цели воспользуемся методом, имеющим название FNR [17]. Основная идея подхода – использование сети Фейстеля N_{AES} на основе блочного шифра AES. До и после передачи данных в сеть Фейстеля используется отображение g_{AB}, переводящее вход длины k в случайный выход длины k (т.е. g_{AB} – псевдослучайная подстановка при случайном выборе параметром A, B).

В результате схема имеет ключ, равный $k * k + k + \mathrm{AES}_K$, где AES_K – размер ключа AES. Пусть $r \geq 7$ – число раундов в сети Фейстеля, k – размер входа FNR, m – число обращений противника к шифру. Тогда стойкость FNR определяется величиной преимущества противника:

$$\frac{r}{2} * \frac{m^2}{2^{\left(1-\frac{1}{r}\right)*k}}.$$

Для достижения второй цели можно применить 8-раундовую сеть Фейстеля в модели случайного оракула [22], что позволит использовать произвольный размер ключей.

Комбинируя оба подхода (используя 8-раундовую сеть Фейстеля вместо AES в схеме FNR), получаем блочный шифр на основе хэш-функции в модели случайного оракула. Для использования произвольного ключа длины p его необходимо разбить на две части: $k_{\mathrm{FNR}} = k * k + k$ бит и $p - k_{\mathrm{FNR}}$ бит. Затем следует использовать первую часть ключа в FNR, а вторую часть ключа — в сети Фейстеля. Для вычисления одного зашифрования шифра требуется 64 вычисления случайного оракула.

8. Параметры схемы LMQSAS

Для схемы с параметрами n, D, a, v, l, ρ размер агрегируемой части составляет $(n-a)$ бит, размер неагрегируемой части – $i(l(a+v)+\rho)$. Для i пользователей коэффициент сжатия подписи:

$$r = 1 - \frac{|\sigma_{ag}|}{i|\sigma|} = 1 - \frac{(n-a)+i(l(a+v)+\rho)}{i\big((n-a)+l(a+v)+\rho\big)}.$$

Размер блока идеального шифра составляет $k = n - a$ бит. Параметр ρ определяет размер в битах случайной строки, которая используется при каждой итерации агрегированной подписи и добавляется в конец подписи. Данный параметр влияет на стойкость, внося множитель перед преимуществом противника в игре против односторонней подстановки:

$$a(p) = \frac{2^{\rho} q_H}{(2^{\rho} - q_H^2)}.$$

Очевидно, что размер параметра ρ при фиксированном параметре стойкости определяет максимальное количество обращений к оракулу H и, как следствие, максимальное количество агрегированных подписей. Заметим, что при $q_H \le 2^{\rho/3}$ полученный множитель равен:

$$a(\rho) \le 2^{p/3} \frac{2^{\rho}}{(2^{\rho} - 2^{2\rho/3})} \le \frac{2^{4\rho/3}}{2^{2p/3}(2^{\rho/3}-1)} \le 2^{\rho/3}\,.$$

Параметр $k = n - a$ также вносит множитель, равный:

$$b(k) = \frac{2^k}{(2^k - q_\pi^2)}.$$

При $q_\pi \le 2^{k/3}$ множитель можно ограничить сверху следующим образом:

$$b(k) = \frac{2^k}{(2^k - 2^{2k/3})} \le \frac{2^{3k/3}}{2^{2k/3}(2^{k/3}-1)} \le \frac{2^{k/3}}{(2^{k/3}-1)} \approx 1.$$

Таким образом, при подписи не более $q = 2^{\rho/3}$ сообщений множитель $a(p)b(k)$ влияет на стойкость, увеличивая слагаемое в преимуществе противника не более чем в q раз. Так, для $q \le 2^{\rho/3}$ имеем преимущество противника, равное:

$$\epsilon(k) \le q\,(\epsilon'(k))^{1/l} + q^2/2^k.$$

При использовании схемы Gui в качестве итеративной расширяемой подстановки с секретом на основе схемы HFEv- с параметром повторения l, выбирая должным образом параметр l, получаем стойкость полученной схемы порядка k бит. Таким образом, $(\epsilon'(k))^{\frac{1}{l}} \le 2^k$. В результате основной вклад в преимущество противника вносит слагаемое $q^2/2^k$, которое для $\rho < k$ не вызывает дополнительных ограничений на число подписываемых сообщений при $q < 2^{k/3}$. Выбор параметра ρ полностью определяется количеством подписываемых сообщений. Предлагаемые параметры для схемы LMQSAS представлены в табл. 1, где n, D, a, v, l, ρ – параметры, введённые ранее, g – определяет используемое поле $K = GF(g)$.

Производительность схемы сравнима с производительностью схемы MQSAS, т.к. для вычисления используется лишь дополнительное вычисление 64 значений случайного оракула, реализуемого произвольной стойкой хэш-функцией, в сети Фейстеля.

Параметр сжатия схемы для 3–6 подписантов составляет 40–50%, в зависимости от параметров схемы. Данное число подписантов представляет наибольший практический

интерес, так как длина цепочки сертификатов в инфраструктуре открытых ключей редко превосходит 4, длина пути в протоколах защищенной маршрутизации не превосходит 6 [5].

Таблица 1. Предлагаемые параметры схемы LMQSAS

Параметры поля и схемы, g, n, D, a, v, l, ρ	**Параметр стойкости, бит**	**Размер открытого ключа**	**Размер единичной подписи**	**Рост размера подписи на одну итерацию**
2,96,5,6,6,2,40	80	55,7 Кб	154 бита	64 бита
2,95,9,5,5,2,40	80	55,5 Кб	150 бит	60 бит
2,94,17,4,4,2,40	80	53,3 Кб	146 бит	56 бит
2,96,65,2,2,2,40	80	55,7 Кб	142 бита	48 бит
7,62,8,2,2,1,40	80	47,1 Кб	104 бита	44 бита
2,127,9,4,6,2,60	120	133,8 Кб	203 бита	80 бит
7,93,8,3,3,1,60	120	156,7 Кб	156 бит	66 бит

Заключение

В данной статье рассмотрен метод построения постквантовых последовательных схем подписи с ленивой проверкой на основе обобщенной конструкции Гентри. Метод использует расширяемые односторонние подстановки с секретом на основе односторонних функций с секретом. Рассмотрены вопросы формального доказательства стойкости существующей схемы постквантовой агрегированной подписи MQSAS.

Разработана схема постквантовой последовательной агрегированной подписи с ленивой проверкой LMQSAS. Благодаря ленивой проверке предложенная схема расширяет возможные области применения схем постквантовых последовательных агрегированных подписей в ряде приложений, включая протоколы защищенной маршрутизации. В качестве основы схема LMQSAS использует HFEv- (в роли односторонней функции с секретом) и сеть Фейстеля в схеме FNR (в качестве идеального шифра). Для предложенной схемы приведены формальные доказательства стойкости в сведении к стойкости используемых примитивов. Размеры индивидуальной подписи для рассмотренных параметров стойкости в 80 и 120 бит составляют 104–203 бит, рост подписи при агрегации составляет 44–80 бит на итерацию, параметр сжатия схемы для 3–6 подписантов составляет ~50 процентов.

СПИСОК ЛИТЕРАТУРЫ:

1. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 1997, vol. 26, no. 5, p. 1484–1509. DOI: https://doi.org/10.1137/S0097539795293172.
2. Patarin J. (1996). Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U. (eds) Advances in Cryptology – EUROCRYPT ’96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-68339-9_4.
3. Petzoldt A., Chen MS., Yang BY., Tao C., Ding J. (2015). Design Principles for HFEv- Based Multivariate Signature Schemes. In: Iwata, T., Cheon, J. (eds) Advances in Cryptology – ASIACRYPT 2015. ASIACRYPT 2015. Lecture Notes in Computer Science, vol 9452. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-48797-6_14.
4. Given N. Gui: Revisiting Multivariate Digital Signature Schemes based on HFEv-. International Conference on the Theory and Application of Cryptology and Information Security, 2014. URL: https://csrc.nist.gov/groups/ST/post-quantum-2015/papers/session1-ding-paper.pdf (дата обращения: 20.05.2023).

5. Makarov A. (2020). A Survey of Aggregate Signature Applications. In: Misyurin, S., Arakelian, V., Avetisyan, A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol. 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_37. – EDN JWCIQD.
6. Makarov A. and Varfolomeev A.A. Extended Classification of Signature-only Signature Models. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia, 2021, p. 2385–2389. DOI: 10.1109/ElConRus51938.2021.9396682. – EDN ESOXBS.
7. Torres W.A.A., Steinfeld R., Sakzad A., Kuchta V. Post-Quantum Linkable Ring Signature Enabling Distributed Authorised Ring Confidential Transactions in Blockchain. IACR Cryptol. ePrint Arch., 2020. URL: https://eprint.iacr.org/2020/1121.pdf (дата обращения: 20.05.2023).
8. Молдовян А.А., Галанов А.И., Синев В.Е. Утверждаемая групповая подпись: новые протоколы. Вопросы Защиты Информации. Утверждаемая групповая подпись. 2016, № 2(113), с. 44–50. – EDN UCBMFU.
9. Fukumitsu, M., Hasegawa, S. (2020). A Lattice-Based Provably Secure Multisignature Scheme in Quantum Random Oracle Model. In: Nguyen, K., Wu, W., Lam, K.Y., Wang, H. (eds) Provable and Practical Security. ProvSec 2020. Lecture Notes in Computer Science, vol 12505. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-62576-4_3.
10. Синев В.Е. Повышение уровня безопасности протокола групповой цифровой подписи, основанного на механизме маскирования открытых ключей. Известия СПбГЭТУ «ЛЭТИ». 2016, № 6, с. 21–25. – EDN WBOQXX.
11. Lysyanskaya A., Micali S., Reyzin L., Shacham H. (2004). Sequential Aggregate Signatures from Trapdoor Permutations. In: Cachin, C., Camenisch, J.L. (eds) Advances in Cryptology – EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-24676-3_5.
12. Gentry C., O'Neill A., Reyzin L. (2018). A Unified Framework for Trapdoor-Permutation-Based Sequential Aggregate Signatures. In: Abdalla, M., Dahab, R. (eds) Public-Key Cryptography – PKC 2018. PKC 2018. Lecture Notes in Computer Science, vol 10770. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-76581-5_2.
13. Neven G. Efficient Sequential Aggregate Signed Data. IEEE Transactions on Information Theory. 2011, vol. 57, no. 3, p. 1803–1815. DOI: https://doi.org/10.1109/TIT.2010.2091434.
14. Brogle K., Goldberg S., Reyzin L. Sequential aggregate signatures with lazy verification from trapdoor permutations. Information and Computation. 2014, vol. 239, p. 356-376. DOI: https://doi.org/10.1016/j.ic.2014.07.001.
15. El Bansarkhani, R., Mohamed, M.S.E., Petzoldt, A. (2016). MQSAS - A Multivariate Sequential Aggregate Signature Scheme. In: Bishop, M., Nascimento, A. (eds) Information Security. ISC 2016. Lecture Notes in Computer Science, vol 9866. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-45871-7_25.
16. Макаров А. Схема пост-квантовой агрегированной подписи на основе теории алгебраического кодирования. Вопросы кибербезопасности. 2019, № 2(30), с. 69–76. DOI: https://doi.org/10.21681/2311-3456-2019-2-69-76. – EDN TNKFZL.
17. Dara, S., Fluhrer, S. (2014). FNR: Arbitrary Length Small Domain Block Cipher Proposal. In: Chakraborty, R.S., Matyas, V., Schaumont, P. (eds) Security, Privacy, and Applied Cryptography Engineering. SPACE 2014. Lecture Notes in Computer Science, vol 8804. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-12060-7_10.
18. Rogaway, P. (2004). On the Role Definitions in and Beyond Cryptography. In: Maher, M.J. (eds) Advances in Computer Science – ASIAN 2004. Higher-Level Decision Making. ASIAN 2004. Lecture Notes in Computer Science, vol 3321. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-30502-6_2.
19. Bellare M., Rogaway P. The Game-Playing Technique. URL: https://cr.yp.to/bib/2004/bellare-games.pdf (дата обращения: 20.05.2023).
20. Coron, J.S., Patarin, J., Seurin, Y. (2008). The Random Oracle Model and the Ideal Cipher Model Are Equivalent. In: Wagner, D. (eds) Advances in Cryptology – CRYPTO 2008. CRYPTO 2008. Lecture Notes in Computer Science, vol 5157. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-85174-5_1.
21. Goldwasser S., Micali S., Rivest R.L. A "Paradoxical" Solution To The Signature Problem. 25th Annual Symposium on Foundations of Computer Science, 1984., Singer Island, FL, USA, 1984, p. 441–448. DOI: http://dx.doi.org/10.1109/SFCS.1984.715946.
22. Dai, Y., Steinberger, J. (2016). Indifferentiability of 8-Round Feistel Networks. In: Robshaw, M., Katz, J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9814. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-53018-4_4.

23. Feigenbaum J. and. Fortnow L. On the random-self-reducibility of complete sets. Proceedings of the Sixth Annual Structure in Complexity Theory Conference, Chicago, IL, USA, 1991, p. 124–132. DOI: https://doi.org/10.1109/SCT.1991.160252.
24. Dodis, Y., Reyzin, L. (2003). On the Power of Claw-Free Permutations. In: Cimato, S., Persiano, G., Galdi, C. (eds) Security in Communication Networks. SCN 2002. Lecture Notes in Computer Science, vol. 2576. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-36413-7_5.

REFERENCES:

[1] Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 1997, vol. 26, no. 5, p. 1484–1509. DOI: https://doi.org/10.1137/S0097539795293172.
[2] Patarin J. (1996). Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U. (eds) Advances in Cryptology – EUROCRYPT ’96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-68339-9_4.
[3] Petzoldt A., Chen MS., Yang BY., Tao C., Ding J. (2015). Design Principles for HFEv- Based Multivariate Signature Schemes. In: Iwata, T., Cheon, J. (eds) Advances in Cryptology – ASIACRYPT 2015. ASIACRYPT 2015. Lecture Notes in Computer Science, vol 9452. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-48797-6_14.
[4] Given N. Gui: Revisiting Multivariate Digital Signature Schemes based on HFEv-. International Conference on the Theory and Application of Cryptology and Information Security, 2014. URL: https://csrc.nist.gov/groups/ST/post-quantum-2015/papers/session1-ding-paper.pdf (accessed: 20.05.2023).
[5] Makarov A. (2020). A Survey of Aggregate Signature Applications. In: Misyurin, S., Arakelian, V., Avetisyan, A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol. 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_37. – EDN JWCIQD.
[6] Makarov A. and Varfolomeev A.A. Extended Classification of Signature-only Signature Models. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia, 2021, p. 2385–2389. DOI: 10.1109/ElConRus51938.2021.9396682. – EDN ESOXBS.
[7] Torres W.A.A., Steinfeld R., Sakzad A., Kuchta V. Post-Quantum Linkable Ring Signature Enabling Distributed Authorised Ring Confidential Transactions in Blockchain. IACR Cryptol. ePrint Arch., 2020. URL: https://eprint.iacr.org/2020/1121.pdf (accessed: 20.05.2023).
[8] Moldovyan A.A., Galanov A. I., Sinev V.E. Group digital signature: new protocols. Voprosy Zashchity Informacii, 2016, no. 2(113), p. 44–50 (in Russian). – EDN UCBMFU.
[9] Fukumitsu, M., Hasegawa, S. (2020). A Lattice-Based Provably Secure Multisignature Scheme in Quantum Random Oracle Model. In: Nguyen, K., Wu, W., Lam, K.Y., Wang, H. (eds) Provable and Practical Security. ProvSec 2020. Lecture Notes in Computer Science, vol 12505. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-62576-4_3.
[10] Sinev V.E. Increasing the level of security of the protocol group digital signature based on the masking mechanism of public keys. Izvestiya SPbGETU “LETI”. 2016, № 6, s. 21–25 (in Russian). – EDN WBOQXX.
[11] Lysyanskaya A., Micali S., Reyzin L., Shacham H. (2004). Sequential Aggregate Signatures from Trapdoor Permutations. In: Cachin, C., Camenisch, J.L. (eds) Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-24676-3_5.
[12] Gentry C., O’Neill, A. Reyzin, L. (2018). A Unified Framework for Trapdoor-Permutation-Based Sequential Aggregate Signatures. In: Abdalla, M., Dahab, R. (eds) Public-Key Cryptography – PKC 2018. PKC 2018. Lecture Notes in Computer Science, vol 10770. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-76581-5_2.
[13] Neven G. Efficient Sequential Aggregate Signed Data. IEEE Transactions on Information Theory, 2011, vol. 57, no. 3, p. 1803–1815. DOI: https://doi.org/10.1109/TIT.2010.2091434.
[14] Brogle K., Goldberg S., Reyzin L. Sequential aggregate signatures with lazy verification from trapdoor permutations. Information and Computation. 2014, vol. 239, p. 356–376. DOI: https://doi.org/10.1016/j.ic.2014.07.001.
[15] El Bansarkhani, R., Mohamed, M.S.E., Petzoldt, A. (2016). MQSAS - A Multivariate Sequential Aggregate Signature Scheme. In: Bishop, M., Nascimento, A. (eds) Information Security. ISC 2016. Lecture Notes in Computer Science, vol 9866. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-45871-7_25.

[16] Makarov A. Apcfs - post-quantum code based aggregate signature scheme. Voprosy kiberbezopasnosti. 2019, no. 2(30), p. 69–76. DOI: https://doi.org/10.21681/2311-3456-2019-2-69-76 (in Russian). – EDN TNKFZL.
[17] Dara, S., Fluhrer, S. (2014). FNR: Arbitrary Length Small Domain Block Cipher Proposal. In: Chakraborty, R.S., Matyas, V., Schaumont, P. (eds) Security, Privacy, and Applied Cryptography Engineering. SPACE 2014. Lecture Notes in Computer Science, vol 8804. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-12060-7_10.
[18] Rogaway, P. (2004). On the Role Definitions in and Beyond Cryptography. In: Maher, M.J. (eds) Advances in Computer Science - ASIAN 2004. Higher-Level Decision Making. ASIAN 2004. Lecture Notes in Computer Science, vol 3321. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-30502-6_2.
[19] Bellare M., Rogaway P. The Game-Playing Technique. URL: https://cr.yp.to/bib/2004/bellare-games.pdf (accessed: 20.05.2023).
[20] Coron, J.S., Patarin, J., Seurin, Y. (2008). The Random Oracle Model and the Ideal Cipher Model Are Equivalent. In: Wagner, D. (eds) Advances in Cryptology – CRYPTO 2008. CRYPTO 2008. Lecture Notes in Computer Science, vol 5157. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-85174-5_1.
[21] Goldwasser S., Micali S., Rivest R.L. A "Paradoxical" Solution To The Signature Problem. 25th Annual Symposium onFoundations of Computer Science, 1984., Singer Island, FL, USA, 1984, p. 441–448. DOI: http://dx.doi.org/10.1109/SFCS.1984.715946.
[22] Dai, Y., Steinberger, J. (2016). Indifferentiability of 8-Round Feistel Networks. In: Robshaw, M., Katz, J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9814. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-53018-4_4.
[23] Feigenbaum J. and. Fortnow L. On the random-self-reducibility of complete sets. Proceedings of the Sixth Annual Structure in Complexity Theory Conference, Chicago, IL, USA, 1991, p. 124–132. DOI: https://doi.org/10.1109/SCT.1991.160252.
[24] Dodis, Y., Reyzin, L. (2003). On the Power of Claw-Free Permutations. In: Cimato, S., Persiano, G., Galdi, C. (eds) Security in Communication Networks. SCN 2002. Lecture Notes in Computer Science, vol. 2576. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-36413-7_5.

Поступила в редакцию – 22 мая 2023 г. Окончательный вариант – 22 августа 2023 г.
Received – May 22, 2023. The final version – August 22, 2023.