УДК 004.942:001.57

ОПИСАНИЕ БАЗОВЫХ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ

Е. В. Борисова, аспирант ФГБОУ ВО «РГРТУ», г. Рязань, Россия;
orcid.org/0000-0002-0198-377X, e-mail: Ekaterina21333@yandex.ru

Квантовая криптография – одна из трех частей, образующих междисциплинарное направление исследований – квантовую информатику. Помимо квантовой криптографии, квантовая информатика включает в себя исследования квантовых компьютеров и теорию квантовой коммуникации. Поскольку квантовая информатика возникла на стыке различных дисциплин, для ее понимания требуется, прежде всего, знание языков и методов квантовой теории и теории классической информации [1].

В данной статье рассматривается квантовая криптография, с одной стороны, как квантовая связь, и в частности, квантовое распределение ключа, а с другой – как квантовые вычисления, которые представляют угрозу для классической криптографии, для протоколов передачи данных с открытым ключом. И то, и другое, по сути, являются разными разделами квантовой информатики – науки о том, как можно передавать и преобразовывать информацию с помощью квантовых систем.

В данной работе определено понятие «кубит», как двумерная квантовая система, то есть суперпозиция двух базисных векторов: 0 и 1 с коэффициентами C0 и C1, которые являются комплексными. Рассмотрено, что от кубитов можно перейти к кудитам, то есть к d-мерной системе, которая, соответственно, будет описываться количеством параметров 2d-2, а также обосновано, что можно перейти к системе из N кубит, размерность которой, в общем случае растет экспоненциально. В случае если система факторизована, то размерность растет линейно.

***Целью работы** является представление математического описания кубита, кудита, системы из N-кубитов и матрицы плотности ансамбля как базовых математических моделей в квантовой криптографии.*

***Ключевые слова:** кубит, кудит, квантовая криптография, матрица плотности ансамбля.*

DOI: 10.21667/1995-4565-2021-75-113-120

Введение

Для начала стоит рассмотреть, что из себя представляет современная классическая криптография и как квантовая физика с ней может быть связана.

Основные направления современной криптографии, – это шифрование с закрытым ключом и шифрование с открытым ключом. И у обоих этих методов есть определенные проблемы. Если говорить о шифровании с закрытым ключом, то появляются вопросы о том, как этот ключ распределить между двумя легитимными пользователями. А если говорить о шифровании с открытым ключом, которое использует в своей основе необратимые функции, то есть функции, которые в одну сторону вычисляются быстро, а в другую экспоненциально долго, то проблема в том, что экспоненциальная сложность обратных алгоритмов, которые взламывают эти функции, вообще говоря, строго математически не доказана. Фактически это просто, в каком-то смысле эмпирически, следует из того, что люди много лет пытались создать алгоритмы взлома, но это так и не получилось.

Теоретическая часть

Более подробно стоит рассмотреть, какое отношение к этому имеет квантовая физика. Двумя приложениями квантовой физики являются квантовая связь и квантовые вычисления. И в том, и в другом случае кодируется информация с помощью квантовых систем. И дальше, если над этими квантовыми системами производить некие операции, то это можно интерпретировать как преобразование информации, то есть как вычисления. Такие квантовые вычис-

лители как квантовые компьютеры, позволяют реализовывать алгоритмы, отличающиеся по своим свойствам от классических алгоритмов. В частности, квантовый компьютер может решать задачи, которые экспоненциально сложны для классического компьютера. Например, квантовый компьютер может взламывать ряд протоколов классической криптографии.

С другой стороны, если кодировать информацию с помощью квантовых систем и передавать ее, тем самым реализуя квантовую связь, то можно реализовать квантовое распределение ключа, надежность которого будет гарантирована законами квантовой физики.

И в этом смысле под квантовой криптографией разные специалисты понимают разное. Некоторые понимают просто узкое направление – квантовое распределение ключа, а некоторые понимают вообще всю квантовую связь, потому что в квантовой связи помимо квантового распределения ключа есть и другие методы секретной передачи информации. Но если рассматривать словосочетание «квантовая криптография» максимально широко, то все квантовое, что имеет отношение к криптографии, логично туда включить. Итак, квантовая криптография – это междисциплинарная область знания, технологии и техники, в которой решается задача обеспечения легитимных пользователей идентичными случайными последовательностями символов посредством передачи квантовых состояний [2].

Следуя этой логике, и квантовые вычисления относим к квантовой криптографии. Потому что сама потенциальная угроза, связанная с возможностями квантового компьютера, это угроза для классической криптографии. Её важно оценивать, с ней важно бороться и классическими способами, которые существуют сейчас или по крайней мере активно разрабатываются. Существуют разные алгоритмы так называемой «постквантовой криптографии», то есть алгоритмы, для которых еще не доказано, что они могут быть взломаны квантовым компьютером, и поэтому для борьбы с потенциальной угрозой нужно чётко осознавать, о чём идёт речь.

Далее будут затрагиваться оба этих направления, то есть будут описаны и квантовые вычисления с точки зрения их перспективности и угрозы для классической криптографии, и квантовая связь, и, в частности, квантовое распределение ключа, как основное приложение квантовой криптографии, которое уже сейчас активно используется.

Математическое описание кубита и системы из *N* кубитов

Необходимо более подробно рассмотреть квантовые вычисления. Но независимо от того, идёт ли речь о квантовых вычислениях или о квантовой связи, так или иначе используется понятие квантовой информации, а единицей квантовой информации является квантовый бит.

Сначала стоит вспомнить, что такое классический бит. Классический бит – это система с двумя хорошо различимыми состояниями, и один бит может принимать только два значения: ноль и единицу. А если кодируется информация квантовой системы, то у этой квантовой системы должно быть два опять же хорошо различимых квантовых состояния. Если квантовые состояния хорошо различимы, значит они ортогональны, то есть они могут образовывать базис. Соответственно, состояние квантового бита может быть записано в виде кет-вектора $|\psi\rangle = C_0|0\rangle + C_1|1\rangle$, то есть он описывается в общем случае двумя комплексными коэффициентами C_0 и C_1.

Способность кубита находиться в состоянии суперпозиции противоречит обыденным представлениям об окружающем физическом мире. Классический бит подобен монете: либо орёл, либо решка. Для несовершенных монет возможны промежуточные состояния, например балансирование на ребре, но в идеальном случае их можно отбросить. Кубит, напротив, до момента наблюдения может находиться в целом континууме состояний между $|0\rangle$ и $|1\rangle$. Необходимо подчеркнуть ещё раз, что измерение кубита всегда даёт 0 или 1 с некоторой вероятностью [3].

Прежде чем более подробно углубиться в математическое описание кубита, логично привести несколько различных примеров его физической реализации.

Кубиты обычно делят на стационарные и flying Q-bits, то есть летающие, передающиеся по пространству кубиты. Если говорить о стационарных кубитах, то это должны быть какие-то квантовые системы, локализованные в пространстве. Это могут быть либо атомы или ионы, в различных магнитно-оптических, дипольных и тому подобных ловушках, это могут быть сверхпроводящие цепи, в которых квантовое состояние имеет так называемый «ток», который в них течет. Если говорить о flying Q-bits, о кубитах, которыми передают информацию, то, как правило, говорят о фотонах или о других состояниях света. Кодировать информацию с помощью состояний света можно по-разному, можно кодировать информацию поляризационным состоянием фотона, можно кодировать ее количеством фотонов, и в принципе фотоны можно использовать не только для передачи, но также и для преобразования информации. Например, можно посылать их на многоканальный интерферометр, где квантовое состояние будет преобразовываться и его результат будет интерпретирован как квантовое вычисление. Так или иначе, существует много разных платформ для реализации кубита. Далее стоит вернуться к математическому описанию кубита. Как уже было сказано, кубит может быть описан как кет-вектора $C_0|0\rangle + C_1|1\rangle$, соответственно $|0\rangle$ и $|1\rangle$ – это базис кубита, и в этом базисе кубит можно представить в виде столбца с коэффициентами C_0 и C_1: $\begin{pmatrix} C_0 \\ C_1 \end{pmatrix}$.

Аналогично можно ввести соответствующий этому кет-вектору бра-вектор ψ, который будет соответственно равен C_0, комплексно сопряженное на бра-вектор ноль, плюс C_1, комплексно сопряженное на бра-вектор один, и такому бра-вектору будет соответствовать строка из комплексных коэффициентов: $(C_0^* \quad C_1^*)$ комплексно сопряженное. Т.е. $|\psi\rangle = C_0|0\rangle + C_1|1\rangle = \begin{pmatrix} C_0 \\ C_1 \end{pmatrix}$ и $\langle\psi| = C_0^*\langle 0| + C_1^*\langle 1| = (C_0^* \quad C_1^*)$.

Поскольку состояния ноль и один должны образовывать базис, то они друг другу ортогональны, то есть скалярное произведение 0 на 1 равно скалярному произведению 1 на 0 и равно нулю. Кроме того, эти состояния должны быть нормированы, потому что базис должен быть ортонормирован, то есть скалярное произведение нуля самого на себя и единицы самой на себя равно тоже единице. Ну а условие нормировки состояния кубита ψ означает, что сумма квадратов модулей коэффициентов C_0 и C_1 также должна быть равна единице. Т.е. можно записать следующее:

условие ортогональности: $\langle 0|1\rangle = \langle 1|0\rangle = 0$;

условие нормировки: $\langle 0|0\rangle = \langle 1|1\rangle = 1$;

$$\langle\psi|\psi\rangle = |\mathrm{C}_0|^2 + |\mathrm{C}_1|^2 = 1.$$

Ясно, что если говорить о квантовых вычислениях, то с одним кубитом больших вычислений нельзя сделать, нужно увеличивать размерность. Есть два пути увеличения размерности. Необходимо сразу обозначить, что только один рациональный. Более сложный путь – это путь увеличения размерности самого квантового состояния, то есть можно перейти от кубита к кутриту, когда есть три состояния, 0-1-2, кукварту, где четыре состояния, куквинту, кусексту, кусепту и так далее. В общем случае такая многомерная квантовая система называется кудитом, она имеет размерность d, а соответственно в этом смысле состояние кудита можно представить, как сумму из d слагаемых, из d ортогональных друг другу, ортонормированных векторов от нуля до d с комплексными коэффициентами: C0, C1, C2 и т.д. до Cd. Также стоит посмотреть количество действительных коэффициентов, которыми описывается такая d-мерная система. Есть d комплексных коэффициентов, то есть 2d действительных коэффициентов, потому что у каждого комплексного коэффициента есть действительная и мнимая часть, но при этом есть условие нормировки, то что сумма квадратов модулей всех коэффициентов равна единице, а также еще есть условие так называемой не наблюдаемости

общей фазы. То есть можно домножить кудит на коэффициент E в степени $i\varphi$. Это действие сохранит его нормировку, а соответствующий кудит будет отвечать тому же самому физическому состоянию квантовой системы. Таким образом, можно занулить мнимую часть у первого коэффициента, и тогда получается, что общее количество действительных параметров, которыми описывается d-мерная система кудит, – это 2d-1. То есть она более или менее линейно растет с увеличением размерности системы.

Другой способ увеличения размерности заключается в том, что можно увеличивать количество кубитов. И вот это уже гораздо интереснее, потому что если, например, перейти к двум кубитам, то кубит первый – это $C_0^{(1)}|0\rangle_1 + C_0^{(1)}|0\rangle_1$, который тензорно домножается на второй кубит: $C_0^{(2)}|0\rangle_2 + C_0^{(2)}|1\rangle_2$. И результат этого тензорного перемножения это сумма четырех элементов с соответствующими комплексными коэффициентами: $|C_{00}|00\rangle + C_{01}|01\rangle + + C_{10}|10\rangle + C_{11}|11\rangle$. То есть в общем случае два кубита описываются четырьмя комплексными коэффициентами. Ну и также есть условие нормировки и выноса общей фазы, то есть две связи уменьшают количество коэффициентов на два.

Вышесказанное увеличение размерности можно описать следующим образом:

кудит: $|\psi\rangle = C_0|0\rangle + C_1|1\rangle + ... + C_{d-1}|d-1\rangle$, где 2d-2 параметров;

два кубита: $|\psi\rangle = (C_0^{(1)}|0\rangle_1 + C_0^{(1)}|0\rangle_1) \otimes (C_0^{(2)}|0\rangle_2 + C_0^{(2)}|1\rangle_2) =$

$= |\psi\rangle = C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle$, где $2\times4-2$ параметров;

N кубитов: $|\psi\rangle = \prod_{i=1}^{N} \otimes (C_0^{(i)}|0\rangle_i + C_1^{(i)}|1\rangle_i)$, где $2\times2^N - 2$ параметров.

Итого общее количество параметров, которыми описываются два кубита, это 2*4-2. А с другой стороны, если дальше увеличивать размерность и взять N кубитов, то такая система будет описываться уже другим образом. Поэтому будет уже 2^N комплексных коэффициентов, то есть $2\times2^N - 2$, с учётом условия нормировки и условия выноса общей фазы. Уже видно, что размерность системы из N кубитов экспоненциально растет с увеличением их количества.

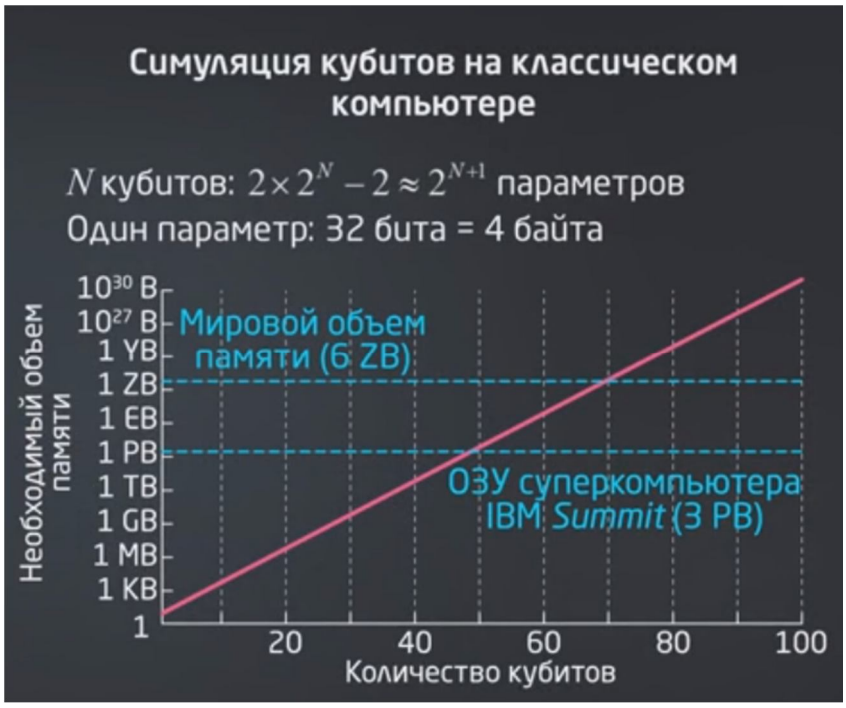
Далее необходимо определить, к чему это ведёт. Допустим, необходимо рассчитать, как будет вести себя система из N кубитов на компьютере. Тогда необходимо каждому действительному коэффициенту сопоставить какой-то объем информации, например 32-битное число, 32 бита это 4 байта. Теперь надо посчитать, сколько понадобится памяти, чтобы описать таким образом N кубитов.

Для описания N кубитов нужно примерно два в степени $N+1$ действительных параметров. Если домножить это все на 4 байта, то можно увидеть график, который представлен на рисунке.

То есть можно увидеть, что для описания 100 кубитов нужен объем памяти порядка 10 в 30-й байт, а при этом мировой объем памяти на всех жестких дисках сейчас оценивается как 6 зеттабайт, что существенно меньше, это соответствует примерно объёму памяти, необходимой для расчета 70 кубитов. Насколько известно, оперативная память самого мощного на сегодняшний день суперкомпьютера составляет три петабайта, и ее хватит на то, чтобы рассчитать примерно 50 кубитов. То есть если есть квантовая система, состоящая из 100 кубитов, то ни один классический компьютер в обозримом будущем не сможет рассчитать, как она будет себя вести.

Значит, если уметь хорошо управлять 100 кубитами, то можно делать нечто, что недоступно классическому компьютеру. Интересным моментом является то, что число 70 кубитов, которое соответствует мировому объему памяти, это как раз то количество кубитов, которое некоторое время назад представила компания Google. То есть Google представила квантовый процессор, состоящий из 72 кубит. Поэтому в каком-то смысле это та система, которую можно описать, разве что используя весь объем жестких дисков мира. Но есть один

нюанс. Для того чтобы N кубитов реально описывалось 2^{N+1} параметрами, нужно, чтобы эти кубиты были запутаны, то есть чтобы эта система огромной размерности из N кубитов не была сведена к произведению состояний отдельных кубитов. Потому что в этом случае можно каждый кубит описывать независимо, а для каждого кубита нужно два параметра. Соответственно N кубитов будет описываться 2^N параметрами. Поэтому в этом случае никакого экспоненциального роста информации внутри квантового компьютера нельзя получить и в этом смысле для эффективных квантовых вычислений нужно, чтобы все N кубитов были перепутаны, что о 72-кубитном компьютере Google пока сказать сложно.



Симуляция кубитов на классическом компьютере
Simulating qubits on classic computer

Итак, перепутанность как ресурс квантовых вычислений:

N кубитов: $2\times 2^N - 2 \approx 2^{N-1}$ параметров.

Один параметр: 32 бита = 4 байта.

N факторизованных кубитов: $|\psi\rangle = \prod_{i=1}^{N} \otimes (C_0^{(i)} |0\rangle_i + C_1^{(i)} |1\rangle_i),|$ где $2N$ параметров.

При измерении одного кубита можно получить не более одного бита информации.

Кроме того, опять же важно понимать, что при измерении каждого квантового бита можно получить только один бит информации. Соответственно и при измерении N кубитов получается N бит информации.

Поэтому весь этот экспоненциальный рост информации находится только внутри квантового компьютера. То есть вычисления происходят следующим образом. Если есть N битов, которые имеют значение от нуля до единицы, то можно в соответствии с ними инициализировать N кубитов также в состоянии с нулем или единицей.

После можно с этими N кубитами произвести какое-то преобразование, а далее каждый кубит можно независимо считать и получить N битов информации на выходе. То есть на входе и выходе есть N бит информации, а внутри вычисления, внутри квантового процесса, можно сказать, «крутятся» 2^N комплексных параметров, что позволяет проводить вычисления более эффективно. Это в свою очередь позволяет реализовать определенные алгоритмы, которые работают экспоненциально быстрее классических [4].

Матрицы плотности ансамбля

Рассмотренные выше понятия были сформулированы для одиночных фотонов, описываемых векторами состояния $|\psi\rangle$, называемых также чистыми состояниями. Далее будет рассмотрен ансамбль чистых состояний $\{p_i, |\psi_i\rangle\}$, в котором каждое состояние $|\psi\rangle$ встречается с вероятностью p_i, причём $\sum_i p_i = 1$. Тогда среднее значение некоторой физической величины $\hat{A}$ по такому ансамблю будет определяться формулой: $\hat{A} = \sum_i p_i \langle\psi_i|\hat{A}|\psi_i\rangle = tr(\hat{A}\hat{\varrho})$, где $\hat{\varrho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ – оператор плотности, $tr\hat{M} = \sum_i \langle i|\hat{M}|i\rangle = \sum_i M_{ij}$ – след оператора, вычисляемый как сумма диагональных элементов матрицы оператора, записанного в ортонормированном базисе $\{|i\rangle\}$.

Матрица плотности ϱ с элементами $\varrho_{ij} = \langle i|\hat{\varrho}|i\rangle$ обладает следующими свойствами:

1) эрмитовость $\varrho^{\dagger} = \varrho$;

2) неотрицательная определённость $\varrho \geq 0$;

3) единичный след $tp\varrho = 1$.

Действительно,

$$1)\ \hat{\varrho}^{\dagger} = \sum_i p_i (|\psi_i\rangle\langle\psi_i|)^{\dagger} = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \hat{\varrho}; \quad (1)$$

$$2)\ \langle\chi|\hat{\varrho}|\chi\rangle = \sum_i p_i \langle\chi|\psi_i\rangle\langle\psi_i|\chi\rangle = \sum_i p_i |\langle\chi|\psi_i\rangle|^2 \geq 0, \forall |\chi\rangle; \quad (2)$$

$$3)\ tr\hat{\varrho} = \sum_i p_i tr(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i \langle\psi_i|\psi_i\rangle = \sum_i p_i = 1. \quad (3)$$

Обратно, пусть имеется оператор $\hat{\varrho}$, удовлетворяющий обозначенным выше свойствам, тогда найдутся вероятности p_i состояния $|\psi_i\rangle$ такие, что $\hat{\varrho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Можно заметить, что в общем случае представление суммой $\hat{\varrho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ не единственно. Один из способов заключается в том, чтобы в качестве p_i взять собственные значения ϱ, а в качестве $|\psi\rangle$ – соответствующие им ортонормированные собственные векторы.

Тогда очевиден вывод, что статистические свойства ансамбля одиночных фотонов полностью определяются оператором плотности.

В этом случае поляризационная матрица плотности имеет вид:

$$\varrho = \begin{pmatrix} \varrho_{HH} & \varrho_{HV} \\ \varrho_{VH} & \varrho_{VV} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 + s_3 & s_1 - is_2 \\ s_1 + is_2 & 1 - s_3 \end{pmatrix},$$ где $s_i = \langle\varrho_i\rangle = tr(\varrho\sigma_i)$ – параметры Стокса в общем случае.

Условие $\varrho \geq 0$ эквивалентно условию $s_1^2 + s_2^2 + s_3^2 \leq 1$ [5].

Заключение

Принцип дополнительности Нильса Бора является одним из краеугольных камней квантовой механики и квантовых информационных технологий. Согласно этому принципу, «данные, получаемые при разных условиях опыта, не могут быть охвачены одной-единственной картиной; эти данные должны, скорее, рассматриваться как дополнительные в том смысле, что только совокупность разных явлений может дать более полное представление о свойствах объекта». Принцип дополнительности настолько важен для описания квантовых явлений, что, например, согласно В. Паули, «по аналогии с термином «теория относительности» современную квантовую теорию можно было бы назвать «теорией дополнительности»».

Формальное описание квантового состояния, основанное на понятиях вектора состояния и матрицы плотности, не сводится к какому-либо одному распределению вероятностей.

Со статистической точки зрения квантовое состояние можно рассматривать как естественное обобщение понятия распределения вероятностей. Квантовая механика обеспечивает более глубокое и полное понимание вероятностных и статистических закономерностей по сравнению с классическими представлениями. Согласно принципу дополнительности, экспериментальное изучение квантового состояния должно базироваться на измерении совокупности взаимно дополнительных распределений.

Например, экспериментальное исследование квантовой системы будет более полным, если данные, полученные при изучении квантового ансамбля в координатном пространстве, дополнить изучением того же ансамбля в канонически сопряженном (импульсном) пространстве. Известная задача Паули (Pauli Problem) как раз и состоит в том, чтобы реконструировать пси-функцию на основе координатного и импульсного распределений. Благодаря развитию техники гомодинирования в современной квантовой оптике, задача об измерении квантового состояния перешла из сугубо теоретической области в область реальных квантовых информационных технологий, причем в более полной постановке, чем это первоначально предполагал В. Паули. [7]

Выводы

1. Кубит – квантовая система с двумя хорошо различимыми (ортогональными) квантовыми состояниями: $|\psi\rangle = C_0 |0\rangle + C_1 |1\rangle$.

2. Кудит: $|\psi\rangle = C_0 |0\rangle + C_1 |1\rangle + \ldots + C_{d-1} |d-1\rangle$, где 2d-2 параметров.

3. *N* кубитов:

$|\psi\rangle = \prod_{i=1}^{N} (C_0^{(i)} |0\rangle_i + C_1^{(i)} |1\rangle_i)$, где $2 \times 2^N - 2$ параметров.

4. Статистические свойства ансамбля одиночных фотонов полностью определяются оператором плотности.

В этом случае поляризационная матрица плотности имеет вид:

$\varrho = \begin{pmatrix} \varrho_{HH} & \varrho_{HV} \\ \varrho_{VH} & \varrho_{VV} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 + s_3 & s_1 - is_2 \\ s_1 + is_2 & 1 - s_3 \end{pmatrix}$, где $s_i = \langle \varrho_i \rangle = tr(\varrho \sigma_i)$ – параметры Стокса в общем случае.

Условие $\varrho \geq 0$ эквивалентно условию $s_1^2 + s_2^2 + s_3^2 \leq 1$.

В данной статье было определено понятие кубита, как квантовой системы с двумя хорошо различимыми ортогональными квантовыми состояниями. Рассмотрено, что от кубитов можно перейти к кудитам, то есть, к d-мерной системе, которая, соответственно, будет описываться количеством параметров 2d-2, а также обосновано, что можно перейти к системе из *N* кубитов, размерность которой в общем случае растет экспоненциально. А в случае, если система факторизована, то растет линейно.

Таким образом, в данной статье представлено математическое описание базовых моделей квантовой физики и, в частности, квантовой криптографии, на описание которых можно опираться при более глубоком рассмотрении вопросов по данной теме.

Библиографический список

1. **Килин С. Я.** Квантовая криптография: идеи и практика / С. Я. Килин, Д. Б. Хорошко, А. П. Низовцев. Минск: Белорусская наука. 2007. 391 с.

2. **Кулик С.** Квантовая криптография //Фотоника. 2010. № 2. С. 36-41.

3. **Нильсен М., Чанг И.** Квантовые вычисления и квантовая информация. М.: «Мир», 2006. 824 с.

4. **Корольков А. В., Катамадзе К. Г., Кулик С. П., Молотков С. Н.** О пассивном зондировании волоконно-оптических квантовых каналов связи // Журнал экспериментальной и теоретической физики. 2010. Т. 110. № 4. С. 561-567.

5. **Филиппов С. Н.** Квантовые поляризационные состояния фотонов: уч.-метод. пособие / сост.: С. Н. Филиппов. М.: МФТИ, 2017. 36 с.

6. **Богданов Ю. И., Авосопянц Г. В., Белинский Л. В. и др.** Статистическое восстановление оптических квантовых состояний на основе взаимно дополнительных квадратурных квантовых измерений // ЖЭТФ. 2016. Т. 150. № 2. С. 246-253.

UDC 004.942:001.57

DESCRIPTION OF BASIC MATHEMATICAL MODELS IN QUANTUM CRYPTOGRAPHY

E. V. Borisova, postgraduate student, RSREU, Ryazan, Russia;
orcid.org/0000-0002-0198-377X, e-mail: Ekaterina21333@yandex.ru

Quantum cryptography is one of the three parts that form interdisciplinary field of research-quantum computer science. In addition to quantum cryptography, quantum information science includes research on quantum computers and quantum communication theory. Since quantum informatics originated at the intersection of various disciplines, its understanding requires, first of all, the knowledge of languages and methods of quantum theory as well as classical information theory [1].

This article discusses quantum cryptography, on the one hand, as quantum communication, in particular, quantum key distribution, and on the other hand, quantum computing, which poses a threat to classical cryptography and to public key data transfer protocols. Both are essentially different branches of quantum computer science – the science of how information can be transmitted and transformed using quantum systems. The concept of a qubit is defined as a simple two-dimensional quantum state, the basis of which is a logical zero and a logical unit. In this paper, we will define the concept of qubit as a two-dimensional quantum system, i.e., a superposition of two basis vectors: 0 and 1, with coefficients C0 and C1 being complex.

***The aim** of this paper is to present a mathematical description of qubit, qudit, N-qubit system, and ensemble density matrix. In this paper, we define the concept of qubit as a quantum system with two well-distinguishable orthogonal quantum states. Qubits are shown to move on to qudits, i.e., to d-dimensional system, which, respectively, will be described by 2d-2 number of parameters, the possibility to move to N qubit system, the dimension of which, in general, growing exponentially is also proved. In case when the system is factorized, it grows linearly.*

Key words: *qubit, qudit, quantum cryptography, ensemble density matrix.*

DOI: 10.21667/1995-4565-2021-75-113-120

References

1 **Kilin S. Ya.** *Kvantovaya kriptografiya: idei i praktika* / S. Ya. Kilin, D. B. Horoshko, A. P. Nizovcev. Minsk: Belorusskaya nauka. 2007. 391 p. (in Russian).

2. **Kulik S.** Kvantovaya kriptografiya. *Fotonika*. 2010, no. 2, pp. 36-41. (in Russian).

3. **Nil'sen M., CHang I.** *Kvantovye vychisleniya i kvantovaya informaciya*. Moscow: Mir. 2006, 824 p. (in Russian).

4. **Korol'kov A. V., Katamadze K. G., Kulik S. P., Molotkov S. N.** O passivnom zondirovanii volokonno-opticheskih kvantovyh kanalov svyazi. *Zhurnal eksperimental'noj i teoreticheskoj fiziki*. 2010, vol. 110, no. 4, pp. 561-567. (in Russian).

5. **Filippov S. N.** *Kvantovye polyarizacionnye sostoyaniya fotonov*: uch.-metod. posobie / sost.: S. N. Filippov. Moscow: MFTI. 2017, 36 p. (in Russian).

6. **Bogdanov Yu. I., Avosopyanc G. V., Belinskij L. V. i dr.** Statisticheskoe vosstanovle-nie optich-eskih kvantovyh sostoyanij na osnove vzaimno dopolnitel'nyh kvadraturnyh kvanto-vyh izmerenij. *ZHETF*. 2016, vol. 150, no. 2, pp. 246-253. (in Russian).