Многофакторная аутентификация с использованием биометрических данных с квантовыми вычислениями

Г. Есмагамбетова, А. Актаева, А.Кубигенова, К. Сагинбаева, А. Исмуканова, Д. Жоламанова

Аннотация. Методы многофакторной аутентификации используются в каждой операции аутентификации пользователей в Киберпространстве. Использование одноразовых паролей с многофакторной аутентификацией является более безопасным методом, чем однофакторная аутентификация, когда две схемы аутентификации, когда две схемы аутентификации осуществляются на разных уровнях. Однако в настоящее время использование одноразовых паролей ограничивает аутентификацию самим устройством, а не пользователем. Развитие технологий также привело к увеличению числа случаев кибермошенничества с использованием одноразовых паролей. Таким образом, возникает необходимость в повышении уровня безопасности на основе использования одноразовых паролей. В данной работе мы используем математически доказанные свойства квантовой криптографии и квантовой запутанности для создания квантовых одноразовых паролей для аутентификации пользователей на основе их биометрических данных. В статье описывается инфраструктура многофакторной аутентификации на основе квантовых алгоритмов, необходимая для реализации предложенной модели, и проводится сравнительный анализ защищенности предложенной моделей от атак типа "человек посередине".

Ключевые слова: биометрия, одноразовый пароль, квантовые вычисления, квантовая криптография, квантовое запутывание, квантовый одноразовый пароль, двухфакторная аутентификация.

I. ВВЕДЕНИЕ

Квантовые вычислители способны решать задачи, которые не под силу классическим машинам, и на данном этапе являются перспективным методом резкого повышения производительности вычислений. Хотя обширное внедрение квантовых вычислителей в массы при текущем уровне развития технологий невозможно, тем не менее, квантовые вычисления уже долгое время считаются одним из наиболее перспективных направлений. Это объясняется тем, что применение квантовых алгоритмов после появления квантовых компьютеров позволяет экспоненциально увеличить скорость решения вычислительных задач. Развитие квантовых вычислений, а также связанная с киберугрозой для современных реализаций шифрования, похоже, остается лишь вопросом времени.

Аутентификация - это процесс определения того, действительно ли физическое или юридическое лицо, получающее доступ к компьютерной системе, является тем, за кого себя выдает. Системы аутентификации принимают бинарное решение. Они разрешают или запрещают доступ на основании учетных данных или других доказательств, предоставленных теми, кто запрашивает доступ. Перед специалистами по защите информации стоит важная задача проектирования систем аутентификации для таких систем. [2,3] Специалисты по информационной безопасности пытаются решить проблемы мошенничества и краж, предлагая различные методы и протоколы для обеспечения безопасности аутентификации физических или юридических лиц [4,5]. Один из таких методов - многофакторная аутентификация [6,7], которая является весьма тонким способом борьбы с мошенничеством, но именно его применение вносит факторы риска. Очень надежным считается использование квантовых одноразовых паролей [8, 9], когда одноразовый пароль предоставляется пользователю устройством аутентификации или поставщиком услуг. Такие одноразовые пароли генерируются в зависимости от времени проведения операции, а также типа операции, но имеют ограниченный срок использования [10, 11]. Генерация квантовых одноразовых паролей, если она осуществляется на стороне пользователя, происходит в синхронном режиме. Поэтому во время генерации квантового одноразового пароля пользователь должен находиться в сети. Другой способ заключается в том, что генерация квантового одноразового пароля осуществляется в автономном режиме, путем ведения счетчика у пользователя и на сервере. Преимущества двойной аутентификации в этом случае могут быть успешно реализованы только в том случае, если поставщик услуг и пользователь заранее надежно согласовывают алгоритм генерации квантового одноразового пароля [12].

Генерация квантовых одноразовых паролей, если она осуществляется на стороне сервера, передается либо в зашифрованном виде по тому же каналу, что и киберпространство, либо в открытом виде, например, SMS. Поскольку квантовые одноразовые пароли генерируются не на стороне сервера, а на стороне пользователя, пользователю и поставщику услуг необходимо взаимно определить способ передачи квантового одноразового пароля. Получив квантовый одноразовый пароль, пользователь передает его поставщику услуг, который сравнивает его с уже хранящейся копией и аутентифицирует пользователя для конкретной операции. Безопасность квантового одноразового пароля зависит от отправителя (сервера), который генерирует квантовый одноразовый пароль [15].

Информационная безопасность делает акцент на безопасности пользователя, для чего идентификация и аутентификация является обязательным условием.[16] Здесь на первый план выходит роль биометрии как инструмент, поскольку она может однозначно идентифицировать пользователя [17]. Она аутентифицирует пользователя наилучшим возможным способом, таким образом, используя технологию квантовых одноразовых паролей в многофакторной схеме аутентификации [18]. Но ее использование имеет различные недостатки, например, перехваченные данные являются зашумленными, так как это двухмерное изображение трехмерной структуры зависит от системы сбора, выбора признаков, системы сравнения (с сохраненными биометрическими данными) допустимого уровня дисперсии в результатах сравнения [19].

Криптография требует точной генерации криптографического ключа с обеих сторон, следовательно, применение биометрии в качестве криптографического инструмента становится затруднительным из-за зашумленности данных. В качестве решения этой проблемы была предложена одна из таких решений, в которой используются коды коррекции ошибок наряду с кодом Рида Хадамарда и код Рида-Соломона для биометрии по радужной оболочке глаза [20]. Ошибки в биометрии по отпечаткам пальцев обрабатываются с помощью предложенных архитектур, таких как нечеткие экстракторы [21], нечеткие обязательства и безопасный эскиз, которые используют коррекцию ошибок, коды с коррекцией ошибок и встраивание сигнала.

Обмен OTP на основе SMS имеет тот недостаток, что он осуществляется в открытом режиме. Следовательно, он может быть легко прочитан, что делает его уязвимым для атаки "человек посередине" (MITM), путем заражения мобильного устройства вредоносным ПО и пересылки SMS на мобильный злоумышленника и в то же время удаляя его с мобильного телефона пользователя. [22] Генерация OTP должна быть настолько случайной, насколько это возможно, то есть энтропия должна быть очень высокой, чтобы предотвратить предсказание OTP. Однако достичь желаемой случайности довольно сложно, поскольку тип транзакций в целом остается неизменным (либо перевод, либо снятие); единственная связь, которую необходимо использовать - это связь временной метки с генерируемыми OTP. Если энтропия меньше, связь OTP-TIME может быть обнаружена с минимальными усилиями, например, с помощью атаки грубой силы на количество образцов, сгенерированных для одной и той же транзакции [23].

Кроме того, как только одноразовый квантовый ключ сгенерирован для транзакции, он имеет срок службы, в течение которого не генерируется новый ключ для того же типа транзакции, даже если пользователь запрашивает. Это открывает злоумышленнику возможности осуществить повторную атаку путем отказа пользователю в предоставлении ключа для его транзакции. Такие атаки очень распространены в транзакциях "Вход в систему" на основе одноразового квантового ключа.

Безопасность, присущая использованию двух внеполосных каналов, снижается при подключении устройств, использующих разные каналы, например, компьютера или мобильного телефона, что приводит к межплатформенным атакам заражения [24]. Одноразовые квантовые ключи наиболее уязвимы в период действия, когда ключ доступен и может быть использован в своих целях. Две сложные техники, известные как code sniffing и request lookup [25], используют межпроцессное взаимодействие для обработки одноразовых квантовых ключей на устройстве пользователя.

Для дальнейшего повышения коэффициента успешности одноразовых квантовых ключей был предложен ряд решений, позволяющих снизить уязвимость одноразовых квантовых ключей. Одно из таких решений заключается в том, что секретны ключ совместно используемый пользователем и сервером, вместе с одноразовым квантовым ключом, полученным на мобильном устройстве, генерирует новый пароль для транзакции, и этот новы пароль используется в веб-интерфейсе [26].

Одно из решений, использующих квантовую криптографию, предполагает создание защищенного канала для обмена открытыми ключами, в котором происходит обмен закрытыми ключами для защиты от MITM, включая целевой фишинг. Этот метод называется безопасной квантовой криптографией одноразовых паролей (POTP) [27]. Однако он основан на создании защищенного канала связи, в котором ключ является статическим. Схемы шифрования, как симметричные, так и асимметричные, требуют длинных ключей, которые практически невозможно хранить. Если ключи генерируются, а не хранятся пользователем на основе каждого использования, как в случае с Advanced Encryption Standard (AES), то сложность запоминания длинных 128-битных паролей снижается, а также устраняет недостатки снижения безопасности простого пароля, контролирующего доступ к ключам AES.

Предложены эффективные решения для генерации одноразового квантового ключа с использованием биометрии [28-30]. Когда пользователь аутентифицируется для проведения транзакции с сервером, сервер генерирует вызов и отправляет его пользователю в открытом режиме. Затем пользователь генерирует ключ с помощью функции, использующей предварительно разделенный ключ, только что сгенерированный биометрический код и вызов, предоставленный сервером. Этот одноразовый квантовый ключ отправляется на сервер, который вычисляет его, сопоставляет полученный код с вычисленным кодом и аутентифицирует пользователя.

II. МАТЕРИАЛЫ И МЕТОДЫ

Мотивацией для проведения исследований в данной работе является создание эффективного решения для двухфакторной аутентификации, гарантирующего, что генерация одноразовых квантовых ключей осуществляется совершенно случайным образом на стороне сервера [31] и передается пользователю по внеполосному каналу. В то же время оно должно гарантировать, что пользователь может работать с одноразовым квантовым ключом без использования своих биометрических данных. Сгенерированный пользователем одноразовый квантовый ключ отправляется обратно на сервер, который затем может использовать для аутентификации пользователя его собственные биометрические данные. Успех или неуспех операции пользователя должен быть подтвержден только сервером.

Оно устраняет недостатки существующих биометрических решений за счет использования свойств квантовой связи, обеспечивающих встроенную защиту связи, таких как отсутствие клонирования [32] и коллапса волновой функции [33]. В этом решении все операции выполняются без знания о передаваемом значении, а окончательное измерение и сравнение производится на стороне сервера, который считается безопасным.

Квантовые вычисления. Базовой единицей квантового компьютера является квантовый бит (кубит), который может выполнять одни и те же операции, используя два четко определенных состояния - |1⟩ или |0⟩. Эти состояния обычно изображаются на сфере Блоха в виде стрелки, указывающей на северный полюс для состояния |0⟩ или на южный полюс для состояния |1⟩. Интересно, что в силу квантовой природы суперпозиция состояний |1⟩ или |0⟩ может быть сгенерирована с помощью $|\psi$. Сгенерировать суперпозицию состояний $|\psi\rangle = a0\ |0\rangle + a1\ |1\rangle$, направленные в любую сторону сферы, где квадраты a0 и a1 являются амплитудой вероятности, следующей за $|a0|2+|a1|2=1$ (см. Рис. 1).

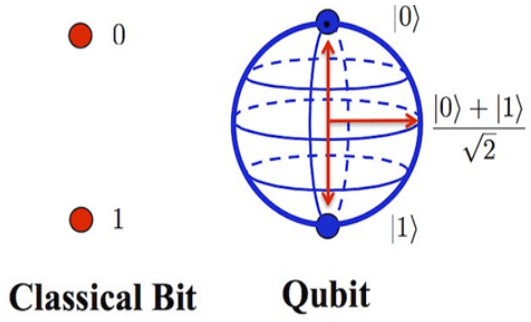

Рис.1. Классический бит и кубит [34]

Эти новые состояния не имеют классических аналогов и представляют собой неортогональные конфигурации с 2^N состояний, где N - число кубитов. Это одно из свойств, которое дает квантовый компьютер потенциальную возможность для выполнения огромных по объему и сложности операций.

Основываясь на квантовых свойствах “суперпозиции” и “запутанности”, n кубитов могут действовать как группа или изолированно, что приводит к экспоненциально большей плотности информации, чем у классического компьютера.

Квантовый бит (или кубит) - это фундаментальная единица информации, используемая в квантовых компьютерах. Это можно сравнить с битом, который используется в классическом компьютере. Кубит, в более технических терминах, представляет собой двумерную квантовую систему

Состояние кубита может быть выражено как

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad (1)$$

Где α и β являются комплексными числами и $|\alpha|2 + |\beta|2 = 1$. В $ket{-}notation$ или $Diracnotation$, $|0\rangle = (10)$ и $|1\rangle = (01)$ используются ля представления базовых состояний двумерного векторного пространства. Следовательно, уравнение (1) действительно показывает состояние кубита в виде двумерного комплексного вектора (αβ).

Разница с классическим битом заключается в том, что кубит нельзя измерить, не изменив его. Измерение кубита или его состояния, заданного уравнением (1), даст классическое значение, равное нулю (|0⟩0) с вероятностью |α|2| или один (|1⟩1) с вероятностью |β|2|.

В дополнение, $\langle\phi|$ сопряженная транспонировка |ϕ⟩ и является вектором строк (известным как bra) с двумя компонентами: $\langle 0| = (10)$ и $\langle 1| = (01)$ Из bra и ket мы можем вычислить внутреннее произведение или внешнее произведение векторов. Дано |u⟩ и $|v\rangle$ их внутренний продукт $\langle u|v\rangle (= \langle u||v\rangle)$, которая является скалярной. Например, $\langle 0|0\rangle = \langle 1|1\rangle = 1$ и $\langle 0|1\rangle = \langle 1|0\rangle = 0$.

Внешний продукт получается с помощью $|u\rangle\langle v$, которая представляет собой оператор в матричной форме. Если $|0\rangle\langle 0|0\rangle\langle 0$ работает на |ϕ⟩ результат α|0⟩ .

Это означает, что оператор $|0\rangle\langle 0|0\rangle\langle 0$ извлечет |0⟩0 компонент из |ϕ⟩ или |ϕ⟩ измеряется в |0⟩0 направлении.

Аналогично, оператор $|1\rangle\langle 1$ извлекает |1⟩1 компонент из |ϕ⟩.

Эффективность квантовых вычислений определяется числом воспроизводимых кубит и временем поддержки вантовой суперпозиции.

Модель квантовых алгоритмов основана на физических законах теории квантовых вычислений, а именно, в вычислениях участвуют унитарные, обратимые квантовые операторы. В общем виде

квантовый алгоритм состоит из трёх основных унитарных операций:

1. суперпозиция;
2. квантовая корреляция (квантовый оракул или запутанные операторы);
3. интерференция;
4. Четвёртый оператор, оператор измерения результатов квантовых вычислений, является необратимым (классическим) [35-36].

Фундаментальный результат теории квантовых вычислений заключается в том, что все операции могут быть реализованы на схеме, состоящей из универсальных базисных элементов. В отличии от классического аналога квантовые алгоритмические ячейки (КАЯ) могут быть выполнены на различных классах универсальных элементов в зависимости от используемого вычислительного базиса.

Квантовые алгоритмические ячейки с фиксированными вычислительным и измерительным базисами обеспечивают описание эволюции некоторого унитарного оператора U которому соответствует квантовый вычислительный процесс:

$|\psi_{fin} \geq U|\psi_{in} >$ где вектор (волновая функция) $|\psi_{in} >$задает начальные условия вычислений (решаемой проблемы), а $|\psi_{fin} >$отражает результат вычислений за счёт действия оператора U на начальное состояние $|\psi_{in} >$.

Выбирая различный вид оператора U (в частности, Гамильтониан), можно сформировать различные модели квантовых вычислений. В общем виде модель квантовых вычислений состоит из пяти этапов:

- приготовление начального (классического или квантового) состояния ψ_{in};
- выполнение преобразования Адамара для начального состояния с целью подготовки состояния суперпозиции;
- применение запутанного оператора или оператора квантовой корреляции (квантового оракула) к суперпозиционному состоянию;
- исполнение оператора интерференции;
- использование оператора измерения для результата квантовых вычислений $|\psi_{in} >$

Квантовые алгоритмы часто демонстрируются в виде квантовых схем, состоящих из квантовых вентилей, которые обрабатывают входные кубиты [36-37].

III. РЕАЛИЗАЦИЯ И АНАЛИЗ БЕЗОПАСНОСТИ

Существующие системы одноразовых паролей предполагают использование классических методов связи и квантовых вычислений, а также технологии биометрии. Предлагаемая модель повышает безопасность транзакций на основе квантовых одноразовых ключей путем постепенной замены классических вычислительных методов квантовыми. Эти методы используют математически доказанные принципы безопасности квантовой коммуникации, такие как неклонирование и коллапс волновой функции, для повышения защищенности квантовых одноразовых ключей - транзакций от угроз. В соответствии с моделью угроз анализ защищенности проводится фильтрация информации, полученной из следующих источников:

- Устройства, подключенные к сети.
- Автономные устройства.
- MITM средств передачи данных.
- Анализ перехваченных данных.

Существующие методы. В качестве существующей методики рассматривается модель транзакций на основе квантовых одноразовых ключей [28]. Блок-схема модели транзакций на основе квантовых одноразовых ключей приведена на рис. 2. Основные этапы выполнения следующие:

Генерация квантовых одноразовых ключей на S

Передача квантовых одноразовых ключей между U и S.

Генерация BC на стороне пользователя.

Классическая операция U.

Классическая операция S.

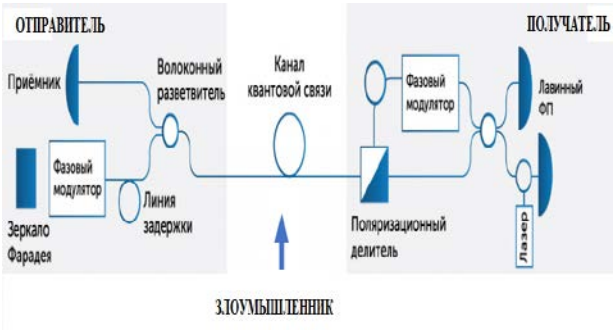

Рис.2. Блок-схема модели транзакций на основе квантовых одноразовых ключей

Реализация. Существующие методы используют генерируемые пользователем параметры в качестве входных данных F для генерации квантовых одноразовых ключей. Пусть рассматриваемые параметры здесь будут T_c и T_s. Случайность дополнительно улучшается за счет использования R_g, который является выходом генератора случайных чисел. Квантовый одноразовый ключ передается пользователю с помощью SMS. После генерации B_C с помощью автономного устройства операция между квантовым одноразовым ключом и B_C выполняется для создания выхода C_1, который передается обратно в S с помощью C_{Ci}. S использует свой сохраненный B_C и далее проводит классические операции над полученным кодом C_1 от U для его аутентификации. (см. Рис. 3)

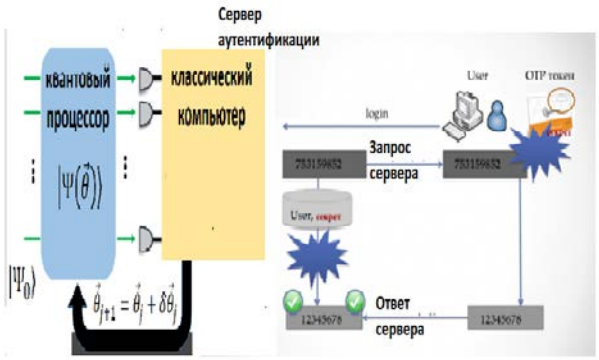

Рис. 3. Схема генерации квантовых одноразовых ключей

Анализ защищенности. Устройства, подключенные к сети, включают в себя пользовательские устройства, получающие ключ, ипользовательские устройства, отправляющие от C_1 в S. Ключ отправляется в S пользовательскими устройствами. Эти устройства скомпрометированы в соответствии с моделью угроз, поэтому эти коды могут быть прочитаны, удалены, манипулированы или использованы злоумышленником в своих целях [22].

Автономные устройства: устройство, генерирующее ключ, является автономным устройством. Учитывая, что устройство не имеет памяти и генерирует биометрический код каждый раз с использованием техники нечеткого экстрактора [38], его физический захват не приводит к утечке информации отправителя, согласно модели угроз.

MITM в среде передачи данных: для передачи кодов между отправителем и получателем используются классические каналы C_{Ci} и C_C, которые в соответствии с моделью угроз подвержены MITM. В результате эти коды могут быть перехвачены, заменены или повторно использованы злоумышленником.

MITM в среде передачи данных: для передачи кодов между U и S используются классические каналы C_{Ci} и C_C, которые в соответствии с моделью угроз подвержены MITM. В результате эти коды могут быть перехвачены, обменяны и повторно использованы.

Анализ перехваченных данных: данные перехватываются с зараженных устройств и уязвимых носителей. Перехваченные коды C_1 и C_2 могут быть проанализированы для извлечения БК, что сводит на нет цель использования биометрии для аутентификации пользователей. Аналогичным образом, несколько пар кодов C_1 и C_2 могут быть использованы вместе с информацией о T_s и T_c для обнаружения функций, используемых для R_g[39] и F[40], особенно с появлением квантовых компьютеров. Уязвимости в таких функциях на стороне сервера могут быть использованы для предсказания кода, генерируемого в последующих транзакциях, что существенно снижает без опасность транзакций на основе квантовых одноразовых ключей. Если не использовать квантово-вычислительно безопасные функции или функции генерации полностью случайных чисел, то, по крайней мере теоретически, угроза безопасности будет существовать всегда.

Пример II: RIQ_{CO}. Блок-схема реализации этой модели показана на рисунке 4. Основные этапы выполнения являются:

1. Генерация квантовых запутанных частиц в качестве квантового одноразового в S.
2. Передача одного из кубитов в U из S и хранение другого кубита.
3. Генерация B_C на стороне пользователя.
4. Квантовая операция над кубитом со стороны U.
5. Квантовая операция измерения кубита и классическая операция S.

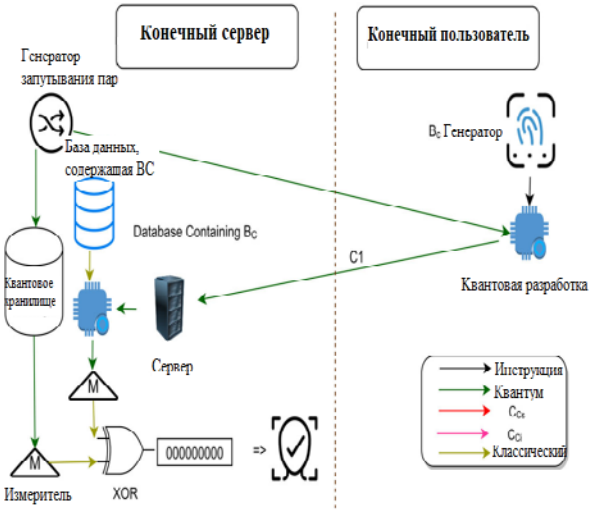

Рис. 4. Реализация RIQ_{CO} []

Реализация. RIQ_{CO} выполняет квантовые операции только на стороне пользователя. S генерирует квантовые запутанные пары так же, как и RIQ_{CM}. Полученные квантовые биты со стороны пользователя обрабатываются B_C для генерации управляемых квантовых битов, которые отправляются обратно в S с помощью Q_C. Кроме того, S далее манипулирует полученными квантовыми битами, измеряет их с помощью сохраненного B_C и сравнивает их с измерениями сохраненных квантовых битов для аутентификации U.

Анализ безопасности. Устройства в сети: устройства, подключенные к сети, включают пользовательские устройства, которые принимают квантовые биты, манипулируют ими и отправляют обратно в сеть. Это устройство выполняет все квантовые манипуляции и не может быть взломано. Поскольку классические манипуляции не производятся, то не существует кода, которым может манипулировать A, и, следовательно, он не может быть атакован.

Автономные устройства: автономные устройства, как описано выше, не представляют угрозы безопасности.

MITM через средства передачи данных: в этом случае классические каналы передачи данных не используются.

Поэтому перехватываются только квантовые передачи. Квантовые передачи, как уже говорилось, являются изначально безопасными. Поэтому атака MITM полностью проваливается.

Анализ перехваченных данных: если попытаться измерить состояния перехваченных кубитов, то эти состояния распадутся на собственные состояния одного из собственных значений. Злоумышленник не может измерить состояние, не будучи обнаруженным. Даже если злоумышленник рискует быть обнаруженным и находит B_C, получить код невозможно, поскольку исходный B_C, преобразованный с помощью квантовых операций над случайными состояниями колокола U перед передачей его в Q_C, неизвестен. Поэтому нет никакой корреляции между B_C и управляющими кубитами, посылаемыми U и S в Q_C.

Поскольку на стороне пользователя не происходит никаких измерений и хранения, этот метод полностью защищен от межпроцессных коммуникационных атак. Данный метод описывает минимальные квантовые возможности, необходимые на обоих концах для повышения безопасности одноразовых квантовых ключей по сравнению с существующими схемами и методами, что математически доказывается возможность использования концепции квантовой криптографии.

Повышение безопасности одного квантового ключа может быть достигнуто за счет уменьшения стойкости квантового ключа U, но все равно не достигает уровня безопасности, обеспечиваемого предлагаемым методом.

На основе этих трех примеров и существующих методов можно проанализировать решение предлагаемой модели. Обобщенное сравнение безопасности, обеспечиваемой существующими методами и примерами использования, с безопасностью исходной информации представлено в таблице 1 и 2 соответственно.

Таблица 1. Сравнение: Безопасность источников

№ пп	Примеры	Информация, полученная от			
		Устройства в сети	Автономные устройства	MITM	Анализ перехваченных данных:
1.	Существующая модель [28]	Да	Нет	Да	Да
2.	RIQ_{CO}	Нет	Нет	Нет	Нет

Таблица 2. Сравнение: Безопасность информации

№ пп	Примеры	Возможность раскрытия информации		
		Одноразовый ключ	Одноразовый ключ генерирующий функции	B_C
1.	Существующая модель [28]	Да	Да	Да
2.	RIQ_{CO}	Нет	Нет	Нет

Неформальный анализ защищенности. Для понимания общих преимуществ предлагаемой модели в плане безопасности можно провести неформальный анализ концепции защищенности. В рамках этого анализа на фоне модели угроз рассматриваются следующие атаки безопасности

a. *Межплатформенные атаки*: эти атаки используют взаимодействия двух различных устройств в двух схемах двухфакторной аутентификации. Одно из устройств может быть скомпрометировано, и взаимодействие между ними может привести к компрометации другого устройства.

b. MITM В этой атаке злоумышленник выступает в роли легитимного U для S и может выполнять транзакции от имени U без его ведома, где нет возможности расшифровывать или раскрывать одноразовый квантовый ключ, но он должен уметь использовать информацию, перехваченную со скомпрометированного устройства, в своих интересах.

c. *Атака повторного воспроизведения* - это атака повторного использования ранее сгенерированного одноразового квантового ключа, если аналогичная операция выполняется с тем же одноразовым квантовым ключом в течение срока действия ранее сгенерированного квантового ключа. Предполагается, что S генерирует тот же одноразовый квантовый ключ для аналогичной транзакции (например, входа в систему) в течение срока действия первого сгенерированного одноразового квантового ключа.

d. *Перехват кода/прослушивание запросов*: атака, при которой злоумышленник считывает ключи в процессе их обработки операционной системой с помощью межпроцессного взаимодействия. Эта атака становится очень сложной, если устройство скомпрометировано, поскольку даже зашифрованные данные должны быть расшифрованы, прежде чем операционная система сможет выполнить с ними какую-либо обработку.

Следующие модели одноразового квантового ключа, были сопоставлены в таблице 3 с возможностью возникновения вышеупомянутых атак.

Таблица 3. Неофициальный анализ безопасности: Возможность атак

№ пп	Атаки	Модели/техники OTP			
		Общий секрет	POTPa	Биометрия	RIQCO
1.	Кросс-платформа	Да	Нет	Нет	Нет
2.	MITM	Да	Нет	Нет	Нет
3.	Воспроизведение	Да	Нет	Да	Нет
4.	Перехват кода/подбор запросов	Да	Нет	Да	Нет

Модификация с помощью общего секретного ключа Одноразовый квантовый ключ, сгенерированный S, модифицируется U с помощью общего ключа. Общий ключ служит для шифрования или хеширования ключа, полученного от S. Если устройство, используемое для обработки полученного ключа, оно считается скомпрометированным:

a. Устройство, обрабатывающее квантовый ключ, имеет общий секретный ключ и поэтому способно к межплатформенной атаке.

b. Общий секретный ключ скомпрометирован, и передача одноразового ключа и может происходить в открытом виде. Таким образом, в данной модели возможны все остальные атаки.

Защищенные одноразовые пароли - передают OTP по зашифрованному каналу. Проблема безопасности здесь заключается в защите ключа, используемого для шифрования канала, а не для обмена OTP. Однако, поскольку ключ не играет никакой роли в работе OTP, предполагается, что общий ключ, используемый для шифрования канала, не был скомпрометирован:

a. скомпрометированное устройство должно взаимодействовать с устройством, связь с которым зашифрована с помощью шифрования зашифрованного канала. Таким образом, возможна кроссплатформенная атака.

b. Скомпрометированное устройство работает с зашифрованными OTP и, следовательно, способно к атакам с подбором кода/запроса.

c. Носитель, передающий OTP, зашифрован. Поэтому атаки типа MITM и replay невозможны.

Биометрическое OTP. Биометрические данные генерируются для каждой новой транзакции и используются для обработки OTP, полученных от S. Биометрические данные хранятся в общем секретном ключе. Это отличается от использования общего секретного ключа, поскольку в общем секретном ключе используется статически хранимый ключ, и использование этого ключа обеспечивает аутентификацию только устройства, хранящего этот ключ. Биометрические OTP, напротив, генерируют коды на основе биометрических данных отдельных устройств, а не используют хранимые коды. При этом аутентифицируется пользователь, а не устройство:

a. Биометрические OTP генерируются на отдельном устройстве, которое не взаимодействует со скомпрометированным устройством. Поэтому межплатформенные атаки невозможны. В отсутствие биометрического кода невозможна и MITM-атака.

b. Управляемые биометрические коды передаются в открытом режиме и поэтому открыты для атак на воспроизведение. Аналогично, возможны атаки типа "сниффинг кода - сниффинг запросов", поскольку OTP обрабатывается операционной системой в открытом режиме.

RIQ_{CO}. Это третий вариант использования предлагаемой модели, в котором U оснащен квантовыми возможностями и выполняет квантовые операции и передачу данных:

a. Все операции являются квантовыми, и квантовое устройство не скомпрометировано. Поэтому межплатформенные или MITM-атаки невозможны.

b. значения измеряются только на стороне сервера. Поэтому атаки на воспроизведение невозможны. Аналогично невозможны межплатформенные – повторные атаки, поскольку операционная система не работает с полученным кодом.

ЗАКЛЮЧЕНИЕ И ДАЛЬНЕЙШАЯ РАБОТА

Классические методы вычислений создают проблемы безопасности, которые могут быть преодолены с помощью квантовых вычислений. Используемые методы аутентификации должны проверять подлинность пользователя, а не устройства, и биометрия играет в этом важную роль. Успешная реализация биометрии для аутентификации пользователя требует безопасной передачи биометрических данных в каждой транзакции.

В данной статье предлагается метод реализации двухфакторной аутентификации, использующий квантовые вычисления для генерации QOTP и биометрию для аутентификации пользователя. В работе описаны три варианта использования, которые определяют различные возможности пользователя, связанные с квантовой средой, основанные на манипулировании, измерении и передаче кубитов. Для этих трех сценариев использования был проведен отдельный анализ безопасности для одной модели угроз. Реалистичность этих сценариев использования подтверждается математическими представлениями и экспериментами по реализации отдельных шагов, описанных в моделях.

Предлагаемое исследование решает проблемы безопасности, с которыми сталкиваются существующие методы при реализации OTP с использованием QOTP. Предложенная модель повышает безопасность передачи биометрических данных за счет использования квантовых каналов связи. Анализ безопасности модели угроз показывает, что уровень безопасности киберпространства на основе OTP повышается по мере увеличения квантовых возможностей пользователей, что подчеркивает влияние и возможности квантовых вычислений.

Таким образом, предложенная в данной работе модель выполняет многофакторную аутентификацию с использованием биометрии на основе квантовых вычислений на QOTP для обеспечения улучшенных функций безопасности по сравнению с текущими используемыми методами по сравнению с существующими методами использования OTP в качестве одной из схем двухфакторной аутентификации.

Будущая работа требует исследования для решения проблем надежности в физической реализации квантовых операций определенных математическими уравнениями.

Библиография

[1]. Mishra D, Kumar V, Mukhopadhyay S., Pairless Identity Based Authentication System for Cloud Computing. Berlin: Springer; https://doi.org/10.1007/978-3-642-38631-2_62

[2]. Kumar V., Jangirala S. & Ahmad M., An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing. J Med Syst 42, 142 (2018). https://doi.org/10.1007/s10916-018-0987-5

[3]. Kumar V., Ahmad M. & Kumari A., A Secure Elliptic Curve Cryptography Based Mutual Authentication Protocol for Cloud-assisted TMIS. Telematics and Informatics (2018). doi:10.1016/j.tele.2018.09.001

[4]. Kumari S., Karuppiah M., Da, A.K. et al., A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74, 6428–6453 (2018). https://doi.org/10.1007/s11227-017-2048-0

[5]. Kumar V., Ahmad M., Kumar P. (2019). An Identity-Based Authentication Framework for Big Data Security. In: Krishna, C., Dutta, M., Kumar, R. (eds) Proceedings of 2nd International Conference on Communication, Computing and Networking. Lecture Notes in Networks and Systems, vol 46. Springer, Singapore. https://doi.org/10.1007/978-981-13-1217-5_7

[6]. Картер Роберт А., Многофакторная аутентификация. US Patent App. 13/124,598; 2011.

[7]. Abhishek K., Roshan S., Kumar P., Ranjan R. (2013). A Comprehensive Study on Multifactor Authentication Schemes. In: Meghanathan, N., Nagamalai, D., Chaki, N. (eds) Advances in Computing and Information Technology. Advances in Intelligent Systems and Computing, vol 177. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31552-7_57

[8]. Haller N., Metz K., Nesser P., Strau M. One-time password system. Request for comments from the network working group. 1998;2289.

[9]. Sharma, M.K., Nene, M.J. (2020). Quantum One Time Password with Biometrics. In: Raj, J., Bashar, A., Ramson, S. (eds) Innovative Data Communication Technologies and Application. ICIDCA 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 46. Springer, Cham. https://doi.org/10.1007/978-3-030-38040-3_36

[10]. Ahn TH. Transaction based One Time Password (OTP) payment system. US patent application. 13/555.442; 2013.

[11]. M'Raihi D, Machani S, Pei M, Rydell J. A time-based one-time password algorithm. Internet Eng Task Force RFC. 2011;6238.

[12]. Popp N, M'raihi D, Hart L. One-time password. US Patent 8,087,074; 2011.

[13]. Roy, U.K., Mahansaria, D. (2020). Two-Factor Authentication Using Mobile OTP and Multi-dimensional Infinite Hash Chains. In: Arai, K., Kapoor, S., Bhatia, R. (eds) Advances in Information and Communication. FICC 2020. Advances in Intelligent Systems and Computing, vol 1129. Springer, Cham. https://doi.org/10.1007/978-3-030-39445-5_50

[14]. Alkatheiri, M.S., Eldefrawy, M.H., Khan, M.K. (2012). BAN Logic-Based Security Proof for Mobile OTP Authentication Scheme. In: J. (Jong Hyuk) Park, J., Leung, V., Wang, CL., Shon, T. (eds) Future Information Technology, Application, and Service. Lecture Notes in Electrical Engineering, vol 164. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-4516-2_6

[15]. Deng, FG., Li, XH., Li, CY.et al. Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements. Eur. Phys. J. D 39, 459–464 (2006). https://doi.org/10.1140/epjd/e2006-00124-1

[16]. Rehman, H.U., Ghani, A., Chaudhry, S.A. et al. A secure and improved multi server authentication protocol using fuzzy commitment. Multimed Tools Appl 80, 16907–16931 (2021). https://doi.org/10.1007/s11042-020-09078-z

[17]. Liu C-H, Wang J-S, Peng C-C, Shyu JZ. Оценка и выбор биометрии в сетевой безопасности. Secur Commun Netw. 2015;8(5):727-739. Doi: 10.1002/sec.1020

[18]. Schultz PT., Multifactor multimedia biometric authentication. US Patent 8,189,878; 2012.

[19]. Jain Anil K, Ross A, Pankanti S. Biometrics: a tool for information security. IEEE Trans Inform Forensics Secur. 2006;1(2):125-143. DOI: 10.1109/TIFS.2006.873653

[20]. Hao, F., Anderson, R., & Daugman, J. (2006). Combining crypto with biometrics effectively. IEEE transactions on computers, 55(9), 1081-1088.

[21]. Dodis, Y., Reyzin, L., Smith, A. (2004). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In: Cachin, C., Camenisch, J.L. (eds) Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24676-3_31

[22]. Peotta L, Holtz Marcelo D, David Bernardo M, Deus Flavio G, De Sousa RT. Formal classification of attacks and vulnerabilities of Internet banking vulnerabilities. Int J Comput Sci Inform Technol. 2011;3(1):186-197. DOI:10.5121/ijcsit.2011.3113

[23]. Dmitrienko, A., Liebchen, C., Rossow, C., Sadeghi, AR (2014). On the (In)Security of Mobile Two-Factor Authentication. In: Christin, N., Safavi-Naini, R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science(), vol 8437. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_24

[24]. Dmitrienko, A., Liebchen, C., Rossow, C., Sadeghi, AR. (2014). On the (In)Security of Mobile Two-Factor Authentication. In: Christin, N., Safavi-Naini, R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science(), vol 8437. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_24

[25]. Yoo, C., Kang, BT. & Kim, H.K. Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. Multimed Tools App 74, 3289–3303 (2015). https://doi.org/10.1007/s11042-014-1888-3

[26]. Hamdare S, Nagpurkar V, Mittal J. Protecting sms-based one-time password technology from man-in-the-middle attacks. arXiv preprint arXiv:1405.4828; 2014. https://doi.org/10.14445/22315381/IJETT-V11P230

[27]. Ganesan R, Sandhu RS, Cottrell A P, Schoppert BJ, Bellare M. Protecting one-time-passwords against man-in-the-middle attacks. US Patent 7,840,993; 2010.

[28]. Plateaux, A., Lacharme, P., Jøsang, A., Rosenberger, C. (2014). One-Time Biometrics for Online Banking and Electronic Payment Authentication. In: Teufel, S., Min, T.A., You, I., Weippl, E. (eds) Availability, Reliability, and Security in Information Systems. CD-ARES 2014. Lecture Notes in Computer Science, vol 8708. Springer, Cham. https://doi.org/10.1007/978-3-319-10975-6_14

[29]. Hosseini, Z. Zareh, and E. Barkhordari. "Enhancement of security with the help of real time authentication and one time password in e-commerce transactions." The 5th Conference on Information and Knowledge Technology. IEEE, 2013. DOI: 10.1109/IKT.2013.6620077

[30]. Zhu H. One-time key agreement scheme with biometric-based ID-password authentication. Secur Commun Netw. 2015;8(13):2350-2360. DOI: 10.1002./sec.1182

[31]. Naren G, Li S, Andréasson J. One-time password generation and two-factor authentication using molecules and light. DOI: 10.1002/cphc.201700074

[32]. Yanofsky Noson S. Introduction to quantum computing. arXiv preprint arXiv:0708.0261; 2007. http://arxiv.org/abs/0708.0261v1

[33]. Nene, M.J., Upadhyay, G. (2016). Shor's Algorithm for Quantum Factoring. In: Choudhary, R., Mandal, J., Auluck, N., Nagarajaram, H. (eds) Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, vol 452. Springer, Singapore. https://doi.org/10.1007/978-981-10-1023-1_33

[34]. Riffel Eleanor G., Polak Wolfgang H. Quantum computing: a gentle introduction. Cambridge, MA: MIT Press; 2011. https://s3.amazonaws.com/arena-attachments/1000401/c8d3f8742d163b7ffd6ae3e4e4e07bf3.pdf

[35]. Lidar Daniel A, Chuang Isaac L, Whaley KB. Coherently incoherent subspaces for quantum computing. Phys Rev Lett. 1998;81(12):2594-2597. https://doi.org/10.1103/PhysRevLett.81.2594

[36]. Bennett CH, Brassard G, Popescu S, Schumacher B, Smolin JA, Wootters WK. Clearing Noise Confusion and True Teleportation through noisy channels. Phys Rev Lett. 1996;76(5):722-725. https://doi.org/10.1103/PhysRevLett.76.722

[37]. Calderbank AR, Rains EM, Shor PM, Sloane Neil JA. Quantum error correction using codes over GF (4). IEEE Trans Infor Theory. 1998;44(4):1369-1387. DOI: 10.1109/18.681315

[38]. Khan, A.A., Kumar, V., Ahmad, M.: An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. J. King Saud Univ. - Comput. Inf. Sci. (2019). https://doi.org/10.1016/j.jksuci.2019.04.013, http://www.sciencedirect.com/science/article/pii\319157819301193

[39]. Kelsey, J., Schneier, B., Wagner, D., Hall, C. (1998). Cryptanalytic Attacks on Pseudorandom Number Generators. In: Vaudenay, S. (eds) Fast Software Encryption. FSE 1998. Lecture Notes in Computer

Science, vol 1372. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-69710-1_12

[40]. Ambeynis A., Rosmanis A., Unrukh D. Quantum attacks on classical proof systems: the hardness of quantum rewinding. New York: IEEE; 2014:474-483. DOI:10.1109/FOCS.2014.57

Multi-factor authentication using biometrics with quantum computing

G.Yesmagambetova, A.Aktayeva, A.Kubigenova, K.Saginbayeva,
A. Ismukanova, D. Zholamanova

Annotation. Multi-factor authentication methods are used in every user authentication operation in cyberspace. The use of one-time passwords with multi-factor authentication is a more secure method than single-factor authentication when two authentication schemes perform at different levels. However, the current use of one-time passwords limits authentication of the device itself and not the user. Advances in technology have also led to an increase in cyber fraud using one-time passwords. Thus, there is a need to improve the level of security based on the use of one-time passwords. In this paper, we use mathematically proven properties of quantum cryptography and quantum entanglement to create quantum one-time passwords to authenticate users based on their biometric data. The paper describes the infrastructure of multi-factor authentication based on quantum algorithms required to implement the proposed model and provides a comparative analysis of the security of the proposed model against man-in-the-middle attacks.

Keywords: biometrics, one-time password, quantum computing, quantum cryptography, quantum entanglement, quantum one-time password, two-factor authentication.

[1] Mishra D, Kumar V, Mukhopadhyay S., Pairless Identity Based Authentication System for Cloud Computing. Berlin: Springer; https://doi.org/10.1007/978-3-642-38631-2_62

[2] Kumar V., Jangirala S. & Ahmad M., An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing. J Med Syst 42, 142 (2018). https://doi.org/10.1007/s10916-018-0987-5

[3] Kumar V., Ahmad M. & Kumari A., A Secure Elliptic Curve Cryptography Based Mutual Authentication Protocol for Cloud-assisted TMIS. Telematics and Informatics (2018). doi:10.1016/j.tele.2018.09.001

[4] Kumari S., Karuppiah M., Da, A.K. et al., A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74, 6428–6453 (2018). https://doi.org/10.1007/s11227-017-2048-0

[5] Kumar V., Ahmad M., Kumar P. (2019). An Identity-Based Authentication Framework for Big Data Security. In: Krishna, C., Dutta, M., Kumar, R. (eds) Proceedings of 2nd International Conference on Communication, Computing and Networking. Lecture Notes in Networks and Systems, vol 46. Springer, Singapore. https://doi.org/10.1007/978-981-13-1217-5_7

[6] Картер Роберт А., Многофакторная аутентификация. US Patent App. 13/124,598; 2011.

[7] Abhishek K., Roshan S., Kumar P., Ranjan R. (2013). A Comprehensive Study on Multifactor Authentication Schemes. In: Meghanathan, N., Nagamalai, D., Chaki, N. (eds) Advances in Computing and Information Technology. Advances in Intelligent Systems and Computing, vol 177. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31552-7_57

[8] Haller N., Metz K., Nesser P., Strau M. One-time password system. Request for comments from the network working group. 1998;2289.

[9] Sharma, M.K., Nene, M.J. (2020). Quantum One Time Password with Biometrics. In: Raj, J., Bashar, A., Ramson, S. (eds) Innovative Data Communication Technologies and Application. ICIDCA 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 46. Springer, Cham. https://doi.org/10.1007/978-3-030-38040-3_36

[10] Ahn TH. Transaction based One Time Password (OTP) payment system. US patent application. 13/555.442; 2013.

[11] M'Raihi D, Machani S, Pei M, Rydell J. A time-based one-time password algorithm. Internet Eng Task Force RFC. 2011;6238.

[12] Popp N, M'raihi D, Hart L. One-time password. US Patent 8,087,074; 2011.

[13] Roy, U.K., Mahansaria, D. (2020). Two-Factor Authentication Using Mobile OTP and Multi-dimensional Infinite Hash Chains. In: Arai, K., Kapoor, S., Bhatia, R. (eds) Advances in Information and Communication. FICC 2020. Advances in Intelligent Systems and Computing, vol 1129. Springer, Cham. https://doi.org/10.1007/978-3-030-39445-5_50

[14] Alkatheiri, M.S., Eldefrawy, M.H., Khan, M.K. (2012). BAN Logic-Based Security Proof for Mobile OTP Authentication Scheme. In: J. (Jong Hyuk) Park, J., Leung, V., Wang, CL., Shon, T. (eds) Future Information Technology, Application, and Service. Lecture Notes in Electrical Engineering, vol 164. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-4516-2_6

[15] Deng, FG., Li, XH., Li, CY.et al. Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements. Eur. Phys. J. D 39, 459–464 (2006). https://doi.org/10.1140/epjd/e2006-00124-1

[16] Rehman, H.U., Ghani, A., Chaudhry, S.A. et al. A secure and improved multi server authentication protocol using fuzzy commitment. Multimed Tools Appl 80, 16907–16931 (2021). https://doi.org/10.1007/s11042-020-09078-z

[17] Liu C-H, Wang J-S, Peng C-C, Shyu JZ. Оценка и выбор биометрии в сетевой безопасности. Secur Commun Netw. 2015;8(5):727-739. Doi: 10.1002/sec.1020

[18] Schultz PT., Multifactor multimedia biometric authentication. US Patent 8,189,878; 2012.

[19] Jain Anil K, Ross A, Pankanti S. Biometrics: a tool for information security. IEEE Trans Inform Forensics Secur. 2006;1(2):125-143. DOI: 10.1109/TIFS.2006.873653

[20] Hao, F., Anderson, R., & Daugman, J. (2006). Combining crypto with biometrics effectively. IEEE transactions on computers, 55(9), 1081-1088.

[21] Dodis, Y., Reyzin, L., Smith, A. (2004). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In: Cachin, C., Camenisch, J.L. (eds) Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24676-3_31

[22] Peotta L, Holtz Marcelo D, David Bernardo M, Deus Flavio G, De Sousa RT. Formal classification of attacks and vulnerabilities of Internet banking vulnerabilities. Int J Comput Sci Inform Technol. 2011;3(1):186-197. DOI:10.5121/ijcsit.2011.3113

[23] Dmitrienko, A., Liebchen, C., Rossow, C., Sadeghi, AR (2014). On the (In)Security of Mobile Two-Factor Authentication. In: Christin, N., Safavi-Naini, R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science(), vol 8437. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_24

[24] Dmitrienko, A., Liebchen, C., Rossow, C., Sadeghi, AR. (2014). On the (In)Security of Mobile Two-Factor Authentication. In: Christin, N., Safavi-Naini, R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science(), vol 8437. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_24

[25] Yoo, C., Kang, BT. & Kim, H.K. Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. Multimed Tools App 74, 3289–3303 (2015). https://doi.org/10.1007/s11042-014-1888-3

[26] Hamdare S, Nagpurkar V, Mittal J. Protecting sms-based one-time password technology from man-in-the-middle attacks. arXiv preprint

arXiv:1405.4828; 2014. https://doi.org/10.14445/22315381/IJETT-V11P230
[27] Ganesan R, Sandhu RS, Cottrell A P, Schoppert BJ, Bellare M. Protecting one-time-passwords against man-in-the-middle attacks. US Patent 7,840,993; 2010.
[28] Plateaux, A., Lacharme, P., Jøsang, A., Rosenberger, C. (2014). One-Time Biometrics for Online Banking and Electronic Payment Authentication. In: Teufel, S., Min, T.A., You, I., Weippl, E. (eds) Availability, Reliability, and Security in Information Systems. CD-ARES 2014. Lecture Notes in Computer Science, vol 8708. Springer, Cham. https://doi.org/10.1007/978-3-319-10975-6_14
[29] Hosseini, Z. Zareh, and E. Barkhordari. "Enhancement of security with the help of real time authentication and one time password in e-commerce transactions." The 5th Conference on Information and Knowledge Technology. IEEE, 2013. DOI: 10.1109/IKT.2013.6620077
[30] Zhu H. One-time key agreement scheme with biometric-based ID-password authentication. Secur Commun Netw. 2015;8(13):2350-2360. DOI: 10.1002./sec.1182
[31] Naren G, Li S, Andréasson J. One-time password generation and two-factor authentication using molecules and light. DOI: 10.1002/cphc.201700074
[32] Yanofsky Noson S. Introduction to quantum computing. arXiv preprint arXiv:0708.0261; 2007. http://arxiv.org/abs/0708.0261v1
[33] Nene, M.J., Upadhyay, G. (2016). Shor's Algorithm for Quantum Factoring. In: Choudhary, R., Mandal, J., Auluck, N., Nagarajaram, H. (eds) Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, vol 452. Springer, Singapore. https://doi.org/10.1007/978-981-10-1023-1_33
[34] Riffel Eleanor G., Polak Wolfgang H. Quantum computing: a gentle introduction. Cambridge, MA: MIT Press; 2011. https://s3.amazonaws.com/arena-attachments/1000401/c8d3f8742d163b7ffd6ae3e4e4e07bf3.pdf
[35] Lidar Daniel A, Chuang Isaac L, Whaley KB. Coherently incoherent subspaces for quantum computing. Phys Rev Lett. 1998;81(12):2594-2597. https://doi.org/10.1103/PhysRevLett.81.2594
[36] Bennett CH, Brassard G, Popescu S, Schumacher B, Smolin JA, Wootters WK. Clearing Noise Confusion and True Teleportation through noisy channels. Phys Rev Lett. 1996;76(5):722-725. https://doi.org/10.1103/PhysRevLett.76.722
[37] Calderbank AR, Rains EM, Shor PM, Sloane Neil JA. Quantum error correction using codes over GF (4). IEEE Trans Infor Theory. 1998;44(4):1369-1387. DOI: 10.1109/18.681315
[38] Khan, A.A., Kumar, V., Ahmad, M.: An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. J. King Saud Univ. - Comput. Inf. Sci. (2019). https://doi.org/10.1016/j.jksuci.2019.04.013, http://www.sciencedirect.com/science/article/pii\319157819301193
[39] Kelsey, J., Schneier, B., Wagner, D., Hall, C. (1998). Cryptanalytic Attacks on Pseudorandom Number Generators. In: Vaudenay, S. (eds) Fast Software Encryption. FSE 1998. Lecture Notes in Computer Science, vol 1372. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-69710-1_12
[40] Ambeynis A., Rosmanis A., Unrukh D. Quantum attacks on classical proof systems: the hardness of quantum rewinding. New York: IEEE; 2014:474-483. DOI:10.1109/FOCS.2014.57

G. Yesmagambetova, lecturer at the Sh. Ualikhanov Kokshetau Universuty. **ID Scopus** 57367260600, ORCID ID:0000-0002-9868-293X. Areas of scientific interest: information technologies, information security, computer vision systems, VR E-mail: gal.esm@mail.ru

A. Aktayeva, dr.Ph. D., ass.prof. at the A.Myrzakhmetov Kokshetau Universuty. ID Scopus 57201382324 ,https://orcid.org/0000-0002-2693-6785 . Areas of scientific interest: information security, quantum computing, AI. E-mail: aaktaewa@list.ru

A. Kubigenova, doctorate at the Saken Seifullin Kazakh Agrotechnical University, ID Scopus 58671284700 , Areas of scientific interest: information technologies, information security, quantum computing. E-mail: akku_kubigenova@mail.ru

K. Saginbayeva, lecturer at the Sh. Ualikhanov Kokshetau Universuty, ID Scopus 57735954600, https://orcid.org/0000-0001-5916-7794. Areas of scientific interest: information technologies, information security, computer science. E-mail: skk_19739@mail.ru

A. Ismukanova, lecturer at the Sh. Ualikhanov Kokshetau Universuty, Areas of scientific interest: information technologies, information networks, computer vision systems, VR. E-mail: aigera_ismukan@mail.ru

D. Zholamanova , lecturer at the Sh. Ualikhanov Kokshetau Universuty, Areas of scientific interest: information technologies, information networks, computer vision systems. E-mail: zholamanova.dinara@inbox.ru