О НЕКОТОРЫХ ПРИКЛАДНЫХ АСПЕКТАХ КВАНТОВОЙ КРИПТОГРАФИИ В КОНТЕКСТЕ РАЗВИТИЯ КВАНТОВЫХ ВЫЧИСЛЕНИЙ И ПОЯВЛЕНИЯ КВАНТОВЫХ КОМПЬЮТЕРОВ

***Корольков Андрей Вячеславович**, кандидат технических наук, доцент, г. Москва*

Рассмотрены прикладные и теоретические вопросы становления квантово-криптографических технологий. Проанализированы взаимосвязанные элементы, составляющие понятие и определяющие прикладное содержание квантовой криптографии. Представлен системный анализ квантовых алгоритмов, квантового шифрования и квантового хеширования. Дано обоснование развития специализированных квантовых компьютеров, ориентированных на решение криптографических задач. Представлен прогноз развития области квантовых коммуникаций. Особо отмечены ближайшие перспективы развития средств квантового распределения криптографических ключей, квантовых каналов связи, каналов связи на основе квантовой телепортации, квантовых сетей высокоточной синхронизации для защищенных систем управления. Отмечено самостоятельное значение квантовой генерации случайных чисел.

***Ключевые слова**: квантовая криптография, вычислительные алгоритмы, квантовое шифрование, квантовая хеш-функция, квантовая цифровая подпись.*

ABOUT SOME APPLIED ASPECTS OF QUANTUM CRYPTOGRAPHY IN THE CONTEXT OF DEVELOPMENT OF QUANTUM CALCULATIONS AND EMERGENCE OF QUANTUM COMPUTERS

***Andrei Korol'kov**, Ph.D., Associate Professor, Moscow*

The applied and theoretical aspects of quantum-cryptographic technologies are considered. The interrelated elements that make up the concept and content determined by the application of quantum cryptography are analyzed. The systematic analysis of quantum algorithms, quantum cryptography and quantum hashing are presented. The development of specialized quantum computers, focused on solving cryptographic problems is justified. The forecast of development of the field of quantum communication is done. The immediate prospects for the development of means of quantum cryptographic key distribution, quantum communication channels, channels of communication based on quantum teleportation, quantum networks of high-precision synchronization for secure management systems are highlighted. The independent significance of quantum random number generation is noted.

***Keywords**: quantum cryptography, computational algorithms, quantum cryptography, quantum hash function, quantum digital signature.*

Введение

Современный уровень развития технологий в области оптики и электроники, немыслимый без широкого использования достижений квантовой теории, неизбежно влечет за собой создание и внедрение в будущем технологий обработки информации, функционирующих на принципах квантовой оптики и квантовой теории информации. Первые практические приложения таких технологий относятся к области защиты информации и обобщенно называются квантовой *криптографией*. Одна из таких технологий - квантовое распределение ключей (КРК) - в настоящее время

вышла на уровень коммерчески доступных изделий, с ближайшей перспективой их сертификации и внедрения в современные телекоммуникационные системы. Безусловная секретность ключей в КРК основана на двух фундаментальных запретах квантовой теории [2]: 1) невозможности копирования неизвестного квантового состояния; 2) невозможности достоверного различения неортогональных квантовых состояний.

Другая квантово-криптографическая технология - квантовое шифрование (КШ), представляет собой развитие базовых идей КРК с целью более *эффективного* (по сравнению с КРК) и *криптографически более стойкого* (по сравнению с классическими шифраторами) решения задачи прямого шифрования данных в современных оптических телекоммуникациях (как волоконно-оптических, так и работающих в открытом пространстве).

В настоящее время в мире наблюдается расширение количества научных программ, посвященных развитию квантовых информационных технологий (далее – КИТ). Основные цели таких программ – достижение превосходства в области квантовой связи и квантовых вычислений – тесно связаны с областью квантовой криптографии. Ниже будут рассмотрены современные достижения по ряду важных областей КИТ, по результатам анализа которых будет сделана попытка спрогнозировать перечень актуальных направлений их развития.

1. Квантовые вычисления и компьютеры

Известно, что на квантовом компьютере принципиально можно решать любые математические задачи, в том числе - задачи криптографического анализа и синтеза. Вопрос в том, насколько эффективно по времени будет это решение. Ускорение вычислительного процесса в работе квантовых устройств объясняется свойством квантового параллелизма. Оно состоит в том, что элементарным шагом при квантовых вычислениях является унитарная операция над n-кубитовой суперпозицией регистра из n кубитов. При этом выполняется параллельная обработка сразу всех 2^n возможных состояний. Для классического компьютера подобная операция требует 2^n шагов.

Квантовая вычислительная система, включающая 1000 эффективно используемых кубитов, эквивалентна использованию $2^n = 2^{1000} = 10^{301}$ битов в классической вычислительной системе. Для сравнения необходимо отметить, что количество элементарных частиц (нуклонов) во Вселенной «всего» примерно 10^{78}. Таким образом, квантовый регистр, состоящий из 1000 кубитов, эффективно используемых для вычислений, является достаточным для решения практически значимых задач.

Большинство из известных на сегодня эффективных квантовых алгоритмов можно условно разделить на две группы: дающие экспоненциальный выигрыш (например, алгоритм Шора) и дающие квадратичный выигрыш (например, алгоритм Гровера).

В связи с тем, что класс задач, решаемых квантовыми алгоритмами за полиномиальное время, пока не удается расширить очень существенно, большое внимание во всем мире уделяется анализу алгоритма Шора и других полиномиальных алгоритмов с целью выявления общности и важнейших свойств этих алгоритмов, а также соответствующих задач, позволяющих добиться полиномиальности.

Систематизация алгоритмов типа Шора для задач алгебры, может быть основана на том, что алгоритм Шора содержит принципиальное ядро и окружение, позволяющее сводить исходную задачу к этому ядру. В алгоритме Шора таким ядром является алгоритм нахождения периода относительно возведения в степень, а именно, нахождение для данных взаимно простых натуральных чисел a и q наименьшего положительного t такого, что $a^t \equiv 1 (\mathrm{mod}\ q)$. Поскольку задача нахождения периода является частным случаем задачи о скрытой подгруппе, большое внимание современными исследователями уделяется изучению особенностей квантовых алгоритмов решения этой задачи, а также связанной с ней задачи об изоморфизме графов.

В результате анализа алгоритмов Шора и Саймона, также сводящегося к задаче о скрытой подгруппе, можно выделить их важные общие части и различия. Так, эти алгоритмы используют идею перехода от группы G к некоторому двойственному объекту, действия с двойственным объектом и перехода обратно. При этом в них используются квантовые преобразования Фурье на группе G. Основным ядром в этих алгоритмах является квантовая подпрограмма, которая по заданному отображению абелевой группы в конечное множество строит специальное вероятностное распределение на группе характеров исходной группы. Анализ показал, что в настоящее время известны три варианта квантовых алгоритмов для задачи о скрытой подгруппе. Два из них находят порядок максимальной циклической подгруппы в скрытой факторгруппе. Третий находит саму скрытую подгруппу.

Интересные результаты дает рассмотрение особенностей квантовых алгоритмов, содержащих различные интегральные преобразования. Показано, что для них оказываются полезными некоторые принципы построения классических быстрых ортогональных преобразований. На сегодня известны рекуррентные структуры на основе квантовых вентилей для квантовых алгоритмов, реализующих следующие ортогональные преобразования (Фурье, Уолша-Адамара, Хартли, а также Wavelet- и Слэнт-преобразование).

Все эти преобразования требуют для своей реализации не более $O(n^2)$ операций на квантовом компьютере с квантовым регистром длины n.

Исследователями выделен также ряд задач алгебры, в которых применение квантового преобразования Фурье дает значительное ускорение. Среди них: задача о сдвиге, задача о скрытом смежном классе, задача о сдвигах характеров конечных полей. Рассмотрены особенности решения задач, связанных с задачей о скрытой подгруппе, когда исходная группа не является абелевой.

Интересны с точки зрения криптографических приложений исследования по оценке трудоемкости квантового алгоритма дискретного логарифмирования Шора для случая группы точек эллиптической кривой, определенной над конечным простым полем.

Сегодня можно утверждать также, что в эффективные квантовые алгоритмы может быть трансформирован ряд современных алгоритмов в области алгебраической геометрии и алгебраической теории чисел. Например, были рассмотрены квантовые алгоритмы, основанные на арифметических свойствах эллиптических и гиперэллиптических кривых над конечными полями. В ходе анализа проблемы дискретного логарифма в группах Якоби гиперэллиптических кривых был предложен способ усовершенствования алгоритма факторизации с использованием сумм Якоби за счет применения субэкспоненциального по трудоемкости алгоритма Ленстры на этапе предварительных вычислений. Эти результаты послужили основой для предположения о том, что эффективными квантовыми реализации могут обладать и итерационные алгоритмы, использующие эллиптические интегралы. Недавно был проведен анализ особенностей реализации итерационных алгоритмов, использующих эллиптические интегралы и метод арифметико-геометрического среднего. Описан высокоэффективный метод построения итерационных алгоритмов, использующий полные эллиптические интегралы, для вычисления значений различных алгебраических функций, тэта-функции и модулярных уравнений.

Современные разработки квантовых алгоритмов ориентированы во многом на новые *направления в создании квантовых вычислительных систем*:

- стандартные квантовые вычислительные системы - квантовые системы, в которых выполнение вычислительных алгоритмов осуществляется с использованием универсального набора квантовых логических гейтов:

- квантовые вычислительные операции на ионах и нейтральных атомах в ловушках; квантовые компьютеры на молекулярных кластерах, квантовые вычислительные устройства на NV-центрах в алмазах; твердотельные кубиты на квантовых точках и вычислительные устройства на их основе;

- квантовые вычислительные устройства на сверхпроводниковых структурах (зарядовые, фазовые и гибридные кубиты на контактах Джозефсона);

- нестандартные квантовые вычислительные системы - квантовые системы, в которых выполнение вычислительных алгоритмов осуществляется без использования универсального набора квантовых логических гейтов): компьютеры, реализующие однонаправленные (one-way) квантовые вычисления; топологические квантовые компьютеры; адиабатические квантовые процессоры.

Данные направления сопровождаются развитием обеспечивающих направлений теории, среди которых выделяются такие, как теория квантовой информации, теория преодоления процессов декогерентизации, алгоритмы квантовых вычислений, методы коррекции ошибок, квантовая память, моделирование работы квантовых вычислителей.

2. Направления развития прикладной квантовой криптографии.

Указанные выше продвижения в области квантовых вычислений накладывают свой отпечаток на работы в области квантовой криптографии и квантовой передачи информации, которые можно сгруппировать по следующим направлениям:

- технологии квантового распределения ключа (КРК) и квантового шифрования в оптоволоконных каналах связи и в открытом пространстве;

- технологии квантового хеширования и квантовой цифровой подписи;

- квантовый криптоанализ;

- технологии квантового сверхплотного кодирования информации с использованием «запутан-

ных» и «гиперзапутанных» частиц (один квантовый бит (кубит) может переносить до двух обычных битов), что позволяет увеличить пропускную способность канала квантовой связи;

- методы и алгоритмы кодирования в системах квантовой передачи информации.

С учетом важности для области квантовой криптографии, остановимся на задачах квантового шифрования и квантовой цифровой подписи.

3. Квантовое шифрование.

Первым примером квантового шифрования (КШ) стала технология потокового шифрования AlphaEta, разработанная по гранту DARPA в США. Принцип шифрования информации, использованный в AlphaEta, базируется на использовании многоуровневого кодирования поляризационных или фазовых степеней свободы когерентных оптических состояний, являющихся в общем случае многофотонными. Система шифрования AlphaEta уже прошла практическую апробацию на реальных волоконно-оптических линиях связи. В частности, в 2004 г. была продемонстрирована возможность ее использования с потоком данных на скорости до 250 Мбит/с в обычных оптоволоконных сетях со спектральным разделением сигналов. Скорость передачи шифрованных данных составляла 155 Мбит/с, квантовый ключ длиной 1 Кбит обновлялся каждые 3 секунды. AlphaEta также была успешно протестирована на существующей волоконно-оптической линии связи длиной около 850 км между Вашингтоном и Бостоном. В этом тесте скорость передачи зашифрованных данных составляла 622 Мбит/с, длина волны фотонов - 1550 нм. Американская компания NuCrypt сообщала о готовности коммерциализировать свою версию системы фотонной криптографии AlphaEta.

В технологии КШ используются те же физические методы кодирования передаваемых состояний, что и в системах КРК, с той разницей, что передаваемые информационные состояния являются не однофотонными, а малофотонными (мезоскопическими). Малофотонность информационных состояний позволяет сохранить их принципиально важное квантовое свойство (неортогональность), на котором и держится принцип фотонного шифрования. Шифрование в технологии КШ реализуется за счет квантово-оптического кодирования передаваемых информационных состояний в большом количестве неортогональных базисов, причем выбор базиса при кодировании каждого двоичного знака открытого текста определяется комбинацией бит на выходе управляющего блока, инициированного общим секретным ключом и непрерывно вырабатывающего управляющую битовую последовательность. Информационные квантовые состояния на выходе аппаратуры Алисы, соответствующие «0» и «1» открытого текста, ортогональны внутри каждого базиса, что обеспечивает их достоверное различение (расшифрование) Бобом, знающим в каком базисе их надо измерять. Нарушитель (Ева), не имеющий информации о ключе (измерительном базисе), должен решать задачу о различении неортогональных квантовых состояний. Выбором параметров криптосистемы квантового шифрования (среднего числа фотонов на информационное состояние и числа базисов кодирования), возможно уменьшение информации Евы об открытом тексте до сколь угодно малого значения.

Таким образом, в квантовых шифраторах возможен такой выбор значений двух основных параметров криптосистемы α и η (среднего числа фотонов в исходном когерентном состоянии и числа базисов шифрования), что вероятность правильного расшифрования бита открытого текста будет удовлетворять требованиям современных телекоммуникаций, а вероятность правильного дешифрования знака шифрсообщения при применении нарушителем оптимальной квантовой процедуры различения двух гипотез будет сколь угодно близкой к 1/2.

Приведем формальное описание протокола квантового шифрования типа $\alpha\eta$ из работы [7], где основные параметры α и η определяются средним числом фотонов в исходном когерентном состоянии и числом базисов шифрования. Схема соответствующей криптосистемы представлена на рис.1.

1) Алиса и Боб имеют заранее распределенный между ними секретный ключ K.

2) Используя функцию расширения ключа K - ENC(·), например, линейный регистр сдвига с обратной связью или AES в режиме поточного шифрования, начальный ключ K преобразуется в управляющую последовательность, которая разделена на n блоков: KMn = ENC(K) = (K1,...,Kmn). Здесь, m = log2(M), так что Zi = (K(i-1)m+1,...,Kim) может принимать M значений. Zi составляет ключевой поток.

3) Для каждого X_i бита открытого текста последовательности $\boldsymbol{X_n} = (X_1,...,X_n)$, Алиса посылает когерентное состояние

$$\left|\psi(X_i, Z_i)\right\rangle = \left|\alpha e^{i\cdot\theta(X_i, Z_i)}\right\rangle.$$

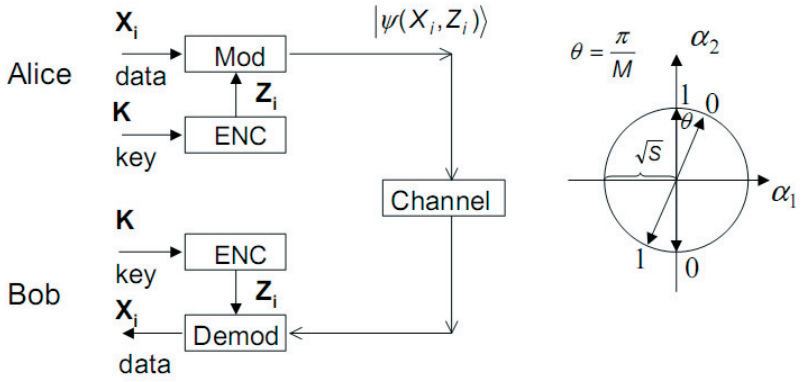

Рис.1. *Криптосхема αη. Слева – схематическое изображение системы шифрования αη. Справа – изображение двух соседних M-базисов с чередующимся логическим распределением битов.*

Здесь $\alpha \in R$ и $\theta(X_i, Z_i)$ принимает значения из набора $\{0,\pi/M,...,(2M-1)\pi/M\}$. Функция $\theta(X_i, Z_i)$, отображает бит данных и символ ключевого потока в угол на круге когерентных состояний и называется преобразователем координат (*mapper*).

Например,

$$\theta(X_i, Z_i) = [Z_i / M + (X_i \oplus Pol(Z_i)] \cdot \pi,$$

где $Pol(Z_i) = 0$ или 1 в зависимости от того, четное или нечетное Z_i.

4) Для декодирования Боб вычисляет функцию, идентичную ENC со своей копией ключа. Для каждого i, зная Z_i, он делает квантовое измерение, чтобы различить два состояния $|\psi(0, Z_i)\rangle$ и $|\psi(1, Z_i)\rangle$, в результате чего восстанавливает бит открытого текста.

Актуальной задачей криптоанализа в настоящее время является поиск возможных подходов к оценке стойкости криптосистем квантового шифрования и возможных атак на них.

4. Квантовое хеширование и квантовая цифровая подпись.

4.1. Квантовое хеширование.

Хеширование имеет ряд важных приложений в различных областях информатики, в частности, криптографические протоколы с открытым ключом основываются на криптографических хеш-функциях. Хеш-функции строятся так, чтобы преобразовывать входные последовательности большой длины (теоретически - любой длины) в короткие хеш-коды (на практике фиксированной длины). При этом требуется, чтобы любое изменение исходного слова вело к значительному изменению его хеш-образа.

Использование техники хеширования в построении систем цифровой подписи рассматривается в криптографическом сообществе в качестве одного из возможных ответов на появление квантовых компьютеров, способных вскрывать RSA-криптосистемы.

Остановимся лишь на одном развиваемом в настоящее время квантовом подходе к хешированию [8, 9], поскольку на основе квантового хеширования открывается возможность развивать системы квантовой цифровой подписи.

В основе понятия квантового хеширования лежит понятие квантовой функции. В последнее десятилетие появилось несколько подходов (в литературе известно, по крайней мере, два подхода) к построению понятия квантовой функции.

Первый подход предложен в работе [1], в которой определяется семейство «классически-классических» функций, аргументами и значениями таких функций являются классические последовательности. Такие функции предположительно являются односторонними не только для классических, но и для квантовых алгоритмов. Авторы называют их квантовыми односторонними функциями.

Другой подход к определению квантовой функции сформулирован в работе [2]. Их функции «классически-квантовые», то есть аргументами функции являются классические последовательности, значениями квантовые состояния. Другая «классически-квантовая» функция определена в работе Бурмана и др. [3]. Данная функция построена на основе двоичных кодов, исправляющих ошибки (в работе [3] использованы коды Джастесена). В работах [2,3] доказано, что предложенные функции являются односторонними в смысле невозможности восстановления исходного слова по его квантовому образу.

Путем использования «классически-квантовых» функций на основе двоичных кодов исправ-

ляющих ошибки предложены различные сценарии построения квантовых систем цифровой подписи [2,4,5].

В работах [8,9] анализируются определенные в [2,3] «классически-квантовые» функции и вводится понятие «классически-квантовой» хеш-функции, которое является естественным обобщением понятия «классически-квантовой» односторонней функции. Авторами предложены «классически-квантовые» хеш-функции, исследованы их криптографические свойства и рассмотрены подходы к построению универсального квантового хеширования.

Классически-квантовой функцией названа функция вида

$$\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s}, \quad \psi : w \mapsto |\psi(w)\rangle,$$
$$(\mathcal{H}^2)^{\otimes s} = \mathcal{H}^2 \otimes \ldots \otimes \mathcal{H}^2 = \mathcal{H}^{2^s}$$

где обозначает 2s-мерное гильбертово пространство, описывающие состояния s кубит.

Квантовой коллизией названа ситуация, когда процедура, проверяющая равенство квантовых хеш-кодов, ошибочно выдает совпадение различных исходных сообщений. Такой процедурой может быть хорошо известный SWAP-тест [3] или специфический для квантовой хеш-функции алгоритм. В любом случае процедура проверки связана с понятием различимости квантовых состояний. Можно ввести понятие δ-ортогональности состояний $|\psi_1\rangle$ и $|\psi_2\rangle$: $|\langle\psi_1|\psi_2\rangle| < \delta$ и обосновать, что для квантовой хеш-функции важна δ-ортогональность квантовых хеш-кодов различных слов, то есть они должны успешно проходить тесты на неравенство.

В тех случаях, когда необходимо проверить, является ли квантовое состояние $|\psi(w)\rangle$ хеш-кодом некоторого классического слова v, можно применить процедуру REVERSE-теста. Суть теста заключается в применении инвертированной процедуры создания квантового хеша, то есть его «раскручивание до начального» состояния.

Формально, пусть процедура создания хеш-кода слова w состоит в применении унитарного преобразования $U(w)$ к начальному состоянию $|0\rangle$, то есть $|\psi(w)\rangle = U(w)|0\rangle$. Тогда *REVERSE*-тест заключается в применении $U^{-1}(v)$ к квантовому хешу $|\psi(w)\rangle$ и проверке полученного состояния. Если $v = w$, то результатом преобразования $U^{-1}(v)|\psi(w)\rangle$ всегда будет $|0\rangle$, и *REVERSE*-тест выдаст равенство; в противном случае результирующее состояние будет δ-ортогонально к $|0\rangle$, поскольку унитарные преобразования сохраняют скалярное произведение:

$$(|0\rangle, U^{-1}(v)|\psi(w)\rangle) = (U^{-1}(v)|\psi(v)\rangle,$$
$$U^{-1}(v)|\psi(w)\rangle) = (|\psi(v)\rangle, |\psi(w)\rangle) < \delta.$$

Значит, при $v \neq w$ *REVERSE*-тест может ошибаться с вероятностью δ. При этом предлагаемый вариант квантового хеширования позволяет применять REVERSE-тест со сколь угодно малой вероятностью ошибки δ.

Таким образом, свойство δ-ортогональности квантовых состояний является важным качеством для обеспечения устойчивости к квантовым коллизиям, что позволяет ввести понятие δ-устойчивости хеш-функций.

Функция $\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s}$ является δ-$R(n;s)$ - квантовой хеш-функцией, если она является квантовой односторонней и δ-устойчивой функцией.

В работах [8,9] показано, как построить квантовые хеш-функции нескольких видов и предложены соответствующие модели генераторов квантовых хеш-функций. Там же предложен подход к построению квантовых хеш-функций, основанный на применении композиции классических семейств ϵ -универсальных хеш-функций и некоторого заданного генератора квантовых хеш-функций. Известно, что конструкции классических семейств ϵ -универсальных хеш-функций связаны с кодами, исправляющими ошибки (см., например, [6]). Данный подход открывает возможности построения новых квантовых хеш-функций на основе уже имеющихся. В частности, было показано, что конструкция кодов Рида-Соломона эффективна для построения квантовых хеш-функций.

4.3. Квантовая цифровая подпись.

Описанное выше универсальное квантовое хеширование может быть использовано в протоколе квантовой цифровой подписи.

Пусть $F=\{h_1,\ldots,h_l\}$ - это ϵ -универсальное семейство хеш-функций. Чтобы подписать сообщение M Алиса случайно выбирает число $D \in \{1,\ldots,l\}$, которое является ее *закрытым* ключом.

Подготовительный этап. На основе закрытого ключа Алиса создает необходимое количество открытых ключей $|\psi_F(D)\rangle$, являющихся результатом универсального квантового хеширования закрытого ключа, и отправляет их потенциальным получателям. Благодаря свойствам квантового хеширования состояния хеш-коды различных закрытых ключей «почти ортогональны», а значит, различимы с высокой вероятностью. Кроме того,

хеширование обеспечивает невозможность извлечения закрытого ключа из его хеш-кода.

Процедура подписи. На этапе подписи Алиса и Боб устанавливают соединение, и Боб измеряет первые $\log|F|$ кубит полученного на подготовительном этапе открытого ключа, получая состояние $|i\rangle|\psi_K(h_i(D))\rangle$ и пересылает число i Алисе.

Далее, чтобы подписать сообщение M, Алиса на основе полученного числа готовит хеш-код $|\psi_K(h_i(M)+h_i(D))\rangle$ значения $h_i(M)+h_i(D)$, который и будет ее подписью под сообщением M. Алиса отправляет его Бобу вместе с сообщением M.

Проверка подписи. Наконец, Боб (получатель подписанного сообщения) проверяет соответствие подписи сообщению, выполняя хеширование значения $h_i(M)$ и используя в качестве начального полученное им ранее состояние $|\psi_K(h_i(D))\rangle$.

Таким образом, Боб получит состояние $|\psi_K(h_i(M)+h_i(D))\rangle$ и сравнит с подписью Алисы с помощью REVERSE-теста.

На базе описанной процедуры могут быть построены различные технологии квантовой цифровой подписи, обеспечивающие конфиденциальность и целостность информации, а также аутентификацию и идентификацию объектов в квантовых информационных системах.

5. Прогнозные оценки.

С учетом изложенных выше прикладных аспектов, а также учитывая результаты многочисленных проводимых научных исследований и разработок, можно с достаточно высокой вероятностью предположить следующий сценарий развития направлений, имеющих непосредственное отношение к квантовой криптографии:

1. В среднесрочной перспективе получат развитие специализированные квантовые компьютеры, ориентированные на решение криптографических задач. Как уже указывалось выше, для решения практически значимых задач требуется создать регистр с числом кубитов, эффективно участвующих в вычислениях, до 1000. При этом использование в квантовой вычислительной системе кодов квантовой коррекции ошибок потребует существенного (примерно на порядок) увеличения числа «запасных» (используемых только для коррекции) кубитов. Поэтому для реализации 1000 эффективно используемых («логических») кубитов потребуется создание квантового регистра с существенно большим общим количеством кубитов.

Ожидается, что для обслуживания 1000 кубитов посредством многолучевой лазерной системы, криогенной системы и других вспомогательных систем не потребуется чрезмерно больших ресурсов. Подобная вычислительная система сможет размещаться в помещении площадью 50-100 м^2, её энергопотребление составит порядка 100-200 кВт, причем квантовый процессор будет потреблять лишь небольшую часть этих ресурсов (1% или менее), а весь остальной ресурс пойдет на вспомогательные системы.

Особую роль будут играть распределенные квантовые вычислительные системы (квантовые симуляторы), которые позволят дополнительно повысить эффективность моделирования сложных процессов в различных областях науки, включая медицину и фармакологию, биологию и генную инженерию, материаловедение и др.

В более отдаленной перспективе возможно обеспечить сопряжение отдельных квантовых вычислительных систем в квантовую сеть.

2. Получит существенное развитие область квантовых коммуникаций:

а) Средства квантового распределения криптографических ключей могут быть созданы ориентировочно к 2020 году и будут обладать следующими характеристиками:

- для волоконно-оптического канала связи: скорость выработки ключей - 10 Гбит/с при дальности до 200 км;

- для атмосферного канала связи: скорость выработки ключей - 1 Гбит/с при дальности до 2 км;

- для канала распределения ключей с Земли через низкоорбитальные космические аппараты: скорость выработки ключей - 1 кбит/с при дальности до 1500 км.

б) В среднесрочной перспективе могут быть созданы квантовые каналы связи, исключающие перехват информации третьей стороной, с дальностью передачи информации порядка 1000-3000 км в космическом пространстве и порядка 100 км в плотных слоях атмосферы со скоростью передачи информации до 100 Мбит/с. Интеграция в эти сети технологий квантового хеширования и квантовой цифровой подписи позволит выйти на новый уровень в безопасности информационных технологий с распределенной обработкой данных.

в) В среднесрочной перспективе могут быть созданы каналы связи на основе квантовой телепортации, обеспечивающие передачу до 10^7 кубит (квантовых состояний) в секунду на расстояние порядка 1000 километров в космическом пространстве.

На базе каналов телепортации квантовых состояний в дальнейшем могут быть созданы квантовые сети, которые смогут использоваться как для передачи квантовой и классической информации, так и для организации распределенных квантовых вычислений.

Один из возможных способов организации квантовых сетей – сети на основе квантовых повторителей (репитеров), ключевым элементом которых является квантовая память. Полноценные образцы квантовой памяти, как основы квантовых повторителей, и образцы самих повторителей могут быть созданы в ближайшем десятилетии. Сопряжение управляемых источников ЭПР пар фотонов с квантовой памятью позволят в перспективе 15 лет создать квантовые сети, способные объединять квантовые вычислители в единую распределенную систему.

г) Квантовая сеть высокоточной синхронизации для защищенных систем управления может быть создана в будущем десятилетии и будет поддерживать глобальное покрытие околоземного космического пространства и иметь сеть из десяти узлов (опорных станций) по 1000 кубитов (атомов) в каждом, что обеспечит стабильность частоты до 10^{-18}, т.е. в 100 раз лучше имеющихся классических аналогов.

Заметим, что отдельные технологии, входящие в состав указанных направлений, такие, как квантовая генерация случайных чисел, могут иметь и уже имеют самостоятельное прикладное значение.

Литература (References)

1. Elham Kashefi and Iordanis Kerenidis. Statistical zero knowledge and quantum one-way functions. Theoretical Computer Science, 378(1):101- 116, Jun 2007.
2. Daniel Gottesman and Isaac Chuang. Quantum digital signatures. Technical Report arXiv:quant-ph/0105032, Cornell University Library, Nov 2001.
3. Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum Engerprinting. Phys. Rev. Lett, 87(16): 167902, Sep 2001.
4. Xin Lu and Dengguo Feng. Quantum digital signature based on quantum oneway functions. In The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005, volume 1, pages 514-517, 2005.
5. JingXian Zhou, YaJian Zhou, XinXin Niu, and YiXian Yang. Quantum proxy signature scheme1 with public verifiability. Science China Physics, Mechanics and Astronomy, 54(10):1828 1832, 2011.
6. D. H. Stinson. On the connections between universal hashing, combinatorial designs and error-correcting codes. In In Proc. Congressus Numerantium 114, pages 7-27, 1996.
7. Ranjith Nair, Horace P. Yuen, «On the Security of the Y-00 (αη) Direct Encryption Protocol», arXiv:quant-ph/0702093v2 1 Mar 2007.
8. F. Ablayev, M. Ablayev, Quantum Hashing via Classical e-universal Hashing Constructions. arXiv:1404.1503v2 [quant-ph] http://arxiv.org/abs/1404.1503
9. F. Ablayev, A. Vasiliev, Quantum Hashing, arXiv:1310.4922vl [quant-ph] http://arxiv.org/abs/1310.4922