УДК 004.82
МРНТИ 28.23.29

https://doi.org/10.55452/1998-6688-2025-22-3-75-84

[1]Капалова Н.А.,
к.т.н., ассоциированный профессор, ORCID ID: 0000-0001-9743-9981,
e-mail: nkapalova@mail.ru
[2]*Абишева А.Ж.,
докторант, ORCID ID: 0000-0002-6557-3067,
*e-mail: ak_maral@mail.ru

[1]Институт информационных и вычислительных технологий КН МНВО РК,
г. Алматы, Казахстан,
[2]Казахский национальный университет им. аль-Фараби,
г. Алматы, Казахстан

СОВРЕМЕННЫЕ ПОДХОДЫ К УПРАВЛЕНИЮ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ И ПРИМЕНЕНИЮ ЦИФРОВОЙ ПОДПИСИ

Аннотация

В данной работе рассматривается проблема управления криптографическими ключами и подчеркивается важность разработки эффективных протоколов, обеспечивающих безопасность и аутентичность обмена ключами между участниками криптографической системы. В качестве одного из результативных и практичных методов проверки подлинности подписи рассматривается схема Шнорра, обладающая свойствами, такими как целостность, невозможность отказа от подписи и защита от повторной передачи сообщений. Также описана модификация данной схемы и процесс формирования непозиционной полиномиальной системы счисления, а также вычисление значений с использованием выбранных оснований. Применение непозиционной полиномиальной системы счисления при разработке нетрадиционных алгоритмов для электронной цифровой подписи и управления ключами в криптографических системах может существенно повысить их надежность и эффективность. Кроме того, рассматривается возможность повышения устойчивости предложенной схемы к квантовым атакам.

Ключевые слова: криптография, управление криптографическими ключами, непозиционные полиномиальные системы счисления, цифровая подпись, схема Шнорра.

Введение

В условиях современной цифровой трансформации, охватывающей все сферы жизнедеятельности, вопросы информационной безопасности становятся особенно важными. Организации сталкиваются с необходимостью защиты своих данных и обеспечения безопасности цифровых процессов, и в этом контексте криптографические ключи играют ключевую роль в обеспечении безопасности шифрования, цифровых подписей и аутентификации. Однако эффективное использование криптографических ключей требует не только внедрения современных криптографических алгоритмов, но и внимательного подхода к их управлению. Для обеспечения надежной защиты конфиденциальной информации и систем организациям необходимо уделять особое внимание правильному управлению ключами. В этой статье рассматриваются основные вопросы и проблемы управления ключами, где алгоритмы шифрования известные, но используемые ключи должны быть или секретными, или открытыми, оставаясь при этом неотъемлемой частью криптографических технологий.

Часто в криптографических приложениях наиболее уязвимым звеном является, как правило, управление ключами. Так как использование криптографии при безопасном хранении, об-

мене ключами и применении между пользователями представляет сложность. Это доказывает, что даже надежные системы защиты могут быть компрометированы по причине уязвимого управления ключами, ведь вся безопасность находится в самих ключах [1].

Эффективная система управления криптографическими ключами в сочетании с современными методами шифрования позволяет обеспечить надежную защиту информационных систем организаций. Процесс управления ключами включает в себя такие этапы, как их генерация, распространение, обновление, отзыв, хранение, резервное копирование и восстановление, импорт и экспорт, контроль использования, установление срока действия и уничтожение. Подходы к управлению ключами зависят от их типа – симметричного или асимметричного. В настоящее время исследования в этой области сосредоточены на стандартизации и обеспечении совместимости систем управления ключами [2].

Актуальность управления ключами в криптографических системах сегодня обусловлена ростом киберугроз, утечек данных и сложностью современных атак, что требует надежных методов защиты конфиденциальной информации. Развитие технологий, таких как облачные вычисления и Интернет вещей, наряду с увеличением числа пользователей и алгоритмов шифрования порождает необходимость в эффективных протоколах аутентификации и безопасного обмена ключами, а ужесточение нормативных требований обязывает организации соответствовать высоким стандартам криптографической безопасности.

Таким образом, в современном мире, где безопасность данных и конфиденциальность информации имеют первостепенное значение, управление ключами в криптографических системах остается одной из главных областей исследований и практики. Оно обеспечивает основу для создания надежных механизмов защиты в условиях постоянно усложняющихся угроз.

Основные проблемы управления криптографическими ключами включают зависимость от надежности центров распределения (KDC), где компрометация может привести к утечке ключей, и вопросы масштабируемости, поскольку физическая доставка ключей не подходит для больших сетей, что часто требует использования доверенных посредников. Дополнительно частые изменения ключей для ограничения потенциального ущерба и необходимость разделения мастер-ключей и сеансовых ключей добавляют сложности, так как неправильное управление может создать уязвимости даже при использовании надежных алгоритмов шифрования.

Одной из основных задач в асимметричной криптографии, в том числе системы электронной цифровой подписи, является управление открытыми ключами. Так как открытый ключ доступен абсолютно всем пользователям, необходимо подтверждение принадлежности идентификатору и его подлинности. Для этого необходимо предоставить доступ к настоящим открытым ключам, обеспечить защиту и предотвратить возможность подмены их злоумышленниками и наладить процесс отзыва в случае небезопасного хранения ключей.

Защита открытых ключей от подмены обеспечивается посредством использования сертификатов, которые предоставляют достоверность информации открытого ключа владельца с помощью цифровой подписи доверенного лица. Существуют централизованные системы сертификации и децентрализованные системы сертификации. В децентрализованных системах пользователи формируют сеть доверия, подписывая сертификаты знакомых и проверенных лиц, в то время как централизованные системы полагаются на специализированные центры сертификации (CA), принадлежащие авторитетным организациям.

Центр сертификации отвечает за создание закрытого ключа, выпуск собственного сертификата, генерацию сертификатов для конечных пользователей с последующим заверением цифровой подписью, а также управляет процессом отзыва устаревших или скомпрометированных сертификатов и ведет реестр активных и отозванных ключей. Пользователи могут обращаться в такие центры для получения личного сертификата, проверки сертификатов других пользователей или уточнения информации о статусе ключей.

Материалы и методы

Существует множество зарубежных исследований в области управления сертификатами ключей в криптографических системах, где ключевое место занимает инфраструктура открытых ключей (PKI), обеспечивающая эффективное управление цифровыми сертификатами и открытыми ключами. Для полного понимания принципов работы систем PKI необходимо ознакомиться с основами криптографии с открытым ключом, поскольку эти системы не только используют этот подход, но и строят свою функциональность на его базе. Несмотря на разнообразие криптографических алгоритмов, для понимания работы PKI достаточно рассмотреть два основных процесса: цифровую подпись и шифрование.

Зарубежные исследования сосредоточены на управлении жизненным циклом сертификатов, где автоматизация процессов выпуска, обновления, отзыва и хранения позволяет повысить безопасность и эффективность системы. Изучаются модели доверия и иерархии сертификации, что включает анализ как иерархических, так и сетевых структур, а также методы управления доверительными отношениями между различными удостоверяющими центрами. Разрабатываются эффективные механизмы отзыва сертификатов, включая использование списков отозванных сертификатов (CRL) и протоколов OCSP, для своевременного исключения скомпрометированных или устаревших сертификатов. Кроме того, исследователи уделяют внимание безопасности и защите PKI, выявляя уязвимости систем и разрабатывая методы их устранения, а также обеспечивая целостность и конфиденциальность сертификатов.

В зарубежной работе [3] рассматриваются протоколы управления сертификатами в рамках инфраструктуры открытых ключей (PKI), включая процессы регистрации, обновления и отзыва сертификатов. Отмечается, что удостоверяющие центры (CA) сталкиваются с проблемами масштабируемости по мере роста числа пользователей и сертификатов, а процедура обновления в крупных системах требует значительных ресурсов. Несмотря на общее описание процессов управления сертификатами, вопросы масштабируемости в условиях глобальных развертываний остаются нерешенными.

Документ [4] содержит профиль использования сертификатов X.509 и списков отозванных сертификатов (CRL) в интернет-среде, а также определяет требования к процессу управления сертификатами. Одной из ключевых проблем, обозначенных в работе, является увеличение размера CRL, что замедляет процесс проверки их актуальности. Хотя обсуждаются механизмы CRL и OCSP, эффективные решения для масштабируемых сетевых инфраструктур не предлагаются. Также альтернативы, такие как использование короткоживущих сертификатов, пока не получили широкого распространения.

В исследовании [5] анализируются политики сертификации и подходы к управлению сертификатами в PKI, а также их влияние на безопасность систем. Несмотря на предложенную стратегию управления сертификатами, не учитываются современные вызовы, связанные с облачными и IoT-средами, где особенно важна поддержка динамического обновления сертификатов без прерывания работы сервисов. Несмотря на достижения в области управления ключевой информацией, остается ряд нерешенных задач, включая дальнейшую стандартизацию PKI, обеспечение масштабируемости, ускорение отзыва сертификатов, интеграцию с новыми технологиями (такими как IoT, облачные платформы и блокчейн), а также усиление защиты удостоверяющих центров.

В данной работе [6] рассматриваются вопросы управления сертификатами и ключами электронных подписей (ЭЦП) в рамках специализированных информационных систем (ИСС), с особым акцентом на системы электронного документооборота (СППЭД). Описывается их роль в обеспечении безопасности и целостности информации, а также основные функции, такие как юридическая значимость электронных сообщений, установление достоверного времени создания, определение авторства документов, централизованный контроль доступа и управление ключами ЭЦП. Особое внимание уделяется методам защиты от компрометации ключей, надежной идентификации и регистрации пользователей, а также процедурам выпу-

ска, отзыва и проверки статуса сертификатов. Автор подчеркивает важность ЭЦП для предотвращения подделок электронных документов, что способствует созданию доверительной цифровой среды для участников документооборота. Однако остаются открытыми вопросы, связанные с полнотой и гибкостью методов защиты от новых угроз, а также с необходимостью практического тестирования предложенных схем, что открывает новые возможности для будущих исследований в области криптографии и защиты информации.

В диссертации [7] рассматривается разработка метода и создание протокола утверждаемой групповой электронной цифровой подписи (ЭЦП), а также протокола коллективной ЭЦП, обладающего улучшенной безопасностью и не требующего использования вспомогательных открытых ключей. Предложен метод для построения протоколов комбинированной коллективной ЭЦП, основанный на вычислениях по простому модулю и отличающийся выполнением дополнительной операции возведения в целочисленную степень по трудно разложимому модулю. Особое внимание уделяется маскировке открытых ключей участников, которые представляют собой значения однонаправленной функции, зависящей от открытых ключей подписантов и секретного ключа руководителя группы. Это обеспечивает повышение уровня безопасности, который предоставляет данный протокол.

Электронная цифровая подпись (ЭЦП) представляет собой дополнительный элемент, прикрепляемый к электронному документу или сообщению, который может быть сформирован исключительно владельцем закрытого ключа – секретной информации. С помощью специального алгоритма можно установить соответствие между данной подписью и закрытым ключом подписывающего, что подтверждает ее подлинность. Под ЭЦП также понимается комплекс криптографических алгоритмов и правил, предназначенных для создания и проверки цифровых подписей [8].

Рассмотрим одну из известных схем электронной цифровой подписи – протокол Шнорра, который был создан криптографом Клаусом Шнорром в 1989 г. [9] и используется для обеспечения аутентификации сообщений и цифровых подписей. Цифровые подписи – это математические алгоритмы, используемые для проверки целостности и подлинности цифровых сообщений, которые доказывают, что они отправлены именно тем пользователем и не было компрометации при передаче.

Нужно отметить, что схема Шнорра имеет ряд преимуществ перед другими протоколами цифровой подписи, а именно: она обеспечивает высокую устойчивость к атакам и исключает возможность подмены сообщений, так как основана на неразрешимости проблем дискретного логарифмирования. Короткие цифровые подписи, создаваемые по схеме Шнорра, способствуют эффективной передаче данных, в отличие от более громоздких подписей, а используемые случайные числа при создании подписи делают взлом методом перебора сложным. При этом следует избегать как повторного использование случайного значения r, чтобы не возник взлом секретного ключа. Данное требование располагает известную теорему сравнений о существовании обратного элемента. Схему Шнорра можно использовать в распределенных сетях для проверки аутентификации нескольких пользователей в системах безопасности коллективной подписи. Для уникальности идентификаторов сообщений схема Шнорра использует криптографические хеш-функции, чтобы защитить данные от подделки и обеспечить целостность [10].

Важно отметить, что квантовые вычисления представляют угрозу безопасности для схемы Шнорра, которая основана на задаче дискретного логарифмирования. Квантовые алгоритмы, например алгоритм Шора, способны эффективно решать эту задачу, что ослабляет защиту схемы Шнорра перед квантовыми атаками. Тем не менее, используя методы защиты, такие как нулевое разглашение информации, можно разработать подходы, способные повысить безопасность данной схемы в постквантовой среде.

Несмотря на уязвимость дискретного логарифма перед квантовыми атаками, схема Шнорра остается полезной в гибридных системах, где применяются дополнительные механизмы защиты, включая хеширование сообщений и другие методы предотвращения модификации

данных. Это делает ее перспективной для интеграции с квантово-устойчивыми протоколами [11]. Дальнейшие исследования необходимы для разработки эффективных способов адаптации таких схем к вызовам квантовых технологий.

В 1970-х годах разрабатывались алгоритмы, основанные на модульной арифметике, такие как RSA (1977), использующий операции возведения в степень по модулю. Однако в этот период системы остаточных классов (СОК) еще не рассматривались в контексте криптографии. Далее появились первые исследования, посвященные применению СОК для ускорения вычислений в криптографических алгоритмах. Одним из первых направлений стало использование СОК в схемах быстрого вычисления модульных операций (остатков от деления). Со временем СОК начала применяться в аппаратных криптографических устройствах, включая ускорители RSA и криптографические процессоры, где она позволяла выполнять вычисления параллельно. После этого начались исследования по использованию СОК в эллиптической криптографии и гомоморфном шифровании. В настоящее время СОК, а также другие нелинейные позиции систем счисления (НПСС) изучаются в контексте постквантовой криптографии, облачных вычислений и криптографических методов, ориентированных на искусственный интеллект, включая интеграцию с нейронными сетями. Несмотря на то что применение НПСС в криптографии начало развиваться еще раньше, наибольший интерес к этой теме возник в конце 1990-х – начале 2000-х годов, когда стало очевидно, что СОК способна значительно повысить эффективность криптографических вычислений.

Алгоритм Шнорра – это криптографический алгоритм, который может быть использован в контексте управления сертификатами, особенно для создания цифровых подписей. Он основан на идее доказательства с нулевым разглашением, позволяя пользователю доказать владение некоторой информацией без раскрытия самой информации.

Приведем краткое описание алгоритма [12]:

Генерация ключей

p, q – простые числа, где $p - 1$ делит q; g порождающий элемент группы Z_p^*; k – случайное число, $1 < k < q$; $y = g^k mod\ p$ – создание открытого ключа. Открытый ключ (p, q, g, y), секретный ключ k.

Вычисление подписи для сообщения M включает следующие шаги:

1. Генерируется случайное число, которое действует как одноразовый секретный ключ r, $1 < r < q$.
2. Вычисляется $R = g^r mod\ p$.
3. К сообщению M присоединяется число R и от значения $H: E = H(M||R)$ вычисляется H хеш-функция. Значение E – это первая часть подписи. Здесь хеш-функция принимает сообщение произвольной длины на вход.
4. Вычисляется вторая часть подписи: $S = r + kE\ mod\ q$, здесь k – секретный ключ.

Проверка подписи.

1. R' вычисление: $R' = g^S y^{-E}\ mod\ p$.

$M||R'$ вычисляется хеш-значение $H: E' = H(M||R')$. Здесь хеш-функция возвращает фиксированный конкретной длины.

2. E и E' значения сравниваются. Если $E = E'$, тогда подпись считается верной.

Результаты и обсуждение

С учетом рациональных преимуществ алгоритма в данной работе предложена модификация схемы электронной цифровой подписи (ЭЦП) с применением непозиционной системы счисления. Алгоритм Шнорра рассматривается в контексте использования непозиционных полиномиальных систем счисления (НПСС), что позволяет повысить эффективность и криптостойкость криптографической схемы. Ниже представлены этапы модифицированного алгоритма Шнорра, реализованного на основе НПСС.

Генерация ключей. Производится формирование непозиционной полиномиальной системы счисления. В качестве рабочих оснований НПСС выбираются неприводимые двоичные полиномы $p_1(x)$, $p_2(x)$, … , $p_n(x)$ со степенями a_1, a_2, … , a_n, соответственно, при этом сумма степеней рабочих оснований должна совпадать с длиной ключа, то есть $\sum_{i=1}^{n} a_i = L$. Для выполнения китайской теоремы об остатках все основания должны быть различными.

Также выбираем $q_1, q_2, \dots, q_n$ – простые числа, удовлетворяющие условие $2^{a_i} - 1 = 0(mod\ q_i),\ i = \overline{1,n}$ (1<q_i < deg($p(x)$)-1), и для каждого основания $p_i(x)$ выбирается примитивный элемент (многочлен) $g_i(x)$, $0 < g_1(x), g_2(x), \dots, g_n(x) < P(x)$, удовлетворяющие условие $g_i(x)^{deg(p_i(x))-1} = 1\ mod\ p_i(x),\ i = \overline{1,n}$.

Выбираем случайные числа $k_i < q_i,\ i = \overline{1,n}$. Значения k_i должны храниться в секрете, так как это закрытый ключ $ЗК = \{k_i\}$.

Для каждого рабочего основания вычисляется выражение
$y_i(x) = g_i(x)^{k_i} mod\ p_i(x),\ i = \overline{1,n}$.

Открытый ключ $ОК = \{P, Q, G, Y\}$, то есть $P = \{p_1(x), p_2(x), \dots, p_n(x)\}$, $Q = \{q_1, q_2, \dots, q_n\}$, $G = \{g_1(x), g_2(x), \dots, g_n(x)\}$, $Y = \{y_1(x), y_2(x), \dots, y_n(x)\}$.

Подпись

A: Для подписи выбирает $r_i < q_i$ случайные числа, $R_i = g_i(x)^{r_i} mod\ p_i(x),\ i = \overline{1,n}$

$A \to B$: вычисляет первую часть подписи $E_i = H(M||R_i),\ i = \overline{1,n}$

A: вычисляет вторую часть подписи $S_i = r_i + k_i * E_i mod\ q_i,\ i = \overline{1,n}$

$A \to B$: Отправляет сообщение M с подписью (E_i, S_i).

Проверка подписи

B: вычисляет $R_i' = g_i(x)^{S_i} y_i(x)^{E_i^{-1}} mod\ p_i(x)$,

$H(M||R_i) = E_i'$ вычисляет хэш-значение.

E_i и E_i' сравниваются. Если $E_i = E_i'$ равны, тогда подпись верна.

Структура представленного алгоритма ориентирована на генерацию криптографических параметров, необходимых для обеспечения безопасного обмена ключевой информацией. Корректное понимание и точная реализация соответствующих криптографических протоколов играют ключевую роль в поддержании надежности и целостности всей системы безопасности.

Схема электронной цифровой подписи Шнорра [13] отличается от алгоритма Эль-Гамаля рядом важных особенностей. Здесь главное преимущество – это размер подписи. Подпись по схеме Шнорра занимает всего 320 бит, при этом обеспечивает высокий уровень безопасности. Чтобы взломать такую подпись, злоумышленнику нужно выполнить как минимум 280 сложных вычислений, что делает взлом крайне трудным. Для сравнения: чтобы добиться такого же уровня защиты в схеме Эль-Гамаля, нужно использовать намного более длинные ключи – 2048 бит. Из-за этого итоговая подпись получается очень большой – около 4096 бит, что в десятки раз больше, чем у Шнорра. Поэтому схема Шнорра гораздо удобнее для практического применения, особенно там, где важны скорость и экономия места.

Схема Шнорра также обладает важным теоретическим свойством: хеш-функция вычисляется сразу после генерации рандомизационного параметра r. Благодаря этому можно логически доказать, что если существует эффективный алгоритм подделки подписи, то существует и эффективный алгоритм решения задачи дискретного логарифмирования [14]. Это подтверждает теоретическую обоснованность стойкости схемы, поскольку ее взлом сводится к решению задачи дискретного логарифмирования, лежащей в основе криптосистемы.

При внедрении квантовых технологий существуют серьезные потенциальные последствия для существующих криптографических систем, такие как уязвимость к квантовому криптоанализу. Существующие криптографические системы могут оказаться устаревшими, и потребуется переход на новые криптографические методы, которые обеспечивают безопасность даже в условиях квантовых атак. Это включает в себя разработку алгоритмов, осно-

ванных на задачах, которые пока не поддаются эффективным квантовым методам, например, задачи решетки или многомерных полиномов.

В связи с этим исследования и анализ в данной статье алгоритма ЭЦП с применением НПСС в управлении криптографическими сертификатами ключей в криптографических системах являются актуальными.

В НПСС основаниями являются не простые числа [15], а неприводимые многочлены над полем GF(2) [16]. Применение НПСС способствует сокращению длины ключей, а также улучшению как стойкости, так и эффективности непозиционных криптоалгоритмов. Эффективность достигается благодаря особенностям НПСС, которые позволяют выполнять все арифметические операции параллельно по модульным основаниям данной системы.

Методы, разработанные на основе таких систем, относятся к категории нетрадиционных криптографических алгоритмов. Использование НПСС в построении криптографических защитных механизмов для хранения и передачи информации значительно повышает их эффективность и стойкость [17].

В рамках нетрадиционных криптосистем процесс формирования ЭЦП осуществляется для сообщений фиксированной длины. В непозиционных криптоалгоритмах криптостойкость определяется не только длиной ключей, но и особенностями самого алгоритма цифровой подписи, включая полный секретный ключ. Кроме того, при увеличении порядка неприводимых многочленов с двоичными коэффициентами наблюдается их значительный рост, что дает широкий выбор полиномиальных оснований для обеспечения надежности системы.

Заключение

В условиях стремительной цифровой трансформации вопросы информационной безопасности, особенно в части управления криптографическими ключами, приобретают первостепенное значение. Эффективное управление ключами – критически важный элемент защиты данных и обеспечения безопасности цифровых процессов. Это требует внимательного подхода к таким операциям, как генерация, распространение, хранение и отзыв ключей. Среди ключевых вызовов можно выделить необходимость доверия к центрам ключевой инфраструктуры, обеспечение масштабируемости систем, а также регулярное обновление ключей. Все это подчеркивает важность разработки надежных, устойчивых к угрозам протоколов.

На фоне растущего числа киберугроз и широкого распространения новых технологий, таких как облачные вычисления, вопросы управления криптографическими ключами остаются в фокусе научных и практических исследований.

Для повышения эффективности криптографических операций в разработанной системе применяется НПСС (непозиционная система счисления). Все операции умножения и возведения в степень двоичных полиномов выполняются в рамках НПСС, что позволяет осуществлять вычисления параллельно по выбранным полиномиальным основаниям $p_1(x), p_2(x), \ldots p_n(x)$. Благодаря этому существенно увеличивается скорость выполнения операций.

На основе этих принципов была модифицирована схема асимметричного шифрования Шнорра. Предложенная система электронной цифровой подписи на базе НПСС реализуется в три этапа: 1) формирование системы НПСС; 2) генерация цифровой подписи; 3) проверка цифровой подписи.

Программные реализации такой криптосистемы способны конкурировать с аппаратными средствами за счет гибкости и высокой производительности. Использование НПСС с подбором подходящих оснований и соответствующих им примитивных неприводимых многочленов, а также персонализированных секретных ключей пользователей позволяет значительно повысить криптостойкость системы и ее эффективность при управлении криптографическими сертификатами.

На фоне быстрого прогресса квантовых технологий все более важной становится задача адаптации существующих криптографических схем к возникающим угрозам. Предлагаемая система может быть дополнительно усилена с использованием, например, решеточных подходов, что откроет путь к созданию квантово-устойчивых решений. Важно акцентировать внимание на необходимости разработки таких систем, которые не только противостоят квантовым атакам, но и остаются доступными и эффективными для широкого круга пользователей.

Информация о финансировании. Данная работа написана в рамках проекта BR24993052 «Разработка и исследование криптографических алгоритмов для защиты информации в системах с ограниченными ресурсами и оценка их стойкости».

REFERENCES

1 Fomina, I.A. Key management in cryptographic systems. Bulletin of the Nizhny Novgorod University named after N.I.Lobachevsky, 4(1),165–169 (2010).

2 Moise, G., Gangea, O. Intelligent Management of the Cryptographic Keys. Int. J. of Computers, Communications & Control, 4(1), 150–157 (2011).

3 Adams, C., & Farrell, S. Internet X.509 Public Key Infrastructure Certificate Management Protocols. RFC 2510. (1999). https://tools.ietf.org/html/rfc2510.

4 Housley, R., Polk, W., Ford, W., & Solo, D. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 3280. (2002). https://tools.ietf.org/html/rfc3280.

5 Chokhani, S., & Ford, W. Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 2527. (1995). https://tools.ietf.org/html/rfc2527.

6 Aristarkhov, I.V. Management of certificates of electronic signature verification keys. Diss. cand. of Technical Sciences. 2012 Moscow

7 Sinev, V.E. Methods of construction and development of practical group signature protocols and algebraic algorithms for protective transformations. Diss. cand. of Technical Sciences. St. Petersburg, 2017, 166 p.

8 Moldovyan, N.A., Moldovyan, A.A. Introduction to public key cryptosystems. Tutorial. St. Petersburg. "BHV-Petersburg", 2005

9 Schnorr, C.P. Efficient Signature Generation by Smart Cards. J. Cryptology, 161–174 (1991).

10 Kolesnikov P.V. Schnorr scheme in cryptography. Computer systems and networks: collection of articles of the 59th scientific conference of postgraduates, master's students and students, Minsk, April 17–21, 2023. Belarusian State University of Informatics and Radioelectronics (Minsk, 2023), pp. 393–396.

11 Watrous, Jo. Zero-knowledge against quantum attacks. Proceedings of the thirty-eighth annual ACM symposium on Theory of Computing. 296–305 (2008). https://doi.org/10.1145/1132516.1132560.

12 Schnorr, C.P. Efficient identification and signatures for smart cards. Advances in cryptology – CRYPTO'89. Springer-Verlag LNCS, 435, 239–252 (1990).

13 Moldovyan, D.N., Moldovyan, N.A. A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols. Proceedings of the international conference MMM-ACNS 2010. I. Kotenko and V. Skormin (Eds.): MMM-ACNS 2010, LNCS. Springer, Heidelberg. V. 6258. P. 183–194.

14 Pointcheval, D., Stern, J. Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 13, 361–396 (2000).

15 Akushsky I. Ya., Yuditsky D.I. Machine arithmetic in residual classes. M.: Sov.radio, 1968. 439 p.

16 Biyashev R.G. Development and research of methods for end-to-end increase of reliability in data exchange systems of distributed automated control systems: Dis. d. tech. sciences. M., 1985. 328 p.

17 Biyashev R.G., Kapalova N.A., Nysanbaeva S.E. Development and study of a modified Diffie-Hellman algorithm based on modular arithmetic. Actual problems of information technology security: Proc. III Int. scientific-practical. conf. Under the general editorship of O.N. Zhdanov, V.V. Zolotarev. Siberian State Aerospace University, Krasnoyarsk, September 9–11, 2009 (Krasnoyarsk, 2009), pp. 18–22.

[1]Капалова Н.А.,
т.ғ.к., қауымдастырылған профессор, ORCID ID: 0000-0001-9743-9981,
e-mail: nkapalova@mail.ru
[2]*Абишева А.Ж.,
докторант, ORCID ID: 0000-0002-6557-3067,
*e-mail: ak_maral@mail.ru

[1]ҚР ҒЖБМ ҒК Ақпараттық және есептеу технологиялары институты,
Алматы қ., Қазақстан
[2]Әл-Фараби атындағы Қазақ ұлттық университеті,
Алматы қ., Қазақстан

КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ БАСҚАРУДЫҢ ЖӘНЕ САНДЫҚ ҚОЛТАҢБАНЫ ҚОЛДАНУДЫҢ ЗАМАНУИ ТӘСІЛДЕРІ

Аңдатпа

Бұл жұмыста криптографиялық кілттерді басқару мәселелері талданады және криптографиялық жүйеге қатысушылар арасындағы кілт алмасудың қауіпсіздігі мен шынайылығын қамтамасыз ететін тиімді хаттамалардың қажеттілігі негізделеді. Қол қоюдан бас тартпау және хабарламаны қайталанудан қорғау қасиеттеріне ие болатын аутентификацияның тиімді әдістерінің бірі – Шнорр схемасы қарастырылады. Позициялық емес полиномды санау жүйесін құру және таңдалған жұмыс негіздері бойынша мәндерді есептеу схемасы мен процедурасының модификациясы сипатталған. Криптографиялық жүйелерде сандық қолтаңбаның және кілттерді басқарудың дәстүрлі емес алгоритмдерін жасауда позициялық емес полиномды санау жүйесін пайдалану осы криптографиялық процедуралардың сенімділігі мен тиімділігін айтарлықтай арттыруға мүмкіндік береді. Ұсынылған схеманы кванттық шабуылдарға қарсы қорғанысты күшейту мүмкіндігі қарастырылған.

Тірек сөздер: криптография, криптографиялық кілттерді басқару, позициялық емес полиномды санау жүйесі, сандық қолтаңба, Шнорр схемасы.

[1]Kapalova N.,
Cand.Tech.Sc., Associate Professor, ORCID ID: 0000-0001-9743-9981,
e-mail: nkapalova@mail.ru
[2]*Abisheva A.,
PhD student, ORCID ID: 0000-0002-6557-3067,
*e-mail: ak_maral@mail.ru

[1]Institute of Information and Computational Technologies CS MSHE RK,
Almaty, Kazakhstan
[2]Al-Farabi Kazakh National University,
Almaty, Kazakhstan

MODERN APPROACHES TO CRYPTOGRAPHIC KEY MANAGEMENT AND APPLICATION OF DIGITAL SIGNATURE

Abstract

This paper explores the challenges associated with cryptographic key management and highlights the importance of developing efficient protocols to ensure secure and trustworthy key exchange in cryptographic systems. It focuses on the Schnorr digital signature scheme, recognized for its features such as indivisibility, non-repudiation, and

resistance to message replay attacks. The study introduces a modified version of the Schnorr scheme, incorporating a non-positional polynomial number system. It outlines the process of generating random numbers for keys and computing necessary values using selected polynomial bases. The implementation of non-positional polynomial number system in the creation of non-traditional digital signature algorithms and key management mechanisms significantly improves both the reliability and performance of cryptographic operations. Furthermore, the paper discusses the potential for adapting the proposed scheme to enhance resistance against quantum computing threats, contributing to the development of quantum-resilient cryptographic solutions.

Keywords: cryptography, cryptographic key management, non-positional polynomial number systems, digital signature, Schnorr scheme.

Дата поступления статьи в редакцию: 23.04.2025