УДК 004.9
МРНТИ 81.96.00

https://doi.org/10.55452/1998-6688-2026-23-1-68-81

[1]Сейткулов Е.Н.,
к. ф.-м. н., научный сотрудник,
ORCID ID: 0000-0002-5172-8339,
e-mail: yerzhan.seitkulov@gmail.com
[1*]Оспанов Р.М.,
магистр, научный сотрудник,
ORCID ID: 0000-0002-0771-575X,
*e-mail: ospanovrm@gmail.com
[1]Ергалиева Б.Б.,
научный сотрудник,
ORCID ID: 0000-0002-1252-857X,
e-mail: banu.yergaliyeva@gmail.com
[2]Утебаев К.А.,
магистрант, научный сотрудник,
ORCID ID: 0009-0004-3032-5049,
e-mail: utebayevkuat@gmail.com
[1]Атанов С.К.,
д.т.н., профессор,
ORCID ID: 0000-0003-2115-7130,
e-mail: atanov_sk@enu.kz

[1]Евразийский национальный университет им. Л.Н.Гумилева,
г. Астана, Казахстан
[2]Алматинский филиал Национального исследовательского
ядерного университета «МИФИ», г. Алматы, Казахстан

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ ВЕРИФИЦИРУЕМО ЗАШИФРОВАННОЙ ПОДПИСИ С ВОЗМОЖНОСТЬЮ ПРОВЕРКИ ЧЕРЕЗ ЗАДАННОЕ ВРЕМЯ

Аннотация

Одним из современных направлений в области защиты информации является постквантовая криптография. Ее целью является разработка новых квантово-устойчивых криптографических алгоритмов. Важный раздел постквантовой криптографии составляют алгоритмы электронной цифровой подписи. Существует ряд различных подходов к проектированию постквантовых подписей. Одним из основных подходов к проектированию постквантовых криптографических алгоритмов цифровой подписи являются схемы постквантовой цифровой подписи, основанные на хешировании. Схемы постквантовой цифровой подписи, основанные на хешировании, являются одним из основных типов постквантовых криптографических алгоритмов цифровой подписи. Они достаточно эффективны и доказуемо безопасны. Установлена их надежная безопасность как против классических, так и против квантовых атак. Для решения различных задач информационной безопасности существует множество видов цифровых подписей, например, групповые подписи, кольцевые подписи, слепые подписи, верифицируемо зашифрованные подписи и т.д. В данной работе предлагается новый криптографический протокол верифицируемо зашифрованной подписи с возможностью проверки через заданное время на базе постквантового криптографического алгоритма цифровой подписи, основанной на хешировании, TANBA-SPHINCS+. Протокол является эффективной комбинацией постквантового алгоритма цифровой подписи TANBA-SPHINCS+, криптографического протокола, обеспечивающего шифрование данных на заданное время, ECTLC, и схемы верифицируемо зашифрованной подписи.

Ключевые слова: криптографический протокол, цифровая подпись, постквантовая криптография, асимметричная криптография, верифицируемо зашифрованная подпись.

Введение

Активное развитие квантовых технологий в последнее время, и особенно современные исследования и разработки в области квантовых вычислений и квантовых компьютеров, приводят к появлению новых задач в области обеспечения информационной безопасности. В частности, перспективным современным направлением в области защиты информации является постквантовая криптография. Целью постквантовой криптографии являются исследования и разработка новых криптографических алгоритмов, устойчивых как к классическим атакам, так и к атакам с помощью квантовых компьютеров. Важный раздел постквантовой криптографии составляют алгоритмы электронной цифровой подписи, играющие ключевую роль в обеспечении подлинности и целостности информации. Существует ряд различных подходов к проектированию постквантовых подписей. Схемы постквантовой цифровой подписи, основанные на хешировании, являются одним из основных типов постквантовых криптографических алгоритмов цифровой подписи. Они достаточно эффективны и доказуемо безопасны. Установлена их надежная безопасность как против классических, так и против квантовых атак.

В работе [1] был предложен новый постквантовый криптографический алгоритм цифровой подписи, основанный на хешировании, TANBA-SPHINCS+. Это вариант реализации известной постквантовой схемы цифровой подписи SPHINCS+, в котором используется криптографическая хеш-функция TANBA, разработанная на базе модифицированной схемы Sponge. TANBA-SPHINCS+ сохраняет основные преимущества SPHINCS+, в том числе и стойкость к атакам на квантовых компьютерах, а также расширяет возможности схемы за счет нового подхода к проектированию криптографических хеш-функций. Это делает алгоритм перспективным решением для задач постквантовой криптографии.

Для решения различных задач информационной безопасности существует множество видов цифровых подписей, например, групповые подписи, кольцевые подписи, слепые подписи, верифицируемо зашифрованные подписи и т.д. Основная идея данной работы – применяя модульный подход, на основе TANBA-SPHINCS+ построить пример одного из таких видов цифровых подписей. В данной работе предлагается новый криптографический протокол верифицируемо зашифрованной подписи с возможностью проверки через заданное время на базе постквантового криптографического алгоритма цифровой подписи, основанной на хешировании, TANBA-SPHINCS+.

Материалы и методы

В данной работе для проектирования криптографического протокола верифицируемо зашифрованной подписи с возможностью проверки через заданное время применяется модульный подход. Модульный подход к проектированию криптографических алгоритмов состоит в разбиении разрабатываемых алгоритмов на отдельные, независимые части, модули, отвечающие за выполнение отдельных конкретных криптографических функций. Подход представляет собой методологию, согласно которой сложные криптографические системы разрабатываются как совокупность отдельных, независимых, взаимозаменяемых, автономных компонентов, модулей, четко определенных по функциям, что позволяет выделить ключевые аспекты и компоненты. В основе лежит принцип разбиения одной большой задачи проектирования алгоритма на множество подзадач. Вместо разработки одного целого монолитного алгоритма весь процесс разбивается на отдельные этапы разработки специализированных модулей. Этот подход упрощает разработку, тестирование, внедрение и обновление отдельных элементов криптографической системы независимо друг от друга, что упрощает сопровождение системы и повышает их надежность, гибкость и устойчивость к различным угрозам безопасности.

Модульный подход при разработке криптографических алгоритмов дает ряд преимуществ. Во-первых, такой подход позволяет выполнять при необходимости замену или обновление отдельных частей разрабатываемого алгоритма без необходимости полной переработки всего алгоритма. Во-вторых, модульность в проектировании алгоритма повышает уровень безопасности системы за счет ограничения зоны влияния потенциальных уязвимостей частей разрабатываемого алгоритма. В-третьих, модульный подход дает возможность выполнять параллельную разработку и тестирование модулей, что, в свою очередь, ускоряет процесс реализации всей системы. В-четвертых, модули одного разрабатываемого алгоритма могут быть легко использованы и адаптированы при проектировании других систем.

Важным аспектом модульного подхода при проектировании криптографических алгоритмов является универсальность интерфейсов. Универсальность интерфейсов означает реализацию неких стандартных способов взаимодействия между модулями системы. Даже если модули были разработаны и реализованы разными разработчиками, с помощью различных технологий и имеют разные сроки использования, это позволяет обеспечивать их согласованную работу. Все модули должны обладать стандартными точками входа и выхода, а также спецификациями взаимодействия между собой. Это позволяет интегрировать модули в системы, созданные разными командами, а также облегчает их замену или обновление. Внутренние реализации модулей должны абстрагироваться от внешнего взаимодействия. Модули предоставляют выходные данные после внутренней обработки входных данных, при этом детали внутренней логики работы не раскрываются.

Следующей существенной составляющей модульного подхода к проектированию криптографических алгоритмов является повторное использование модулей. Повторное использование заключается в том, что один и тот же модуль или его реализации можно использовать в различных алгоритмах, протоколах, системах. Причем модули должны быть достаточно универсальными и абстрактными, чтобы их можно было бы использовать для широкого круга криптографических задач.

Еще одной сильной стороной модульного подхода является изоляция ошибок. Изоляция ошибок означает, что какая-нибудь уязвимость или сбой в одном модуле не распространяется на другие и не должна отрицательно влиять на функционирование других модулей или приводить к полному, окончательному нарушению безопасности.

Также ключевым моментом модульного подхода является масштабируемость и гибкость разрабатываемых алгоритмов. Масштабируемость заключается в способности системы сохранять эффективное функционирование при возрастании вычислительных нагрузок и использования памяти. Гибкость заключается в способности системы адаптироваться к любым изменениям относительно угроз или новых требований к безопасности.

В данной работе, применяя модульный подход, при проектировании за основу выбрана схема верифицируемо зашифрованной подписи. Схема верифицируемо зашифрованной подписи позволяет отправителю сообщения зашифровывать свою подпись с использованием открытого ключа доверенной третьей стороны так, что получатель может убедиться, что зашифрованная подпись содержит действительную подпись для сообщения, но не может получить никакой иной информации о подписи. Историю развития, теорию и практику применения, а также различные примеры реализаций этой схемы можно проследить по многочисленным публикациям, например [2–16].

Схемой верифицируемо зашифрованной подписи называется совокупность семи алгоритмов: алгоритм формирования ключевой пары, алгоритм формирования подписи, алгоритм проверки подписи, алгоритм формирования ключевой пары арбитра, алгоритм формирования верифицируемо зашифрованной подписи, алгоритм проверки верифицируемо зашифрованной подписи, алгоритм арбитража. В схеме взаимодействуют три участника: подписывающий сообщение, получатель сообщения и арбитр.

Алгоритм формирования ключевой пары. В результате работы алгоритма получают пару открытого pk и закрытого sk ключей подписывающего.

Алгоритм формирования подписи. Входными данными алгоритма являются сообщение M , закрытый ключ sk подписывающего сообщение. В результате работы алгоритма получают сообщение M с подписью σ.

Алгоритм проверки подписи. Входными данными алгоритма являются открытый ключ pk подписывающего сообщение, сообщение M и подпись σ. В результате работы алгоритма подпись принимается, если она действительна, или отклоняется в противном случае.

Примечание. Алгоритмы формирования ключевой пары, формирования подписи и проверки подписи являются стандартными алгоритмами схемы цифровой подписи.

Алгоритм формирования ключевой пары арбитра. В результате работы алгоритма получают пару открытого apk и закрытого ask ключей арбитра.

Алгоритм формирования верифицируемо зашифрованной подписи. Входными данными алгоритма являются сообщение M, закрытый ключ sk подписывающего сообщение и открытый ключ apk арбитра. В результате работы алгоритма получают сообщение M с верифицируемо зашифрованной подписью ves.

Алгоритм проверки верифицируемо зашифрованной подписи. Входными данными алгоритма являются открытый ключ pk подписывающего сообщение, открытый ключ apk арбитра и сообщение M с верифицируемо зашифрованной подписью ves. В результате работы алгоритма подпись принимается, если она действительна, или отклоняется в противном случае.

Алгоритм арбитража. Входными данными алгоритма являются открытый ключ pk подписывающего сообщение, закрытый ключ ask и открытый ключ apk арбитра и сообщение M с верифицируемо зашифрованной подписью ves. В результате работы алгоритма получают исходную подпись s сообщения M.

Подписывающий с помощью алгоритма формирования ключевой пары получает открытый ключ pk и закрытый ключ sk и с помощью алгоритма формирования подписи получает подпись s сообщения M. Арбитр с помощью алгоритма формирования ключевой пары арбитра получает открытый ключ apk и закрытый ключ ask. Подписывающий с помощью алгоритма формирования верифицируемо зашифрованной подписи получает сообщение M уже с верифицируемо зашифрованной подписью ves и отправляет получателю. Получатель, получив сообщение M с верифицируемо зашифрованной подписью ves, с помощью алгоритма проверки верифицируемо зашифрованной подписи проверяет полученную подпись и принимает ее, если она действительна, или отклоняет в противном случае. Получатель может обратиться к арбитру и с помощью алгоритма арбитража получить исходную подпись s сообщения M, и далее с помощью алгоритма проверки подписи проверить ее.

Важным практическим применением схем верифицируемо зашифрованной подписи является онлайн-подписание контрактов. Стороны, участвующие в сделке, ведут переговоры онлайн без личных встреч. Они просто обмениваются своими верифицируемо зашифрованными подписями по согласованному контракту, проверяют их и, наконец, обмениваются соответствующими обычными подписями. Если же вдруг один из участников сделки попытается по каким-либо корыстным причинам злоупотребить частично подписанным документом, не предоставляя свою исходную подпись, то арбитр может вмешаться и раскрыть его подпись. Контракт становится обязательным, несмотря на попытку этого участника отказаться от него.

Основным компонентом схемы является некоторая стандартная цифровая подпись. В данной работе используется постквантовая цифровая подпись TANBA-SPHINCS+ [1]. Это вариант реализации схемы цифровой подписи SPHINCS+ [17, 18], известного постквантового криптографического алгоритма, основанного на хешировании. SPHINCS+ является основой стандарта FIPS 205 [19] проекта по стандартизации алгоритмов постквантовой криптографии Национального института стандартов и технологий США (NIST). Основополагающим компонентом схемы SPHINCS+ является криптографическая хеш-функция, свойства безопасности которой обеспечивают безопасность схемы в целом. Схема предоставляет возможность проектировать алгоритмы цифровой подписи с любой безопасной криптографической хеш-функцией. SPHINCS+ предполагает реализации с использованием криптографических хеш-

функций SHA2, SHAKE и Haraka, а вариант схемы, изложенный в стандарте FIPS 205, использует только алгоритмы SHA2 или SHAKE. Существуют реализации SPHINCS+ с использованием ряда других криптографических хеш-функций, например, варианты представленные в работах [20, 21]. Алгоритм цифровой подписи TANBA-SPHINCS+ использует криптографическую хеш-функцию TANBA, построенную на основе модифицированной схемы Sponge. Sponge – это известная схема криптографической хеш-функции, лежащая в основе множества различных современных криптографических алгоритмов хеширования, в том числе и стандартов. Основным компонентом схемы Sponge является так называемая внутренняя функция. В модифицированной схеме вместо одной внутренней функции используется множество внутренних функций.

Следующим важным компонентом проектируемого протокола является криптографический протокол, обеспечивающий шифрование данных на заданное время, Elliptic Curves Time-Lapse Cryptography (ECTLC) [22]. Составляющими компонентами протокола является ряд алгоритмов криптографии на эллиптических кривых, а именно протокол генерации распределенного ключа, основанный на дискретном логарифмировании на эллиптических кривых [23], протокол проверяемого порогового разделения секрета Педерсена [24] и алгоритм шифрования Эль-Гамаля на эллиптических кривых [25].

Тем самым ключевыми свойствами проектируемого протокола являются постквантовая стойкость и возможность проверки подписи через заданное время. В таблице 1 приводится сравнение некоторых уже существующих схем верифицируемо зашифрованной подписи по этим критериям. Такие же параметры, как вычислительная сложность, размеры компонентов, в таблицу не включены, так как они не являются определяющими в рамках данной работы и будут анализированы отдельно.

Таблица 1 – Сравнение схем верифицируемо зашифрованной подписи по постквантовой стойкости и возможности проверки через заданное время

Схема	Используемая схема подписи	Стойкость против квантовых атак	Возможность проверки через заданное время
[2]	ElGamal	-	-
[3]	BLS	-	-
[4]	RSA	-	-
[5]	Waters	-	-
[6]	RSA	-	-
[7]	lattice-based	+	-
[8]	RSA	-	-
[9]	Waters	-	-
[10]	Waters dual	-	-
[11]	lattice-based	+	-
[12]	lattice-based	+	-
[13]	ECDSA	-	-
[14]	Schnorr	-	-
[15]	ECDSA	-	-
[16]	lattice-based	+	-
Данная работа	hash-based	+	+

Результаты и обсуждение

На основе вышеуказанных алгоритмов можно построить криптографический протокол верифицируемо зашифрованной подписи с возможностью проверки через заданное время. Протокол описывает взаимодействие трех участников. Первый участник – это отправитель

подписанного сообщения (далее – Отправитель). Второй участник – получатель сообщения, проверяющий подпись (далее – Получатель). Третий участник – арбитр с возможностью шифрования на заданное время (далее – Арбитр). Протокол предназначен для решения следующей задачи. Пусть M – некоторое сообщение. В некоторый момент времени T Отправитель хочет отправить Получателю подписанное сообщение M так, чтобы Получатель смог проверить подпись не раньше заданного Отправителем будущего момента времени $T + \delta$.

Пошаговое описание протокола.

Формирование пары ключей и подписи (шаги 1 и 2) соответствуют алгоритму постквантовой подписи TANBA-SPHINCS+.

1) Отправитель с помощью некоторого криптографически стойкого генератора псевдослучайных чисел получает закрытый ключ $sk = sk_{seed} \parallel sk_{prf} \parallel pk_{seed} \parallel pk_{root}$ и открытый ключ $pk = pk_{seed} \parallel pk_{root}$.

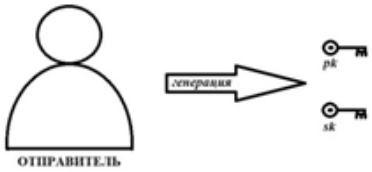

Рисунок 1 – Шаг 1

2) Затем Отправитель формирует подпись $\sigma = R \parallel \sigma_{FORS} \parallel \sigma_{HT}$, где $R = PRF_{msg}(sk_{prf}, opt, M)$ – n-битовая строка рандомизации, $PRF_{msg}: \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ – псевдослучайная функция, opt – некоторое дополнительное случайное n-битовое значение, σ_{FORS} – подпись FORS и σ_{HT} – подпись гипердерева, определенные с помощью R.

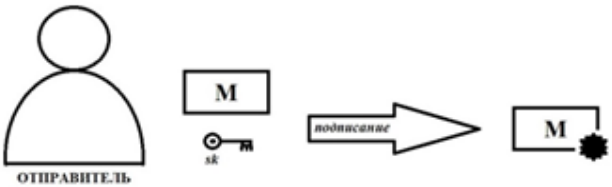

Рисунок 2 – Шаг 2

3) Далее Отправитель запрашивает у Арбитра открытый ключ Арбитра apk, указывая момент времени $T + \delta$.

4) Получив запрос, Арбитр формирует открытый ключ apk согласно криптографическому протоколу ECTLC и передает его Отправителю.

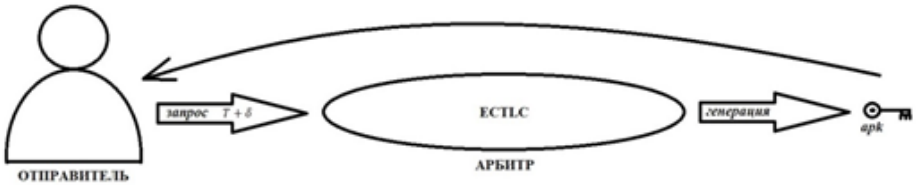

Рисунок 3 – Шаги 3–4

5) Получив открытый ключ Арбитра apk, Отправитель формирует зашифрованную подпись $\sigma_{ves} = E_{apk}(R) \parallel \sigma_{FORS} \parallel \sigma_{HT}$, где $E_{apk}(R)$ – зашифрованное с помощью открытого ключа Арбитра значение R из исходной подписи согласно криптографическому протоколу ECTLC.

6) Отправитель отправляет сообщение M с зашифрованной подписью σ_{ves} Получателю.

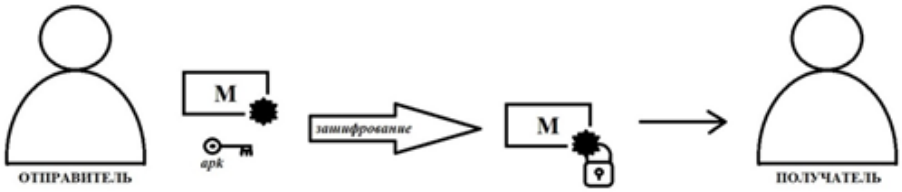

Рисунок 4 – Шаги 5–6

7) Получив сообщение M с зашифрованной подписью σ_{ves}, Получатель запрашивает у Арбитра закрытый ключ Арбитра ask.

8) Получив запрос, Арбитр проверяет время. Если текущее время уже достигло момента времени $T + \delta$, Арбитр формирует закрытый ключ ask согласно криптографическому протоколу ECTLC и передает его Получателю. Если же текущее время еще не достигло момента времени $T + \delta$, Арбитр отказывает в запросе и отправляет Получателю сообщение о том, что проверка подписи не доступна до указанного момента времени.

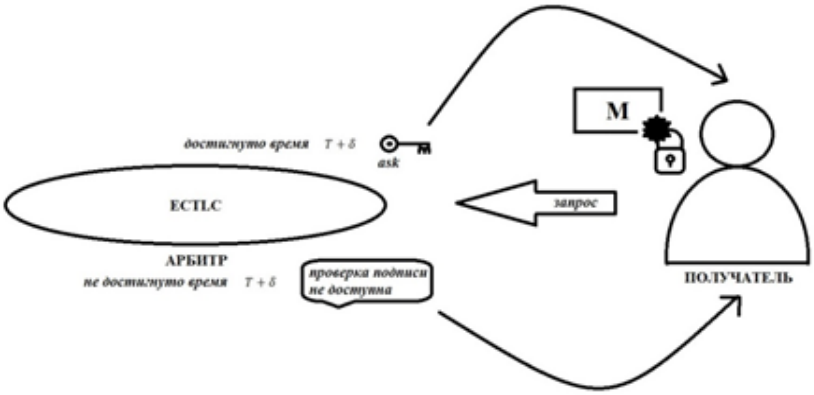

Рисунок 5 – Шаги 7–8

9) При получении отказа от Арбитра Получатель ожидает указанное время, при достижении которого заново отправляет запрос Арбитру. Получив закрытый ключ Арбитра ask, Получатель вычисляет $R = D_{ask}(E_{apk}(R))$ – расшифрованное с помощью закрытого ключа Арбитра исходное значение R из исходной подписи согласно криптографическому протоколу ECTLC.

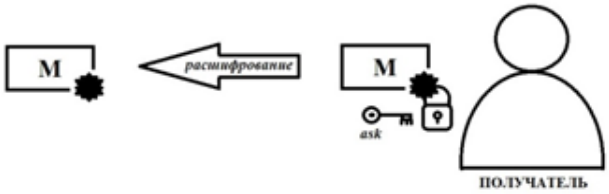

Рисунок 6 – Шаг 9

10) Расшифровав исходное значение R, Получатель выполняет проверку полученной подписи $\sigma = R \parallel \sigma_{FORS} \parallel \sigma_{HT}$ согласно алгоритму постквантовой подписи TANBA-SPHINCS+.

Все шаги протокола проиллюстрированы на следующем рисунке.

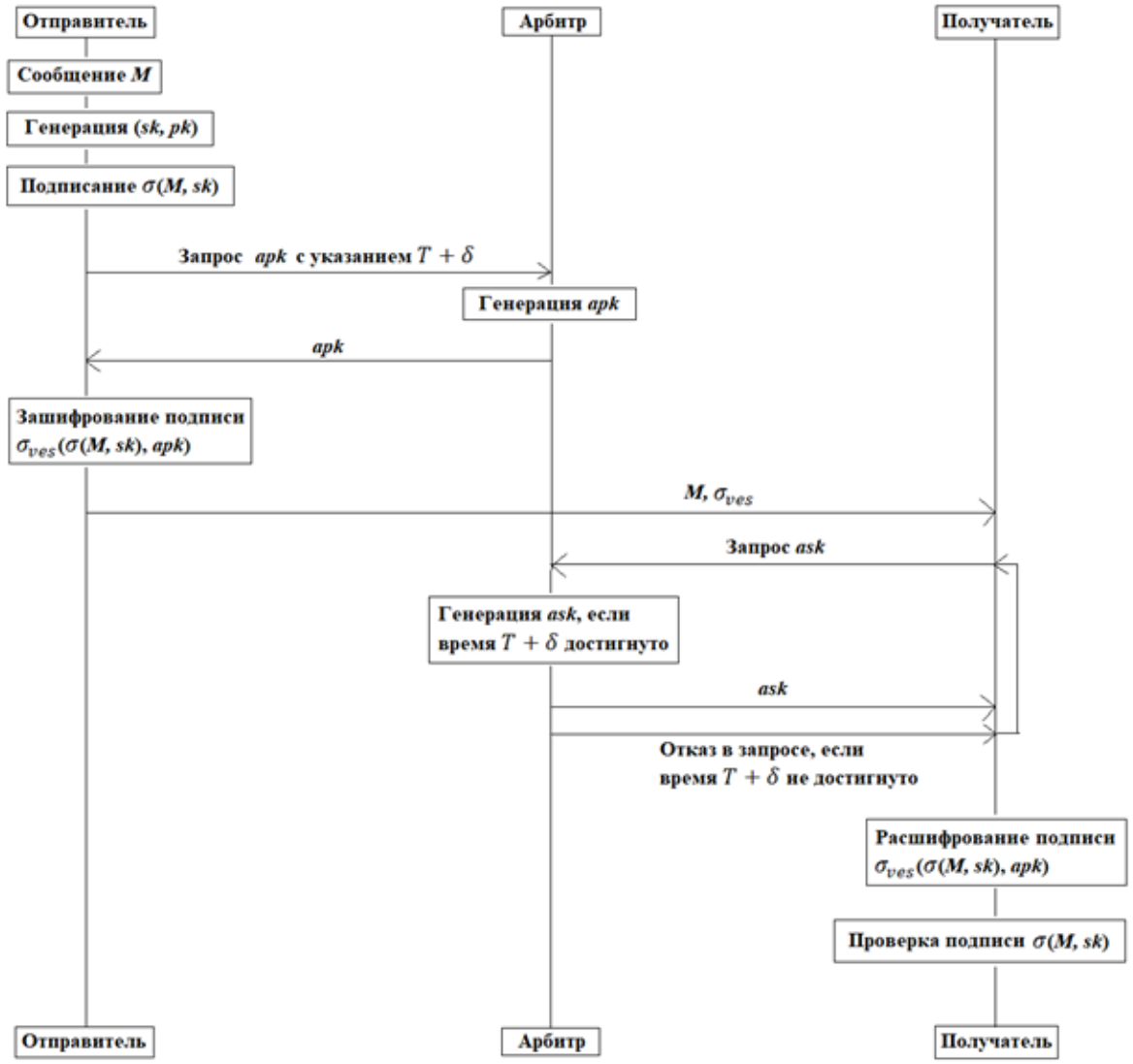

Рисунок 7 – Криптографический протокол верифицируемо зашифрованной подписи с возможностью проверки через заданное время

Ключевую роль в данном протоколе играет Арбитр. Он предоставляет остальным участникам протокола сервис шифрования данных на заданное время. Арбитр является некоторой сетью из n распределенных серверов с неким порталом для приема и обработки заявок на шифрование. Эти серверы согласно протоколу ECTLC выполняют вычисления, осуществляют хранение секретных данных, а также имеют возможности для резервного копирования данных в случае аварийных ситуаций. Предполагается, что серверы не вступают в сговор между собой, т.е. они не обмениваются конфиденциальной информацией, не предусмотренной протоколом, друг с другом. Также предполагается, что существует некоторое пороговое значение « t», при котором максимум $t-1$ серверов могут нарушать протокол, и, по крайней мере, t серверов считаются честно придерживающимися протокола. Должно выполняться условие

$n \geq 2t - 1$ ($t \leq (n+1)/2$). И если один или несколько серверов (максимум $t - 1$ серверов) выйдут из строя, то система будет продолжать работать. Применение в рамках данного протокола алгоритма распределенной генерации ключей на основе дискретного логарифма на эллиптических кривых усиливает в целом отказоустойчивость системы. Если один или несколько серверов Арбитра, участвующих в генерации ключей, выйдут из строя или будут скомпрометированы, Арбитр посредством взаимодействия остальных серверов (достаточного количества (порог)) сможет генерировать запрашиваемые криптографические ключи.

Далее перейдем к аналитической оценке вычислительных характеристик протокола. Пусть далее n, w, k, t, h, d, len – параметры алгоритма TANBA-SPHINCS+, аналогичные стандартным параметрам схемы SPHINCS+, функции $PRF, PRF_{msg}, H_{msg}, T_l, F, H$ – криптографические хеш-функции, используемые в схеме SPHINCS+, определяемые с помощью криптографической функции TANBA.

В рамках протокола Отправитель выполняет генерацию ключей, требующую 3 вызова генератора псевдослучайных чисел (для генерации sk_{seed}, sk_{prf}, pk_{seed}), $2^{h/d} - 1$ вызовов функции H, $2^{h/d} \cdot w \cdot len$ вызовов функции F, $2^{h/d} \cdot len$ вызовов функции PRF, $2^{h/d}$ вызовов функции T_{len} для вычисления pk_{root}. Далее Отправитель выполняет подписание, требующее $k \cdot (t-1) + d \cdot (2^{h/d} - 1)$ вызовов функции H, $k \cdot t + d \cdot 2^{h/d} \cdot w \cdot len$ вызовов функции F, $k \cdot t + d \cdot 2^{h/d} \cdot len$ вызовов функции PRF, $d \cdot 2^{h/d}$ вызовов функции T_{len}, а также по одному вызову функций PRF_{msg}, H_{msg}, T_k. И наконец, Отправитель выполняет одну операцию зашифрования $E_{apk}(R)$. Арбитр не участвует в операциях вычисления хеш-значений и подписи, а только генерирует ключи для зашифрования и расшифрования, осуществляет проверку времени. Отправитель выполняет одну операцию расшифрования и последующую проверку подписи, требующую $k \cdot log\ t + h$ вызовов функции H, $k + d \cdot w \cdot len$ вызовов функции F, d вызовов функции T_{len}, а также по одному вызову функций H_{msg}, T_k

Основные затраты на память связаны с ключами sk (длина $4n$), pk (длина $2n$), подписью σ (длина $(h + k \cdot (log\ t + 1) + d \cdot len + 1) \cdot n$), а также с зашифрованной подписью σ_{ves} и ключами Арбитра ask, apk.

Далее формализуем модель безопасности, определим криптографические свойства, которыми обладает протокол, и предположения, при которых эти свойства гарантируются. Безопасность протокола рассматривается в стандартной модели вероятностно-полиномиального противника, который полностью контролирует каналы связи, обладает полными знаниями алгоритмов и публичных параметров. Предполагается, что Арбитр является честным и обладает надежными и точными часами. Предполагается, что используемый в протоколе алгоритм цифровой подписи обладает свойством экзистенциальной неподделываемости при атаке с выбором сообщений (EUF-CMA). Кроме того, использование алгоритма на базе постквантовой схемы позволяет опираться на стойкость криптографических хеш-функций и обеспечивает устойчивость к атакам с помощью квантовых компьютеров. Также предполагается, что компонент шифрования подписи обладает свойством неразличимости при атаке с выбором открытых текстов (IND-CPA). Это гарантирует сокрытие подписи до наступления условия ее раскрытия (до наступления заданного момента времени). При указанных предположениях протокол обладает следующими свойствами. До заданного момента времени никакой противник не может с ненулевой вероятностью восстановить корректную подпись по зашифрованной подписи. До заданного времени зашифрованная подпись неотличима от зашифрованного любого другого значения той же длины. После раскрытия подписи при наступлении заданного времени противник не может сформировать корректную подпись для нового сообщения.

Лежащий в основе рассматриваемого протокола криптографический алгоритм TANBA-SPHINCS+ сочетает в себе основные преимущества оригинальной схемы постквантовой подписи SPHINCS+ и новые возможности, которые дает Sponge-подобная хеш-функция TANBA. Это делает протокол перспективным для применения в решении различных задач

постквантовой криптографии, позволяя адаптировать его под конкретные требования безопасности и производительности.

Заключение

Предлагаемый в данной работе криптографический протокол верифицируемо зашифрованной подписи с возможностью проверки через заданное время демонстрирует возможности модульного подхода в проектировании криптографических алгоритмов. Протокол является эффективной комбинацией постквантового алгоритма цифровой подписи TANBA-SPHINCS+, криптографического протокола, обеспечивающего шифрование данных на заданное время, ECTLC, и схемы верифицируемо зашифрованной подписи. Это показывает определенные преимущества модульного подхода. Во-первых, он упрощает разработку за счет разделения проектируемого алгоритма на независимые компоненты, каждый из которых можно разрабатывать и тестировать отдельно. Во-вторых, модули могут быть повторно использованы в других криптографических алгоритмах. В-третьих, при необходимости можно заменить один компонент алгоритма без изменения всей архитектуры. Модульная структура делает проектируемый алгоритм более гибким и адаптируемым, что важно для решения задач, связанных с безопасностью. Модульный подход делает проектирование криптографических алгоритмов структурированным и управляемым. Он обеспечивает удобство разработки, легкость адаптации к новым требованиям, возможность повторного использования компонентов и создание масштабируемых, надежных алгоритмов. Такой подход является не только практичным, но и необходимым для соответствия современным вызовам в области информационной безопасности.

Благодарность

Работа выполнена при финансовой поддержке КН МНВО РК, No AP23486901.

ЛИТЕРАТУРА

1 Оспанов Р., Сейткулов Е., Ергалиева Б., Утебаев К., Атанов С. TANBA-SPHINCS+ - постквантовый криптографический алгоритм цифровой подписи, основанной на хешировании // Вестник КазНПУ имени Абая. Серия: Физико-математические науки. – 2025. – №1(89). – С. 235–246. https://doi.org/10.51889/2959-5894.2025.89.1.020.

2 Asokan N., Shoup V., Waidner M. Optimistic fair exchange of digital signatures // Advances in Cryptology - EUROCRYPT'98. EUROCRYPT 1998. LNCS. – 1998. – Vol. 1403. – P. 591–606. https://doi.org/10.1007/BFb0054156.

3 Boneh D., Gentry C., Lynn B., Shacham H. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. // Advances in Cryptology – EUROCRYPT 2003. EUROCRYPT 2003. Lecture Notes in Computer Science. – 2003. – Vol. 2656. – P. 416–432. https://doi.org/10.1007/3-540-39200-9_26.

4 Ateniese G. Verifiable encryption of digital signature and applications // ACM Transactions on Information and System Security. – 2004. – Vol. 7(1). – P. 1–20. https://doi.org/10.1145/984334.984335.

5 Lu S., Ostrovsky R., Sahai A., Shacham H., Waters B. Sequential aggregate signatures and multisignatures without random oracles // Advances in Cryptology - EUROCRYPT 2006. EUROCRYPT 2006. LNCS. – 2006. – Vol. 4004. – P. 465–485. https://doi.org/10.1007/11761679_28.

6 Rückert M. Verifiably encrypted signatures from RSA without NIZKs // Progress in Cryptology - INDOCRYPT 2009. INDOCRYPT 2009. LNCS. – 2009. – Vol. 5922. – P. 363–377. https://doi.org/10.1007/978-3-642-10628-6_24.

7 Kim K.S., Jeong I.R. Efficient verifiably encrypted signatures from lattices // Int. J. Inf. Secur. – 2014. – Vol. 13. – P. 305–314. https://doi.org/10.1007/s10207-014-0226-0.

8 Shao, Zuhua and Yipeng Gao. Certificate- based verifiably encrypted RSA signatures // Transactions on Emerging Telecommunications Technologies. – 2015. – Vol. 26. – P. 276–289. https://doi.org/10.1002/ett.2607.

9 Shao Z., Gao Y. Practical verifiably encrypted signature based on Waters signatures // IET Information Security. – 2015. – Vol. 9(3). – P. 185–193. https://doi.org/10.1049/iet-ifs.2013.0385.

10 Nishimaki R., Xagawa K. Verifiably encrypted signatures with short keys based on the decisional linear problem and obfuscation for encrypted VES // Cryptology ePrint Archive. – 2015. – Paper 2015/248. https://eprint.iacr.org/2015/248.

11 Zhang Y., Hu Y. A New Verifiably Encrypted Signature Scheme from Lattices // J. Comput. Res. Develop. – 2017. – Vol. 54. – P. 305–312. https://dx.doi.org/10.7544/issn1000-1239.2017.20150887.

12 Wang F., Shi S. Lattice-Based Encrypted Verifiably Encryption Signature Scheme for the Fair and Private Electronic Commence // IEEE Access. – 2019. – Vol. 7. – P. 147481–147489. https://doi.org/10.1109/ACCESS.2019.2946272.

13 Yang X., Lau W.F., Ye Q., Au M.H., Liu J.K., Cheng J. Practical escrow protocol for Bitcoin // IEEE Trans. Inf. Forensics Security. – 2020. – Vol. 15. – P. 3023–3034. https://doi.org/10.1109/TIFS.2020.2976607.

14 Fournier L. One-Time Verifiably Encrypted Signatures AKA Adaptor Signatures. – 2019. URL: https://raw.githubusercontent.com/LLFourn/one-time-VES/master/main.pdf.

15 Yang X., Liu M., Au M.H., Luo X., Ye Q. Efficient Verifiably Encrypted ECDSA-Like Signatures and Their Applications // IEEE Trans. Inf. Forensics Secur. – 2022. – Vol. 17. – P. 1573–1582. https://doi.org/10.1109/TIFS.2022.3165978.

16 Lu X., Yin W., Zhang P. Lattice-Based Verifiably Encrypted Signature Scheme Without Gaussian Sampling for Privacy Protection in Blockchain // Sustainability. – October 31, 2022. – Vol. 14. – No. 21. – P. 14225. https://doi.org/10.3390/su142114225.

17 Aumasson J.-P., Bernstein D.J., Beullens W., Dobraunig C., Eichlseder M., Fluhrer S., Gazdag S.-L., Hülsing A., Kampanakis P., Kölbl S. et al. SPHINCS+ // Submission to the 3rd Round of the NIST Post-Quantum Project. – 2022. – Vol. 3.1. https://sphincs.org/data/sphincs+-r3.1-specification.pdf.

18 Bernstein D. J., Hülsing A., Kölbl S., Niederhagen R., Rijneveld J., Schwabe P.The SPHINCS+ signature framework // Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). – London, UK, 2019. – P. 2129–2146.

19 National Institute of Standards and Technology. Stateless Hash-Based Digital Signature Standard. – Washington, D.C.: Department of Commerce, 2024. – (Federal Information Processing Standards Publications; FIPS 205). https://doi.org/10.6028/NIST.FIPS.205.

20 Kiktenko E., Bulychev A., Karagodin P., Pozhar N., Anufriev M., Fedorov A. SPHINCS+ post-quantum digital signature scheme with Streebog hash function // AIP Conference Proceedings. – 2020. – Vol. 2241. – P. 020014.

21 Sim M., Eum S., Song G., Kwon H., Jang K., Kim H., Kim H., Yang Y., Kim W., Lee W. K. et al. K-XMSS and K-SPHINCS+: Hash-based signatures with Korean cryptography algorithms // Cryptology ePrint Archive. – 2022. – Report 2022/152. – URL: https://eprint.iacr.org/2022/152.

22 Tasmagambetov O., Seitkulov Ye., Ospanov R., Yergaliyeva B. Fault-tolerant backup storage system for confidential data in distributed servers // TELKOMNIKA (Telecommunication Computing Electronics and Control). – 2023. – Vol. 21. – No. 5. – P. 1030–1038. https://doi.org/10.12928/telkomnika.v21i5.25305.

23 Tang C., Chronopoulos A.T. An efficient distributed key generation protocol for secure communications with causal ordering // Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS 2005). – Fukuoka, Japan, July 20–22, 2005. – Vol. 2. – P. 285–289.

24 Pedersen T.P. Non-interactive and information-theoretic secure verifiable secret sharing // Lecture Notes in Computer Science. – 1991. – Vol. 576. – P. 129–140. (Proc. of CRYPTO'91).

25 Trung M. M., Do L. P., Tuan D. T., Thanh N. V., Tri N. Q. Design a cryptosystem using elliptic curves cryptography and Vigenère symmetric key // International Journal of Electrical and Computer Engineering (IJECE). – 2023. – Vol. 13. – No. 2. – P. 1734–1743. https://doi.org/10.11591/ijece.v13i2.

REFERENCES

1 Ospanov, R., Sejtkulov, E., Ergalieva, B., Utebaev, K., Atanov, S. TANBA-SPHINCS+ - postkvantovyj kriptograficheskij algoritm cifrovoj podpisi, osnovannoj na heshirovanii. Vestnik KazNPU imeni Abaya. Seriya: Fiziko-matematicheskie nauki, 1(89), 235–246 (2025). https://doi.org/10.51889/2959-5894.2025.89.1.020. (in Russian)

2 Asokan, N., Shoup, V., Waidner, M. Optimistic fair exchange of digital signatures. Advances in Cryptology – EUROCRYPT 1998, 1403, 591–606 (1998). https://doi.org/10.1007/BFb0054156.

3 Boneh, D., Gentry, C., Lynn, B., Shacham, H. Aggregate and verifiably encrypted signatures from bilinear maps. Advances in Cryptology – EUROCRYPT 2003, 2656, 416–432 (2003). https://doi.org/10.1007/3-540-39200-9_26.

4 Ateniese, G. Verifiable encryption of digital signatures and applications. ACM Transactions on Information and System Security, 7(1), 1–20 (2004). https://doi.org/10.1145/984334.984335

5 Lu, S., Ostrovsky, R., Sahai, A., Shacham, H., Waters, B. Sequential aggregate signatures and multisignatures without random oracles. Advances in Cryptology – EUROCRYPT 2006, 4004, 465–485 (2006). https://doi.org/10.1007/11761679_28

6 Rückert, M. Verifiably encrypted signatures from RSA without NIZKs. Progress in Cryptology – INDOCRYPT 2009, 5922, 363–377 (2009). https://doi.org/10.1007/978-3-642-10628-6_24

7 Kim, K. S., Jeong, I. R. Efficient verifiably encrypted signatures from lattices. International Journal of Information Security, 13, 305–314 (2014). https://doi.org/10.1007/s10207-014-0226-0

8 Shao, Z., Gao, Y.Certificate-based verifiably encrypted RSA signatures. Transactions on Emerging Telecommunications Technologies, 26, 276–289 (2015). https://doi.org/10.1002/ett.2607

9 Shao, Z., Gao, Y. Practical verifiably encrypted signature based on Waters signatures. IET Information Security, 9(3), 185–193 (2015). https://doi.org/10.1049/iet-ifs.2013.0385

10 Nishimaki, R., Xagawa, K. Verifiably encrypted signatures with short keys based on the decisional linear problem and obfuscation for encrypted VES. Cryptology ePrint Archive, Report 2015/248 (2015). URL: https://eprint.iacr.org/2015/248

11 Zhang, Y., Hu, Y. A new verifiably encrypted signature scheme from lattices. Journal of Computer Research and Development, 54, 305–312 (2017). https://doi.org/10.7544/issn1000-1239.2017.20150887

12 Wang, F., Shi, S. Lattice-based encrypted verifiably encryption signature scheme for fair and private electronic commerce. IEEE Access, 7, 147481–147489 (2019). https://doi.org/10.1109/ACCESS.2019.2946272

13 Yang, X., Lau, W. F., Ye, Q., Au, M. H., Liu, J. K., Cheng, J. Practical escrow protocol for Bitcoin. IEEE Transactions on Information Forensics and Security, 15, 3023–3034 (2020). https://doi.org/10.1109/TIFS.2020.2976607

14 Fournier, L. One-time verifiably encrypted signatures (adaptor signatures). Technical report (2019). URL: https://raw.githubusercontent.com/LLFourn/one-time-VES/master/main.pdf

15 Yang, X., Liu, M., Au, M. H., Luo, X., Ye, Q. Efficient verifiably encrypted ECDSA-like signatures and their applications. IEEE Transactions on Information Forensics and Security, 17, 1573–1582 (2022). https://doi.org/10.1109/TIFS.2022.3165978

16 Lu, X., Yin, W., Zhang, P. Lattice-based verifiably encrypted signature scheme without Gaussian sampling for privacy protection in blockchain. Sustainability, 14(21), 14225 (2022). https://doi.org/10.3390/su142114225

17 Aumasson, J.-P., Bernstein, D. J., Beullens, W., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S.-L., Hülsing, A., Kampanakis, P., Kölbl, S. et al. SPHINCS+. Submission to the NIST Post-Quantum Cryptography Project, version 3.1 (2022). URL: https://sphincs.org/data/sphincs+-r3.1-specification.pdf

18 Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., Schwabe, P. The SPHINCS+ signature framework. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2129–2146 (2019).

19 National Institute of Standards and Technology. Stateless hash-based digital signature standard. Federal Information Processing Standards Publications, FIPS 205 (2024). https://doi.org/10.6028/NIST.FIPS.205

20 Kiktenko, E., Bulychev, A., Karagodin, P., Pozhar, N., Anufriev, M., Fedorov, A. SPHINCS+ post-quantum digital signature scheme with Streebog hash function. AIP Conference Proceedings, 2241, 020014 (2020).

21 Sim, M., Eum, S., Song, G., Kwon, H., Jang, K., Kim, H., Kim, H., Yang, Y., Kim, W., Lee, W. K. et al. K-XMSS and K-SPHINCS+: Hash-based signatures with Korean cryptography algorithms. Cryptology ePrint Archive, Report 2022/152 (2022). URL: https://eprint.iacr.org/2022/152

22 Tasmagambetov, O., Seitkulov, E., Ospanov, R., Yergaliyeva, B. Fault-tolerant backup storage system for confidential data in distributed servers. TELKOMNIKA, 21(5), 1030–1038 (2023). https://doi.org/10.12928/telkomnika.v21i5.25305

23 Tang, C., Chronopoulos, A. T. An efficient distributed key generation protocol for secure communications with causal ordering. Proceedings of the International Conference on Parallel and Distributed Systems, 2, 285–289 (2005).

24 Pedersen, T. P. Non-interactive and information-theoretic secure verifiable secret sharing. Lecture Notes in Computer Science, 576, 129–140 (1991).

25 Trung, M. M., Do, L. P., Tuan, D. T., Thanh, N. V., Tri, N. Q. Design a cryptosystem using elliptic curves cryptography and Vigenère symmetric key. International Journal of Electrical and Computer Engineering, 13(2), 1734–1743 (2023). https://doi.org/10.11591/ijece.v13i2.pp1734-1743

[1]Сейткулов Е.Н.,
ф.-м.ғ.к., ғылыми қызметкер,
ORCID ID: 0000-0002-5172-8339,
e-mail: yerzhan.seitkulov@gmail.com
[1*]Оспанов Р.М.,
магистр, ғылыми қызметкер,
ORCID ID: 0000-0002-0771-575X,
*e-mail: ospanovrm@gmail.com
[1]Ерғалиева Б.Б.,
ғылыми қызметкер,
ORCID ID: 0000-0002-1252-857X,
e-mail: banu.yergaliyeva@gmail.com
[2]Утебаев К.А.,
магистрант, ғылыми қызметкер,
ORCID ID: 0009-0004-3032-5049,
e-mail: utebayevkuat@gmail.com
[1]Атанов С.К.,
т.ғ.д., профессор,
ORCID ID: 0000-0003-2115-7130,
e-mail: atanov_sk@enu.kz

[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Астана қ., Қазақстан
[2]«МИФИ» ұлттық ядролық зерттеу университетінің Алматы филиалы,
Алматы қ., Қазақстан

БЕЛГІЛІ УАҚЫТТАН КЕЙІН ТЕКСЕРУ МҮМКІНДІГІ БАР ТЕКСЕРІЛЕТІН ШИФРЛАНҒАН ҚОЛТАҢБАНЫҢ КРИПТОГРАФИЯЛЫҚ ХАТТАМАСЫ

Андатпа

Ақпараттық қауіпсіздік саласындағы заманауи бағыттардың бірі – постквanттық криптография. Оның мақсаты кванттық төзімді жаңа криптографиялық алгоритмдерді әзірлеу. Постквanттық криптографияның маңызды бөлімдерінің бірі – электрондық цифрлық қолтаңба алгоритмдері. Постквanттық қолтаңбаларды жобалаудың әртүрлі тәсілдері бар. Постквanттық криптографиялық цифрлық қолтаңба алгоритмдерін жобалаудың негізгі тәсілдерінің бірі – хэштеуге негізделген постквanттық цифрлық қолтаңба схемалары. Хэш негізіндегі постквanттық цифрлық қолтаңба схемалары постквanттық криптографиялық цифрлық қолтаңба алгоритмдерінің негізгі түрлерінің қатарына жатады. Олар тиімділігі жоғары әрі қауіпсіздігі сенімді. Олардың қауіпсіздігі классикалық және кванттық шабуылдарға қарсы дәлелденген. Ақпараттық қауіпсіздіктің әртүрлі міндеттерін шешуге арналған сандық қолтаңбалардың көптеген түрлері бар, соның ішінде топтық қолтаңбалар, сақиналы қолтаңбалар, соқыр қолтаңбалар, тексерілетін шифрланған қолтаңбалар және басқалары. Бұл құжат TANBA-SPHINCS+ – постквanттық криптографиялық цифрлық қолтаңба алгоритміне негізделген, белгілі бір уақыт өткеннен кейін тексеру мүмкіндігін қамтамасыз ететін жаңа тексерілетін шифрланған қолтаңба криптографиялық хаттамасын ұсынады. Ұсынылған хаттама TANBA-SPHINCS+ постквanттық цифрлық қолтаңба алгоритмінің, деректерді белгілі бір уақытқа дейін шифрлауды қамтамасыз ететін ECTLC криптографиялық хаттамасының және тексерілетін шифрланған қолтаңба схемасының тиімді комбинациясын қамтиды.

Тірек сөздер: криптографиялық хаттама, цифрлық қолтаңба, постквanттық криптография, асимметриялық криптография, тексерілетін шифрланған қолтаңба.

[1]Seitkulov Ye.N.,
Cand. Phys.-Math. Sc., Research Fellow,
ORCID ID: 0000-0002-5172-8339,
e-mail: yerzhan.seitkulov@gmail.com
[1*]Ospanov R.M.,
MSc (Tech.), Research Fellow,
ORCID ID: 0000-0002-0771-575X,
*e-mail: ospanovrm@gmail.com
[1]Yergaliyeva B.B.,
Research Fellow,
ORCID ID: 0000-0002-1252-857X,
e-mail: banu.yergaliyeva@gmail.com
[2]Utebayev K.A.,
Master's student, Research Fellow,
ORCID ID: 0009-0004-3032-5049,
e-mail: utebayevkuat@gmail.com
[1]Atanov S.K.,
Dr. Tech. Sc., Professor,
ORCID ID: 0000-0003-2115-7130,
e-mail: atanov_sk@enu.kz

[1]L.N. Gumilyov Eurasian National University,
Astana, Kazakhstan
[2]Almaty branch of the National Research Nuclear University MEPhI,
Almaty, Kazakhstan

CRYPTOGRAPHIC PROTOCOL OF VERIFIABLY ENCRYPTED SIGNATURE WITH POSSIBILITY OF VERIFICATION AFTER A SPECIFIED TIME

Abstract

One of the modern directions in the field of information security is post-quantum cryptography. Its purpose is to develop new quantum-resistant cryptographic algorithms. An important section of post-quantum cryptography is electronic digital signature algorithms. There are a number of different approaches to designing post-quantum signatures. One of the main approaches to designing post-quantum cryptographic digital signature algorithms is hash-based post-quantum digital signature schemes. Hash-based post-quantum digital signature schemes are one of the main types of post-quantum cryptographic digital signature algorithms. They are quite efficient and provably secure. Their reliable security has been established against both classical and quantum attacks. There are many types of digital signatures for solving various information security problems, such as group signatures, ring signatures, blind signatures, verifiably encrypted signatures, etc. This paper proposes a new cryptographic protocol of verifiably encrypted signature with possibility of verification after a specified time based on the post-quantum cryptographic algorithm of hash-based digital signature, TANBA-SPHINCS+. The protocol is an efficient combination of the post-quantum digital signature algorithm TANBA-SPHINCS+, the cryptographic protocol providing data encryption for a specified time, ECTLC, and the verifiably encrypted signature scheme.

Keywords: cryptographic protocol, digital signature, post-quantum cryptography, asymmetric cryptography, verifiably encrypted signature.

Received: August 8, 2025; revised: December 12, 2025; accepted: January 17, 2026.