DOI: 10.55648/1998-6920-2025-19-2-98-111 УДК 004.056.55

Интеграция квантового распределения ключей с классическими криптографическими схемами: повышение безопасности в условиях постквантовых вызовов

Е. Ф. Кустов[1], А. Ф. Хуцаева[1,2], А. П. Кирьянова[1], И. Д. Иогансон[1], Ж.-М. Н. Дакуо[1,2], С. В. Беззатеев[1,2]

[1] Университет ИТМО
[2] Санкт-Петербургский государственный университет аэрокосмического приборостроения

Аннотация: В работе исследуются подходы к обеспечению информационной безопасности с использованием квантового распределения ключей (КРК) в сочетании с классическими криптографическими схемами: схемой Блома, KDP и схемой Лагранжа. Показано, как квантовые технологии повышают безопасность и эффективность этих методов. Предложенные схемы обеспечивают устойчивость к атакам классических и квантовых компью- теров, устраняя уязвимости традиционных методов генерации ключей. Рассмотрены при- меры применения в защищённых сетях IoT, облачных вычислениях и распределённых си- стемах. Результаты демонстрируют, что комбинация КРК с криптографическими схемами является перспективным решением для постквантовой эры.

Работа выполнена в рамках государственного задания (проект FSER-2025-0003).

Ключевые слова: квантовое распределение ключей, схема Блома, Key Distribution Pattern (KDP), схема Лагранжа, информационная безопасность, распределённые системы

Для цитирования: Кустов Е. Ф., Хуцаева А. Ф., Кирьянова А. П., Иогансон И. Д., Дакуо Ж.- М. Н., Беззатеев С.В. Интеграция квантового распределения ключей с классическими криптографическими схемами: повышение безопасности в условиях постквантовых вызовов // Вестник СибГУТИ. 2025. Т. 19, № 2. С. 98–111. https://doi.org/10.55648/1998-6920-2025-19-2-98-111.

Статья поступила в редакцию 08.03.2025;
переработанный вариант – 30.04.2025;
принята к публикации 05.05.2025.

1. Введение

В современном мире информационной безопасности одной из ключевых задач является обеспечение конфиденциальности и целостности данных. С развитием квантовых технологий, включая квантовые компьютеры и квантовые коммуникации, традиционные криптографические методы становятся уязвимыми. Квантовые компьютеры способны взламывать широко используемые криптографические алгоритмы, такие как RSA и ECC, что ставит под угрозу безопасность данных в будущем. Однако развитие квантовых коммуникаций, в частности квантового распределения ключей (КРК), открыло новые возможности для обеспечения безопасности на основе законов квантовой физики. КРК

позволяет создавать ключи, защищённые от перехвата и взлома, что делает его перспективным инструментом для защиты информации в условиях постквантовой эры.

В данной работе рассматриваются три основных сценария использования КРК в сочетании с различными криптографическими схемами:

1. КРК и схема Блома – для распределения ключей между участниками сети.
2. КРК и KDP (Key Distribution Pattern) – для управления ключами в сетях с большим количеством пользователей.
3. КРК и схема Лагранжа – для разделения секрета между несколькими пользователями.

Каждый из этих сценариев демонстрирует, как квантовые технологии могут быть интегрированы в существующие криптографические протоколы для повышения их безопасности и эффективности. В работе подробно описаны математические основы каждой схемы, их преимущества и недостатки, а также предложены алгоритмы для их реализации в сочетании с КРК. Развитие квантовых коммуникаций не только предоставляет новые инструменты для защиты данных, но и требует пересмотра существующих подходов к криптографии. Внедрение квантовых технологий в криптографические протоколы позволяет создавать системы, устойчивые к атакам как классических, так и квантовых компьютеров. Это особенно важно для критически важных инфраструктур, таких как финансовые системы, государственные сети и системы управления ключами в распределённых системах.

Цель данной работы – продемонстрировать, как квантовое распределение ключей может быть эффективно интегрировано с классическими криптографическими схемами для создания безопасных и масштабируемых решений. Результаты исследования демонстрируют, что комбинация КРК с такими методами, как схема Блома, KDP и схема Лагранжа, обеспечивает высокий уровень безопасности и может быть применена в различных сценариях, включая защищённые сети IoT, облачные вычисления и распределённые системы. В общем виде совместное использование КРК и рассматриваемых схем представлено на рисунке 1.

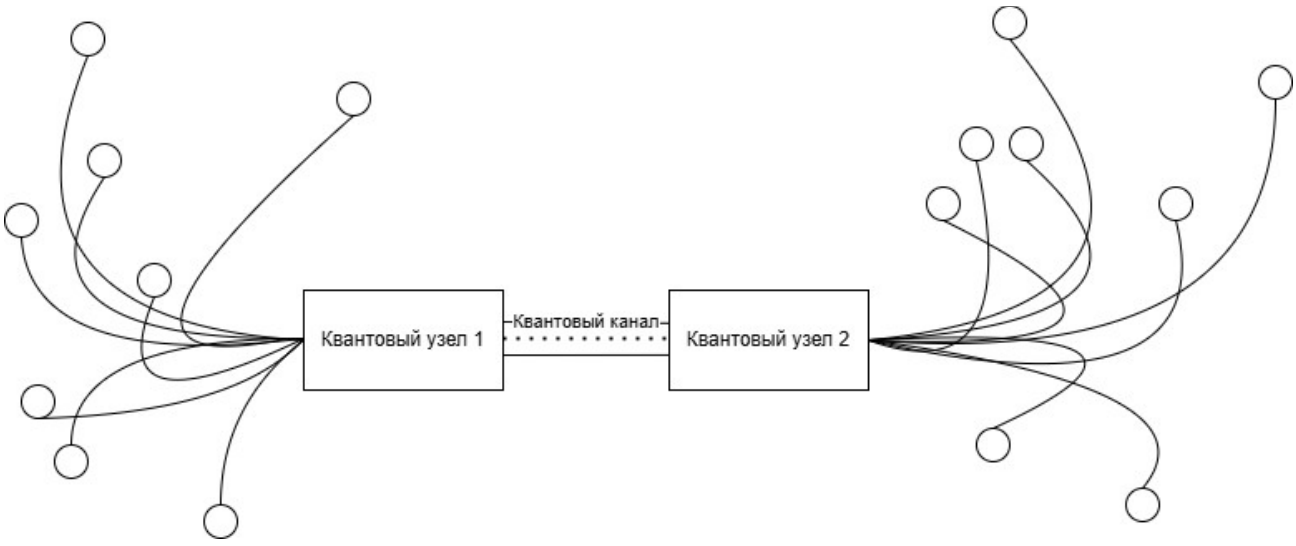

Рис. 1. Совместное использование КРК и классических схем

2. Совместное использование КРК и схемы Блома

Схема Блома — это схема распределения ключей с доверенным центром, которая генерирует секретную симметричную матрицу над конечным полем. После этого доверенный центр при помощи секретной матрицы создаёт и передаёт секретный ключ каждому участнику. Затем участники самостоятельно или при помощи доверенной стороны по секретному ключу создают соответствующий открытый ключ и представляют открытый

ключ доверенному центру, чтобы тот сертифицировал его. После этого пользователи обмениваются своими открытыми ключами, при этом обмен может проходить по незащищённому каналу, и на основе полученных открытых ключей формируют общий сеансовый ключ. В настоящее время схема Блома применяется в протоколе HDCP в целях защиты видео от копирования.

Инициализация:

- На первом этапе доверенный центр выбирает конечное поле $GF(q)$ – чем больше q, тем больше участников может быть задействовано.
- Каждый участник выбирает или получает от доверенного центра свой открытый ключ r_i, где $r_i \in GF(q)$. При этом $r_i \neq r_j$ для $i \neq j$.
- Далее доверенный центр генерирует секретный симметричный многочлен:

$$f(x, y) = \sum_{i=0}^{t} \sum_{j=0}^{t} a_{ij} x^i y^j, a_{ij} = a_{ji},$$

где t – параметр безопасности, $1 \leq t < n$. Коэффициенты a берутся из секретной матрицы $\mathbf{S}^{t \times t}$, хранящейся у доверенного центра.

Распределение ключей:

- Для каждого участника вычисляется полином от одной переменной:

$$g_i(x) = f(x, r_i) = \sum_{i=0}^{t} \sum_{j=0}^{t} a_{ij} x^i r_i^j,$$

- Так как полином f симметричный, то

$$g_i(r_j) = f(r_j, r_i) = f(r_i, r_j) = g_j(r_i)$$

- Для создания общего сеансового ключа два пользователя передают друг другу свои r и вычисляют:

$$g_i(r_j) = g_j(r_i)$$

Добавление нового участника:

1. Новый участник выбирает r_N, который не должен совпадать с r_i.
2. Далее доверенный центр вычисляет $g_N(x)$ и передаёт новому участнику.

Безопасность схемы основывается на сложности восстановления секретной матрицы. Для восстановления матрицы необходимо иметь число ключей, равное количеству строк матрицы.

2.1. Связь с КРК

Рассмотрим вариант применения схемы Блома с КРК, где узел КРК будет выступать в качестве доверенного центра. В начале КРК вырабатывает набор квантовых ключей $Q^{t \times t}$, полученные ключи используются для заполнения секретной матрицы **S**. На данный момент для получения матрицы **S** используется функция формирования ключей (*key derivation function*, KDF). Данная функция не обладает свойствами доказуемой безопасности, в отличие от способа получения ключей с помощью КРК. Также KDF использует в качестве источника начальной ключевой информации генераторы псевдослучайных чисел (ГСПЧ). Современные ГСПЧ, в отличие от КРК, не могут гарантировать случайное распределение полученных ключей. Так, в 2010-м году компания Intel, которая является «доверенным центром» для пользователей системы защиты HDCP, подтвердила, что криптоаналитикам удалось найти секретную матрицу (точнее, аналогичную ей), используемую для генерации ключей в упомянутой системе предотвращения копирования высококачественного видеосигнала.

Разработанный алгоритм работает следующим образом:

1. `QkeyGen()` → **S**: используя квантовый канал связи, доверенные центры вырабатывают n общих секретов длины m и заполняют матрицу $\mathbf{S}^{n \times m}$.

2. ShareKey(**S**, n, k) → $P = g_i(r_j)$: центры генерируют и раздают ключи участникам.

3. RecoverKey(P) → $g_j(r_i)$: с помощью схемы Блома пользователи могут выработать общий сеансовый ключ $g_i(r_j) = g_j(r_i)$.

Вместо использования традиционных методов генерации ключей секретная матрица **S** заполняется с использованием квантовых ключей, полученных с помощью КРК. Это обеспечивает случайность и безопасность матрицы **S**, так как квантовые ключи обладают свойствами доказуемой безопасности. Это означает, что их случайность и безопасность могут быть математически доказаны, что повышает доверие к схеме. Участники сети могут использовать квантовые ключи для генерации своих открытых и секретных ключей. Это повышает безопасность схемы, так как квантовые ключи устойчивы к атакам с использованием квантовых компьютеров. Общий сеансовый ключ, вычисленный с использованием квантовых ключей, также обладает свойствами квантовой безопасности. Это делает его устойчивым к атакам, основанным на перехвате или взломе классических криптографических алгоритмов. В традиционной схеме Блома доверенный центр является единой точкой отказа. Использование КРК позволяет распределить генерацию ключей между несколькими узлами, что снижает риск компрометации системы.

2.2. Пример совместного использования КРК и схемы Блома

Предположим, у нас есть сеть из нескольких участников (например, серверов или устройств), которые должны безопасно обмениваться данными. Для этого необходимо распределить ключи между участниками так, чтобы каждый мог безопасно общаться с любым другим участником. Схема Блома позволяет эффективно распределить ключи, а КРК обеспечивает безопасность генерации и передачи этих ключей.

1. Генерация ключей с использованием КРК: Доверенный центр использует протокол КРК (например, TF-QKD [1], MDI-QKD [2] или CV-QKD [3]) для создания квантовых ключей. Эти квантовые ключи используются для заполнения секретной матрицы **S**. Каждый элемент матрицы **S** заполняется с использованием квантовых ключей.

2. Распределение ключей участникам: для каждого участника i доверенный центр вычисляет полином $(x) = f(x, r_i)$, где $f(x, y)$ – симметричный многочлен, построенный на основе матрицы **S**. Участник i получает свой секретный ключ $g_i(x)$ и открытый идентификатор r_i.

3. Обмен ключами между участниками: участники обмениваются своими открытыми идентификаторами r_i по незащищённому каналу. Для генерации общего ключа между участниками i и j используется формула: $K_{ij} = g_i(r_j) = g_j(r_i)$.

Поскольку $f(x, y)$ симметричен, $g_i(r_j) = g_j(r_i)$, и оба участника получают одинаковый ключ.

Квантовые ключи обеспечивают доказуемую безопасность, а схема Блома гарантирует, что ключи могут быть эффективно распределены между участниками. Система устойчива как к классическим, так и к квантовым атакам. Подход может быть адаптирован для различных сетевых конфигураций и требований безопасности.

3. Совместное использование КРК и KDP

Одной из важных проблем при построении защищённых систем обмена сообщениями между двумя пользователями является управление ключами в схеме с большим количеством участников. Пусть существует сеть пользователей p_1, p_2, …, p_v, которые хотят взаимодействовать только друг с другом по защищённому каналу. Тогда каждая пара пользователей $\{P_i, P_j\}$ должна обладать общим секретным ключом, который используется для шифрования и расшифрования сообщений, отправляемых между ними. Цикл жизни секретного ключа в такой схеме можно разделить на 4 фазы: генерация, обмен, обновление и

уничтожение. Камнем преткновения является вопрос о хранении и обмене сгенерированных секретных ключей.

Основным вариантом для обмена ключами является схема распределения ключей (*key distribution scheme*, KDS). В этом случае предполагается активное участие доверенного центра только на этапе распространения секретной информации. Такой подход не покрывает вопрос защищённости полностью, так как сеть может быть небезопасна, и информация, сгенерированная и распространенная доверенным центром, в теории может быть получена любым пользователем сети.

Для устранения данных недостатков была предложена схема предварительного распределения ключей (*key predistribution scheme*, KPS). Но при таком подходе в сети из v пользователей требуется порядка $O(v^2)$ отдельных ключей для каждой пары $\{P_i, P_j\}$, что при достаточно большом v может стать затруднительно.

Одним из вариантов решения данной проблемы является использование KDP-схемы (*Key Distribution Pattern*). Преимуществом схем такого типа является минимизация объёма хранилища ключей до $O(\lg v)$ и безопасность коммуникации между пользователями.

Введём совокупность $(\mathscr{P}, \mathscr{K}, \mathscr{I})$ такую, что:

- множество пользователей $\mathscr{P} = \{p_1, p_2, \ldots, p_v\}$, где v – количество пользователей, принимающих участие в сети,
- множество подключей $\mathscr{K} = \{k_1, k_2, \ldots, k_m\}$,
- отношение принадлежности $\mathscr{I}$ такое, что $\mathscr{I} \subset \mathscr{P} \times \mathscr{K}$.

Если $(p, k) \in I$ для $p \in \mathscr{P}$ и $k \in \mathscr{K}$, то можно сказать, что p инцидентно k. Отметим обозначения:

- p – конкретный пользователь;
- k – подключ;
- (p) – множество инцидентых пользователю p подключей k;
- (k) – множество инцидентых подключу k пользователей p;
- $r(i) = |(p_i)|$ $(i \in \{1, \ldots, v\})$ – количество инцидентных пользователю p подключей k;
- $k(j) = |(k_j)|$ $(j \in \{1, \ldots, m\})$ – количество инцидентных подключу k пользователей;

Наконец, положим, что $\lambda(i, j) = |(p_i) \cap (p_j)|$ и $s(i, j) = |(k_i) \cap (k_j)|$.

Совокупность $(\mathscr{P}, \mathscr{K}, \mathscr{I})$ будет являться KDP [5] тогда и только тогда, когда выполняется:

$$\forall\, p_i, p_j \in \mathscr{P}, (p_i) \cap (p_j) \subset (p_m) \leftrightarrow (m = i \vee m = j)$$

То есть для построения подобной схемы необходимо построить семейство подмножеств $\mathscr{K}$, что для любой пары подмножеств их пересечение не содержится ни в одном другом подмножестве. Такие семейства называются семействами Шпернера – это семейство подмножеств $S = \{S_1, \ldots, S_n\}$ таких , что при выполнении условия $S_i \cap S_j \subset S_t$ обязательно следует $t = i$ или $t = j$.

Теорема 1 [6]. Если $\mathscr{G}$ – это множество подмножеств множества $\mathscr{K}$, и $\mathscr{G}$ образует семейство Шпернера, то

$$|\mathscr{G}| \le C^m_{m/2},$$

где C^i_j — биномиальный коэффициент, а $m = |\mathscr{K}|$.

В KDP-схемах каждый пользователь знает только инцидентные ему подключи, а отношение принадлежности $\mathscr{I}$, хранящее индексы пользователей и соответствующих подключей, открыто и известно всем пользователям. Тогда если пара пользователей p_i и p_j захочет выработать общий ключ K_{ij}, то они должны вычислить $S_{ij} \subset \{1, \ldots, m\}$ – пересечение множеств индексов, инцидентных подключам пользователей p_i и p_j. Далее вычисляется $K_{ij} = f(\{k_t \mid t \in S_{ij}\})$, где $f()$ – некая односторонняя функция, принимающая на вход множество подключей и дающая на выходе ключ определённой длины.

Примером такой KDP-схемы является подход, предложенный Чэнем и Вэй в [7]. Один из описанных ими алгоритмов строится следующим образом:

Пусть $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ – это структура конечного инцидента, представленная в виде двоичной матрицы 5 × 5

$$\begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{array} \begin{array}{c} \begin{array}{ccccc} x_1 & x_2 & x_3 & x_4 & x_5 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Тогда $\mathcal{K}$ – это схема ($\mathcal{G}$, $\mathcal{F}$)–KDP, где

$$\mathcal{G} = \{\{P_1, P_2, P_4, P_5\}, \{P_2, P_3, P_5\}, \{P_1, P_3, P_4\}, \{P_1, P_2, P_3\}, \{P_1, P_4, P_5\}, \{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_5\}, \{P_1\}, \{P_2\}, \{P_3\}, \{P_5\}\}$$

$$\mathcal{F} = \{\{P_1\}, \{P_2\}, \{P_3\}, \{P_5\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_5\}, \{P_4, P_5\}\}$$

3.1. Связь с КРК

Рассмотрим случай, когда пользователям, находящимся вне квантовой сети, необходимо выработать общий секретный ключ для установки безопасной связи.

Пусть имеется два доверенных центра распределения ключей (*Key Distribution Center*, KDC), соединенных квантовым каналом связи, которые управляют KDP-схемой. Часть пользователей по классическому каналу подключена к доверительному центру №1, а другая часть – к доверительному центру №2. Тогда два доверенных центра могут совместно выработать общее множество подключей $\mathcal{K}$, используя протоколы квантового распределения ключей. Выработав таким образом ключи, они смогут избежать необходимости передавать подключи пользователям, находящимся на большом расстоянии от них, через внешние сети, что позволит снизить риск утечки информации.

Разработанный алгоритм работает следующим образом:

1. `QkeyGen()` $\rightarrow \mathcal{K}$: Используя квантовый канал связи, доверенные центры вырабатывают общее множество случайных подключей $\mathcal{K}$.
2. `IncidencyRelationGen(`$\mathcal{P}, \mathcal{K}$`)` $\rightarrow \mathcal{I}$: Центры генерируют отношение принадлежности $\mathcal{I}$, определяющие инцидентность индексов ключей и пользователей, и публикуют $\mathcal{I}$.
3. `SubkeyDistribution(`$\mathcal{P}, \mathcal{K}, \mathcal{I}$`)` : Доверенные центры распределяют подключи в соответствии с отношением принадлежности $\mathcal{I}$ между своими локальными пользователями.
4. `KDP(`$\mathcal{I}, (p_i), (p_j)$`)` $\rightarrow K_{ij}$: С помощью KDP-схемы пользователи p_i и p_j вырабатывают конечный сессионный ключ.

При совместном использовании схемы КРК и KDP-схемы обеспечивается большая безопасность за счёт законов физики при выработке ключей между доверенными центрами, а KDP-подход к созданию общей сети пользователей поможет снизить общий объём ключей, хранимый для каждой пары (p_i, p_j). Таким образом, квантовая часть обеспечивает безопасность и аутентифицируемость доверенных центров, а схема распределения ключей KDP обеспечит более выгодное (с точки зрения памяти) хранение всего объёма ключевой информации.

В случае, если пользователи хотят выработать общий ключ, но у них нет возможности получить его от доверенного центра, или они не хотят делиться им с доверенным центром, то КРК обеспечивает возможность генерации защищённых ключей в схеме «точка-точка», а масштабируемость данного подхода от двух до n пользователей поможет организовать KDP-схему.

3.2. Пример совместного использования КРК и KDP-схемы

Пусть есть несколько участников сети, которые хотят установить попарную безопасную связь, не имея возможности получить ключи от доверенного центра.

Первым шагом для установки безопасной связи будет начальное распределение ключей с использованием КРК: это включает в себя настройку оборудования на каждом узле, передачу квантовых состояний по оптическому каналу и создание общего ключа путём установки базисов и просеивания ключевого материала по классическому каналу.

После этого используется KDP-схема для эффективного управления ключами. Применяя схему KDP, каждая пара пользователей периодически обновляет свои общие ключи. Например, они могут решить генерировать новый ключ каждый час или после каждых 100 сообщений. Процесс генерации квантовых ключей повторяется для генерации новых ключей в соответствии с графиком KDP-схемы.

Кроме того, КРК может быть использован для создания квантового ключа, который впоследствии будет применён для шифрования сеансовых ключей (то есть формирования квантово-защищённых ключей). А схема оптимального и эффективного распределения полученных квантово-защищённых ключей будет построена по типу KDP.

4. Совместное использование КРК и схемы Лагранжа

Схема разделения секрета на основе интерполяционного многочлена Лагранжа – это криптографический метод, предложенный Ади Шамиром в 1979 году. Она обеспечивает безопасное разделение секретной информации на несколько частей (долей), при этом для восстановления оригинала требуется лишь заранее определённое минимальное их количество. Схема основывается на интерполяции полиномов над конечными полями, что гарантирует её стойкость к атакам и возможность гибкого управления доступом к секретной информации. Этот метод активно применяется в системах, где необходимо распределить доступ к данным между несколькими участниками или разделить ключ для надежного хранения и применения.

Актуальность использования схемы Лагранжа возрастает с развитием технологий распределённых систем и блокчейна. Системы децентрализованных финансов, распределённые хранилища данных и смарт-контракты используют данный подход для повышения безопасности при управлении приватными ключами и другими критически важными данными. Также исследования в этой области включают расширение схемы на динамические и адаптивные сценарии, такие как обновление долей без раскрытия исходного секрета.

Эффективность схемы Лагранжа в условиях возрастающих угроз кибербезопасности делает её одним из ключевых инструментов в современном криптографическом арсенале. Она позволяет минимизировать риск единой точки отказа, что особенно важно для организаций, работающих с конфиденциальными данными. Среди направлений дальнейшего развития – улучшение производительности и расширение применения в таких областях, как интернет вещей (IoT), распределённые реестры и облачные вычисления.

Опишем работу схемы Лагранжа.

Подготовительный этап. Пусть необходимо разделить секрет S между n пользователями, чтобы k из них смогли восстановить его (пороговая схема k – n). Выбирается простое число $p > S$. Оно задает поле $GF(p)$. Над этим полем строится многочлен степени $k - 1$:

$$F(x) = a_{k-1}\, x^{k-1} + a_{k-2}\, x^{k-2} + \ldots + a_1\, x + S \pmod{p}$$

В этом многочлене S – это разделяемый секрет, а остальные коэффициенты a_i – некоторые случайные числа, которые нужно будет «забыть» после того, как процедура разделения секрета будет завершена.

Генерация долей секрета. Вычисляются доли следующим образом в n различных точках, при условии, что $x = 0$.

$$k_1 = F(1) = a_{k-1} \cdot 1^{k-1} + a_{k-2} \cdot 1^{k-2} + \ldots + a_1 \cdot 1 + S \pmod p$$
$$k_2 = F(2) = a_{k-1} \cdot 2^{k-1} + a_{k-2} \cdot 2^{k-2} + \ldots + a_1 \cdot 2 + S \pmod p$$
$$\ldots$$
$$k_i = F(i) = a_{k-1} \cdot i^{k-1} + a_{k-2} \cdot i^{k-2} + \ldots + a_1 \cdot i + S \pmod p$$
$$\ldots$$
$$k_n = F(n) = a_{k-1} \cdot n^{k-1} + a_{k-2} \cdot n^{k-2} + \ldots + a_1 \cdot n + S \pmod p$$

Аргументы могут быть любыми, а главное, разными по модулю p. После формирования каждый участник получает пару (k_i, x), где $x = i$, а a_i и S «забывается».

Восстановление секрета. Собираются любые k и больше участников, которые могут восстановить секретное значение. Это происходит с помощью вычисления интерполяционного многочлена Лагранжа. Формула выглядит следующим образом:

$$F(x) = \sum_i l_i(x) k_i \pmod p$$
$$l_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \pmod p$$

4.1. Связь с КРК

Рассмотрим сценарий с двумя доверенными центрами, каждый из которых способен генерировать квантовый ключ. В этом случае оба центра могут совместно выработать секрет S, представляющий собой квантовый ключ, и затем разделить его между n пользователями с помощью схемы Лагранжа. При этом устанавливается порог k, что означает: для восстановления исходного секрета потребуется объединение как минимум k долей. Такая структура позволяет гарантировать высокий уровень безопасности, так как восстановление секрета невозможно при отсутствии минимально необходимого количества долей.

Важно отметить, что данная схема применима и в контексте квантовых ключей. Пользователи могут объединить свои доли и восстановить секрет S, сохранив квантовые свойства ключа, даже если его передача происходит вне квантовой сети. Это становится возможным благодаря тому, что процесс разделения и восстановления ключа по схеме не изменяет квантовую природу секретных данных, обеспечивая их целостность и конфиденциальность в условиях классических каналов связи. Таким образом, использование схемы Лагранжа в комбинации с квантовой криптографией обеспечивает надежный способ управления доступом к секретным квантовым данным в распределенных системах.

Разработанный алгоритм работает следующим образом:

1. `QkeyGen()` → S: Используя квантовый канал связи, доверенные центры вырабатывают общий секрет S.
2. `ShareKey(`S`,`n`,`k`)` → $P = k_i, x$: Центры генерируют и раздаются доли секретов участникам.
3. `RecoverKey(`P`)` → S: С помощью схемы Лагранжа пользователи восстанавливают секрет S.

4.2. Примеры использования КРК и схемы Лагранжа

Предположим, что в облачной инфраструктуре требуется надёжное хранение квантовых ключей, используемых для шифрования данных. Однако доверять одной облачной платформе хранение всего ключа небезопасно, так как возможны утечки данных

или атаки на хранилище. Для защиты ключа можно использовать комбинацию КРК и схемы Лагранжа:

1. Два квантовых узла (например, в дата-центрах разных провайдеров) проводят квантовое распределение ключа, формируя общий секретный ключ S.
2. Разделение ключа: ключ S разделяется на n частей с порогом восстановления k с использованием схемы Лагранжа.
3. Распределённое хранение: доли секретного ключа хранятся в разных облачных провайдерах или распределённых узлах сети.
4. Восстановление ключа: когда пользователю или сервису требуется ключ для расшифрования данных, достаточно получить хотя бы k долей из n и восстановить ключ с помощью интерполяции Лагранжа.

Преимущества подобного подхода:

- Квантовая безопасность за счёт использования ключей, переданных по КРК.
- Защита от компрометации облачного провайдера, так как утечка одной или нескольких частей ключа не приведёт к его раскрытию.
- Гибкость в управлении доступом, поскольку можно менять порог восстановления k в зависимости от уровня доверия к участникам системы.

Этот подход может применяться для защиты критически важных данных, таких как финансовые транзакции, зашифрованные документы или государственные архивы.

Другим примером использования предложенного подхода может быть система управления доступом к квантовым данным, и требуется гарантировать, что доступ к секретной информации возможен только при наличии нескольких доверенных лиц. Простая аутентификация пользователя (например, паролем или биометрией) недостаточна, так как в случае компрометации учётных данных злоумышленник сможет получить полный доступ к данным.

1. Генерация квантового ключа: квантовые узлы выполняют распределение квантового ключа S между участниками системы безопасности. Этот ключ предназначен для расшифрования конфиденциальных данных.
2. Разделение ключа по схеме Лагранжа: ключ делится на n частей, например, между главным администратором, начальником отдела безопасности и независимым аудитором. Устанавливается порог k, например 2 из 3, что означает, что для доступа к данным необходимо участие минимум двух из трёх доверенных лиц.
3. Авторизация и доступ к данным: когда кто-то из сотрудников требует доступ к квантово-защищённым данным, система проверяет, есть ли у него необходимые части ключа. Если у него только одна доля, доступ заблокирован. Если два или более участника вводят свои части ключа, система восстанавливает секретный ключ и предоставляет доступ.

Преимущества подобного подхода такие же как и у предыдущего варианта.

5. Безопасность

Безопасность предложенных схем, объединяющих квантовое распределение ключей и криптографические методы (схема Блома, KDP и схема Лагранжа), основывается на безопасности их составных частей. Рассмотрим каждый из компонентов и их вклад в общую безопасность системы.

КРК обеспечивает безопасность на уровне квантовой механики, что делает его устойчивым к атакам с использованием классических и квантовых компьютеров. Основные принципы безопасности КРК:

1. Теорема о запрете клонирования: злоумышленник не может скопировать неизвестное квантовое состояние без разрушения его суперпозиции. Это исключает возможность скрытого перехвата квантовых ключей.

2. Эффект измерения: любое вмешательство злоумышленника в процесс передачи ключа приводит к неизбежным изменениям квантовых состояний, которые могут быть детектированы.

3. Информационно-теоретическая безопасность: КРК обеспечивает абсолютную безопасность, так как любая попытка перехвата ключа нарушает квантовое состояние и может быть обнаружена.

Схема Блома обеспечивает безопасность за счёт сложности восстановления секретной матрицы S. Основные аспекты безопасности:

1. Сложность восстановления матрицы: для восстановления секретной матрицы S необходимо иметь доступ к большому количеству ключей, что делает эту задачу вычислительно сложной.

2. Использование квантовых ключей: заполнение матрицы S с использованием квантовых ключей, полученных через КРК, обеспечивает случайность и доказуемую безопасность.

3. Минимизация риска единой точки отказа: использование КРК позволяет распределить генерацию ключей между несколькими узлами, что снижает риск компрометации системы.

KDP обеспечивает безопасность за счёт использования семейства Шпернера и минимизации объёма хранилища ключей. Основные аспекты безопасности:

1. Семейство Шпернера: пересечение любых двух подмножеств подключей не содержится в других подмножествах, что делает невозможным восстановление ключа без необходимого количества подключей.

2. Использование квантовых ключей: квантовые ключи, полученные через КРК, обеспечивают случайность и безопасность подключей K.

3. Минимизация риска компрометации: даже если злоумышленник получит доступ к некоторым подключам, он не сможет восстановить общий ключ без необходимого количества подключей.

Схема Лагранжа обеспечивает безопасность за счёт интерполяции полиномов над конечными полями. Основные аспекты безопасности:

1. Информационно-теоретическая безопасность: любое количество долей меньше порога k не даёт никакой информации о секрете S, так как соответствующие уравнения недоопределены.

2. Использование квантовых ключей: квантовые ключи, полученные через КРК, обеспечивают случайность и безопасность секрета S.

Безопасность всей системы, объединяющей КРК и криптографические схемы (Блома, KDP и Лагранжа), строится на общих принципах. Каждый из компонентов системы (КРК, схема Блома, KDP и схема Лагранжа) обладает доказанной безопасностью, что делает всю систему устойчивой к атакам. Использование квантовых ключей делает систему устойчивой к атакам с использованием квантовых компьютеров. Распределение ключей и секретов между несколькими узлами снижает риск единой точки отказа.

Предложенные схемы, объединяющие КРК и криптографические методы (схему Блома, KDP и схему Лагранжа), обеспечивают высокий уровень безопасности благодаря использованию квантовых ключей и информационно-теоретически безопасных криптографических протоколов. Это делает их пригодными для использования в постквантовую эпоху, где традиционные методы шифрования становятся уязвимыми.

6. Заключение

В данной работе рассмотрены три основных сценария совместного использования КРК с криптографическими схемами: схемой Блома, KDP (Key Distribution Pattern) и схемой Лагранжа. Каждый из этих подходов демонстрирует, как квантовые технологии могут быть

интегрированы в существующие криптографические протоколы для повышения их безопасности и эффективности.

Все рассмотренные схемы обеспечивают информационно-теоретическую безопасность, что делает их устойчивыми к атакам с использованием как классических, так и квантовых компьютеров. Использование квантовых ключей устраняет уязвимости, связанные с классическими методами генерации ключей, такими как генераторы псевдослучайных чисел. Предложенные подходы могут быть адаптированы для различных приложений, включая защищённые сети IoT, облачные вычисления и распределённые системы.

Комбинация КРК с криптографическими схемами (Блома, KDP и Лагранжа) является перспективным решением для обеспечения безопасности в эпоху постквантовой криптографии. Эти подходы сочетают в себе преимущества квантовой криптографии и эффективных методов распределения ключей, что делает их пригодными для защиты данных в современных распределённых системах. Дальнейшие исследования в этой области позволят расширить область применения и повысить эффективность предложенных методов.

Литература

1. *Lucamarini M. et al.* Overcoming the rate–distance limit of quantum key distribution without quantum repeaters //Nature. – 2018. – Т. 557. – №. 7705. – С. 400-403.
2. *Lo H. K., Curty M., Qi B.* Measurement-device-independent quantum key distribution //Physical review letters. – 2012. – Т. 108. – №. 13. – С. 130503.
3. *Zhang Y. et al.* Long-distance continuous-variable quantum key distribution over 202.81 km of fiber //Physical review letters. – 2020. – Т. 125. – №. 1. – С. 010502.
4. *Dyer M. et al.* On key storage in secure networks //Journal of Cryptology. – 1995. – Т. 8. – С. 189-200.
5. *Mitchell C. J., Piper F. C.* Key storage in secure networks //Discrete applied mathematics. – 1988. – Т. 21. – №. 3. – С. 215-228.
6. *Sperner E.* Ein satz über untermengen einer endlichen menge //Mathematische Zeitschrift. – 1928. – Т. 27. – №. 1. – С. 544-548.
7. *Chen S., Wei H.* Constructions for key distribution patterns //Frontiers of Mathematics in China. – 2017. – Т. 12. – С. 301-323.
8. *Shamir A.* How to share a secret //Commun. ACM. – 1979. – Т. 22. – С. 612-613.
9. *Nakamoto S.* Bitcoin: A peer-to-peer electronic cash system. – 2008.
10. *Мазур Э. М.* Распределенные системы хранения данных: анализ, классификация и выбор //Перспективы развития информационных технологий. – 2015. – №. 26. – С. 33-60.
11. *Вашкевич А. М.* Смарт-контракты: что, зачем и как //М.: Симплоер. – 2018. – Т. 89.
12. *Wootters W. K., Zurek W. H.* A single quantum cannot be cloned //Nature. – 1982. – Т. 299. – №. 5886. – С. 802-803.
13. Ekert A. K. Quantum cryptography based on Bell's theorem //Physical review letters. – 1991. – Т. 67. – №. 6. – С. 661.
14. *Gisin N. et al.* Quantum cryptography //Reviews of modern physics. – 2002. – Т. 74. – №. 1. – С. 145.
15. *Golub G. H., Van Loan C. F.* Matrix computations, 4th //Johns Hopkins. – 2013.
16. *Bennett C. H., Brassard G*. Quantum cryptography: Public key distribution and coin tossing //Theoretical computer science. – 2014. – Т. 560. – С. 7-11.
17. *Shannon C. E.* Communication theory of secrecy systems //The Bell system technical journal. – 1949. – Т. 28. – №. 4. – С. 656-715.

Кустов Елизар Филаретович
аспирант факультета безопасности информационных технологий, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО, 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А), тел. +79818341460, e-mail: elizarkustov@mail.ru, ORCID ID: 0000-0002-0191-1178.

Хуцаева Алтана Феликсовна
аспирант факультета безопасности информационных технологий, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО, 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А), e-mail: afkhutsaeva@itmo.ru, ORCID ID: 0000-0001-5494-7142.

Кирьянова Анастасия Павловна
аспирант факультета безопасности информационных технологий, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО, 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А), e-mail: anastacia.kiryanova@itmo.ru, ORCID ID: 0009-0006-0344- 5111.

Иогансон Иван Дмитриевич
аспирант факультета безопасности информационных технологий, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО, 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А), тел. +7 905 227 85 19, e-mail: ivan.ioganson@yandex.ru, ORCID ID: 0000-0002-0856-2249.

Дакуо Жан-Мишель Никодэмович
аспирант факультета безопасности информационных технологий, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО, 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А), тел. +7 921 786 31 22, e-mail: jeandakuo@mail.ru, ORCID ID: 0000-0002-4084-8829.

Беззатеев Сергей Валентинович
д.т.н., профессор, заведующий кафедрой информационной безопасности, института кибернетических систем Санкт-Петербургского университета аэрокосмического приборостроения, директор лаборатории криптографических методов защиты информации, ФБИТ, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО, 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А), e-mail: sergey.bezzateev@gmail.com, ORCID ID: 0000-0002- 0924-6221.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внёс равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Integration of Quantum Key Distribution with Classical Cryptographic Schemes: Enhancing Security in the Face of Post-Quantum Challenges

E. Kustov[1] , A. Khutsaeva[1,2] , A. Kiryanova[1] , I. Ioganson[1] , Z.-M. Dakuo[1,2] , S. Bezzateev[1,2]

[1] ITMO University
[2] Saint-Petersburg State University of Aerospace Instrumentation

Abstract: The paper explores approaches to ensuring information security using quantum key distribution (QKD) in combination with classical cryptographic schemes: the Blom scheme, Key Distribution Pattern (KDP), and the Lagrange scheme. It demonstrates how quantum technologies enhance the security and efficiency of these methods. The proposed schemes provide resilience against attacks by both classical and quantum computers, addressing vulnerabilities in traditional key generation methods. Examples of applications in secure IoT networks, cloud computing, and distributed systems are discussed. The results show that the combination of QKD with cryptographic schemes is a promising solution for the post-quantum era.

Keywords: Quantum key distribution (QKD), Blom's scheme, Key Distribution Pattern (KDP), Lagrange scheme, information security, distributed systems.

For citation: Kustov E. F., Khutsaeva A. F., Kiryanova A. P., Ioganson I. D., Dakuo Z.-M. N. P., Bezzateev S. Integration of Quantum Key Distribution with Classical Cryptographic Schemes: Enhancing Security in the Face of Post-Quantum Challenges // Vestnik SibGUTI, 2025, vol. 19, no. 2, pp. 98–111. https://doi.org/10.55648/1998-6920-2025-19-2-98-111.

The article was submitted: 08.03.2025;
revised version: 30.04.2025;
accepted for publication 05.05.2025.

References

1. Lucamarini M. et al. *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters*. Nature, 2018, vol. 557, no. 7705, pp. 400-403.
2. Lo H. K., Curty M., Qi B. *Measurement-device-independent quantum key distribution*. Physical review letters, 2012, vol. 108, no. 13, pp. 130503.
3. Zhang Y. et al. *Long-distance continuous-variable quantum key distribution over 202.81 km of fiber*. Physical review letters, 2020, vol. 125, no. 1, pp. 010502.
4. Dyer M. et al. *On key storage in secure networks*. Journal of Cryptology, 1995, vol. 8, pp. 189-200.
5. Mitchell C. J., Piper F. C. *Key storage in secure networks*. Discrete applied mathematics, 1988, vol. 21, no. 3, pp. 215-228.
6. Sperner E. *Ein satz über untermengen einer endlichen menge*. Mathematische Zeitschrift, 1928, vol. 27, no. 1, pp. 544-548.
7. Chen S., Wei H. *Constructions for key distribution patterns*. Frontiers of Mathematics in China, 2017, vol. 12, pp. 301-323.
8. Adi S. *How to share a secret*. Commun. ACM, 1979, vol. 22, pp. 612-613.
9. Nakamoto S. *Bitcoin: A peer-to-peer electronic cash system*. 2008.
10. Mazur E. M. *Raspredelennye sistemy hraneniya dannyh: analiz, klassifikaciya i vybor*. Perspektivy razvitiya informacionnyh tekhnologij, 2015, no. 26, pp. 33-60.
11. Vashkevich A. M. *Smart-kontrakty: chto, zachem i kak*. M.: Simploer, 2018, vol. 89.
12. Wootters W. K., Zurek W. H. *A single quantum cannot be cloned*. Nature, 1982, vol. 299, no. 5886, pp. 802-803.

13. Ekert A. K. *Quantum cryptography based on Bell's theorem*. Physical review letters, 1991, vol. 67, no. 6, pp. 661.
14. Gisin N. et al. *Quantum cryptography*. Reviews of modern physics, 2002, vol. 74, no. 1, pp. 145.
15. Golub G. H., Van Loan C. F. *Matrix computations, 4th*. Johns Hopkins, 2013.
16. Bennett C. H., Brassard G. *Quantum cryptography: Public key distribution and coin tossing*. Theoretical computer science, 2014, vol. 560, pp. 7-11.
17. Shannon C. E. *Communication theory of secrecy systems*. The Bell system technical journal, 1949, vol. 28, no. 4, pp. 656-715.

Elizar F. Kustov
PhD student, Faculty of Information Security Technologies, Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO"(ITMO University, 197101, Saint Petersburg, Kronverksky Ave., 49, lit. A), phone +7 981 834 14 60, e-mail: elizarkustov@mail.ru, ORCID ID: 0000-0002-0191-1178.

Altana F. Khutsaeva
PhD student, Faculty of Information Security Technologies, Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO"(ITMO University, 197101, Saint Petersburg, Kronverksky Ave., 49, lit. A), e-mail: afkhutsaeva@itmo.ru, ORCID ID: 0000-0001-5494-7142.

Anastasia P. Kiryanova
PhD student, Faculty of Information Security Technologies, Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO"(ITMO University, 197101, Saint Petersburg, Kronverksky Ave., 49, lit. A), e-mail: anastacia.kiryanova@itmo.ru, ORCID ID: 0009-0006-0344-5111.

Ivan D. Ioganson
PhD student, Faculty of Information Security Technologies, Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO"(ITMO University, 197101, Saint Petersburg, Kronverksky Ave., 49, lit. A), phone +7 905 227 85 19, e-mail: ivan.ioganson@yandex.ru, ORCID ID: 0000-0002-0856-
2249.

Zhan-Michel N. Dakuo
PhD student, Faculty of Information Security Technologies, Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO"(ITMO University, 197101, Saint Petersburg, Kronverksky Ave., 49, lit. A), phone +7 921 786 31 22, e-mail: jeandakuo@mail.ru, ORCID ID: 0000-0002-4084-8829.

Sergey V. Bezzateev
PhD, Professor, Head of the Department of Information Security, Institute of Cybernetic Systems, St. Petersburg University of Aerospace Instrumentation, director of Laboratory of Cryptographic methods for information security, FSIT, Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO"(ITMO University, 197101, Saint Petersburg, Kronverksky Ave., 49, lit. A), e-mail: sergey.bezzateev@gmail.com, ORCID ID: 0000-0002-0924-6221.