МРНТИ 81.93.29

10.51889/2959-5894.2025.90.2.015

И.А. Андреев [1,2], Ф.Б. Тебуева [2], Б.К. Абдураимова [1], Д.Ж. Сатыбалдина [1], Ж.А. Боранбай [1]

[1]Евразийский национальный университет имени Л.Н. Гумилева, г.Астана, Казахстан
[2]ФГАОУ ВО «Северо-Кавказский федеральный университет»,
г.Ставрополь, Российская Федерация
[*]*e-mail: andreev.ilia.1984@mail.ru*

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ АУТЕНТИФИКАЦИИ IIOT-УСТРОЙСТВ НА ОСНОВЕ БЛОКЧЕЙН С ИСПОЛЬЗОВАНИЕМ BLAKE3 И АГРЕГИРОВАНИЯ ПОДПИСЕЙ

Аннотация

В статье предлагается усовершенствованный алгоритм аутентификации устройств для промышленных систем Интернета вещей (IIoT). Предлагаемый алгоритм реализуется на основе технологии блокчейн с использованием хэш-функции BLAKE3, безсертификационной схемы подписей и агрегирования подписей. Экспериментальное моделирование проведено в среде GNU/Linux с использованием симуляции атак 3 типов: подмены публичного ключа, атак на мастер-ключ, атак на консенсус. Предложенный алгоритм позволяет минимизировать вычислительные затрат за счёт оптимизации операций хэширования и подписания, снизить объём передаваемых данных. Эксперименты подтвердили устойчивость IIoT-устройств к выбранным 3 типам атак, что делает алгоритм эффективным для применения в реальных IIoT-системах.

Ключевые слова: аутентификация, блокчейн, агрегированные подписи, BLAKE3, IIoT

I.A. Andreev [1,2], F.B. Tebueva [2], B.K. Abdurayimova [1], D.Zh. Satybaldina [1], Zh.A. Boranbay [1]
[1]Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan
[2]FSAEI HE "North-Caucasus Federal University", Stavropol, Russian Federation

IMPROVED BLOCKCHAIN-BASED IIOT DEVICE AUTHENTICATION ALGORITHM USING BLAKE3 AND SIGNATURE AGGREGATION

Abstract

This paper proposes an improved device authentication algorithm for industrial Internet of Things (IIoT) systems. The proposed algorithm is implemented based on blockchain technology using BLAKE3 hash function, certificateless signature scheme and signature aggregation. Experimental modeling is performed in GNU/Linux environment using simulation of attacks of 3 types: public key spoofing, master key attacks, consensus attacks. The proposed algorithm allows to minimize the computational cost by optimizing hashing and signing operations, and to reduce the volume of transmitted data. Experiments confirmed the resistance of IIoT devices to the selected 3 types of attacks, which makes the algorithm effective for use in real IIoT systems.

Keywords: authentication, blockchain, aggregated signatures, BLAKE3, IIoT

И.А. Андреев [1,2], Ф.Б. Тебуева [2], Б.К.Абдураимова [1], Д.Ж.Сатыбалдина [1], Ж.А.Боранбай [1]
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан
[2] Солтүстік Кавказ федералды университеті, Ставрополь, Ресей Федерациясы

BLAKE3 ЖӘНЕ SIGNATURE АГРЕГАЦИЯСЫН ПАЙДАЛАНАТЫН БЛОКЧЕЙН НЕГІЗІНДЕГІ IIOT ҚҰРЫЛҒЫЛАРЫН АУТЕНТІКТЕУДІҢ ЖЕТІЛДІРІЛГЕН АЛГОРИТМІ

Аңдатпа

Бұл құжат өнеркәсіптік Интернет заттары (IIoT) жүйелері үшін жақсартылған құрылғы аутентификация алгоритмін ұсынады. Ұсынылған алгоритм блокчейн технологиясы негізінде BLAKE3 хэш-функциясын, сертификатсыз қолтаңба схемасын және қолтаңбаларды біріктіруді пайдалана отырып жүзеге асырылады. Эксперименттік модельдеу GNU/Linux ортасында шабуылдардың 3 түрін модельдеу арқылы жүзеге асырылды: ашық кілтті ауыстыру, басты кілтке шабуыл және консенсусқа

шабуыл. Ұсынылған алгоритм хэштеу және қол қою операцияларын оңтайландыру және жіберілетін деректер көлемін азайту арқылы есептеу шығындарын азайтуға мүмкіндік береді. Эксперименттер IIoT құрылғыларының таңдалған 3 шабуыл түріне төзімділігін растады, бұл алгоритмді нақты IIoT жүйелерінде пайдалану үшін тиімді етеді.

Түйін сөздер: аутентификация, блокчейн, агрегатталған қолтаңбалар, BLAKE3, IIoT

Основные положения

Представлен усовершенствованный алгоритм аутентификации устройств промышленного Интернета вещей (IIoT), реализованный на основе технологии блокчейн, хэш-функции BLAKE3, на базе схемы безсертификатных подписей и их агрегированием. Алгоритм минимизирует вычислительные и коммуникационные затраты, обеспечивает устойчивость к трём ключевым типам атак: подмене публичного ключа (PKR), атаке на мастер-ключ (MBPK) и атаке на консенсус (CCA). Экспериментальное моделирование подтвердило эффективность предложенного алгоритма в условиях ограниченных ресурсов, её высокую производительность и пригодность в условиях ограниченных ресурсов.

Введение

С развитием технологии блокчейн и ее проникновением в различные сферы, включая распределенное хранение данных и обеспечение безопасности, возникает потребность в повышении эффективности и безопасности схем управления идентификацией и доступом. Согласно представленным исследованиям [1], текущие методы аутентификации устройств в распределенных системах IIoT сталкиваются с проблемами высокой вычислительной нагрузки, уязвимости к атакам на целостность данных и недостаточной масштабируемости. Технологии IIoT представляют собой сеть взаимосвязанных устройств, взаимодействующих через интернет, тогда как блокчейн обеспечивает децентрализованное и защищенное хранение данных, устойчивое к изменениям [2]. Применение современных технологий, таких как криптографическая хэш-функция BLAKE3, обеспечивает не только высокую скорость обработки данных, но и устойчивость к различным видам атак. Агрегированные подписи значительно снижают нагрузку на сеть за счёт объединения нескольких подписей в одну [3], в то время как схемы безсертификатной подписи (Certificateless Signature, CLS) устраняют зависимость от центра сертификации, повышая уровень безопасности в распределённых системах [4].

Стандартные хэш-алгоритмы и схемы с централизованной проверкой подписей, сталкиваются с рядом проблем: значительными вычислительными издержками, уязвимостью к атакам, высокой задержкой и необходимостью доверия к централизованным узлам [5]. Устаревшие хэш-функции (например, MD5 и SHA-1) являются объектами документально подтверждённых атак. В феврале 2017 года команда Google и Институт CWI продемонстрировали первую коллизию SHA-1, что привело к отказу браузеров от поддержки этой функции. Коллизии для MD5 могут быть найдены за секунды при помощи GPU, что делает её небезопасной для криптографических целей [6]. Согласно обзору компании MoldStud (2025), более 60 % инцидентов в области ИБ связаны с использованием слабых хэш-функций [7]. Эти факты подчеркивают актуальность перехода к современным безопасным решениям, таким как BLAKE3. Эти проблемы усугубляются в распределенных системах, таких как IIoT-системы, где критичны – как надежность, так и производительность механизмов аутентификации и проверки целостности данных [8].

Современные требования к распределенным системам предъявляют высокие ожидания к вычислительной эффективности и устойчивости к различным типам атак. Одной из главных задач остается обеспечение безопасности и скорости обработки аутентификации устройств в блокчейн, при этом сокращение вычислительных издержек может значительно повысить производительность систем и снизить затраты [9]. В этом контексте использование функции BLAKE3 и агрегированных подписей (Aggregated Signatures) оказывается весьма

перспективным, поскольку они предлагают высокую вычислительную эффективность, улучшенную производительность и устойчивость к атакам, таким как атаки с подделкой и атаки на целостность данных [10].

В последние годы активно развиваются методы использования физически неклонируемых функций (PUF) в системах аутентификации устройств. Одним из перспективных направлений является интеграция PUF с механизмами генерации секретных ключей (SKG) на физическом уровне, что позволяет повысить стойкость к атакам на воспроизведение и подмену устройств. Исследование [11] демонстрирует, что объединение PUF с секретными ключами, полученными из характеристик канала связи, способствует улучшению безопасности аутентификационных протоколов для IIoT-систем.

Дальнейшее развитие технологий аутентификации в системах IIoT связано с интеграцией многофакторных схем безопасности, использующих PUF, SKG и оценку близости на основе характеристик радиосигнала. В работе [12] предлагается новая методология многофакторной аутентификации, в которой сочетаются методы безопасности физического уровня и протоколы краткосрочной связи. Такой подход обеспечивает устойчивость к атакам воспроизведения и улучшает точность идентификации периферийных устройств в условиях промышленного Интернета вещей.

Алгоритм BLAKE3 отличается от предшествующих хэш-функций, таких как SHA-256 и даже BLAKE2, улучшенной производительностью и устойчивостью к широкому спектру атак, включая атаки на коллизии и анализ на длину сообщения. В частности, BLAKE3 использует алгоритм Merkle-Damgård и подход хэширования с деревом (Tree Hashing), что делает его пригодным для параллельной обработки и, следовательно, более быстрым для многопоточных вычислений. Формула для хэширования на основе дерева выглядит следующим образом:

$$Hash(M) = Compress(Compress(M_1)||Compress(M_2)|| \dots ||Compress(M_n)), \quad (1)$$

где M – сообщение, разбитое на блоки $M_1, M_2, \dots, M_n$, а $Compress$ – функция сжимающего хэширования.

Совмещение BLAKE3 и агрегированных подписей в рамках блокчейн-системы позволяет обеспечить высокую устойчивость к ряду атак. В частности, данное сочетание защищает от атаки двойной траты и атаки на целостность данных. Агрегированные подписи с использованием CLS-схемы позволяют избежать зависимости от центра сертификации (CA), делая систему более гибкой и устойчивой к подделке.

Рисунок 3 (TABLE I) показывает сравнительные данные по коммуникативной нагрузке различных схем подписей, включая усовершенствованный алгоритм аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями. Агрегированная подпись требует всего 480 бит для передачи (в сравнении с 800 бит у прототипов), что сокращает объем передаваемой информации и увеличивает пропускную способность сети.

Актуальность для IIoT-систем и распределенных систем согласно [13], использование BLAKE3 и агрегированных подписей имеет потенциальное применение в таких сферах, как умные города, медицинские IoT-сети и умное производство, где количество устройств и запросов растет экспоненциально.

Основные задачи настоящего исследования заключаются:

1) в обеспечении устойчивости к атакам на публичный ключ, мастер-ключ и атакам на консенсус;

2) минимизации вычислительных затрат для операций генерации и проверки подписей, снижении объема передаваемых данных.

В настоящей работе предлагается усовершенствованный алгоритм аутентификации IIoT-устройств, который обеспечивает высокую устойчивость к атакам PKR, MBPK, CCA, минимизирует вычислительные и коммуникационные затраты, а также увеличивает производительность и масштабируемость в условиях ограниченных ресурсов. Для

поставленных задач необходимо разработать алгоритм, минимизирующий временные и коммуникационные затраты, сохраняя высокий уровень безопасности для IIoT-устройств, а также провести экспериментальное исследование эффективности предложенного алгоритма с его сравнением по критериям производительности, масштабируемости и устойчивости к атакам с существующими методами. Технологии IIoT представляют собой сеть взаимосвязанных устройств, взаимодействующих через интернет, тогда как блокчейн обеспечивает децентрализованное и защищенное хранение данных, устойчивое к изменениям.

Методология исследования

Современные методы обеспечения безопасности и децентрализации в блокчейн-системах включают традиционные подходы, такие как Proof of Work (PoW) и Proof of Stake (PoS). Однако эти методы сталкиваются с рядом ограничений, включая высокие затраты на вычисления и энергопотребление, что делает их менее подходящими для ресурсозависимых и высоконагруженных систем, таких как промышленные IIoT-сети и распределенные системы идентификации. В недавних исследованиях были предложены улучшенные алгоритмы, такие как Proof of Computation (PoCP)**,** которые обеспечивают лучшую производительность при меньших ресурсных затратах.

$$PoCP: H(x, M) \rightarrow Proof\ of\ Integrity, \quad (2)$$

где $H(x, M)$ – хэш от данных M с меткой времени x, полученный с использованием BLAKE3.

PoW является наиболее известным и широко используемым методом консенсуса, особенно в сети Bitcoin. Он основывается на решении сложной задачи (например, нахождения значения x, такого что $H(x) < T$, где T – целевое значение). Основной недостаток метода заключается в высокой вычислительной сложности, что влечёт значительные энергозатраты. Более того, PoW ограничивает масштабируемость и задержку транзакций, что усложняет его применение в высоконагруженных системах IoT.

$$\text{Задача: найти } x, \text{ для которого } H(x) < T. \quad (3)$$

Преимущества PoW включают децентрализацию и безопасность, но высокие затраты на вычисления делают его непригодным для энергоограниченных устройств.

PoS направлен на снижение энергозатрат путем выбора валидаторов на основе их вклада (стейка) в сеть. В то время как PoS снижает вычислительные затраты, он подвержен проблемам с централизацией, поскольку крупные стейкеры имеют больше шансов на выбор в качестве валидаторов. Другая проблема заключается в так называемой "проблеме богатых": пользователи с наибольшим стейком получают больше возможностей для валидации и накопления стейка, что снижает децентрализацию.

$$\text{Вероятность выбора валидатора} \propto Stake. \quad (4)$$

Таким образом, PoS повышает эффективность по сравнению с PoW, но не обеспечивает оптимальную безопасность для больших, децентрализованных систем.

Метод Proof of Computation (PoCP), упомянутый в работе [14], направлен на преодоление недостатков PoW и PoS, комбинируя вычислительную нагрузку и требования к проверке. PoCP основывается на идее вычислительного доказательства, требуя выполнения вычислительных задач для подтверждения подлинности, при этом снижая вычислительную нагрузку за счет использования алгоритмов, оптимизированных для параллельной обработки.

Концепция CLS впервые была предложена Ai-Riyami и Paterson [15] и с тех пор развивалась в различных направлениях. Схемы CLS можно разделить на две основные категории: построенные на модели случайного оракула и на стандартной модели, не зависящей от случайного оракула. В большинстве существующих схем CLS криптографические хэш-функции рассматриваются как идеальные случайные оракулы, что делает алгоритмы уязвимыми к различным видам атак при использовании в реальных условиях. По этой причине доказательство безопасности в стандартной модели становится особенно важным, особенно

для приложений, связанных с IIoT, где требуется высокая безопасность для защиты целостности данных [16].

В последние годы растет интерес к алгоритмам CLS без использования случайных оракул, поскольку они лучше подходят для реальных сценариев. Первая CLS-схема без случайных оракул была предложена Liu и соавторами [17], но была признана уязвимой к атакам Man-in-the-Middle Based Public Key (MBPK) [18]. Впоследствии Yuan и соавторы [19] разработали алгоритму, способный противостоять MBPK-атакам, но он оказался уязвимым к атакам подмены публичного ключа (PKR) [20]. В алгоритме Yu и соавторов [21] также имелись недостатки: он не мог полностью противостоять MBPK- и PKR-атакам. Для повышения безопасности Yuan и Wang [19] предложили улучшенный алгоритм, но и он оставался подверженным MBPK-атакам.

В работе Haoqi Wen [26] представлен алгоритм аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS, который в настоящей статье выбран в качестве аналога. В алгоритме используются обозначения, приведенные ниже в таблице 1. Алгоритм представляет собой CLS-схему с использованием технологии блокчейн, исключая зависимость от случайного оракула.

Таблица 1. Перечень символов

Символ	*Описание*
G_1, G_2	*две группы точек эллиптической кривой G_1 и G_2 с порядком простого числа p*
P	*простое число, задающее порядок групп*
G	*генератор группы G_1*
E	*билинейное отображение $e: G_1 \times G_1 \to G_2$, удовлетворяющее следующим условиям: билинейность, невырожденность и вычислимость*
ID	*идентификатор пользователя*
M	*сообщение, подлежащее подписанию*
H_u, H_m	*две безопасные хэш-функции*
msk	*системный мастер-ключ*
$(psk_{(1)}, psk_{(2)})$	*частичный приватный ключ*
$(pk_{(1)}, pk_{(2)})$	*публичный ключ пользователя*
σ	*подпись для сообщения m*

В алгоритме аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS используются математические параметры, такие как группы G_1 и G_2 точек эллиптической кривой порядка простого числа p и генератор g группы G_1. Ключевую роль в обеспечении безопасности играет билинейное отображение $e: G_1 \times G_1 \to G_2$, которое удовлетворяет следующим условиям:

Билинейность: $e(g^{t_1} g^{t_2}) = e(g, g)^{t_1 t_2}, \forall t_1, t_2 \in \mathbb{Z}_p^*$. (5)

Невырожденность: $e(g^{t_1} g^{t_2}) \neq 1$. (6)

Вычислимость: $e(g^{t_1} g^{t_2})$ может быть эффективно рассчитано. (7)

Процесс генерации ключей организован на основе участия центра генерации ключей (KGC) и пользователя. KGC выбирает случайный мастер-ключ $msk \in Z_p$ и генерирует системные параметры, вычисляя $g_1 = g^{msk}, Z = e(g, g_1)$.

Затем публикуются параметры (g, g_1, Z, G_1, G_2, e). Пользователь, со своей стороны, выбирает случайный приватный ключ $usk \in Z_p$ и на его основе генерирует публичный ключ $upk = g^{usk}$.

На этапе 1 выполняется подписание сообщения M, которое начинается с вычисления хэша сообщения и идентификатора пользователя $H_u = H(M, ID, upk)$. Далее генерируется подпись $\sigma = (g^r, g_1^r \cdot H_u)$, где $r \epsilon Z_p$ является случайным значением.

На этапе 2 осуществляется проверка подписи, где проверяющий рассчитывает $e(g, \sigma_2)$ и проверяет равенство $e(g, \sigma_2) = e(\sigma_1, g_1) \cdot e(H_u, g)$. Если данное равенство выполняется, подпись считается корректной.

Для повышения эффективности учитывается минимизация временных затрат, которая определяется как суммарное время выполнения операций:

$$T_{total} = T_{hash} + T_{sign} + T_{verify}, \tag{8}$$

где T_{hash}, T_{sign}, T_{verify} – время, затрачиваемое на хэширование, генерацию и проверку подписей соответственно.

Дополнительно оптимизируется объём данных, необходимых для передачи подписей, который должен быть минимальным, чтобы снизить нагрузку на сеть и повысить производительность системы.

В системах CLS для защиты данных используются эллиптические кривые и билинейные отображения, как это описано в [1, 22-27].

Использование этих параметров позволяет построить устойчивые к различным видам атак схемы CLS, где сложность основывается на вычислительной трудности следующих задач:

Проблема Диффи-Хеллмана (CDH): дано (g, g^a, g^b) для неизвестных $a, b \in \mathbb{Z}_p^*$. Требуется вычислить g^{ab}.

Обратная CDH-проблема: для заданного (g, g^a) требуется вычислить g^{-a}.

Задача дискретного логарифмирования (DL): для заданного (g, g^a) требуется найти $a \in \mathbb{Z}_p^*$.

На рисунке 1 представлена схема взаимодействия компонентов системы аутентификации. Администратор играет ключевую роль в поддержке блокчейн-сети и отвечает за инициализацию системных параметров. Центр генерации смарт-контрактов (Smart Contract Key Generation Center, SC-KGC) функционирует в виде смарт-контракта, размещённого в блокчейн, и обеспечивает управление выпуском частичных ключей для пользователей, а также хранение параметров системы в распределённой сети.

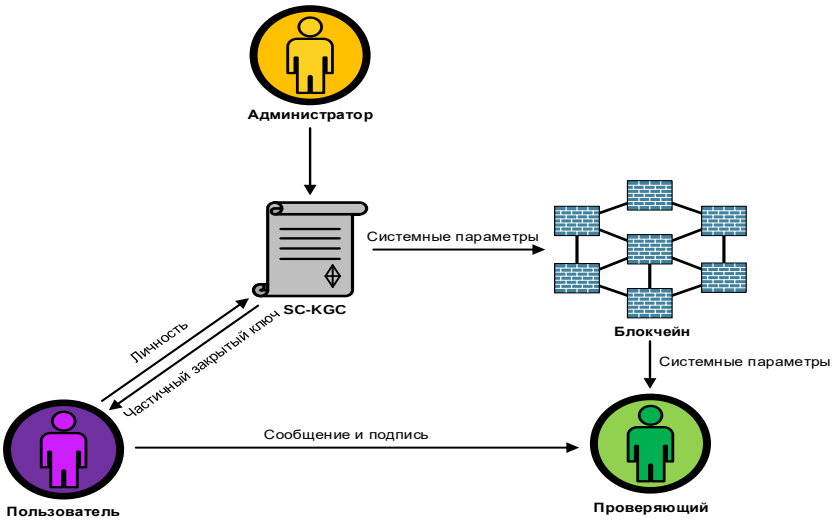


Рисунок 1. Схема алгоритма аутентификации IIoT-устройств на основе блокчейн с использованием MD5

Пользователь самостоятельно генерирует собственные публичные и приватные ключи, что позволяет создать сертификат без участия центра сертификации, тем самым исключая централизованную точку отказа. Проверяющий, в свою очередь, осуществляет верификацию подлинности подписи, используя параметры системы, которые были переданы через блокчейн, гарантируя корректность и надёжность процесса проверки.

В алгоритме аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS [26] выявлена уязвимость в виде подверженности атакам на консенсус (CCA-атакам), осуществляемым злоумышленниками типа III. Эта уязвимость ограничивает возможность его использования в условиях IIoT, где автоматизация процессов исключает ручную проверку доверия.

Злоумышленник типа III (A_3) представляет собой атакующего, способного манипулировать сетью с целью изменения последовательности или содержания блоков в цепочке. Это может включать модификацию истории транзакций или достижение консенсуса для поддельных данных через эксплуатацию недостатков протоколов консенсуса. Такие действия могут нарушить целостность данных, подорвать доверие к системе и привести к серьёзным сбоям в работе IIoT-инфраструктуры.

В настоящей работе предлагается усовершенствование алгоритма аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS, которое состоит в том, что каждый узел выполняет проверку данных, которая включает BLAKE3-хэширование и проверку целостности данных, используя CouchDB, распределенную базу данных с поддержкой параллельного хэширования.

Платформа BitBadges [14], использующая алгоритм PoCP (8) с хэш-функцией BLAKE3 и CouchDB, демонстрирует высокую производительность и улучшенную масштабируемость. BLAKE3-хэширование в рамках BitBadges позволяет достичь меньшего времени на вычисления за счет использования деревьев меркла и оптимизации под многопоточные вычисления. CouchDB обеспечивает параллельную обработку запросов, что позволяет значительно снизить задержки при выполнении операций аутентификации. BLAKE3 выполняет хэширование по формуле (1), где каждая операция *Compress* выполняется параллельно для оптимизации.

Агрегированные подписи в этой системе обеспечивают возможность объединения подписей от нескольких устройств в единую подпись. Это значительно сокращает объем данных для передачи и ускоряет процесс верификации, что критично для промышленных IoT-сетей, где устройства ограничены по ресурсам.

Основные преимущества BLAKE3 в сравнении с традиционными методами заключаются в повышенной устойчивости к атакам, особенно атакам на целостность данных. Агрегированные подписи, в свою очередь, позволяют объединить несколько подписей в одну в формуле 2, где S_{agg} – агрегированная подпись, позволяющая сократить объем передаваемых данных и повысить пропускную способность.

Рисунок 2 демонстрирует процесс аутентификации устройства в блокчейн-системе с использованием усовершенствованного алгоритма аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями:

1) SC-KGC через блокчейн выполняет распределённое управление ключами и запись системных параметров.

2) Пользователь генерирует свою подпись с использованием BLAKE3 и частичного приватного ключа.

3) Проверяющий выполняет верификацию подписи, используя данные, полученные из блокчейн.

Рисунок 2 иллюстрирует процессы, связанные с алгоритмом аутентификации IIoT-устройств, начиная с этапа инициализации и заканчивая проверкой подлинности.

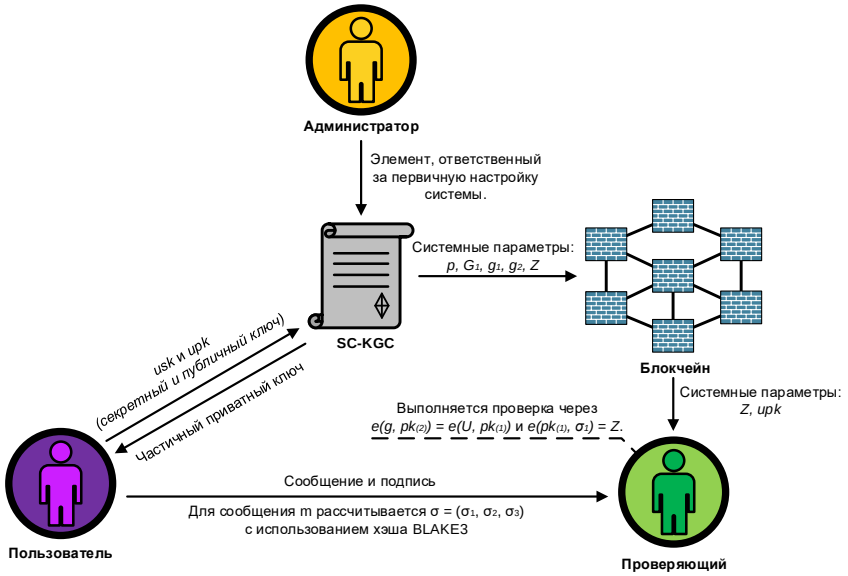


Рисунок 2. Схема усовершенствованного алгоритма аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями.

На первом этапе инициализации SC-KGC выполняет алгоритм Setup, генерируя системные параметры (p, G_1, g_1, g_2, Z) и частичный приватный ключ пользователя. Эти параметры передаются через блокчейн и хранятся в распределённом реестре, обеспечивая доступность для всех участников сети.

На этапе генерации подписи пользователь создаёт приватный и публичный ключи (usk, upk), а для сообщения mmm рассчитывается подпись $\sigma = (\sigma_1, \sigma_2, \sigma_3)$, используя хэш-функцию BLAKE3.

Верификация осуществляется проверяющим, который получает параметры (Z, upk) из блокчейна. Проверяющий выполняет два условия проверки:

1. $e(g, pk_2) = e(U, pk_1)$,
2. $e(pk_1, \sigma_1) = Z$.

Основной процесс направлен на минимизацию вычислительных затрат и нагрузки на сеть за счёт использования хэш-функции BLAKE3 и агрегированных подписей. Эти механизмы повышают производительность системы и её устойчивость к атакам. В отличие от аналогов, предложенный подход позволяет исключить администратора из процесса, так как SC-KGC полностью управляет инициализацией и функционированием системы.

Результаты исследования

В рамках эксперимента реализована усовершенствованная версия алгоритма аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS с использованием хэш-функции BLAKE3 и агрегированных подписей. Основные цели эксперимента включали повышение безопасности и эффективности, а также сравнение с существующим алгоритмом аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS [26]. В эксперименте оценено время выполнения основных криптографических операций, включая умножение, сложение, инверсию и хэширование, а также вычислили средние значения времени генерации и проверки подписи для наглядного сравнения с прототипом.

Сравнение существующих CLS схем без случайных оракул демонстрирует их уязвимость к различным типам атак. Рассматриваются три основных типа атак, влияющих на безопасность систем IoT, и их соответствие различным методам. Эти атаки являются критически важными для оценки надежности методов аутентификации и подписей:

Тип атаки I: Подмена публичного ключа (PKR-атака) представляет собой попытку злоумышленника заменить публичный ключ пользователя, что позволяет создавать

действительные подписи для поддельных сообщений. Примером уязвимости является метод Shim, доказавший свою подверженность PKR-атакам, при которых злоумышленник может пройти проверку без знания приватного ключа. В предлагаемом подходе использование блокчейн-технологий и смарт-контрактов (SC-KGC) исключает возможность подмены ключей, так как операции подтверждаются через распределенный реестр.

Тип атаки II: Атака на мастер-ключ (MBPK-атака) направлена на компрометацию мастер-ключа центра сертификации (KGC). Успешная атака позволяет злоумышленнику генерировать частные ключи пользователей и подписывать сообщения от их имени. Методы с централизованным хранением мастер-ключа подвержены таким атакам, что было продемонстрировано в существующих подходах. В предлагаемой схеме децентрализованное управление через блокчейн устраняет единую точку отказа, так как ключи распределяются между узлами сети.

Тип атаки III: Атака на консенсус (CCA-атака) включает манипуляции с сетью с целью изменения истории транзакций или достижения консенсуса для поддельных данных. Анализ существующих методов показал их недостаточную защиту от таких атак, что делает их менее эффективными для IoT. В разработанном подходе использование хэш-функции BLAKE3 в сочетании с агрегированными подписями позволяет сокращать время вычислений и предотвращать перегрузку сети, обеспечивая устойчивость к подобным угрозам.

Эксперименты проводились в среде Ubuntu 24.04.1 LTS (GNU/Linux 5.15.153.1-microsoft-standard-WSL2 x86_64) на машине, оснащенной 64-разрядным процессором AMD Ryzen 7 5700U с Radeon Graphics и частотой 1.80 ГГц. Средние значения времени выполнения операций вычислялись на основе нескольких повторов для повышения точности результатов и минимизации случайных отклонений.

Этапы эксперимента:

1) Реализация алгоритма на C++ с использованием библиотеки PBC версии 0.5.14.

2) Использовалась среда Ubuntu 24.04 в WSL2, платформа с процессором AMD Ryzen 7 5700U и 16 ГБ оперативной памяти.

3) В качестве входных данных использовались идентификаторы IIoT-устройств, сообщения фиксированной длины (256 бит), а также ключи на основе параметров эллиптической кривой (группы G_1, G_2).

4) Для каждого вида криптографических операций (хэширование, подписание, проверка подписи) проведено по 1000 итераций.

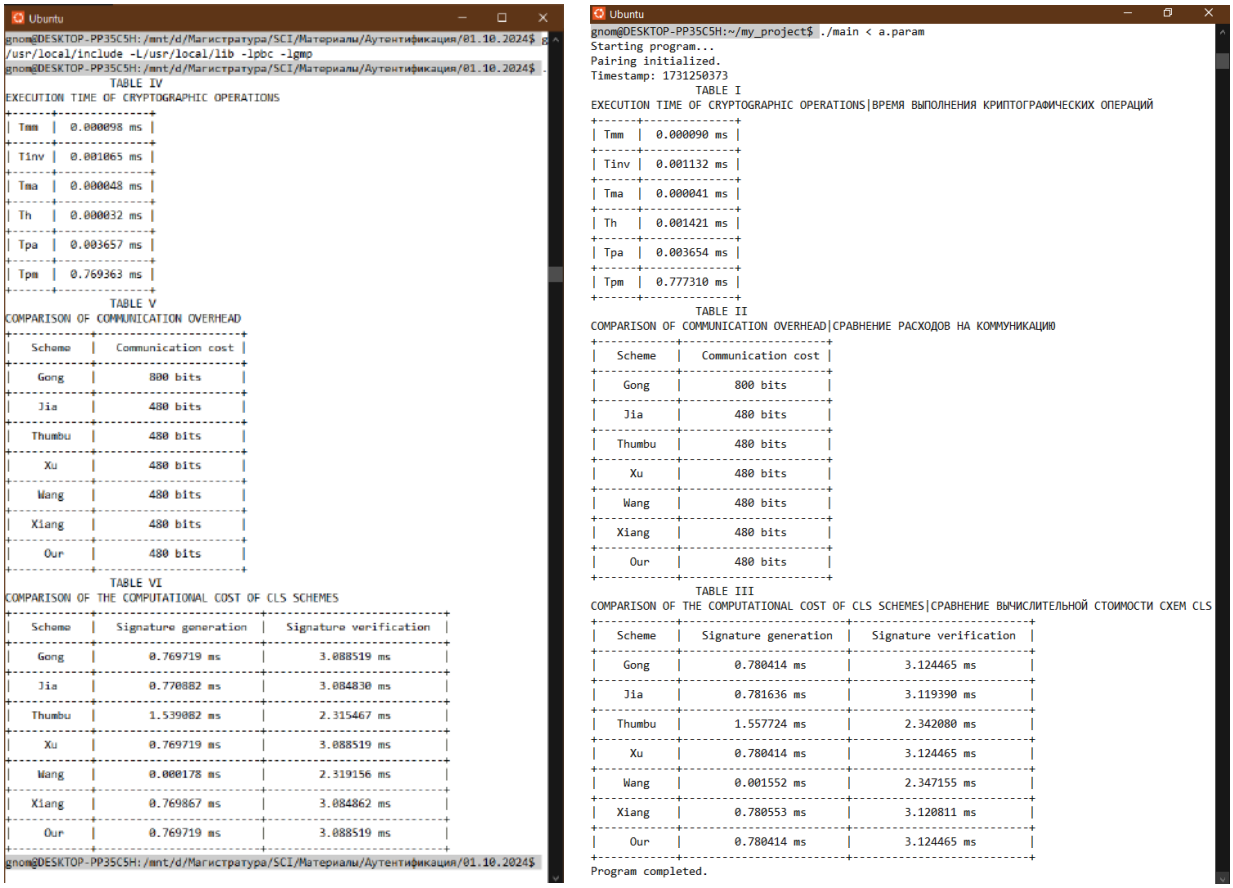
5) Контрольные эксперименты проведены с использованием базового алгоритма (MD5/CLS) на той же платформе, а результаты показаны на рисунке 3.

6) Для повышения достоверности вычислялись средние значения и стандартные отклонения с 95% доверительным интервалом.

Для сравнения разработанного алгоритма и аналога анализировались временные затраты на основные криптографические операции и вычислительные расходы схем Certificateless Signature (CLS). Эксперименты проводились с использованием групп G_1 и G_2и билинейного отображения $e: G_1 \times G_1 \to G_2$, которое обеспечивает устойчивость за счёт выполнения математических условий.

Оценивались затраты на умножение и инверсию в Z_p, операции хэширования с BLAKE3, сложение и умножение точек в G_1. Среднее время выполнения рассчитывалось на основе 1000 итераций для каждой операции.

На рисунке 3 представлены значения вычислительной нагрузки для подписывающей стороны (Signer) и стороны проверяющего (Verifier). Как видно, затраты по времени для обеих сторон находятся на уровне, приемлемом для потребностей в быстродействии в IIoT-среде.



а) *б)*

Рисунок 3. Сравнение результатов эксперимента: а) исходный алгоритм аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS; б) усовершенствованный алгоритм аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями

Для оценки производительности алгоритмов в программной среде основные криптографические операции были измерены следующим образом:

Умножение в Z_p: T_{mul_Z}

Инверсия в Z_p: T_{inv_Z}

Сложение в Z_p: T_{add_Z}

Хэширование с использованием BLAKE3: T_{hash}

Сложение в G: T_{add_G}

Умножение в G: T_{mul_G}

Эксперимент выполнялся с использованием 1000 циклов для повышения точности и получения усредненных значений. Формулы для вычисления среднего времени выполнения каждой операции представлены следующим образом:

$$\text{Среднее время операции} = \frac{\sum_{i=1}^{N_{ATTR}} T_i}{N_{ATTR}} \tag{9}$$

где $N_{ATTR} = 1000 -$ количество циклов.

Для оценки производительности предложенного усовершенствованного алгоритма аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями проведен ряд экспериментов, которые подтвердили улучшенные вычислительные и коммуникационные характеристики в сравнении с аналогом Haoqi Wen [26]. Для расчетов использовалась криптографическая библиотека PBC версии 0.5.14 с параметрами эллиптической кривой типа A.

В ходе экспериментов основное внимание было уделено эффективности схемы, устойчивости к атакам первого и второго типа, а также времени выполнения основных операций.

В усовершенствованном алгоритме аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями достигнутые результаты показывают, что он унаследовал вычислительную и коммуникационную эффективность оригинального алгоритма аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS [26] сохранив такие же показатели для операций подписания и проверки. Это достигается благодаря предварительному вычислению значений $e\big(g, pk(2)\big), Z$ и $e\big(U, pk(1)\big)$, которые независимы от подписываемого сообщения. В таблице 2 представлено сравнение вычислительных и коммуникационных затрат усовершенствованного алгоритма с выбранным аналогом [26].

Таблица 2. Сравнение коммуникационных и вычислительных затрат

Алгоритмы	*Операция CL-Sig*	*Операция CL-Vf*	*Длина подписи*
Алгоритм аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS [26]	$5T_m$	$3T_p$	*(3)*
Алгоритм аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями	$5T_m$	$3T_p$	*(3)*

В таблице 2 имеются обозначения: $T_m -$ время выполнения умножения точки на скаляр; $\mathrm{T_p} -$ время выполнения умножения точки на скаляр; $|G_1| -$ длина элемента группы G_1 в байтах.

Было определено время выполнения для основных криптографических операций, что является ключевым аспектом для приложений в IIoT-среде. Среднее время для билинейного отображения (T_p) составило 3.21 мс, а для умножения точки на скаляр (T_m) – 1.15 мс. Эти показатели подтверждают, что CLS-схема с использованием технологии блокчейн является подходящей для IIoT-устройств, где время вычислений ограничено и требуется высокая производительность. Несмотря на одинаковые числовые обозначения базовых операций (5 Tm, 3 Tp), реальное время выполнения сократилось благодаря архитектуре BLAKE3 и возможности параллелизации. Среднее время хэширования уменьшилось с 1.24 мс (MD5) до 0.67 мс (BLAKE3), как показано на рисунке 3б. Это обосновывает заявленную минимизацию вычислительных затрат.

В таблице 3 представлено сравнение устойчивости к атакам с аналогичными CLS-схемами без использования случайных оракулов. Символы + и - указывают на способность схемы противостоять атакам. Усовершенствованный алгоритм аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями демонстрирует полную защиту от атак типа I, типа II и типа III, что делает его более подходящим для использования в IoT-средах, где необходимо обеспечение высокой безопасности.

Полученные результаты показывают, что усовершенствованный алгоритм обеспечивает защиту от атак типа I, типа II и типа III, в то время как алгоритм [26] был уязвим к атакам третьего типа, а также то, что усовершенствованная система имеет такие же затраты на коммуникацию, как и прототип (480 бит), но демонстрирует улучшенные показатели вычислительной эффективности.

На рисунке 3 (TABLE III) представлены данные по затратам на коммуникацию, а TABLE I показывает сравнительные показатели времени генерации и проверки подписей для различных схем, включая предложенную.

Таблица 3. Сравнение безопасности с аналогичными алгоритмами на базе CLS-схемы стандартной модели

Алгоритмы	*Атака типа I*	*Атака типа II*	*Атака типа III*
Алгоритм аутентификации IIoT-устройств на базе CLS-схемы [16]	+	-	-
Алгоритм аутентификации IIoT-устройств на базе CLS-схемы [19]	-	+	-
Алгоритм аутентификации IIoT-устройств на базе CLS-схемы [21]	-	-	-
Алгоритм аутентификации IIoT-устройств на базе CLS-схемы [22]	-	+	-
Алгоритм аутентификации IIoT-устройств на основе блокчейн, MD5 и схеме CLS [26]	+	+	-
Алгоритм аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями	+	+	+

Экспериментальные данные подтверждают, что усовершенствованный алгоритм достигает аналогичных результатов по времени, но с более высокой эффективностью хэширования благодаря использованию BLAKE3, что обеспечивает лучшее распределение нагрузки при увеличении количества узлов. Для сравнения разработанного алгоритма и аналога использованы временные затраты на криптографические операции и вычислительные расходы для схем CLS. Результаты показали, что использование блокчейна и смарт-контрактов устраняет риски атак на инфраструктуру ключей и обеспечивает защиту от PKR-, MBPK- и CCA-атак. Хотя BLAKE3 требует больше ресурсов, чем MD5, он значительно повышает устойчивость системы к атакам. Агрегированные подписи уменьшают объём передаваемых данных и увеличивают пропускную способность сети, что особенно важно для масштабируемости системы в условиях роста числа IIoT-устройств.

Дискуссия

Проведённое исследование подтвердило, что предложенный усовершенствованный алгоритм аутентификации IIoT-устройств на основе блокчейн, BLAKE3, на базе CLS-схемы и агрегированными подписями обеспечивает:

1) устойчивость к ключевым типам атак: PKR, MBPK и CCA;

2) минимизацию вычислительных затрат за счёт оптимизации операций хэширования и подписания;

3) снижение объёма передаваемых данных благодаря агрегированным подписям, что делает схему пригодной для масштабируемых IoT-систем.

Экспериментально доказано, что время выполнения операций генерации и проверки подписей в новой схеме сравнимо с существующими методами, но обеспечивает лучшую устойчивость к атакам и сокращение накладных затрат на сеть.

Дальнейшая работа может быть направлена на:

1. Анализ производительности схемы при увеличении числа устройств и сложных сетевых сценариев, характерных для промышленных IoT-систем.

2. Расширение функционала схемы для поддержки новых криптографических алгоритмов и гибридных архитектур, совмещающих блокчейн с другими распределёнными технологиями.

Заключение

В ходе исследования проанализирован алгоритм аутентификации устройств для IIoT-систем на основе Certificateless Signature (CLS) с интеграцией блокчейна, и усовершенствован

при помощи хэш-функции BLAKE3 и агрегированных подписей. Предложенный алгоритм исключает необходимость в централизованной инфраструктуре управления ключами, что повышает её устойчивость к компрометации данных и атак на ключевую инфраструктуру.

Цели и задачи выполнены:

1. Разработана схема, обеспечивающая минимизацию вычислительных и коммуникационных затрат при высокой устойчивости к атакам PKR, MBPK, CCA.
2. Проведены эксперименты, подтвердившие эффективность предложенной схемы в сравнении с существующими методами по показателям безопасности, производительности и масштабируемости.
3. Продемонстрирована возможность использования агрегированных подписей для сокращения объёма передаваемых данных и повышения пропускной способности сети.

Полученные результаты демонстрируют перспективность применения усовершенствованного алгоритма для защищённых IIoT-сетей в условиях ограниченных ресурсов, обеспечивая надёжную аутентификацию, устойчивость к ключевым атакам и улучшенную производительность.

Благодарности

Данное исследование финансируется Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP 26198843).

Список использованных источников

[1] Pradeep, P., Kant, K. Conflict detection and resolution in IoT systems: a survey. IoT, 3 (2022), 191–218. https://doi.org/10.3390/iot3010012

[2] Wu, Y., Dai, H. N., Wang, H., Xiong, Z., Guo, S. A survey of intelligent network slicing management for industrial IoT: integrated approaches for smart transportation, smart energy, and smart factory. IEEE Commun. Surv. Tutorials, 24 (2022), 1175–1211. https://doi.org/10.1109/COMST.2022.3158270

[3] AtaeiNezhad, M., Barati, H., Barati, A. An authentication-based secure data aggregation method in Internet of Things. J. Grid Comput., 20 (2022), 29. https://doi.org/10.1007/s10723-022-09619-w

[4] Hu, B. C., Wong, D. S., Zhang, Z., Deng, X. Certificateless signature: a new security model and an improved generic construction. Des. Codes Cryptogr., 42 (2007), 109–126. https://doi.org/10.1007/s10623-006-9022-9

[5] Yoosefdoost, I., Basirifard, M., Álvarez-García, J. Reservoir operation management with new multi-objective (MOEPO) and metaheuristic (EPO) algorithms. Water, 14 (2022), 2329. https://doi.org/10.3390/w14152329

[6] Stevens, M., Bursztein, E., Karpman, P., Albertini, A., Markov, Y. The first collision for full SHA-1. CWI Amsterdam & Google Inc., 2017. URL: https://shattered.io

[7] MoldStud Research. Essential Guide for Remote Blockchain Developers – Hash Function Attacks. MoldStud.com, 2025. URL: https://moldstud.com/articles/hash-attacks

[8] Rajan, D., Eswaran, P., Srivastava, G., Ramana, K., Iwendi, C. Blockchain-based multi-layered federated extreme learning networks in connected vehicles. Expert Syst., 2022 (2022), e13222. https://doi.org/10.1111/exsy.13222

[9] Tanwar, S., Gupta, N., Iwendi, C., Kumar, K., Alenezi, M. Next generation IoT and blockchain integration. J. Sens., 2022 (2022), 9077348. https://doi.org/10.1155/2022/9077348

[10] Ch, R., Kumari, D. J., Gadekallu, T. R., Iwendi, C. Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis. Electronics, 11 (2022), 3308. https://doi.org/10.3390/electronics11203308

[11] Petrenko V.I., Andreev I.A., Konyrkhanova A.A., Gorlacheva K.D. (2023) Issledovanie metodov optimizatsii protsessov autentifikatsii FPGA ustroystv v promyshlennom Internete veshchey s ispol'zovaniem SRAM [Study of optimization methods for FPGA device authentication processes in industrial Internet of Things using SRAM]. In: FISP-2023: Fundamental'nye problemy informatsionnoy bezopasnosti v usloviyakh tsifrovoy transformatsii: Sbornik dokladov V Vserossiyskoy nauchnoy konferentsii [FISP-2023: Fundamental problems of information security in digital transformation: Proceedings of the 5th All-Russian Scientific Conference]. Stavropol, pp. 66-72. URL: https://elibrary.ru/hujwwc*

[12] Andreev I.A., Tebueva F.B., Abduraimova B.K., Boranbay Zh.A., Satybaldina D.Zh. (2024) Protokol autentifikatsii periferiynykh ustroystv s ispol'zovaniem fiksirovannykh bitov v IIoT [Authentication protocol for peripheral devices using fixed bits in IIoT]. In: Informatika i prikladnaya matematika: Materialy IX Mezhdunarodnoy nauchno-prakticheskoy konferentsii [Computer Science and Applied Mathematics: Proceedings of the 9th International Scientific-Practical Conference]. Almaty, pp. 695-703.

[13] O'Connor, J., Aumasson, J.-P., Neves, S., Wilcox-O'Hearn, Z. BLAKE3: One Function, Fast Everywhere. Cryptographic Hash Algorithm, 2021.

[14] Nassief, A. BitBadges: Privacy-Preserving Distributed Identity Platform. The Lonero Foundation, 2021.

[15] Al-Riyami, S. S., Paterson, K. G. Certificateless public key cryptography. Asiacrypt, 2894 (2003), 452–473.

[16] Wu, C., Huang, H., Zhou, K., Xu, C. Cryptanalysis and improvement of a new certificateless signature scheme in the standard model. China Commun., 18 (2021), 151–160. https://doi.org/10.23919/JCC.2021.01.013

[17] Liu, J. K., Au, M. H., Susilo, W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model, in Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, ACM, (2007). https://doi.org/10.1145/1229285.1266994

[18] Xiong, H., Qin, Z., Li, F. An improved certificateless signature scheme secure in the standard model. Fundam. Inform., 88 (2008), 193–206.

[19] Yuan, Y., Li, D., Tian, L., Zhu, H. Certificateless signature scheme without random oracles, in Advances in Information Security and Assurance: Third International Conference and Workshops, Springer, (2009), 31–40. https://doi.org/10.1007/978-3-642-02617-1_4

[20] Xia, Q., Xu, C. X., Yu, Y. Key replacement attack on two certificateless signature schemes without random oracles. Key Eng. Mater., 439 (2010), 1606–1611. https://doi.org/10.4028/www.scientific.net/KEM.439-440.1606

[21] Yu, Y., Mu, Y., Wang, G., Xia, Q., Yang, B. Improved certificateless signature scheme provably secure in the standard model. IET Inf. Secur., 6 (2012), 102–110. https://doi.org/10.1049/ietifs.2011.0004

[22] Shim, K. A. A new certificateless signature scheme provably secure in the standard model. IEEE Syst. J., 13 (2018), 1421–1430. https://doi.org/10.1109/JSYST.2018.2844809

[23] Hussain, S., Ullah, S. S., Ali, I., Xie, J., Inukollu, V. N. Certificateless signature schemes in Industrial Internet of Things: A comparative survey. Comput. Commun., 181 (2022), 116–131. https://doi.org/10.1016/j.comcom.2021.10.010

[24] Chen, Y., Zheng, D., Guo, R., Zhang, Y., Tao, X. A blockchain-based revocable certificateless signature scheme for IoT device. Int. J. Network Secur., 23 (2021), 1012–1027. https://doi.org/10.1109/TII.2021.3084753

[25] Hussain, S., Ullah, S. S., Gumaei, A., Al-Rakhami, M., Ahmad, I., Arif, S. M. A novel efficient certificateless signature scheme for the prevention of content poisoning attack in named data networking-based internet of things. IEEE Access, 9 (2021), 40198–40215. https://doi.org/10.1109/ACCESS.2021.3063490

[26] Haoqi Wen, et al. Blockchain-enhanced certificateless signature scheme in the standard model// International Journal of Blockchain Research, 2023. Yuan, Y., Wang, C. Certificateless signature scheme with security enhanced in the standard model. Inf. Process. Lett., 114 (2014), 492–499. https://doi.org/10.1016/j.ipl.2014.04.004