УДК 004.9 **DOI 10.52167/1609-1817-2024-134-5-157-167**

Р. Оспанов[1], Е. Сейткулов[1], К. Утебаев[2], Б. Ергалиева[1], Г. Сергазин[1]
[1]Евразийский национальный университет имени Л.Н. Гумилева,
Астана, Казахстан
[2]Алматинский филиал Московского инженерно-физического института,
Алматы, Казахстан
E-mail: yerzhan.seitkulov@gmail.com

О МЕТОДАХ ПРОЕКТИРОВАНИЯ ПОСТКВАНТОВОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Аннотация. Данная работа посвящена методам проектирования постквантового криптографического алгоритма электронной цифровой подписи. Существуют несколько основных направлений, каждое из которых опирается на уникальные математические проблемы, которые считаются трудноразрешимыми даже для квантовых компьютеров. К этим направлениям относятся: криптографические алгоритмы, основанные на хешировании, на решетках, на кодах, на многомерных многочленах и на изогениях. Каждая из этих категорий имеет свои сильные и слабые стороны, и выбор схемы постквантовой подписи для использования будет зависеть от конкретных требований и ограничений приложения. Среди кандидатов на постквантовую подпись на основе хеширования является многообещающим кандидатом для обеспечения безопасных цифровых подписей. Они полагаются на свойства односторонних хеш-функций, которые, как считается, защищены как от классических, так и от квантовых компьютеров. Подписи на основе хеширования также привлекательны, поскольку они просты, быстры и эффективны. Их можно реализовать с относительно небольшими размерами ключей, и они требуют минимальных вычислений как для подписи, так и для проверки.

Ключевые слова. Криптографический алгоритм, электронная цифровая подпись, криптографическая хеш-функция, постквантовая криптография, асимметричная криптография.

Введение.

Глобальная информатизация и компьютеризация общества сегодня сопровождается увеличением объема конфиденциальных данных. Увеличение вычислительной мощности, распространение облачных вычислений и расширение доступа к сетям общего назначения существенно усложнили защиту информационно-коммуникационных систем. Обеспечение информационной безопасности - одна из ключевых и приоритетных задач современного общества. Одним из необходимых условий решения этой задачи является защита информации с помощью криптографии.

Интернет-банкинг, электронная коммерция, телемедицина, мобильная связь и облачные вычисления в корне зависят от безопасности базовых криптографических алгоритмов. Криптографические алгоритмы с открытым ключом особенно важны, поскольку они обеспечивают цифровые подписи и позволяют безопасно общаться без личного контакта.

Сегодня практически все приложения основаны на RSA, задаче дискретного логарифма в конечных полях или эллиптических кривых. Криптографы оптимизируют выбор параметров и особенности реализации этих систем, а также построение протоколов на их основе, в то время как криптоаналитики оттачивают атаки на эти системы и

устанавливают точный уровень безопасности. Альтернативные системы менее заметны в исследованиях и не известны на практике.

Можно подумать, что наличие трех систем предлагает достаточное разнообразие, но все они будут взломаны, как только будут созданы крупные квантовые компьютеры. Правительства по всему миру вкладывают значительные средства в разработку квантовых компьютеров; общество должно быть готово к последствиям, включая криптоаналитические атаки, ускоренные этими машинами. Долгосрочные конфиденциальные документы, такие как медицинские записи пациентов и государственные секреты, должны оставаться защищенными на протяжении многих лет, но информация, зашифрованная сегодня с помощью RSA или эллиптических кривых и хранимая до появления квантовых компьютеров, будет легко расшифрована, подобно тому, как сегодня легко расшифровываются сообщения, зашифрованные машиной Enigma.

В последние годы проведено значительное количество исследований квантовых компьютеров - машин, использующих квантовые механические явления для решения математических задач, трудных или нерешаемых для обычных компьютеров. Если будут построены крупномасштабные квантовые компьютеры, они смогут взломать многие современные криптосистемы с открытым ключом. Это серьёзно подорвёт конфиденциальность и целостность цифровой связи в Интернете и других сферах. Целью постквантовой криптографии (также называемой квантово-устойчивой криптографией) является разработка криптографических систем, защищенных как от квантовых, так и от классических компьютеров, и способных взаимодействовать с существующими коммуникационными протоколами и сетями [1].

Вопрос о том, когда будет построен крупномасштабный квантовый компьютер, остаётся сложным. Хотя раньше было неясно, возможны ли такие машины с физической точки зрения, теперь многие учёные считают это значительным инженерным вызовом. Некоторые инженеры даже предсказывают, что в течение ближайших двадцати лет могут быть созданы достаточно мощные квантовые компьютеры, способные взломать практически все современные криптосистемы с открытым ключом.

На данный момент уже достигнуты значительные успехи в разработке квантовых компьютеров.

Отметим, что существующие разработки в основном предназначены для решения оптимизационных задач и не подходят для криптоанализа. Возможность появления квантовых компьютеров, способных выполнять криптоаналитические задачи, оценивается в 10−40 лет или даже дольше.

Исторически на развертывание современной инфраструктуры криптографии с открытым ключом потребовались десятилетия. Поэтому, независимо от того, когда именно наступит эра квантовых вычислений, мы должны уже сейчас начать подготовку наших систем информационной безопасности, чтобы противостоять квантовым угрозам. Нам необходимо проводить научные исследования по поиску алгоритмов, устойчивых к квантовым атакам, проверять существующие решения и реализовывать пилотные проекты. Злоумышленники могут уже сегодня перехватывать конфиденциальную зашифрованную информацию, чтобы расшифровать её, как только появятся квантовые компьютеры. Переход на новые методы защиты информации требует значительных изменений в инфраструктуре, текущих методах работы и финансовых вложений, поэтому необходимо начать этот процесс как можно скорее.

Постквантовая криптография представляет собой ответ на вызовы, связанные с развитием квантовых технологий. Цель постквантовой криптографии – создание алгоритмов, которые будут устойчивы как к классическим, так и к квантовым атакам. Особое внимание уделяется разработке алгоритмов электронной цифровой подписи,

поскольку они играют ключевую роль в обеспечении целостности и подлинности данных в цифровом мире. Проектирование постквантовых криптографических алгоритмов требует учета различных математических и криптографических подходов. Существуют несколько основных направлений, каждое из которых опирается на свои уникальные математические проблемы, которые считаются трудноразрешимыми даже для квантовых компьютеров. Среди таких направлений можно выделить: криптографические алгоритмы, основанные на хешировании, криптографические алгоритмы, основанные на решетках, криптографические алгоритмы, основанные на кодах, криптографические алгоритмы, основанные на многомерных многочленах, криптографические алгоритмы, основанные на изогениях. Каждое из этих направлений имеет свои преимущества и недостатки, и выбор конкретного подхода зависит от множества факторов, включая требуемый уровень безопасности, эффективность и практическую применимость.

В данной статье мы рассмотрим основные методы проектирования постквантовых криптографических алгоритмов электронной цифровой подписи. Алгоритмы цифровой подписи, основанные на хешировании, заслуживают особого внимания из-за их простоты и доказанной безопасности. Они используют хеш-функции для создания подписи и верификации, что делает их устойчивыми к атакам квантовых компьютеров. В отличие от других методов, эти алгоритмы не требуют сложных математических структур, что упрощает их реализацию и уменьшает вероятность ошибок в реализации.

Материалы и методы.

Международное сообщество активно готовится к наступлению постквантовой эры.

В 2006 году состоялась первая международная конференция PQCrypto [2], посвященная направлениям исследования и разработки криптографических алгоритмов, стойких относительно анализа как с использованием классических, так и квантовых вычислений. И с тех пор PQCrypto проводится каждые 1–2 года. В 2015 год опубликован меморандум АНБ о переходе на постквантовые алгоритмы [3]. В 2017 году объявлен конкурс NIST в области синтеза постквантовых криптоалгоритмов [4]. Всего были поданы описания 69 криптографических алгоритмов, разработанных авторскими коллективами из различных стран, в том числе международными. 30 января 2019 г. были опубликованы результаты первого раунда этого конкурса. В июле 2022 года NIST объявил о завершении третьего раунда, в результате было выбрано четыре алгоритма-кандидата для стандартизации (CRYSTALS-KYBER [5], CRYSTALS-Dilithium [6], FALCON [7], SPHINCS+ [8]), и четыре дополнительных алгоритма были выбраны для участия в четвертом раунде (BIKE [9], Classic McEliece [10], HQC [11], SIKE [12] (в 2022 году был признан небезопасным [13])). И в августе 2023 года NIST опубликовал проекты стандартов для трех из четырех алгоритмов, выбранных им в 2022 году. В конечном итоге завершенные стандарты постквантовых криптографических алгоритмов заменят криптографические стандарты и руководства, которые наиболее уязвимы для квантовых компьютеров.

В 2018 году CACR, китайская ассоциация криптологических исследований (Chinese Association for Cryptologic Research) объявила национальный конкурс перспективных постквантовых криптографических алгоритмов. В феврале 2019 года прием заявок был завершен, а уже в январе 2020 года были объявлены победители. На конкурс было подано 36 заявок только от китайских специалистов. В итоге трем алгоритмам были присуждены первые места, четыре алгоритма получили вторые места, и шесть третьи места [14].

В 2019 году в России по решению технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) создали рабочую группу по разработке проектов национальных стандартов Российской Федерации, определяющих постквантовые криптографические алгоритмы [15].

Международная организации по стандартизации (ISO) совместно с Международной электротехнической комиссией (IEC) инициировала работы по разработке документа, в котором будут отражены основные направления создания постквантовых криптографических алгоритмов [16].

Таким образом, очевидна необходимость разработки семейства постквантовых криптографических алгоритмов, а также и подготовки всей отечественной информационной инфраструктуры к появлению квантовых компьютеров достаточной для задач криптоанализа производительности.

В настоящее время можно выделить несколько основных направлений исследований и разработок постквантовых схем подписей, каждое из которых основано на различных математических проблемах и подходах.

1. Схемы цифровой подписи, основанные на хешировании. Эти схемы основаны на использовании криптографических хеш-функций, которые, как считается, защищены даже от квантовых компьютеров. Безопасность схемы цифровой подписи, основанной на хешировании, при правильной реализации зависит исключительно от устойчивости к нахождению прообраза ее криптографической хеш-функции. Иными словами, безопасность этой схемы определяется свойствами выбранного алгоритма хеширования. Примерами цифровой подписи, основанной на хешировании, являются XMSS (eXtended Merkle Signature Scheme) [17], SPHINCS+ [8].

2. Схемы цифровой подписи, основанные на решетках. Эти схемы основаны на сложности определенных задач теории решеток (задача нахождения кратчайшего вектора SVP, задача нахождения ближайшего вектора CVP, задача поиска короткого целочисленного решения SIS, задача обучения с ошибками LWE). Эти задачи считаются сложными как для классических, так и для квантовых компьютеров. Примерами являются схемы подписей CRYSTALS-Dilithium [6], FALCON [7], Raccoon [18].

3. Схемы цифровой подписи, основанные на кодах. Эти схемы основаны на сложности кодирования и декодирования определенных кодов с исправлением ошибок (коды Гоппы, линейные коды, полярные коды, циклические коды (коды Боуза-Чоудхури-Хоквингема, сокращённо БЧХ-коды, коды Рида-Соломона)). Эти задачи кодирования считаются сложными для квантовых компьютеров. Примерами являются CROSS [19], Enhanced pqsigRM [20], LESS [21].

4. Схемы цифровой подписи, основанные на многомерных многочленах. Эти схемы основаны на сложности решения систем многомерных многочленов над конечным полем. Безопасность таких алгоритмов опирается на предположение, что задача решения систем многомерных многочленов над конечным полем, в общем случае, является NP-полной задачей в сильном смысле или просто NP-полной, и сложны как для классических, так и для квантовых компьютеров. Примерами являются Rainbow [22], GeMSS [23], DME-Sign [24].

5. Схемы цифровой подписи, основанные на изогениях. Эти схемы основаны на использовании изогений, которые представляют собой отображения между эллиптическими кривыми. Безопасность таких схем основана на сложности поиска изогений между двумя заданными эллиптическими кривыми, что является проблемой, которую квантовые компьютеры в настоящее время не способны эффективно решать. SIKE [12], CSI-FiSh [25], SQIsign [26] являются примерами подписи, основанной на изогении.

Также существуют разработки алгоритмов, которые не относятся к вышеперечисленным направлениям, например, KAZ-SIGN [27], ALTEQ [28].

Каждая категория схем постквантовой подписи опирается на некоторую базовую математическую задачу или подход, предоставляя разнообразный набор инструментов для обеспечения криптографической безопасности в эпоху квантовых вычислений.

Исследователи активно работают над оптимизацией этих схем для повышения их эффективности, уменьшения размеров ключей и обеспечения надежной защиты от квантовых угроз.

Каждая из этих категорий имеет свои сильные и слабые стороны, и выбор схемы постквантовой подписи для использования будет зависеть от конкретных требований и ограничений приложения. Среди кандидатов на постквантовую подпись подпись на основе хеширования является многообещающим кандидатом для обеспечения безопасных цифровых подписей. Они полагаются на свойства односторонних хеш-функций, которые, как считается, защищены как от классических, так и от квантовых компьютеров. Подписи на основе хеширования также привлекательны, поскольку они просты, быстры и эффективны. Их можно реализовать с относительно небольшими размерами ключей и они требуют минимальных вычислений как для подписи, так и для проверки.

Результаты и обсуждение.

Безопасность схемы цифровой подписи, основанной на хешировании, при правильной реализации опирается только на устойчивость к прообразу ее компонента криптографической хеш-функции [29]. Другими словами, безопасность схемы может быть сведена к свойствам выбранного алгоритма хеширования. Это свойство уже является основой безопасности многих одобренных NIST криптографических алгоритмов и протоколов, и не известно ни одного алгоритма квантовых вычислений, который мог бы представлять практическую угрозу в обозримом будущем. Также к преимуществам схем цифровой подписи, основанной на хешировании, можно отнести их гибкость, поскольку их можно использовать с любой безопасным криптографическим алгоритмом хеширования. И если окажется, что в используемом алгоритме хеширования обнаружена ошибка, то просто необходимо в схеме поменять на новый и безопасный алгоритм хеширования, чтобы позволить схеме оставаться эффективной. Современные схемы цифровой подписи, основанной на хешировании, можно разделить на схемы с сохранением состояния и без сохранения состояния. В схемах с сохранением состояния для подписания требуется обновление секретного ключа, в отличие от обычных схем цифровой подписи, подписание требует сохранения состояния используемых одноразовых ключей и обеспечения того, чтобы они никогда не использовались повторно. Примером схемы с сохранением состояния является XMSS (eXtended Merkle Signature Scheme) [17], а без сохранения состояния SPHINCS+ [8]. На основе последней схемы были построены варианты алгоритмов, использующих различные криптографические хеш-функции [30], [31]. В схемах цифровой подписи, основанной на хешировании, в качестве основного элемента используются схемы одноразовой подписи. Каждый уникальный одноразовый ключ подписи ограничен безопасной подписью одного сообщения, при этом раскрывая часть ключа подписи. Безопасность схем одноразовой подписи, основанной на хешировании, зависит исключительно от безопасности базовой хеш-функции. Известные схемы одноразовой подписи включают схему Лэмпорта-Диффи, схему Винтерница и ее усовершенствования, такие как схема W-OTS+. В отличие от исходной схемы Лэмпорта–Диффи, схема Винтерница и ее варианты могут одновременно подписывать несколько битов, что определяется параметром Винтерница. Этот параметр обеспечивает компромисс между размером и скоростью: большие значения приводят к более коротким подписям и ключам, но более медленному подписанию и проверке. Обычно на практике для этого параметра используется значение 16. Для подписей, основанных на хешировании, без сохранения состояния используются схемы малоразовых подписей, позволяющие постепенно снижать безопасность при повторном использовании многократного ключа. Основная концепция схем подписи, основанной на хешировании, предполагает объединение многочисленных пар одноразовых ключей в единую структуру

с использованием дерева Меркла. Это облегчает практическое подписание, выходящее за пределы однократного использования, с использованием открытого и закрытого ключей, генерируемых по базовой одноразовой схеме. Глобальный открытый ключ, расположенный наверху дерева Меркла, получается на основе выбранной хеш-функции, в результате чего его типичный размер составляет 32 байта. Действительность глобального открытого ключа связана с конкретным одноразовым открытым ключом через путь аутентификации, хранящийся в подписи, что помогает верификаторам восстановить путь узла между двумя ключами. Глобальный закрытый ключ обычно управляется с помощью генератора псевдослучайных чисел, для получения которого требуется только начальное значение. Этот подход обеспечивает небольшой размер глобального закрытого ключа, часто около 32 байтов. Эффективный обход дерева имеет решающее значение для производительности подписи, и для повышения скорости подписи были введены различные методы. Некоторые схемы подписи, основанной на хешировании, используют несколько уровней деревьев для достижения более быстрой подписи за счет более крупных подписей. В таких схемах для подписи сообщений используется только самый нижний уровень деревьев, тогда как более высокие уровни подписывают корневые значения нижних деревьев. Свойства схем подписи, основанной на хешировании, зависят от предположений безопасности, связанных с базовой хеш-функцией, и может использоваться любая хеш-функция, удовлетворяющая этим предположениям. Следовательно, каждая подходящая хеш-функция приводит к отдельной схеме подписи на основе хеш-функции. Некоторые схемы, такие как XMSS с генерацией псевдослучайного ключа, являются защищенными в прямом направлении, то есть предыдущие подписи остаются действительными, даже если секретный ключ скомпрометирован. Примечательной характеристикой схем подписи на основе хеш-функции являются минимальные предположения о безопасности, которые обычно полагаются исключительно на безопасную криптографическую хеш-функцию. Хотя это предположение необходимо для любой схемы цифровой подписи, другие схемы могут потребовать дополнительных предположений о безопасности, чего в данном случае нет. Из-за того, что они полагаются на базовую схему одноразовой подписи, схемы подписи, основанной на хешировании, могут безопасно подписывать только фиксированное количество сообщений. В случае схем Меркла и XMSS максимум составляет 2h сообщений, где h представляет собой общую высоту дерева Меркла. Также известно, что основным недостатком большинства разработанных в настоящее время схем постквантовой электронной цифровой подписи является большой суммарный размер открытого ключа и цифровой подписи.

В работе [32] представлен новый криптографический алгоритм хеширования, основанный на модифицированной схеме «Sponge», схеме криптографических алгоритмов хеширования («криптографическая губка»). В модифицированной схеме предусматривается множество внутренних функций. В построенном алгоритме используется множество, состоящее из трех различных внутренних функций. С помощью функции выбора из данного множества выбирается внутренняя функция f. Для построения первой функции из данного множества применяется обобщенная методологии проектирования AES. Этот подход дает возможность достаточно просто строить блочные шифры. Рабочие данные представляются в виде многомерных массивов, и затем большие блоки открытого текста зашифровываются с помощью небольших компонентов. Для построения второй функции применяются, так называемые, словарные регистры сдвига с обратной связью по переносу кольцевой конфигурации. Для построения третьей функции применяется перестановка Keccak, но с рядом отличий. Операции выполняются над состоянием S размера 2048 бит. Состояние представляет собой трехмерный битовый массив размера 4 × 8 × 64. Используется 8-битовый S-блок. В оригинальной перестановке

Keccak используется 5-битовый S-блок. При создании раундовых констант используется словарный регистр сдвига с обратной связью по переносу кольцевой конфигурации. Также можно отметить, что модифицированная схема «Sponge» позволяет строить алгоритмы с любым количеством внутренних функции (например, с одной, двумя или четыремя функциями). Для этого достаточно модифицировать функцию выбора. Так например, в [33] представлена программная реализация криптографической хеш-функции «ТАҢБА», основанной на модифицированной схеме «Sponge».

Упомянутая выше схема SPHINCS+ является перспективным фреймворком для проектирования постквантовых алгоритмов цифровой подписи. Взяв его за основу, и выбрав в качестве базового криптографического преобразования хеш-функции «ТАҢБА», можно построить новый постквантовый алгоритм цифровой подписи, основанной на хешировании.

Заключение.

Развитие квантовых вычислений представляет собой значительный вызов для современной криптографии, в частности, для алгоритмов электронной цифровой подписи. Уязвимость существующих криптосистем, основанных на RSA, задаче дискретного логарифма в конечных полях или эллиптических кривых, перед квантовыми атаками подчеркивает необходимость перехода к постквантовым криптографическим схемам.

Методы проектирования постквантовых криптографических алгоритмов электронной цифровой подписи охватывают различные математические подходы, каждый из которых предлагает уникальные преимущества и решает конкретные проблемы безопасности. Схемы, основанные на хешировании, основанные на решетках, основанные на кодах, основанные на многомерных многочленах, основанные на изогениях, а также другие схемы играют важную роль в формировании устойчивых к квантовым атакам криптографических алгоритмов.

Безопасность схемы цифровой подписи, основанной на хешировании, при правильной реализации зависит исключительно от стойкости к нахождению прообраза ее криптографической хеш-функции, и определяется свойствами выбранного алгоритма хеширования. Одним из преимуществ схем цифровой подписи, основанных на хешировании, является их гибкость: их можно использовать с любым безопасным криптографическим алгоритмом хеширования. Если в используемом алгоритме хеширования будет обнаружена уязвимость, достаточно заменить его на новый безопасный алгоритм, чтобы схема оставалась эффективной.

Внедрение постквантовых алгоритмов требует значительных усилий в области научных исследований, разработки и тестирования. Существующие решения необходимо тщательно проверять на устойчивость к квантовым атакам, а новые подходы должны быть исследованы и внедрены в пилотных проектах. Этот процесс требует координации усилий между академическими, промышленными и государственными учреждениями.

Подготовка к эре квантовых вычислений требует проактивного подхода к разработке и внедрению постквантовых криптографических решений. Обеспечение долгосрочной безопасности информации требует от нас уже сегодня начать переход к новым криптографическим стандартам, чтобы противостоять будущим угрозам. Только комплексный и систематический подход позволит нам сохранить конфиденциальность и целостность данных в мире, где квантовые вычисления станут реальностью.

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

ЛИТЕРАТУРА

[1] Bernstein D., Lange T. Post-quantum cryptography // Nature 549, 188–194 (2017), https://doi.org/10.1038/nature23461

[2] Post-quantum cryptography for long-term security PQCRYPTO ICT-645622, https://pqcrypto.eu.org

[3] Cryptography Today // National Security Agency, Information Assurance, 2009, https://web.archive.org/web/20150815072948/https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[4] Post-Quantum Cryptography // NIST, CSRC, https://csrc.nist.gov/projects/post-quantum-cryptography

[5] Bos J. et al. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM // 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 2018, pp. 353-367, doi: 10.1109/EuroSP.2018.00032.

[6] Ducas, Leo & Kiltz, Eike & Lepoint, Tancrède & Lyubashevsky, Vadim & Schwabe, Peter & Seiler, Gregor & Stehlé, Damien. (2018). CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme // IACR Transactions on Cryptographic Hardware and Embedded Systems. 238-268. 10.46586/tches. v2018.i1.238-268.

[7] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte and Zhenfei Zhang. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Specification v1.2 — 01/10/2020. NIST PQC Competition, 2019. https://falcon-sign.info/falcon.pdf.

[8] Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. 2019. The SPHINCS+ Signature Framework. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 2129–2146. https://doi.org/10.1145/3319535.3363229.

[9] Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor, Valentin Vasseur, Santosh Ghosh, Jan Richter-Brokmann. BIKE: Bit Flipping Key Encapsulation. Round 4 Submission. Specification Version: 5.1. 2022. NIST PQC Competition, 2022. https://bikesuite.org/files/v5.0/BIKE_Spec.2022.10.10.1.pdf.

[10] Bernstein D.J., Chou T., Lange T., Mauri I.V., Misoczki R., Niederhagen R., Persichetti E., Peters C., Schwabe P., Sendrier N., Szefer J., Wang W. Classic McEliece: conservative code-based cryptography: cryptosystem specification. NIST PQC Competition, 2022. https://classic.mceliece.org/mceliece-spec-20221023.pdf.

[11] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Jerome Lacan, Jean-Marc Robert, Pascal Veron. Hamming Quasi-Cyclic (HQC). Fourth round version. 2023. NIST PQC Competition, 2022. https://pqc-hqc.org/doc/hqc-specification_2023-04-30.pdf.

[12] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, Aaron Hutchinson. Supersingular Isogeny Key Encapsulation. 2022. NIST PQC Competition, 2022. https://sike.org/files/SIDH-spec.pdf.

[13] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). Cryptology ePrint Archive, Report 2022/975, 2022. http://eprint.iacr.org/2022/975.

[14] Chinese Association for Cryptologic Research (CACR), www.cacrnet.org.cn

[15] Technical Committee for Standardization "Cryptographic Protection of Information", Structure, https://tc26.ru/about/structure/

[16] ISO and IEC Joint Technical Committee (JTC 1), https://jtc1info.org/

[17] Buchmann J., Dahmen E., Huelsing A. XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions // Lecture Notes in Computer Science, Volume 7071, Post-Quantum Cryptography, DOI 10.1007/978-3-642-25405-5_8, 2011.

[18] del Pino R., Espitau T., Katsumata S., Maller M., Mouhartem F., Prest T., Rossi M., Saarinen M-J. Raccoon. A Side-Channel Secure Signature Scheme // The specification document, https://raccoonfamily.org/wp-content/uploads/2023/07/raccoon.pdf

[19] Marco Baldi, Alessandro Barenghi, Sebastian Bitzer, Patrick Karl, Felice Manganiello, Alessio Pavoni, Gerardo Pelosi, Paolo Santini, Jonas Schupp, Freeman Slaughter, Antonia Wachter-Zeh, Violetta Weger CROSS. Codes and Restricted Objects Signature Scheme // Submission to the NIST Post-Quantum Cryptography Standardization Process. Algorithm Specifications and Supporting Documentation. Version 1.2 - February 3, 2024, https://www.cross-crypto.com/CROSS_Specification_v1.2.pdf

[20] Jinkyu Cho, Jong-Seon No, Yongwoo Lee, Young-Sik Kim, Zahyun Koo Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature and Fast Verification for Post-Quantum Cryptography // The specification document, https: //csrc.nist.gov /csrc/media /Projects/pqc-dig-sig/documents/round-1/spec-files/Enhanced-pqsigRM-spec-web.pdf

[21] Marco Baldi, Alessandro Barenghi, Luke Beckwith, Jean-François Biasse, Andre Esser, Kris Gaj, Kamyar Mohajerani, Gerardo Pelosi, Edoardo Persichetti, Markku-Juhani O. Saarinen, Paolo Santini, Robert Wallace LESS: Linear Equivalence Signature Scheme // The specification document, https://www.less-project.com/LESS-2024-02-19.pdf

[22] Ding J., Schmidt D. Rainbow, a New Multivariable Polynomial Signature Scheme // Ioannidis, J., Keromytis, A., Yung, M. (eds) Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science, vol 3531. Springer, Berlin, Heidelberg, 2005, https://doi.org/10.1007/11496137_12

[23] Casanova A., Faugere J.-C., Macario-Rat G., Patarin J., Perret L., Ryckeghem J. GeMSS: A Great Multivariate Short Signature https://www-polsys.lip6.fr/Links/NIST/GeMSS_specification_round2_V2.pdf

[24] Ignacio Luengo, Mart'in Avendano DME: Multivariate signature public key scheme // // The specification document, https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/DME_SIGN-spec-web.pdf

[25] Beullens, W., Kleinjung, T., Vercauteren, F.: Csi-fish: efficient isogeny-based signatures through class group computations. In: Advances in Cryptology–ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, Proceedings, Part I. pp. 227–247. Springer (2019)

[26] Jorge Chavez-Saab, Maria Corte-Real Santos, Luca De Feo, Jonathan Komada Eriksen, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Michael Meyer, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Francisco Rodríguez Henríquez, Sina Schaeffler, Benjamin Wesolowski SQIsign. Algorithm specifications and supporting documentation. Version 1.0. June 1, 2023, https://sqisign.org/spec/sqisign-20230601.pdf

[27] Muhammad Rezal Kamel Ariffin, Nur Azman Abu, Terry Lau Shue Chien, Zahari Mahad, Amir Hamzah Abd Ghafar, Nurul Amiera Sakinah Abdul Jamal Kriptografi Atasi Zarah Digital Signature (KAZ-SIGN) // Algorithm Specifications and Supporting Documentation (Version 1.6.3), https://www.antrapol.com/KAZ-SIGN/files?fileid=v1.6.3-spec

[28] Markus Blaser, Dung Hoang Duong, Anand Kumar Narayanan, Thomas Plantard, Youming Qiao, Arnaud Sipasseuth, Gang Tang The ALTEQ Signature Scheme: Algorithm Specifications and Supporting Documentation // Document Version 2023-06-01, https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ALTEQ-Spec-web.pdf

[29] Buchmann J., Dahmen E., Szydlo M. Hash-based Digital Signature Schemes // Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg, 2009, https://doi.org/10.1007/978-3-540-88702-7_3.

[30] Kiktenko E., Bulychev A., Karagodin P., Pozhar N., Anufriev M., Fedorov A. Sphincs+ postquantum digital signature scheme with streebog hash function // AIP Conference Proceedings. vol. 2241, p. 020014. AIP Publishing LLC (2020)

[31] 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, https://eprint.iacr.org/2022/152.pdf

[32] Ospanov R.M., Seitkulov Ye.N., Yergaliyeva, B.B. A cryptographic hash function based on a modified SPONGE scheme // Eurasian Journal of Mathematical and Computer Applications, 2022, 10(2), pp. 55–70

[33] Ospanov R.M., Seitkulov Y.N., Sissenov N.M. Software implementation of the cryptographic hash function "Tanba" // Copyright Certificate, No. 28399 dated August 22, 2022.

Руслан Оспанов, ғылыми қызметкері, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, ospanovrm@gmail.com

Ержан Сейткулов, ф.-м.ғ.к., профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, yerzhan.seitkulov@gmail.com

Куат Утебаев, студент, Мәскеу инженерлік-физикалық институтының Алматы филиалы, Алматы, Қазақстан, tash.nur@mail.com

Бану Ергалиева, ғылыми қызметкер, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, banu.yergaliyeva@gmail.com

Гани Сергазин, PhD, қауымдастырылған профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

ЭЛЕКТРОНДЫҚ САНДЫҚ ҚОЛҒА АРНАЛҒАН ПОСТКВАНТТЫҚ КРИПТОГРАФИЯЛЫҚ АЛГОРИТМНІ ЖОБАЛАУ ӘДІСТЕРІ ТУРАЛЫ

Андатпа. Бұл жұмыс электрондық цифрлық қолтаңбаның постквантты криптографиялық алгоритмін құрастыру әдістеріне арналған. Бірнеше негізгі бағыттар бар, олардың әрқайсысы тіпті кванттық компьютерлер үшін шешілмейтін болып саналатын бірегей математикалық есептерге сүйенеді. Бұл салаларға мыналар жатады: хэштеу негізіндегі криптографиялық алгоритмдер, торлар, кодтар, көпөлшемді полиномдар және изогениялар. Осы санаттардың әрқайсысының өзінің күшті және әлсіз жақтары бар және пайдалану үшін пост кванттық қолтаңба схемасын таңдау қолданбаның нақты талаптары мен шектеулеріне байланысты болады. Үміткерлердің арасында хэшингке негізделген постквантты қолтаңба қауіпсіз цифрлық қолтаңбаны қамтамасыз ету үшін перспективалы үміткер болып табылады. Олар классикалық және кванттық компьютерлерге қарсы қауіпсіз деп есептелетін бір жақты хэш функцияларының қасиеттеріне сүйенеді. Хэш негізіндегі қолтаңбалар да тартымды, себебі олар қарапайым, жылдам және тиімді. Олар салыстырмалы түрде шағын кілт өлшемдерімен жүзеге асырылуы мүмкін және қол қою мен тексеру үшін ең аз есептеуді қажет етеді.

Түйінді сөздер. Криптографиялық алгоритм, электрондық цифрлық қолтаңба, криптографиялық хэш функциясы, постквanттық криптография, асимметриялық криптография.

Ruslan Ospanov, researcher, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, ospanovrm@gmail.com
Yerzhan Seitkulov, candidate of physical and mathematical sciences, professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, yerzhan.seitkulov@gmail.com
Kuat Utebayev, student, Almaty Branch of the Moscow Institute of Engineering and Physics Almaty, Kazakhstan, yerzhan.seitkulov@gmail.com
Banu Yergaliyeva, researcher, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan, banu.yergaliyeva@gmail.com
Gani Sergazin, PhD, associate professor, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan

ON METHODS OF DESIGNING A POST-QUANTUM CRYPTOGRAPHIC ALGORITHM FOR AN ELECTRONIC DIGITAL SIGNATURE

Abstract. This paper focuses on methods for designing a post-quantum cryptographic digital signature algorithm. There are several main directions, each relying on unique mathematical problems that are considered intractable even for quantum computers. These directions include hash-based, lattice-based, code-based, multivariate polynomial-based, and isogeny-based cryptographic algorithms. Each of these categories has its own strengths and weaknesses, and the choice of which post-quantum signature scheme to use will depend on the specific requirements and constraints of the application. Among the post-quantum signature candidates, hash-based signatures are promising candidates for providing secure digital signatures. They rely on the properties of one-way hash functions, which are believed to be secure against both classical and quantum computers. Hash-based signatures are also attractive because they are simple, fast, and efficient. They can be implemented with relatively small key sizes, and they require minimal computation for both signing and verification.

Keywords. Cryptographic algorithm, electronic digital signature, cryptographic hash function, post-quantum cryptography, asymmetric cryptography.

****

Получено: 06 апрель 2024 г.; принято: 16 сентябрь 2024 г.