

Экз. № \_\_\_\_\_  
На правах рукописи

**МАТВЕЕВ Евгений Анатольевич**

**ПРИМЕНЕНИЕ КВАНТОВОМЕХАНИЧЕСКИХ ЭФФЕКТОВ  
В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ**

Специальность: 05.13.19 – Методы и системы защиты информации,  
информационная безопасность

**ДИССЕРТАЦИЯ**  
на соискание ученой степени  
кандидата физико-математических наук

Научный руководитель:  
академик РАН,  
доктор технических наук, профессор  
Соколов Игорь Анатольевич

Соискатель:

Пенза – 2019

# ОГЛАВЛЕНИЕ

<b>ВВЕДЕНИЕ</b>	4
<b>ГЛАВА 1. Квантовые ресурсы, используемые в криптографических приложениях</b>	21
§ 1.1. Теорема о невозможности клонирования	22
§ 1.2. Несепарабельные состояния квантовых систем	31
§ 1.3. Математическое определение несепарабельности состояния $n$ -кубитной квантовой системы	34
§ 1.4. Состояние спиновый синглет	41
§ 1.5. Состояния квантовых систем, близкие по своим свойствам к состоянию спиновый синглет	51
<b>Выводы по главе 1</b>	64
<b>ГЛАВА 2. Достаточные признаки несепарабельности состояний многокубитных квантовых систем</b>	67
§ 2.1. Булевы маски состояний квантовых систем	68
§ 2.2. Нумераторы весов состояний квантовых систем	74
§ 2.3. Алгоритм определения неразложимости состояния квантовой системы в тензорное произведение состояний меньшей размерности с использованием редукций булевых функций	82
<b>Выводы по главе 2</b>	87
<b>ГЛАВА 3. Квантовые криптографические системы</b>	89
§ 3.1. Квантовые криптографические системы на основе ресурса невозможности клонирования неизвестного квантового состояния	90
§ 3.2. Квантовые криптографические системы на основе двух	94

ресурсов: невозможности клонирования неизвестного квантового состояния и несепарабельности	
§ 3.3. Квантовая криптографическая система <b>АКМ2017</b> на основе ресурса несепарабельности состояния спиновый синглет	96
§ 3.4. Сеансовый ключ квантовой криптографической системы <b>АКМ2017</b> как еще одна степень усиления криптографической стойкости	106
§ 3.5. Восстановление состояний носителей-кубитов для формирования ключевой информации квантовой криптографической системы <b>АКМ2017</b>	116
<b>Выводы по главе 3</b>	126
<b>ЗАКЛЮЧЕНИЕ</b>	128
<b>СПИСОК ЛИТЕРАТУРЫ</b>	130
Приложение А	141
Приложение Б	143
Приложение В	145
Приложение Г	149
Приложение Д	154

## ВВЕДЕНИЕ

Информационная безопасность является одной из важнейших составляющих национальной безопасности Российской Федерации и её значение только возрастает. Применение средств обеспечения информационной безопасности зарубежного производства содержит в себе значительные угрозы для России и ее граждан, особенно в области информационно-коммуникационных технологий и при использовании возможностей, предоставляемых глобальной информационной сетью Интернет. Поэтому разработка и создание доверенных отечественных технологий и средств защиты информации, отвечающих российским стандартам и требованиям информационной безопасности, относится к первоочередному направлению обеспечения национальной безопасности России. Об свидетельствуют положения **Доктрины информационной безопасности Российской Федерации**, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, которая представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере [40]. Так, в этом документе в подпункте (в) пункта 8 части II (Национальные интересы в информационной сфере) подчеркивается, что национальными интересами в информационной сфере являются «... совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности ...».

В комплексном подходе к обеспечению информационной безопасности особое место занимают криптографические методы. В России сложилась своя научная криптографическая школа с устоявшимися традициями и на этой базе успешно развивается отрасль промышленности по разработке и созданию криптографической техники для решения задач обеспечения информационной безопасности.

Однако возможное появление широко рекламируемых в последние годы квантовых технологий обработки информации и квантовых вычислительных

устройств может внести существенные коррективы в сложившийся в области криптографии порядок вещей как в России, так и во всем мире. Многократно увеличилось количество и мнимых, и действительных угроз информационной безопасности. Считается, что появление «полноценного квантового компьютера» сведет на нет возможности обеспечения информационной безопасности путем применения асимметричных криптографических систем и симметричных систем с ограниченной длиной ключа, не являющихся теоретически стойкими. Такое развитие событий может привести к существенному уменьшению парка криптографической техники, пригодной для практических применений. При этом бескомпромиссную надежность сохраняет лишь имеющая соответствующее заключение регулятора криптографическая техника, в которой реализованы теоретически стойкие криптографические алгоритмы.

Теоретически стойкие криптографические системы (по Шеннону, совершенные шифры [80]) при всех своих отличных показателях по стойкости обладают рядом недостатков, существенно затрудняющих их практическое применение в области обеспечения информационной безопасности. Самым значимым среди них является сложность подсистемы управления ключами, под которой понимается подсистема генерации, распределения, применения и утилизации ключевой информации. Как правило, по причине сложности подсистемы управления ключами, теоретически стойкие криптографические системы являются громоздкими в практической эксплуатации, дорогими по затратам при выработке и распределении ключевой информации, подвержены повышенной опасности компрометации ключевой информации вне контролируемых зон. Поэтому они имеют ограниченное применение и в нынешнем своем состоянии не могут полностью и полноценно удовлетворить практические потребности при решении задач информационной безопасности.

Налицо *противоречие* между все нарастающей потребностью в обеспечении информационной безопасности, как в личностном плане, так и в общегосударственном масштабе, и потенциально возможным сокращением (в

связи с возможным появлением квантового компьютера) парка технических средств, в том числе, и криптографических, пригодных для полноценной защиты информации.

В настоящее время существенным вкладом в направлении преодоления указанного выше противоречия может служить разработка и широкое применение новых механизмов защиты информации, основанных на природных явлениях, не имеющих аналогов в классической физике, но которые изучаются в квантовой механике. Результаты, полученные в данной диссертационной работе, демонстрируют, что такие механизмы представляют собой новый ресурс, при задействовании которого, можно противостоять попыткам взлома с помощью квантовых компьютеров с эффективностью не менее, чем теоретически стойкие классические криптографические системы. Эти механизмы лишены отмеченных выше недостатков, препятствующих полноценному широкому практическому использованию. Отмеченные обстоятельства служат основанием **актуальности** выбранного направления диссертационного исследования.

**Актуальность темы диссертационной работы** напрямую отмечена в перечне «Приоритетные проблемы научных исследований в области обеспечения информационной безопасности Российской Федерации» (в пунктах 2.2.2.1 и 2.2.2.5 раздела «Научно-технические проблемы обеспечения информационной безопасности Российской Федерации» [67]).

**Цель** диссертационного исследования заключается в изучении и применении ресурсов, предоставляемых квантовой механикой, при построении элементов теоретически стойких криптографических систем защиты информации. Привлечение квантовых ресурсов с одной стороны может улучшить их потребительские и эксплуатационные характеристики, а с другой – способствовать появлению новых положительных для целей защиты информации свойств и качеств (принципиально невозможных в классических криптографических системах). К числу таких свойств относятся:

улучшение вероятностных свойств ключевого материала

криптографической системы защиты информации, за счет использования фундаментально случайных процессов, выявленных и исследованных в квантовой механике и получивших название «истинных» случайных процессов;

повышение стойкости криптографической системы при компрометации ключевого материала за счет реализации его на квантовых носителях;

возможность дистанционного приведения использованных квантовых носителей ключевого материала криптографической системы в состояние, пригодное для повторного использования (дистанционная регенерация).

В настоящее время основными квантовыми ресурсами, используемыми для построения систем квантовой криптографии, являются:

невозможность клонирования неизвестных квантовых состояний (no-cloning theorem, запрет клонирования) и эквивалентная ей невозможность идеального различения неортогональных квантовых состояний [94], [108];

несепарабельные состояния квантовых систем [24];

фундаментально случайный процесс – «истинная» случайность [43].

С использованием ресурсов невозможности клонирования неизвестных квантовых состояний и эквивалентной ей невозможности идеального различения неортогональных квантовых состояний построены квантовые криптографические системы BB84 [88], B92 [89], SARG04 [105] и др.

С использованием ресурсов несепарабельных состояний квантовых систем, невозможности клонирования неизвестных квантовых состояний и «истинной» случайности построена квантовая криптографическая система E91 [96].

Все указанные квантовые криптографические системы для формирования ключевого материала используют фотоны. В настоящее время не существует механизмов долговременного хранения фотонов. Поэтому в данных криптографических системах отсутствует в принципе возможность независимой выработки ключевого материала, в режиме, так сказать, «офлайн». Кроме того, сформированный ключевой материал хранится на

классических носителях, что влечёт те же проблемы, что и в классических реализациях криптографических систем.

В квантовых криптографических системах BB84 [88], B92 [89], SARG04 [105] и др., построенных на запрете клонирования неизвестных квантовых состояний и эквивалентной ей невозможности идеального различения неортогональных квантовых состояний, ключевой материал генерируется с использованием классических генераторов случайных последовательностей. Квантовый ресурс используется лишь для защиты от атак, возможных при распределении и доведении носителей-фотонов до потребителей-абонентов. Поэтому ключевой материал является реализацией случайного процесса в классическом понимании и не является реализацией фундаментально случайного процесса – квантового ресурса «истинной» случайности [43].

Таким образом, два из перечисленных выше трех новых положительных для целей защиты информации свойств, принципиально невозможны не только для классических криптографических систем. Ими не обладают и сертифицированные, широко применяемые в настоящее время квантовые криптографические системы.

Отметим также, что свойство, выражающееся в улучшении вероятностных свойств ключевого материала криптографической системы защиты информации, за счет использования фундаментально случайных процессов, выявленных и исследованных в квантовой механике и получивших название «истинных» случайных процессов, в настоящее время присуще только квантовой криптографической системе E91 [96].

Представляется, что одним из возможных путей построения новых квантовых криптографических систем, обладающих перечисленными выше положительными свойствами, может служить применение других носителей ключевого материала. В этом случае использование вместо фотонов массивных квантовых объектов, может позволить системе находиться в несепарабельном состоянии в течение времени, достаточном для криптографических приложений. Остановимся на этом более подробно.

Традиционными источниками несепарабельных квантовых состояний являются процессы каскадного распада атомных возбуждений и спонтанного параметрического рассеяния света в нелинейных кристаллах [29], [30], [49], [51], [52], [58], [69], [82]. С помощью этих процессов в лабораторных и промышленных условиях создают фотонные пары с несепарабельными состояниями поляризации, которыми затем управляют при помощи зеркал и поляризаторов. Однако подобные источники несепарабельных состояний обладают рядом недостатков.

С одной стороны, процессы распада высокочастотного фотона на фотонную пару и релаксационного распада атомных возбуждений являются случайными, так как они обусловлены квантовыми флуктуациями в рассматриваемой среде [51], [52], [69], [82].

С другой стороны, созданные фотонные пары распространяются со скоростью света, так что их трудно локализовать и сохранить для последующего использования [49], [52], [69], [82].

Именно эти причины и привели к необходимости уделить внимание в плане практической реализации несепарабельных квантовых состояний еще и разработке и применению *детерминистских* (в противоположность случайным) методов создания несепарабельных квантовых состояний *массивных* частиц (в противоположность фотонам) – прежде всего отдельных атомов и ионов, захваченных в ловушках соответствующих типов [33], [34], [82]. Здесь под детерминизмом понимается возможность создавать нужное несепарабельное квантовое состояние данных частиц в любой заданный момент времени и сохранять это состояние длительно, то есть в течение временных отрезков, обусловленных потребностями конкретных практических приложений.

В ходе выполнения исследований стало ясно, что два указанных вида «носителей» несепарабельных квантовых состояний (фотоны и атомы (или ионы)) в некотором смысле дополняют друг друга [33], [34], [49], [63], [82]. Если удастся создать надежные устройства для генерации и

манипулирования несепарабельными квантовыми состояниями массивных частиц (атомов или ионов), а также управления взаимодействием этих массивных частиц со светом (фотонами), то в результате появится идеальная практическая база для всех необходимых технических решений. При этом частицы предоставят возможность долговременного хранения специфической квантовой информации, а фотоны обеспечат возможность манипулирования ею.

В настоящее время уже выполнен целый ряд практических работ, которые подтвердили возможности искусственного создания и сохранения несепарабельных квантовых состояний в формах, пригодных для технического воплощения [34], [49], [63], [82], [97], [98], [101]. Перечислим основные технологические направления, используемые в этих работах:

технологии, основанные на использовании оптических фотонов в качестве носителей несепарабельных квантовых состояний;

различного рода технические методы квантовой электродинамики резонаторов;

технологии, основанные на использовании ионов в ловушках;

технологии, основанные на использовании нейтральных атомов в ловушках;

технологии и технические методы ядерного магнитного резонанса;

технологии, основанные на использовании носителей зарядов в сверхпроводниках;

технологии, основанные на использовании квантовых точек, изготовленных из полупроводников;

технологии, основанные на использовании дефектов в полупроводниках и др.

Выполненные исследования показали, в частности, что большая часть трудностей, с которыми сталкиваются экспериментаторы при технических реализациях «долгоживущих» несепарабельных квантовых

состояний, связана с необходимостью технического решения задачи исключения декогеренции [30]. Здесь под *декогеренцией* понимается физический процесс, при котором происходит потеря когерентности квантового состояния, то есть в результате декогеренции квантовое состояние перестает быть чистым. Например, уменьшается или полностью исчезает квантовая несепарабельность между составными частями квантовой системы в результате ее взаимодействия с окружением. В настоящее время задача исключения декогеренции решается путем улучшения изолированности квантовой системы от окружающей среды. Таким образом, чем лучше изолирована квантовая система, находящаяся в запутанном квантовом состоянии, тем меньше она подвержена декогеренции. Отметим, что исключение декогеренции относится к числу тех задач, для которых продолжающееся совершенствование в искусстве проведения физических экспериментов способно произвести существенные изменения в сторону улучшения ситуации.

В плане решения задачи обеспечения «длительности жизни» несепарабельных квантовых состояний наилучшим обнадеживающим ориентиром является следующий результат: теоретические расчеты «времени жизни» несепарабельных квантовых состояний, реализованных с использованием спинов ядер атомов некоторых химических элементов, дают результат - около 3000000 лет [63].

Таким образом, построение квантовых криптографических систем с использованием массивных частиц в качестве носителей для формирования ключевого материала в плане возможностей практической реализации является перспективным направлением.

Исходя из представленных выше соображений, **цель диссертационной работы** заключается в повышении эффективности криптографической защиты информации путем разработки и применения квантовых криптографических систем, основанных на использовании «долгоживущих» в несепарабельных состояниях массивных частиц.

**Объект исследования** – процесс защиты сообщений в информационных сетях.

**Предмет исследования** – модели и алгоритмы защиты конфиденциальной информации в локальных и глобальных информационных сетях с использованием квантовых технологий.

**Границы исследования:**

- в качестве используемых квантовых ресурсов при разработке криптографических систем рассматриваются такие квантовомеханические эффекты, как:

несепарабельные состояния квантовых систем;

фундаментально случайный процесс – «истинная» случайность;

- разрабатываемые криптографические системы ориентированы на использование «долгоживущих» в несепарабельных состояниях массивных частиц в качестве носителей для формирования ключевого материала.

Для достижения поставленной в диссертационной работе цели решается **научная задача** разработки криптографической системы, которой присущи следующие свойства:

криптографическая система является теоретически стойкой;

ключевой материал криптографической системы формируется исключительно за счет использования фундаментально случайных процессов, выявленных и исследованных в квантовой механике и получивших название «истинных» случайных процессов;

криптографическая система остается идеально стойкой при компрометации ключевого материала;

существует возможность дистанционной регенерации использованных квантовых носителей ключевого материала криптографической.

Данная научная задача декомпозируется на следующие частные задачи, решение которых представлено в диссертационной работе:

- 1) описание и анализ квантовых криптографических ресурсов с позиции

их пригодности и эффективности для применения при построении криптографических систем;

2) исследование и выявление эффективно проверяемых признаков многокубитного состояния, по которым можно определить несепарабельно это состояние или нет;

3) исследование и выявление среди состояний многокубитных квантовых систем класса состояний, пригодных для построения криптографической системы со свойствами, перечисленными в формулировке научной задачи диссертационной работы;

4) анализ известных квантовых криптографических систем с позиции обоснования необходимости разработки новой квантовой криптографической системы;

5) математическое описание основных структурных элементов новой теоретически стойкой квантовой криптографической системы (разработанной в рамках проведения диссертационных исследований и названной **АКМ2017**);

6) математическое обоснование того, что квантовая криптографическая система **АКМ2017** является теоретически стойкой и обладает всеми свойствами, перечисленными в формулировке научной задачи диссертационной работы.

**Методы исследований.** Алгебраические методы, методы теории алгоритмов, теории вероятностей, квантовой физики, квантовой информатики, классической криптографии, квантовой криптографии.

**Достоверность** результатов работы обеспечивается строгостью применения математических моделей, согласованностью полученных результатов с известными. Добавочно подтверждается результатами расчетов, апробации и внедрения предложенных в диссертации методов в технологические процессы создания технических средств защиты информации в научно-техническом предприятии «Криптософт» и в Институте инженерной физики при выполнении научно-исследовательской работы «Рубас».

**Научная новизна результатов диссертационной работы** заключается в следующем:

1) выявлены на основе применения аналитического аппарата **булевых масок** состояний квантовых систем эффективно проверяемые достаточные признаки многокубитного состояния, по которым можно определить, несепарабельно это состояние или нет;

2) выявлены на основе применения аналитического аппарата **нумераторов весов** состояний квантовых систем эффективно проверяемые достаточные признаки многокубитного состояния, по которым можно определить несепарабельно это состояние или нет;

3) разработан алгоритм решение задачи бинарной классификации квантовых состояний (то есть, задачи определения к какому из двух классов – классу сепарабельных состояний или классу несепарабельных состояний – принадлежит заданное многокубитное состояние) через вычисление всех возможных **редукций** булевых функций, векторы значений которых являются булевыми масками квантовых состояний;

4) выявлен и описан класс состояний многокубитных квантовых систем, во многом по своим свойствам аналогичных двухкубитному состоянию спиновый синглет;

5) разработана квантовая криптографическая система **АКМ2017** и математически обоснована ее теоретическая стойкость;

6) выявлено и математически обосновано, что квантовая криптографическая система **АКМ2017** сохраняет идеальную стойкость при компрометации носителей ключевого материала; данное свойство в принципе невозможно для всех классических криптографических систем и известных квантовых криптографических систем, отличных от **АКМ2017**;

7) выявлено и математически обосновано, что для квантовой криптографической системы **АКМ2017** существует возможность дистанционной регенерации использованных шифрблоков; данное свойство в принципе невозможно для всех классических криптографических

систем и известных квантовых криптографических систем, отличных от АКМ2017; разработан алгоритм дистанционной регенерации использованных квантовых носителей ключевого материала криптографической системы.

**Публикации.** По теме диссертации автором и при его активном участии выполнены 23 публикации ([9], [11], ... , [24], [25], [59], [60], [61], [62], [84]), в том числе 1 монография (в соавторстве) [24]. Статьи [11], [12], [25], [62], [84], [113], [114] опубликованы в научных изданиях, входящих в перечень ВАК. Работы [84], [113] и [114] опубликованы в изданиях, входящих в перечень RSCI.

**Апробация работы.** Основные научные результаты работы докладывались на 5 межведомственных научных семинарах, организованных Институтом проблем информатики Российской академии наук и научно-техническим предприятием «Криптософт», а также на следующих 6 научно-технических форумах:

6-я Всероссийская научно-техническая школа-семинар «Информационная безопасность – актуальная проблема современности». – Краснодар, 2013 г;

7-я Всероссийская научно-техническая школа-семинар «Информационная безопасность – актуальная проблема современности». – Краснодар, 2013 г.;

12-я Всероссийская научно-техническая школа-семинар «Информационная безопасность – актуальная проблема современности». – Краснодар, 2016 г;

13-я Всероссийская научно-техническая школа-семинар «Информационная безопасность – актуальная проблема современности». – Краснодар, 2016 г.;

12-я Научно-техническая конференция по криптографии. – Москва, 2016 г.;

14-я Всероссийская научно-техническая школа-семинар «Информационная безопасность – актуальная проблема современности». –

Краснодар, 2017 г.

**На защиту выносятся:** обоснование актуальности, научная, теоретическая и практическая значимость работы, следующие **положения, которые подтверждаются результатами исследования**, представленными далее в Заключение диссертации.

1. Установленные в рамках проведения диссертационных исследований достаточные признаки несепарабельности состояний многокубитных квантовых систем, основанные на аналитических аппаратах булевых масок и нумераторов весов квантовых состояний.

2. Теоретически стойкая квантовая криптографическая система **АКМ2017**, основанная на применении двух ресурсов квантовой физики, не имеющих классических аналогов, – ресурса несепарабельных состояний квантовых систем и ресурса фундаментально случайного процесса («истинной» случайности).

3. Сохранение квантовой криптографической системой **АКМ2017** идеальной стойкости при компрометации носителей ключевого материала; данное свойство в принципе невозможно для всех классических криптографических систем и известных квантовых криптографических систем, отличных от **АКМ2017**;

4. Алгоритм дистанционной регенерации использованных квантовых носителей ключевого материала криптографической системы **АКМ2017**.

**Структура и объем работы.** Диссертация состоит из введения, трех глав, заключения, списка литературы и 5 приложений. Каждая глава состоит из нескольких параграфов, снабжена отдельным введением и заканчивается выводами о представленных в ней результатах. Общий объем работы составляет 157 стр.

В работе принята трехпозиционная последовательная единая нумерация объектов (определений, утверждений, теорем, замечаний и формул) в каждом параграфе. В номере каждого объекта первая позиция соответствует номеру главы, вторая номеру параграфа, третья – порядковому номеру объекта внутри

параграфа.

**В главе 1** обсуждаются ресурсы квантовой механики, применяемые в настоящее время при построении криптографических систем, и методологические основы данной работы. Приводятся все необходимые для понимания дальнейшего определения и факты. Глава состоит из пяти параграфов.

Параграф 1.1 посвящен достаточно подробному описанию одного из основных ресурсов квантовой механики, широко востребованному для построения протоколов квантовой криптографии. Этот ресурс заключается «в невозможности клонирования неизвестных квантовых состояний и эквивалентной ей «невозможности идеального различения неортогональных квантовых состояний». Он обеспечивает возможность защиты информации методами квантовой криптографии путем использования квантовых носителей. Теоретическое описание обсуждаемого ресурса представлено в виде теоремы о невозможности клонирования. Результаты, представленные в параграфе 1.1, составляют основу ряда квантовых криптографических систем, таких, как BB84, B92, E91, представленных в параграфе 3.1.

В параграфе 1.2 осуществлено неформальное введение в теорию несепарабельных состояний квантовых систем. Несепарабельные состояния являются еще одним квантовым ресурсом, широко используемым для построения криптографических систем. Рассмотрены исторические аспекты становления и развития научного направления исследования несепарабельности квантовых состояний. Указаны современные технологии физической реализации несепарабельных квантовых состояний.

В параграфе 1.3 изложены математические определения понятий сепарабельности и несепарабельности состояний многокубитных квантовых систем, учитывающие сложную специфику связей их составных компонент. Приведены сформулированные вместе с соавторами критерии несепарабельности состояний двухкубитной и трехкубитной квантовых систем, использующие коэффициенты представления состояний в

соответствующих вычислительных базисах. В Приложениях приводятся новые, основанные на аппарате линейной алгебры, доказательства этих критериев.

В параграфе 1.4 уделено внимание одному уникальному состоянию двухкубитной квантовой системы, называемому по историческим причинам «спиновый синглет». Если про ресурс несепарабельности мы говорим как о полезном для криптографических приложений ресурсе и удивительном физическом явлении, не имеющему аналогов в классической физике, то спиновый синглет является в еще большей степени удивительным явлением в мире несепарабельных квантовых состояний, приносящим при своем использовании в криптографических приложениях новые полезные качества, отсутствующие в классических криптографических системах. Формулируется и доказывается утверждение относительно свойств состояния спиновый синглет, которое используется в главе 3 при обосновании идеальной стойкости криптографической системы **АКМ2017**.

В параграфе 1.5 доказывается новое утверждение, что близкими по своим свойствам к состоянию спиновый синглет являются некоторые состояния трех и более кубитных квантовых систем. Далее исследуются состояния их подсистем из двух крайних (первого и последнего) кубитов. Доказывается, что состояния указанных подсистем совпадают с состоянием спиновый синглет.

Результаты, представленные в параграфе 1.5, необходимы для построения алгоритма (см. параграф 3.5) дистанционной регенерации квантовых носителей ключевого материала криптографической системы **АКМ2017**.

**Вторая глава** диссертационной работы посвящена исследованию и выявлению эффективно проверяемых достаточных признаков несепарабельности для состояний многокубитных квантовых систем.

В параграфе 2.1 вводится понятие булевой маски состояния многокубитной квантовой системы. Такой подход мотивирован тем, что

иногда распределение нулей в значениях координат векторов квантовых состояний позволяет судить об их разложимости в тензорное произведение. Учитывая, что вопрос сепарабельности или несепарабельности для булевой маски состояния многокубитной квантовой системы решается проще, чем для самого состояния, нужно и можно констатировать выявление эффективного подхода для определения несепарабельности состояния в том случае, когда несепарабельной является его булева маска.

Другой подход для выявления несепарабельных квантовых состояний многокубитных квантовых систем основан на использовании их нумераторов весов. Изучению данного подхода посвящен параграф 2.2. Как и в случае булевых масок, так и в случае нумераторов весов удастся получить только достаточные условия для несепарабельности состояний.

В параграфе 2.3 представлен алгоритм решения задачи о неразложимости состояния квантовой системы в тензорное произведение состояний меньшей размерности через вычисление всех возможных редукций булевых функций, векторы значений которых являются булевыми масками квантовых состояний.

**Глава 3** состоит из пяти параграфов.

В параграфе 3.1 представлены квантовые криптографические системы, использующие ресурс, заключающийся «в невозможности клонирования неизвестных квантовых состояний». Указанный ресурс обеспечивает возможность защиты информации методами квантовой криптографии путем использования квантовых носителей. Теоретическое описание этого ресурса представлено в виде теоремы о невозможности клонирования в главе 1.

В параграфе 3.2 представлено описание квантовой криптографической системы, основанной на использовании двух квантовых ресурсов: ресурсе невозможности клонирования неизвестных квантовых состояний и ресурсе несепарабельных квантовых состояний.

В параграфе 3.3 изложены результаты по разработке на основе ресурса несепарабельных квантовых состояний совершенно стойкой квантовой

криптографической системы **АКМ2017**. Обсуждаются её качественные свойства, в том числе и те, которыми в принципе не могут обладать классические криптографические системы.

Параграф 3.4 посвящен обоснованию сохранения свойства идеальной стойкости для квантовой криптографической системы **АКМ2017** при компрометации квантовых шифрблокнотов.

В параграфе 3.5. изложено описание алгоритма дистанционной регенерации использованных квантовых шифровальных блокнотов (их носителей-кубитов) квантовой криптографической системы **АКМ2017**.

**В заключении** подведены итоги и даны предложения по направлениям дальнейших исследований.

В приложениях приведены вспомогательные материалы к главе 1 диссертационной работы.

## ГЛАВА 1. КВАНТОВЫЕ РЕСУРСЫ, ИСПОЛЬЗУЕМЫЕ В КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

В первой главе диссертации описаны ресурсы квантовой физики, используемые в настоящее время при построении квантовых криптографических систем:

невозможность клонирования неизвестных квантовых состояний;  
несепарабельные состояния квантовых систем.

Среди несепарабельных состояний двухкубитных квантовых систем в качестве особо примечательного (с позиции использования в криптографических приложениях) выделяется состояние спиновый синглет. Исследованы свойства этого состояния, которые существенны для построения квантовых криптографических систем. Автором установлено, что такие свойства присущи целому классу состояний квантовых систем из трех и более кубитов.

## § 1.1. Теорема о невозможности клонирования

Информация – основное понятие научно-практических направлений, изучающих процессы передачи, обработки и хранения различных данных. Суть понятия информации обычно поясняется на примерах. Формальное определение не дается, поскольку понятие информации относится к фундаментальным понятиям [41]. Информацию в таком, традиционном, ее понимании принято называть *классической информацией* [63], [66], [77]. Кроме известных и широко распространенных способов ее передачи, она может быть также «записана» (закодирована) в состояниях квантовых систем, например, в поляризационных состояниях одиночных фотонов и передана через соответствующий физический канал связи. Так, например, происходит при распределении криптографических ключей методами квантовой криптографии [49].

В то же время, квантовое состояние (то есть состояние квантово-механической системы) само по себе представляет особого рода информационный ресурс, содержащий сведения о статистике всевозможных измерений над данной квантовой системой [66]. Информация, содержащаяся в квантовом состоянии, имеет качественные отличия от классической информации и поэтому для нее применяют специальный термин *квантовая информация* [63], [66]. Наиболее ярким отличием квантовой информации от классической является невозможность копирования произвольного неизвестного квантового состояния (no cloning [77]). Этот факт известен как «теорема о невозможности клонирования» и составляет математическую основу надёжности всех современных протоколов квантовой криптографии, кроме **АКМ2017**. Формулировка теоремы и её доказательство приводятся в конце данного параграфа, а здесь обсуждаются некоторые математические аспекты копирования информации.

Единицей классической информации является бит. Копирование классической информации по сути дела копирование конечной битовой

последовательности. Поэтому решить задачу копирования классической информации можно, например, путем решения задачи копирования одного бита и повторения этого решения необходимое число раз по отношению ко всем битам, составляющим исходный информационный массив.

Копирование одного бита можно осуществить, например, с помощью классического логического элемента CNOT [63], реализующего функцию

$$f(x, y) = \begin{pmatrix} x \\ x \oplus y \end{pmatrix}$$

(где  $x$  и  $y$  двоичные переменные,  $\oplus$  - знак операции сложения по модулю 2). Подав на вход элемента CNOT копируемый бит (в неизвестном состоянии  $x$ , то есть неизвестно  $x=0$  или  $x=1$ ) и бит «заготовку», инициализированную нулем (то есть  $y=0$ ), на выходе классического логического элемента CNOT будут два бита, имеющие одинаковые значения  $x$ . Реализуя эту процедуру по отношению к каждому биту информации, создаем ее копию.

В случае квантовой информации ситуация более сложная. Здесь принято использовать вместо термина «копирование» термин «клонирование», подчеркивая тем самым физический характер квантовой информации [66], [77].

В качестве единицы квантовой информации используется кубит. Более подробно, **кубит** – это фундаментальное понятие в области квантовых вычислений и квантовой информации, имеющее смысл единицы квантовой информации. Этот смысл понятия представляет кубит, как математический объект [63].

Кубиты, в квантовой области являются «аналогами» таких классических объектов как биты.

Напомним, что **бит** - это фундаментальное понятие в области классических вычислений и классической информации, имеющее смысл единицы классической информации. Классический бит может находиться в состоянии 0 или 1.

Состояниями кубита являются векторы двумерного гильбертова

пространства  $\mathbf{C}^2$  над полем комплексных чисел  $\mathbf{C}$  вида  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , где  $\alpha, \beta \in \mathbf{C}$ ,  $|\alpha|^2 + |\beta|^2 = 1$ ;  $\{|0\rangle, |1\rangle\}$  – ортонормированный базис пространства  $\mathbf{C}^2$ . И это главное различие между битами и кубитами.

Векторы  $|0\rangle$  и  $|1\rangle$  называются **состояниями вычислительного базиса** в случае одного кубита и вектор  $|\psi\rangle$  при этом является **суперпозицией** (линейной комбинацией) векторов  $|0\rangle$  и  $|1\rangle$ . В качестве состояний вычислительного базиса может быть взята и любая другая ортонормированная система из двух векторов пространства  $\mathbf{C}^2$ . Для определенности положим

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Можно рассматривать квантовые конструкции и из более чем одного кубита. Состояниями системы из  $k$  ( $k \geq 1$ ) кубитов являются нормированные векторы, принадлежащие  $k$ -той тензорной степени пространства  $\mathbf{C}^2$ , то есть  $2^k$ -мерного гильбертова пространства  $\mathbf{C}^{2^k} = \mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \dots \otimes \mathbf{C}^2$  над полем комплексных чисел  $\mathbf{C}$ . Эти векторы, называемые **суперпозициями** (**линейными комбинациями**), можно представить в следующем виде:

$$\alpha_0 \underbrace{|000\dots 00\rangle}_k + \alpha_1 |000\dots 01\rangle + \alpha_2 |000\dots 10\rangle + \dots + \alpha_{2^k-1} |111\dots 11\rangle,$$

где

$$\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_{2^k-1} \in \mathbf{C}, |\alpha_0|^2 + |\alpha_1|^2 + \dots + |\alpha_{2^k-1}|^2 = 1,$$

$$|\varphi_1 \varphi_2 \varphi_3 \dots \varphi_{k-1} \varphi_k\rangle = |\varphi_1\rangle |\varphi_2\rangle |\varphi_3\rangle \dots |\varphi_{k-1}\rangle |\varphi_k\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes |\varphi_3\rangle \otimes \dots \otimes |\varphi_{k-1}\rangle \otimes |\varphi_k\rangle,$$

$$\varphi_m \in \{0; 1\}, m = \overline{1, k}.$$

Состояния  $\underbrace{|000\dots 00\rangle}_k, |000\dots 01\rangle, \dots, |111\dots 11\rangle$  называются **состояниями**

**вычислительного базиса** в случае системы из  $k$  кубитов. Они составляют ортонормированный базис гильбертова пространства  $\mathbf{C}^{2^k}$ .

*Клонирование* – это копирование квантовой информации. Клонирование

– обязательно физический процесс [71].

В некоторых случаях можно клонировать квантовую информацию, а в других нет. Конечно, это можно сделать каждый раз специальным прибором для данного конкретного известного квантового состояния (и даже для фиксированного набора ортогональных квантовых состояний). Но не существует универсального прибора, который бы размножал (клонировал) произвольное неизвестное квантовое состояние.

Рассмотрим пример, когда квантовую информацию можно клонировать. Предположим, что квантовая информация представлена кубитами, состояние каждого из которых принадлежит множеству  $\{|0\rangle, |1\rangle\}$ .

Возьмем любой из этих кубитов и обозначим его состояние  $|x\rangle = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ , где  $x_1, x_2 \in \{0, 1\}$  и справедливы равенства:

$$x_1 \cdot x_2 = 0, \quad x_1 + x_2 = 1.$$

Это состояние нам неизвестно. Мы знаем только то, что  $|x\rangle \in \{|0\rangle, |1\rangle\}$ .

Далее мы хотим использовать двухкубитный квантовый логический элемент **CNOT**, который на множестве состояний квантовой системы из двух кубитов реализует унитарный оператор с 4x4 матрицей

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (1.1.1)$$

Поэтому нам необходим еще второй «вспомогательный» кубит. Этот второй кубит инициализируем в состоянии  $|0\rangle$ . Таким образом, на вход квантового логического элемента **CNOT** подаем два кубита в общем состоянии

$$|x\rangle |0\rangle = |x\rangle \otimes |0\rangle = \begin{pmatrix} x_1 \\ 0 \\ x_2 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 x_1 \\ x_1 x_2 \\ x_2 x_2 \\ x_1 x_2 \end{pmatrix}.$$

Умножив матрицу (1.1.1) на это состояние, получаем для двух кубитов на выходе квантового логического элемента **CNOT** следующее общее

состояние:

$$\mathbf{CNOT}|x\rangle|0\rangle = \mathbf{CNOT}|x\rangle \otimes |0\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 x_1 \\ x_1 x_2 \\ x_2 x_2 \\ x_1 x_2 \end{pmatrix} = \begin{pmatrix} x_1 x_1 \\ x_1 x_2 \\ x_2 x_1 \\ x_2 x_2 \end{pmatrix}$$

=

$$= \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \otimes \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = |x\rangle \otimes |x\rangle = |x\rangle |x\rangle.$$

Таким образом, нам удалось с помощью квантового логического элемента **CNOT** получить два кубита в общем состоянии  $|x\rangle|x\rangle$ , то есть мы убедились в том, что с помощью квантового логического элемента **CNOT** можно успешно клонировать квантовую информацию, представленную кубитами, состояние каждого из которых принадлежит множеству  $\{|0\rangle, |1\rangle\}$ .

Теперь рассмотрим общий случай, когда кубит находится в неизвестном состоянии

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

где  $\alpha, \beta \in \mathbf{C}$ ,  $|\alpha|^2 + |\beta|^2 = 1$ . Это состояние неизвестно в том смысле, что неизвестны значения комплексных чисел  $\alpha$  и  $\beta$ . Точно также, как и выше, для клонирования кубита в состоянии  $|\psi\rangle$  воспользуемся квантовым логическим элементом **CNOT** и вторым «вспомогательным» кубитом в состоянии  $|0\rangle$ . Таким образом, на вход квантового логического элемента **CNOT** подаем два кубита в общем состоянии

$$|\psi\rangle|0\rangle = |\psi\rangle \otimes |0\rangle = \alpha|00\rangle + \beta|10\rangle = \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix}. \quad (1.1.2)$$

Умножив матрицу (1.1.1) на состояние (1.1.2), получаем для двух кубитов на выходе квантового логического элемента **CNOT** следующее общее состояние:

$$\mathbf{CNOT}|\psi\rangle|0\rangle = \mathbf{CNOT}|\psi\rangle \otimes |0\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{pmatrix} =$$

$$= \alpha|00\rangle + \beta|11\rangle. \quad (1.1.3)$$

С другой стороны, для состояния  $|\psi\rangle|\psi\rangle$  справедливо равенство

$$|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle. \quad (1.1.4)$$

Следовательно, состояния (1.1.3) и (1.1.4) совпадают тогда и только тогда, когда справедливы равенства:

$$\alpha^2 = \alpha, \beta^2 = \beta, \alpha\beta = 0. \quad (1.1.5)$$

Отсюда, с учетом условия  $|\alpha|^2 + |\beta|^2 = 1$ , следует, что клонирование квантовой информации с помощью квантового логического элемента **CNOT** возможно лишь в том случае, когда оно представлено кубитами, состояние каждого из которых принадлежит множеству  $\{|0\rangle, |1\rangle\}$ . Такое клонирование не зависит от того, известны состояния кубитов или нет.

С учётом равенства (1.1.3) можно сделать следующее

**Замечание 1.1.6.** Хотя, квантовый логический элемент **CNOT** пригоден как инструмент клонирования квантовой информации только в определенных ограничениях условиях, он (т. е. **CNOT**), как следует из равенства (1.1.3), представляет собой эффективный инструмент для построения **запутанных состояний** квантовой системы из двух кубитов на основе кубита в произвольном состоянии  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  и кубита в состоянии  $|0\rangle$  при условии, что  $\alpha \cdot \beta \neq 0$ . Квантовая запутанность или, точнее, запутанность состояний квантовых систем из двух и более кубитов, является новым ресурсом квантовой механики, пригодным для применений в области информационных и телекоммуникационных технологий. Вопросам запутанности посвящён следующий параграф.

Возвращаясь теперь к обсуждаемым в данном параграфе вопросам, отметим, что установлено - клонирование кубита с помощью квантового логического элемента **CNOT** не всегда возможно. Оказывается, что это касается не только элемента **CNOT**. Это свойство (что кубиты в неизвестном состоянии нельзя клонировать) носит более общий характер и известно как теорема *о невозможности клонирования* [92], [107].

Прежде чем сформулировать теорему *о невозможности клонирования* имеет смысл на качественном уровне объяснить, что следует из этой теоремы.

Во-первых, физического прибора (инструмента) в самом широком смысле этого понятия, позволяющего осуществить клонирование кубита в произвольном неизвестном состоянии

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

где  $\alpha, \beta \in \mathbf{C}$ ,  $|\alpha|^2 + |\beta|^2 = 1$ , **не существует.**

Более того, не существует физического прибора (инструмента), позволяющего клонировать кубит в неизвестном состоянии, принадлежащем известному множеству состояний, содержащему не менее чем два неортогональных состояния. Например, не существует физического прибора (инструмента), позволяющего клонировать кубит в неизвестном состоянии, который принадлежит множеству состояний  $\{|0\rangle, \frac{|0\rangle + |1\rangle}{\sqrt{2}}\}$ . Понимается

последнее предложение в следующем смысле: пусть  $|\psi_1\rangle, |\psi_2\rangle \in \{|0\rangle, \frac{|0\rangle + |1\rangle}{\sqrt{2}}\}$ ,  $|\psi_1\rangle \neq |\psi_2\rangle$ ,  $|s\rangle$  - произвольное однокубитное состояние; тогда не существует прибора (инструмента), позволяющего при подаче на свой вход двух кубитов в общем состоянии  $|\psi_1\rangle \otimes |s\rangle$  на выходе получить два кубита в общем состоянии  $|\psi_1\rangle \otimes |\psi_1\rangle$  и при подаче на свой вход двух кубитов в общем состоянии  $|\psi_2\rangle \otimes |s\rangle$  на выходе получить два кубита в общем состоянии  $|\psi_2\rangle \otimes |\psi_2\rangle$ .

Во-вторых, для любых двух ортогональных состояний  $|\psi_1\rangle$  и  $|\psi_2\rangle$  **существует** физический прибор (инструмент), позволяющий осуществить клонирование кубита в неизвестном состоянии  $|\psi\rangle \in \{|\psi_1\rangle, |\psi_2\rangle\}$ . При этом, если состояния  $|\psi_1\rangle$  и  $|\psi_2\rangle$  известны, то **можно построить** квантовый логический элемент, позволяющий клонировать квантовую информацию, представленную кубитами, состояние каждого из которых неизвестно, но

принадлежит множеству  $\{|\psi_1\rangle, |\psi_2\rangle\}$ .

В-третьих, свойство, установленное в теореме о *невозможности клонирования*, представляет собой одно из главных различий между квантовой и классической информацией [66]. Оно является новым квантовым ресурсом, эффективно применяемым, например, в квантовой криптографии при построении квантовых криптографических систем генерации и распределения ключей (квантовые криптографические протоколы BB84 [88], B92 [89], SARG04 [105] и др. [49], [63]).

Существует несколько вариантов формулировки и доказательства теоремы о *невозможности клонирования*. В заключение данного параграфа приведем вариант ([93], [108]), наиболее близкий по используемому математическому аппарату и методологии настоящему диссертационному исследованию.

**Теорема 1.1.7.** Пусть  $|\psi\rangle$  и  $|\phi\rangle$  - произвольные состояния произвольной квантовой системы  $K$  такие, что их скалярное произведение  $\langle\psi|\phi\rangle$  удовлетворяет условиям

$$\langle\psi|\phi\rangle \neq 0, \quad |\langle\psi|\phi\rangle| \neq 1 \quad (1.1.8)$$

(то есть состояния  $|\psi\rangle$  и  $|\phi\rangle$  не ортогональны и не совпадают).

Тогда для любого состояния  $|s\rangle$  квантовой системы  $K$  не существует унитарной матрицы  $U$ , такой, что одновременно справедливы равенства

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \quad (1.1.9)$$

и

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle. \quad (1.1.10)$$

**Доказательство.** Докажем методом от противного. Допустим, что существует унитарная матрица  $U$ , такая, что одновременно справедливы равенства (1.1.9) и (1.1.10). Отсюда следует, что должны быть равны скалярное произведение левых частей равенств (1.1.9) и (1.1.10) и скалярное

произведение правых частей равенств (1.1.9) и (1.1.10), то есть, должно быть справедливо равенство

$$\left\langle U(|\psi\rangle \otimes |s\rangle) \left| U(|\phi\rangle \otimes |s\rangle) \right. \right\rangle = \left\langle (|\psi\rangle \otimes |\psi\rangle) \left| (|\phi\rangle \otimes |\phi\rangle) \right. \right\rangle \quad (1.1.11)$$

Для скалярного произведения левых частей равенств (1.1.9) и (1.1.10) в силу унитарности матрицы  $U$  и свойств тензорного произведения справедлива следующая цепочка равенств

$$\begin{aligned} \left\langle U(|\psi\rangle \otimes |s\rangle) \left| U(|\phi\rangle \otimes |s\rangle) \right. \right\rangle &= \left\langle U^* U(|\psi\rangle \otimes |s\rangle) \left| (|\phi\rangle \otimes |s\rangle) \right. \right\rangle = \\ &= \left\langle (|\psi\rangle \otimes |s\rangle) \left| (|\phi\rangle \otimes |s\rangle) \right. \right\rangle = \langle \psi | \phi \rangle \cdot \langle s | s \rangle = \langle \psi | \phi \rangle. \end{aligned} \quad (1.1.12)$$

Аналогично, для скалярного произведения правых частей равенств (1.1.9) и (1.1.10) из свойств тензорного произведения следует справедливость следующей цепочки равенств

$$\left\langle (|\psi\rangle \otimes |\psi\rangle) \left| (|\phi\rangle \otimes |\phi\rangle) \right. \right\rangle = \langle \psi | \phi \rangle \cdot \langle \psi | \phi \rangle = \langle \psi | \phi \rangle^2. \quad (1.1.13)$$

Из равенств (1.1.11), (1.1.12) и (1.1.13) следует справедливость равенства

$$\langle \psi | \phi \rangle = \langle \psi | \phi \rangle^2. \quad (1.1.14)$$

Равенство (1.1.14) справедливо при  $\langle \psi | \phi \rangle = 0$ , что противоречит первому из условий (1.1.8), и при  $\langle \psi | \phi \rangle = 1$ , что противоречит второму из условий (1.1.8). Следовательно, допущение о существовании унитарной матрицы  $U$ , такой, что одновременно справедливы равенства (1.1.9) и (1.1.10), является неверным допущением. Теорема доказана.

## § 1.2. Несепарабельные состояния квантовых систем

**Несепарабельные состояния** (по-другому, запутанные состояния) квантовых систем и их свойства представляют большой научный и практический интерес. Они относятся к ряду основных объектов и ресурсов современных квантовых технологий хранения, обработки и передачи информации, не имеющих классических аналогов. Теория несепарабельных состояний квантовых систем является бурно развивающейся составной частью квантовой механики. Понятийный аппарат и методы исследования этого научного направления являются новыми, можно сказать, что они, в определенном смысле, находятся на переднем крае современной физики. В контексте данной работы несепарабельные состояния служат, с одной стороны, источником угроз для квантовой криптографии, как показано в предыдущем параграфе, с другой стороны, их свойства лежат в основе некоторых протоколов и, в том числе, протокола **АКМ2017**, представленного далее, в главе 3.

В качестве синонима для термина **несепарабельность** в квантовой теории информации используются также термины: **запутанность, перепутанность, сцепленность** [34], [63], [66], [77]. Представляется полезным предварительное краткое знакомство с историей возникновения, становления и современным содержанием теории несепарабельных состояний квантовых систем, не претендуя при этом на исчерпывающий охват всей информации в этой области. Это необходимо с позиции более точного понимания содержания дальнейшей части данной работы.

Сразу после возникновения квантовой механики были обнаружены новые, противоречащие привычной интуиции эффекты. Попытки их описания, толкования и объяснения повлекли за собой споры и дискуссии ученых-физиков. В результате был сформулирован ряд так называемых концептуальных проблем [39], [43], [58] от разрешения которых зависело дальнейшее существование и направление развития самой квантовой

механики как науки. Среди них, прежде всего, отметим проблему полноты описания мира квантовой механикой [39], [43], [58]. При попытках её разрешения физики 20-го века столкнулись с таким явлением как несепарабельные (запутанные) состояния (entangled states) квантовой системы, характеризующиеся наличием нелокальных корреляций частиц, составляющих квантовую систему.

Несепарабельные квантовые состояния не имеют аналога в классической физике. Однако было установлено [43], [45], [58], [73], [85], [86], [90], [92], [97], [98], [101], [102], [107], что они - не теоретическая абстракция, которую ввели физики-теоретики, а объективный факт окружающей действительности. Это – то, что существует в природе независимо от наших представлений. Напомним (см. [24]) описание этого явления природы.

В соответствии с положениями квантовой физики вполне возможно и даже обычно для двух или более разделенных пространством объектов образовывать в действительности единое целое в том смысле, что если мы потревожим один из этих объектов, то среагируют **все**. Это и называется несепарабельностью. Состояние такой единой целой квантовой системы называется несепарабельным состоянием, а сама квантовая система называется несепарабельной квантовой системой.

Здесь выражение «разделенных пространством» по отношению к объектам, составляющим квантовую систему, понимается, прежде всего, как **отсутствие между ними любого вида классической коммуникации**.

В процессе разрешения проблемы полноты описания мира квантовой механикой, что само по себе является выдающимся теоретическим результатом в общенаучном смысле, произошло и нечто другое, не менее грандиозное для практических приложений в различных направлениях информационных технологий, что фундаментальным образом изменило отношение научного сообщества к квантовым запутанным состояниям. Это нечто представляет собой осознание того, что несепарабельность (запутанность) состояний квантовых систем – это новый, не имеющий

классических аналогов, реализуемый на практике (экспериментально) физический ресурс. Такое осознание произошло в 80-х – 90-х годах 20-го века. С этого времени акценты, как экспериментаторов, так и теоретиков сместились в сторону прикладных исследований и технического применения несепарабельных квантовых состояний. Большие усилия были направлены на то, чтобы понять роль несепарабельных состояний в природе, найти возможность их практического применения в качестве принципиально нового нелокального ресурса в технических устройствах в области создания квантовых криптографических систем и квантовых компьютеров [1], [2], ..., 9, 11, ... , [25], [29], [30], [34], [43], [47], [49], [59], [60], [61]. [63], [65], [66], [77], [84], [88], [89], [105].

В современных протоколах квантовой криптографии, использующих несепарабельность, применяется, как правило, запутанность двухкубитных систем. Несепарабельные состояния трёх и более кубитов изучены в значительно меньшей степени. В следующем параграфе представлены результаты исследований некоторых вопросов, относящиеся к таким состояниям.

### § 1.3. Математическое определение несепарабельности состояния $n$ -кубитной квантовой системы

В этом параграфе вводится в рассмотрение понятие несепарабельности для многокубитных квантовых систем, отражающее результаты исследований, выполненных при активном участии автора. Изложение следует материалам, представленным в монографии [24]. Отметим, что далее в настоящей работе определение «несепарабельности» отличается от ставшего традиционным понятия «запутанности», когда число кубитов в квантовой системе равно трём (и более).

Пусть  $A_1A_2\dots A_n$  - квантовая система, состоящая из  $n$  кубитов  $A_1, A_2, \dots, A_n$ ;  $S_n$  – симметрическая группа подстановок [38] на множестве  $\{1, 2, \dots, n\}$ .

Пусть  $|\psi\rangle \in \mathbb{C}^{2^n}$  - произвольное состояние  $n$ -кубитной квантовой системы  $A_1A_2\dots A_n$ . Состояние  $|\psi\rangle$  можно представить в виде

$$\begin{aligned} |\psi\rangle &= \alpha_0 \underbrace{|000\dots 00\rangle}_n + \alpha_1 |000\dots 01\rangle + \alpha_2 |000\dots 10\rangle + \dots + \alpha_{2^n-1} |111\dots 11\rangle = \\ &= \sum_{\phi=0}^{2^n-1} \alpha_\phi |\phi\rangle = \sum_{\phi=0}^{2^n-1} \alpha_\phi |\phi_1\phi_2\dots\phi_n\rangle, \end{aligned} \quad (1.3.1)$$

где

$$\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_{2^n-1} \in \mathbb{C}, |\alpha_0|^2 + |\alpha_1|^2 + \dots + |\alpha_{2^n-1}|^2 = 1;$$

$$\phi \in \{0, 1, \dots, 2^n-1\}, \phi = \phi_1 \cdot 2^{n-1} + \phi_2 \cdot 2^{n-2} + \dots + \phi_n \cdot 2^0, \phi_m \in \{0; 1\}, m = \overline{1, n};$$

$$|\phi\rangle = |\phi_1\phi_2\dots\phi_n\rangle = |\phi_1\rangle |\phi_2\rangle \dots |\phi_n\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \dots \otimes |\phi_n\rangle.$$

Тогда для любой подстановки  $s = \begin{pmatrix} 1 & 2 & \dots & n \\ s(1) & s(2) & \dots & s(n) \end{pmatrix} \in S_n$  через  $|\psi^{(s)}\rangle$

обозначим состояние

$$|\psi^{(s)}\rangle = \sum_{\phi=0}^{2^n-1} \alpha_\phi |\phi_{s(1)}\phi_{s(2)}\dots\phi_{s(n)}\rangle. \quad (1.3.2)$$

квантовой системы  $A_{s(1)} A_{s(2)} \dots A_{s(n)}$ , в которой кубиты рассматриваются в порядке, определяемом перестановкой  $(s(1), s(2), \dots, s(n))$  чисел  $1, 2, \dots, n$ .

**Определение 1.3.3.** Состояние  $|\psi\rangle$   $n$ -кубитной квантовой системы  $A_1A_2\dots A_n$  называется **сепарабельным состоянием**, если найдется подстановка  $s \in S_n$ , такая, что состояние  $|\psi^{(s)}\rangle$  квантовой системы  $A_{s(1)}A_{s(2)} \dots A_{s(n)}$  разлагается в тензорное произведение состояний размерности меньшей, чем  $2^n$ .

Состояние  $|\psi\rangle$   $n$ -кубитной квантовой системы  $A_1A_2\dots A_n$  называется **несепарабельным состоянием**, если оно не является сепарабельным состоянием.

Это определение совпадает в случае двухкубитных квантовых систем с определениями понятий сепарабельное (незапутанное) состояние и несепарабельное (запутанное) состояние, приведенных в работах [71], [77]. Приведем эти определения.

**Определение 1.3.4.** Пусть вектор  $|\psi\rangle \in C^4 = C^2 \otimes C^2$  является состоянием двухкубитной квантовой системы  $AB$ , состоящей из кубитов  $A$  и  $B$ . Состояние  $|\psi\rangle$  называется **сепарабельным состоянием (незапутанным состоянием)** двухкубитной квантовой системы  $AB$ , если существует состояние  $|\psi_1\rangle \in C^2$  кубита  $A$  и состояние  $|\psi_2\rangle \in C^2$  кубита  $B$ , такие, что справедливо равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle.$$

Состояние  $|\psi\rangle \in C^4$  двухкубитной квантовой системы  $AB$  называется **несепарабельным состоянием (запутанным состоянием)**, если оно не является сепарабельным состоянием.

Из данного определения следует, что условие несепарабельности состояния двухкубитной квантовой системы равносильно условию его неразложимости в тензорное произведение состояний однокубитных подсистем рассматриваемой двухкубитной квантовой системы.

**Определение 1.3.5.** Состояниями Белла или ЭПР-состояниями (состояниями Эйнштейна, Подольского, Розена), или ЭПР-парами

называются состояния  $|\psi_{00}\rangle, |\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{11}\rangle \in \mathbf{C}^4$ , где

$$|\psi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}; |\psi_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}; \quad (1.3.6)$$

$$|\psi_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}; |\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

**Утверждение 1.3.7.** Состояния Белла являются несепарабельными состояниями.

Доказательство данного утверждения можно найти, например, в работе [63]. Кроме этого отметим, что справедливость утверждение 1.3.7 вытекает из утверждения 1.3.11, сформулированного далее в настоящем параграфе.

Более сложные несепарабельные состояния могут образовываться как суперпозиции многокубитных состояний. Примером такого несепарабельного состояния служит известное состояние Гринбергера-Хорна-Цайлингера (называемое ГХЦ-состоянием или cat-состоянием) [29], [34], [39], [42], [66], [111], [112]. Это состояние квантовой системы из трех кубитов принадлежит гильбертовому пространству  $\mathbf{C}^8$  и определяется равенством:

$$|\psi_{\text{cat}}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \quad (1.3.8)$$

Другим трехкубитным несепарабельным состоянием является W-состояние [94]

$$|\psi_w\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}. \quad (1.3.9)$$

Существуют и другие многокубитные несепарабельные состояния [29], [30], [63], [94].

Принципиально важным является вопрос о возможности эффективного выявления несепарабельных состояний. Для случая двухкубитных состояний ответ на поставленный вопрос является довольно простым и может быть сформулирован в виде следующего утверждения, представленного, например, в [34].

Введём необходимые для дальнейшего изложения обозначения. В вычислительном базисе из векторов  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$ ,  $|11\rangle$  произвольное двухкубитное состояние  $|\psi\rangle$  можно представить в следующем общем виде:

$$|\psi\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle, \quad (1.3.10)$$

где  $a_0, a_1, a_2, a_3 \in \mathbf{C}$ ,  $|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 1$ .

Теперь сформулируем критерий несепарабельности для двухкубитных состояний.

**Утверждение 1.3.11 (критерий  $K_2$ ).** Двухкубитное состояние  $|\psi\rangle$ , представленное равенством (1.3.10), является несепарабельным состоянием тогда и только тогда, когда выполняется неравенство  $a_0a_3 - a_1a_2 \neq 0$ .

**Доказательство** данного утверждения можно найти, например, в [24]. В данной диссертационной работе для доказательства развиваются новые подходы, представленные в Приложениях, позволяющие получить те же самые соотношения в единообразном ключе.

Для трех и более кубитной квантовой системы условие несепарабельности состояния не равносильно условию неразложимости состояния в тензорное произведение состояний подсистем рассматриваемой квантовой системы. Из несепарабельности состояния трех и более кубитной квантовой системы следует его неразложимость в тензорное произведение состояний меньшей размерности. Однако обратное в общем случае неверно, то есть, из неразложимости состояния трех и более кубитной квантовой системы в тензорное произведение состояний меньшей размерности не следует его несепарабельность.

Приведем критерий неразложимости в тензорное произведение состояний подсистем [24] и критерий несепарабельности [24] для состояния трехкубитной квантовой системы, предварительно определив общий вид состояний трехкубитных квантовых систем в соответствующем вычислительном базисе.

В вычислительном базисе из векторов  $|000\rangle$ ,  $|001\rangle$ ,  $|010\rangle$ ,  $|011\rangle$ ,  $|100\rangle$ ,

$|101\rangle$ ,  $|110\rangle$  и  $|111\rangle$  произвольное состояние  $|\psi\rangle \in \mathbf{C}^8$  трехкубитной квантовой системы можно представить в следующем общем виде:

$$\begin{aligned} |\psi\rangle = & a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + a_4|100\rangle + \\ & + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle, \end{aligned} \quad (1.3.12)$$

где  $\mathbf{C}$  – поле комплексных чисел;  $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbf{C}$ ,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1.$$

Определим наборы величин  $V_0, V_1$  и  $V_2$  через следующие равенства:

$$\begin{aligned} V_0 = \{ & a_0 a_5 - a_1 a_4, a_0 a_6 - a_2 a_4, a_0 a_7 - a_3 a_4, \\ & a_1 a_6 - a_2 a_5, a_1 a_7 - a_3 a_5, a_2 a_7 - a_3 a_6 \}, \end{aligned} \quad (1.3.13)$$

$$\begin{aligned} V_1 = \{ & a_0 a_3 - a_1 a_2, a_0 a_5 - a_1 a_4, a_0 a_7 - a_1 a_6, \\ & a_2 a_5 - a_3 a_4, a_2 a_7 - a_3 a_6, a_4 a_7 - a_5 a_6 \}, \end{aligned} \quad (1.3.14)$$

$$\begin{aligned} V_2 = \{ & a_0 a_3 - a_1 a_2, a_0 a_6 - a_2 a_4, a_0 a_7 - a_2 a_5, \\ & a_1 a_6 - a_3 a_4, a_1 a_7 - a_3 a_5, a_4 a_7 - a_5 a_6 \}. \end{aligned} \quad (1.3.15)$$

Тогда имеет место следующие утверждения [24], в формулировке и доказательстве которых автор принимал активное участие. В приложениях автором развивается иной, отличный от [24], математический аппарат, позволяющий не только по-новому доказывать эти и подобные утверждения, но и дающий более общий взгляд на проблематику в целом.

**Утверждение 1.3.16.** Состояние  $|\psi\rangle$  трехкубитной квантовой системы  $A_1A_2A_3$ , представленное равенством (1.3.12), неразложимо в тензорное произведение состояний размерности меньшей 8 тогда и только тогда, когда для любого  $i \in \{0, 1\}$  в наборе  $V_i$  имеется хотя бы одна величина, неравная нулю.

Утверждение 1.3.16 является очевидным следствием (см. пункт (в) следствия 2.3.5 в [24]) утверждения 2.3.4, сформулированного и доказанного в [24]. Утверждение 2.3.4 из [24] представлено также в виде утверждения В.4 и в приложении В к данной диссертационной работе. В этом же приложении изложено доказательство (отличное от того, что в [24]) утверждения В.4, а утверждение 1.3.16 представлено как следствие В.5, непосредственно

вытекающее из утверждения В.4.

**Утверждение 1.3.17 (критерий  $K_3$ ).** Состояние  $|\psi\rangle$  трехкубитной квантовой системы  $A_1A_2A_3$ , представленное равенством (1.3.12), является несепарабельным состоянием тогда и только тогда, когда для любого  $i \in \{0, 1, 2\}$  в наборе  $V_i$  имеется хотя бы одна величина, неравная нулю.

Утверждения 1.3.17 является непосредственным следствием (пункт (б) следствия 2.5.27 [24]) утверждения 2.5.21 в [24], которое вместе с доказательством (отличным от того, что в [24]) представлено также в виде утверждения Г.7 и в приложении Г к данной диссертационной работе.

Аналогичные утверждения имеют место для состояний  $n$ -кубитной квантовой системы при любом  $n \geq 3$  (например, для  $n=4$  соответствующее утверждение приводится в [24]).

Утверждения 1.3.11 и 1.3.17 иллюстрируют эффективную возможность решения задачи бинарной классификации состояний многокубитных квантовых систем (то есть задачи определения, к какому из двух классов - классу сепарабельных состояний или классу несепарабельных состояний - принадлежит заданное многокубитное состояние). Однако надо отметить, что для решения задачи бинарной классификации состояний квантовой системы из  $n$  кубитов (где  $n$  - натуральное число,  $n > 1$ ) число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, равно  $2^{n-1} - 1$  [24]. Тогда как при решении задачи выяснения неразложимости (или разложимости) состояния квантовой системы в тензорное произведение состояний меньшей размерности число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, равно  $n-1$  [24].

Таким образом, с ростом числа кубитов  $n$ , число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, при решении задачи выяснения неразложимости (или разложимости) состояний  $n$ -кубитных квантовых систем в тензорное произведение состояний меньшей размерности, растет **линейно**. В то же время число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента,

при решении задачи бинарной классификации состояний (сепарабельные или несепарабельные)  $n$ -кубитных квантовых систем, растет экспоненциально с ростом числа кубитов  $n$ .

Поэтому представляют интерес в общем случае (т.е. при условии, что число кубитов  $n$  – произвольное достаточно большое натуральное число) в эффективно проверяемые (на наличие или отсутствие) признаки  $n$ -кубитного состояния, по которым можно определить, несепарабельно это состояние или нет. Некоторые достаточные признаки несепарабельности состояний  $n$ -кубитной квантовой системы могут быть установлены через использование соответствующих этим состояниям булевых масок или нумераторов [24], [59], [60], [61]. Соответствующие результаты будут представлены в главе 2.

## § 1.4. Состояние спиновый синглет

В этом параграфе вводятся основные определения и представляются результаты исследования некоторых свойств состояния «спиновый синглет». Материал параграфа используется далее в описании протокола **АКМ2017**.

Рассмотрим состояние Белла

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (1.4.1)$$

двухкубитной квантовой системы АВ. По историческим причинам это состояние принято называть **спиновым синглетом** [63].

Как следует из утверждения 1.3.7 (или из утверждения 1.3.11), состояние  $|\psi_{11}\rangle$  является несепарабельным состоянием системы из двух кубитов.

Напомним [24], [63], под *измерением компоненты спина вдоль оси v*, где  $v = (v_1, v_2, v_3)$  – единичный вектор (то есть вектор  $v$  является нормированным вектором [63]) в трехмерном пространстве над полем действительных чисел  $\mathbf{R}$ , понимается измерение наблюдаемой

$$v \cdot \sigma = v_1 \sigma_1 + v_2 \sigma_2 + v_3 \sigma_3, \quad (1.4.2)$$

где  $\sigma_1, \sigma_2, \sigma_3$  – вентили Паули;

$$\sigma_1 = \sigma_x = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (1.4.3)$$

и представляет собой квантовый аналог классического логического элемента NOT; действует на однокубитное состояние  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , где  $\alpha, \beta \in \mathbf{C}$ ,  $|\alpha|^2 + |\beta|^2 = 1$  следующим образом

$$\sigma_1 |\psi\rangle = \sigma_x |\psi\rangle = \mathbf{X} |\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |\psi\rangle = \beta |0\rangle + \alpha |1\rangle; \quad (1.4.4)$$

$$\sigma_2 = \sigma_y = \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (1.4.5)$$

и действует на однокубитное состояние  $|\psi\rangle$  следующим образом

$$\sigma_2 |\psi\rangle = \sigma_Y |\psi\rangle = \mathbf{Y}|\psi\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} |\psi\rangle = -\beta i |0\rangle + \alpha i |1\rangle \quad (1.4.6)$$

где  $i \in \mathbf{C}$ ,  $i$  – мнимая единица, то есть  $i^2 = -1$ ;

$$\sigma_3 = \sigma_Z = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (1.4.7)$$

и действует на однокубитное состояние  $|\psi\rangle$  следующим образом

$$\sigma_3 |\psi\rangle = \sigma_Z |\psi\rangle = \mathbf{Z}|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} |\psi\rangle = \alpha |0\rangle - \beta |1\rangle. \quad (1.4.8)$$

Для наблюдаемой  $v \cdot \sigma$  имеют место равенства:

$$v \cdot \sigma = v_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + v_2 \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} + v_3 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} v_3 & v_1 - i v_2 \\ v_1 + i v_2 & -v_3 \end{pmatrix}. \quad (1.4.9)$$

Вычислим характеристический многочлен  $\chi_{v \cdot \sigma}(\lambda)$  полученной матрицы (учитывая, что  $v_1^2 + v_2^2 + v_3^2 = 1$ ):

$$\chi_{v \cdot \sigma}(\lambda) = \begin{vmatrix} \lambda - v_3 & -v_1 + i v_2 \\ -v_1 - i v_2 & \lambda + v_3 \end{vmatrix} = \lambda^2 - 1.$$

Отсюда следует, что возможные значения наблюдаемой  $v \cdot \sigma$  равны

$$\lambda_{1,2} = \pm 1, \quad (1.4.10)$$

независимо от значений координат единичного вектора  $v = (v_1, v_2, v_3)$ .

Таким, образом, при выполнении измерения компоненты спина вдоль оси  $v = (v_1, v_2, v_3)$  для обоих кубитов А и В, то есть измерения наблюдаемой  $v \cdot \sigma$  для каждого из кубитов А и В, получим для каждого из них «1» или «-1». Других значений быть не может, так как выше было показано, что возможные значения наблюдаемой  $v \cdot \sigma$  равны  $\pm 1$  независимо от значений координат единичного вектора  $v$ .

Более того, имеет место важное утверждение, которое играет существенную роль в данной работе при построении квантовых криптографических систем. Перед формулировкой и доказательством этого утверждения проведем необходимые для дальнейшего вычисления.

Выразим через координаты вектора  $v = (v_1, v_2, v_3)$  координаты собственных состояний  $|a\rangle$  и  $|b\rangle$  наблюдаемой  $v \cdot \sigma$ , отвечающих собственным значениям «1» и «-1» соответственно. И, кроме того, выразим векторы  $|0\rangle$  и  $|1\rangle$  через векторы  $|a\rangle$  и  $|b\rangle$ .

Отдельно будем рассматривать три случая в зависимости от значения координаты  $v_3$  вектора  $v$ :  $v_3 = 1$ ,  $v_3 = -1$ ,  $v_3 \notin \{\pm 1\}$ .

Пусть  $v_3 = 1$ . Тогда из равенства

$$v_1^2 + v_2^2 + v_3^2 = 1$$

следует, что  $v_1 = v_2 = 0$ . Отсюда и из равенств (1.4.9) следует, что

$$v \cdot \sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

что, в свою очередь, влечет справедливость равенств

$$|a\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |b\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (1.4.11)$$

Из (1.4.11) следует, что

$$|0\rangle = |a\rangle, |1\rangle = |b\rangle. \quad (1.4.12)$$

Пусть  $v_3 = -1$ . Тогда из равенства

$$v_1^2 + v_2^2 + v_3^2 = 1$$

следует, что  $v_1 = v_2 = 0$ . Отсюда и из равенств (1.4.9) следует, что

$$v \cdot \sigma = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

это, в свою очередь, влечет справедливость равенств

$$|a\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |b\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \quad (1.4.13)$$

Из (1.4.13) следует, что

$$|0\rangle = |b\rangle, |1\rangle = |a\rangle. \quad (1.4.14)$$

Пусть  $v_3 \notin \{\pm 1\}$ . Тогда, с учетом (1.4.9),

из равенств

$$v \cdot \sigma |a\rangle = |a\rangle, v \cdot \sigma |b\rangle = -|b\rangle \quad (1.4.15)$$

получаем:

$$|a\rangle = \left( \frac{\frac{v_1 - iv_2}{\sqrt{(1-v_3)^2 + (v_1^2 + v_2^2)}}}{1 - v_3} \right), \quad (1.4.16)$$

$$|b\rangle = \left( \frac{\frac{-v_1 + iv_2}{\sqrt{(1+v_3)^2 + (v_1^2 + v_2^2)}}}{1 + v_3} \right). \quad (1.4.17)$$

Из (1.4.16) и (1.4.17) следует, что

$$|0\rangle = \frac{(v_1 + iv_2)(1 + v_3)k_a}{2(v_1^2 + v_2^2)}|a\rangle + \frac{(v_1 + iv_2)(-1 + v_3)k_b}{2(v_1^2 + v_2^2)}|b\rangle, \quad |1\rangle = \frac{k_a}{2}|a\rangle + \frac{k_b}{2}|b\rangle, \quad (1.4.18)$$

где

$$k_a = \sqrt{(1 - v_3)^2 + (v_1^2 + v_2^2)} = \sqrt{2 - 2v_3},$$

$$k_b = \sqrt{(1 + v_3)^2 + (v_1^2 + v_2^2)} = \sqrt{2 + 2v_3}, \quad (1.4.19)$$

В свете вышеприведённых определений и обозначений имеет место следующее утверждение.

**Утверждение 1.4.20.** Пусть квантовая система АВ из двух кубитов А и В находится в состоянии  $|\psi_{11}\rangle$ , то есть в состоянии спиновый синглет. Тогда для такой системы справедливы следующие выводы.

а) Для любого единичного вектора  $v = (v_1, v_2, v_3)$  над полем действительных чисел  $\mathbf{R}$  в результате измерения наблюдаемой  $v \cdot \sigma$  для каждого из кубитов А и В (вне зависимости какой из них подвергается измерению первым, а какой – вторым) получается значение результата первого измерения равное «1» или «-1» с вероятностью 0,5; а значение результата второго измерения с вероятностью 1 равно значению результата первого измерения с противоположным знаком.

б) Для любого единичного вектора  $v = (v_1, v_2, v_3)$  над полем действительных чисел  $\mathbf{R}$  в результате измерения наблюдаемой  $v \cdot \sigma$  для кубита А и измерение наблюдаемой  $(-v) \cdot \sigma$  для кубита В (вне зависимости какой из кубитов А или В подвергается измерению первым, а какой вторым) получается

значение результата первого измерения равное «1» или «-1» с вероятностью 0,5; а значение результата второго измерения с вероятностью 1 равно значению результата первого измерения.

в) Для любого единичного вектора  $v = (v_1, v_2, v_3)$  над полем действительных чисел  $\mathbf{R}$  в результате последовательного измерения сперва наблюдаемой  $(0, 0, 1) \cdot \sigma$  для кубита А и затем наблюдаемой  $v \cdot \sigma$  для того же кубита А получается значение результата первого измерения равное «1» или «-1» с вероятностью 0,5; а при  $v_3 \notin \{\pm 1\}$  результат второго измерения имеет следующее значение в зависимости от результата первого измерения:

если результат первого измерения равен «1», то результат второго измерения равен «1» с вероятностью  $P_A(1)$  или равен «-1» с вероятностью  $P_A(-1)$ , где

$$P_A(1) = \frac{k_b^2}{4} = \frac{1+v_3}{2}, P_A(-1) = \frac{k_a^2}{4} = \frac{1-v_3}{2}; \quad (1.4.21)$$

если результат первого измерения равен «-1», то результат второго измерения равен «1» с вероятностью  $P_A(1)$  или равен «-1» с вероятностью  $P_A(-1)$ , где

$$P_A(1) = \frac{k_a^2}{4} = \frac{1-v_3}{2}, P_A(-1) = \frac{k_b^2}{4} = \frac{1+v_3}{2}. \quad (1.4.22)$$

г) Для любого единичного вектора  $v = (v_1, v_2, v_3)$  (где  $v_3 \notin \{\pm 1\}$ ) над полем действительных чисел  $\mathbf{R}$  в результате измерения сперва наблюдаемой  $(0, 0, 1) \cdot \sigma$  для кубита А получается значение результата этого измерения равное «1» или «-1» с вероятностью 0,5; в этом случае последующее измерение наблюдаемой  $v \cdot \sigma$  для того же кубита А дает значение результата второго измерения, не зависящее от значения результата первого измерения и равное «1» или «-1» с вероятностью 0,5 тогда и только тогда, когда  $v_3 = 0$ .

**Доказательство.** а) Пусть  $v_3 = 1$ . В этом случае искомый результат очевидным образом следует из равенств (1.4.12).

Пусть  $v_3 = -1$ . В этом случае искомый результат очевидным образом следует из равенств (1.4.14).

Пусть  $v_3 \notin \{\pm 1\}$ . Тогда из равенств (1.4.18) следует, что

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = k_{ab} \frac{|ab\rangle - |ba\rangle}{\sqrt{2}}, \quad (1.4.23)$$

где

$$\begin{aligned} k_{ab} &= \frac{(v_1 + iv_2)(1 + v_3)k_a}{2(v_1^2 + v_2^2)} \cdot \frac{k_b}{2} - \frac{(v_1 + iv_2)(-1 + v_3)k_b}{2(v_1^2 + v_2^2)} \cdot \frac{k_a}{2} = \\ &= (v_1 + iv_2) \frac{k_a k_b}{2(v_1^2 + v_2^2)}. \end{aligned} \quad (1.4.24)$$

Вычислим модуль  $|k_{ab}|$  величины  $k_{ab}$ . Из определения модуля комплексного числа и равенств (1.4.19) следует, что

$$\begin{aligned} |k_{ab}| &= \sqrt{v_1^2 + v_2^2} \cdot \frac{k_a k_b}{2(v_1^2 + v_2^2)} = \\ &= \sqrt{v_1^2 + v_2^2} \cdot \frac{\sqrt{((1 - v_3)^2 + (v_1^2 + v_2^2))((1 + v_3)^2 + (v_1^2 + v_2^2))}}{2(v_1^2 + v_2^2)} = \\ &= \sqrt{v_1^2 + v_2^2} \cdot \frac{\sqrt{4(v_1^2 + v_2^2)}}{2(v_1^2 + v_2^2)} = 1. \end{aligned} \quad (1.4.25)$$

Из равенств (1.4.23) и (1.4.25) следует, что состояния

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

и

$$\frac{|ab\rangle - |ba\rangle}{\sqrt{2}}$$

совпадают с точностью до ненаблюдаемого при измерении общего множителя  $k_{ab}$ . Таким образом, если выполнено измерение наблюдаемой  $v \cdot \sigma$  для каждого из кубитов А и В (вне зависимости какой из кубитов А или В подвергается измерению первым, а какой – вторым), то результат «1» или «-1», полученный при первом измерении, приводит к результату «-1» (или «1») при втором измерении.

Действительно, допустим, что первым измерению подвергался кубит А и получен результат «1». Тогда после этого измерения квантовая система АВ из двух кубитов А и В окажется в состоянии  $|ab\rangle$ , что предопределяет

значение «-1» результата второго измерения уже над кубитом В наблюдаемой  $v \cdot \sigma$ , у которой состояние  $|b\rangle$  отвечает собственному значению «-1».

Аналогично, если первым измерению подвергался кубит А и получен результат «-1», то после этого измерения квантовая система АВ из двух кубитов А и В окажется в состоянии  $|ba\rangle$ , что предопределяет значение «1» результата второго измерения уже над кубитом В наблюдаемой  $v \cdot \sigma$ , у которой состояние  $|a\rangle$  отвечает собственному значению 1.

б) Из равенств (1.4.16) и (1.4.17) собственных состояний  $|a\rangle$  и  $|b\rangle$  наблюдаемой  $v \cdot \sigma$ , отвечающих собственным значениям «1» и «-1» соответственно, следует, что те же векторы  $|a\rangle$  и  $|b\rangle$  являются собственными состояниями наблюдаемой  $(-v) \cdot \sigma$ , отвечающих тем же собственным значениям, но в другом порядке следования, то есть «-1» и «1» соответственно,

Тогда, если при измерении наблюдаемой  $v \cdot \sigma$  для кубита А получен результат, равный 1, то после измерения квантовая система АВ из двух кубитов А и В окажется в состоянии  $|ab\rangle$ , что предопределяет значение 1 результата второго измерения наблюдаемой  $(-v) \cdot \sigma$ , у которой, как было показано выше, состояние  $|b\rangle$  отвечает собственному значению 1.

Аналогично, если при измерении наблюдаемой  $v \cdot \sigma$  для кубита А получен результат, равный «-1», то после измерения квантовая система АВ из двух кубитов А и В окажется в состоянии  $|ba\rangle$ , что предопределяет значение «-1» результата второго измерения наблюдаемой  $(-v) \cdot \sigma$ , у которой, как было показано выше, состояние  $|a\rangle$  отвечает собственному значению «-1».

в) Из равенств (1.4.12) следует, что первое измерения наблюдаемой  $(0, 0, 1) \cdot \sigma$  сперва для кубита А дает значение результата измерения равное 1 или «-1» с вероятностью 0,5.

если результат первого измерения над кубитом А равен 1, то после

измерения квантовая система АВ из двух кубитов А и В окажется в состоянии  $|01\rangle = |0\rangle \otimes |1\rangle$ , то есть кубит А окажется в состоянии  $|0\rangle$ , а кубит В – в состоянии  $|1\rangle$ . Для состояния  $|0\rangle$  кубита А из условия  $v_3 \notin \{\pm 1\}$  и (1.4.18) следует справедливость равенства

$$|0\rangle = \frac{(v_1 + iv_2)(1 + v_3)k_a}{2(v_1^2 + v_2^2)} |a\rangle + \frac{(v_1 + iv_2)(-1 + v_3)k_b}{2(v_1^2 + v_2^2)} |b\rangle.$$

Так как измерение наблюдаемой  $v \cdot \sigma$  для кубита А в состоянии  $|0\rangle$  означает проекционное измерение в базисе из векторов  $|a\rangle$  и  $|b\rangle$ , то результат этого измерения равен 1 с вероятностью

$$P_A(1) = \frac{(1 + v_3)^2 k_a^2}{4(v_1^2 + v_2^2)},$$

или «-1» с вероятностью

$$P_A(-1) = \frac{(-1 + v_3)^2 k_b^2}{4(v_1^2 + v_2^2)}.$$

Подставив в правые части данных равенств вместо  $k_a$  и  $k_b$  их значения в соответствии с (1.4.19) и воспользовавшись затем равенством

$$v_1^2 + v_2^2 + v_3^2 = 1,$$

получаем:

$$\begin{aligned} P_A(1) &= \frac{(1 + v_3)^2 ((1 - v_3)^2 + (v_1^2 + v_2^2))}{4(v_1^2 + v_2^2)} = \frac{(1 - v_3)^2 + (1 + v_3)^2 (v_1^2 + v_2^2)}{4(v_1^2 + v_2^2)} = \\ &= \frac{(v_1^2 + v_2^2)^2 + (1 + v_3)^2 (v_1^2 + v_2^2)}{4(v_1^2 + v_2^2)} = \frac{(v_1^2 + v_2^2) + (1 + v_3)^2}{4} = \frac{1 + v_3}{2}, \end{aligned}$$

$$\begin{aligned} P_A(-1) &= \frac{(-1 + v_3)^2 ((1 + v_3)^2 + (v_1^2 + v_2^2))}{4(v_1^2 + v_2^2)} = \frac{(-1 + v_3)^2 + (-1 + v_3)^2 (v_1^2 + v_2^2)}{4(v_1^2 + v_2^2)} = \\ &= \frac{(v_1^2 + v_2^2)^2 + (-1 + v_3)^2 (v_1^2 + v_2^2)}{4(v_1^2 + v_2^2)} = \frac{(v_1^2 + v_2^2) + (1 - v_3)^2}{4} = \frac{1 - v_3}{2}. \end{aligned}$$

Аналогично, если результат первого измерения равен «-1», то после измерения квантовая система АВ из двух кубитов А и В окажется в состоянии  $|10\rangle = |1\rangle \otimes |0\rangle$ , то есть кубит А окажется в состоянии  $|1\rangle$ , а кубит В – в состоянии  $|0\rangle$ . Для состояния  $|1\rangle$  кубита А из условия  $v_3 \notin \{\pm 1\}$  и (1.4.18) следует справедливость равенства

$$|1\rangle = \frac{k_a}{2}|a\rangle + \frac{k_b}{2}|b\rangle.$$

Так как измерение наблюдаемой  $v \cdot \sigma$  для кубита  $A$  в состоянии  $|1\rangle$  означает проекционное измерение в базисе из векторов  $|a\rangle$  и  $|b\rangle$ , то результат этого измерения равен 1 с вероятностью

$$P_A(1) = \frac{k_a^2}{4} = \frac{1-v_3}{2},$$

или (-1) с вероятностью

$$P_A(-1) = \frac{1+v_3}{2}.$$

Пункт в) утверждения 1.4.20 доказан.

г) первая часть данного пункта касающаяся первого измерения над кубитом  $A$  совпадает с первой частью пункта в). Пусть в результате этого измерения получено значение 1. Тогда из пункта в) данного утверждения следует, что при последующем измерении наблюдаемой  $v \cdot \sigma$  для кубита  $A$  результат равен 1 или (-1) соответственно с вероятностями

$$P_A(1) = \frac{1+v_3}{2}, P_A(-1) = \frac{1-v_3}{2}.$$

В этом случае путем проведения соответствующих вычислений убеждаемся в том, что система равенств

$$\begin{cases} P_A(1) = 0,5 \\ P_A(-1) = 0,5 \end{cases}$$

выполняется тогда и только тогда, когда  $v_3 = 0$ .

Аналогично, пусть в результате первого измерения получено значение «-1». Тогда из пункта в) данного утверждения следует, что при последующем измерении наблюдаемой  $v \cdot \sigma$  для кубита  $A$  результат равен «1» или «-1» соответственно с вероятностями

$$P_A(1) = \frac{1-v_3}{2}, P_A(-1) = \frac{1+v_3}{2}.$$

В этом случае непосредственной проверкой убеждаемся, что система равенств

$$\begin{cases} P_A(1) = 0,5 \\ P_A(-1) = 0,5 \end{cases}$$

выполняется тогда и только тогда, когда  $v_3 = 0$ .

Утверждение 1.4.20 доказано.

Утверждение 1.4.20 служит математической основой квантовой криптографической системы **АКМ2017**, представленной далее в главе 3. В **АКМ2017** вектор, вдоль которого производится измерение компонента спина, служит тем, что в криптографии принято называть синхропосылкой, а результат измерения используется при выработке бита ключа.

В следующем параграфе будет показано, что выводы Утверждения 1.4.20 справедливы для более широкого класса квантовых систем, которые возникают в процессе дистанционной регенерации кубитов к спиновому синглету.

### §1.5. Состояния квантовых систем, близкие по своим свойствам к состоянию спиновый синглет

В процессе выполнения шагов протокола дистанционной регенерации кубитов к спиновому синглету (Глава 3) возникают квантовые состояния, отличающиеся от спинового синглета. В данном параграфе автором формулируются и доказываются теоремы, необходимые для строгого обоснования безопасности протокола **АКМ2017**, который является целевым в контексте настоящей диссертации и подробно описан далее.

Утверждение 1.4.20 из предыдущего параграфа справедливо для более широкого класса состояний многокубитных квантовых систем. А именно, имеет место следующая теорема.

**Теорема 1.5.1.** Пусть квантовая система  $AA_1A_2 \dots A_mB$  из  $m+2$  (где  $m \in \mathbb{N}$ ) кубитов  $A, A_1, A_2, \dots, A_m$  и  $B$  находится в состоянии

$$\frac{|0t_{12\dots m}1\rangle - |1t_{12\dots m}0\rangle}{\sqrt{2}} = \frac{|0\rangle|t_{12\dots m}\rangle|1\rangle - |1\rangle|t_{12\dots m}\rangle|0\rangle}{\sqrt{2}}, \quad (1.5.2)$$

где  $|t_{12\dots m}\rangle$  – произвольное состояние квантовой системы  $A_1A_2 \dots A_m$  из  $m$  кубитов  $A, A_1, A_2, \dots, A_m$ .

Тогда для квантовой системы  $AA_1A_2 \dots A_mB$  справедливы выводы а), б), в) и г) утверждения 1.4.20.

**Доказательство.** Из равенств (1.4.18), (1.4.24) и (1.4.25) следует, что имеют место равенства

$$|0\rangle = \alpha|a\rangle + \beta|b\rangle, \quad (1.5.3)$$

$$|1\rangle = \gamma|a\rangle + \delta|b\rangle, \quad (1.5.4)$$

$$k_{ab} = \alpha\delta - \beta\gamma \quad (1.5.5)$$

и

$$|k_{ab}| = 1, \quad (1.5.6)$$

где

$$\alpha = \frac{(v_1 + iv_2)(1 + v_3)k_a}{2(v_1^2 + v_2^2)},$$

$$\beta = \frac{(v_1 + iv_2)(-1 + v_3)k_b}{2(v_1^2 + v_2^2)},$$

$$\gamma = \frac{k_a}{2},$$

$$\delta = \frac{k_b}{2}.$$

Подставив в правую часть равенства (1.5.2) вместо  $|0\rangle$  и  $|1\rangle$  правые части равенств (1.5.3) и (1.5.4) соответственно, и используя равенство (1.5.5), получаем

$$\begin{aligned} & \frac{|0t_{12\dots m}1\rangle - |1t_{12\dots m}0\rangle}{\sqrt{2}} = \\ & = \\ & \frac{(\alpha|a\rangle + \beta|b\rangle)|t_{12\dots m}\rangle(\gamma|a\rangle + \delta|b\rangle) - (\gamma|a\rangle + \delta|b\rangle)|t_{12\dots m}\rangle(\alpha|a\rangle + \beta|b\rangle)}{\sqrt{2}} = \\ & = \frac{1}{\sqrt{2}}(\alpha\gamma|a\rangle|t_{12\dots m}\rangle|a\rangle + \alpha\delta|a\rangle|t_{12\dots m}\rangle|b\rangle + \beta\gamma|b\rangle|t_{12\dots m}\rangle|a\rangle + \beta\delta|b\rangle|t_{12\dots m}\rangle|b\rangle - \\ & - \gamma\alpha|a\rangle|t_{12\dots m}\rangle|a\rangle - \gamma\beta|a\rangle|t_{12\dots m}\rangle|b\rangle - \delta\alpha|b\rangle|t_{12\dots m}\rangle|a\rangle - \delta\beta|b\rangle|t_{12\dots m}\rangle|b\rangle) = \\ & = \frac{1}{\sqrt{2}}(\alpha\delta - \beta\gamma)(|a\rangle|t_{12\dots m}\rangle|b\rangle - |b\rangle|t_{12\dots m}\rangle|a\rangle) = \\ & = k_{ab} \left( \frac{|at_{12\dots m}b\rangle - |bt_{12\dots m}a\rangle}{\sqrt{2}} \right). \end{aligned} \tag{1.5.7}$$

Из равенств (1.5.6) и (1.5.7) следует, что состояния

$$\frac{|0t_{12\dots m}1\rangle - |1t_{12\dots m}0\rangle}{\sqrt{2}}$$

и

$$\frac{|at_{12\dots m}b\rangle - |bt_{12\dots m}a\rangle}{\sqrt{2}}$$

совпадают с точностью до ненаблюдаемого при измерении общего множителя  $k_{ab}$ . Дальнейший ход доказательства теоремы 1.5.1 аналогичен

доказательству утверждения 1.4.20.

Теперь обратим внимание на следующее. В работе [24] приведен пример 2.4.3 сепарабельного состояния квантовой системы ABC из трех кубитов A, B и C, которое не разлагается в тензорное произведение состояний меньшей размерности. Несмотря на то, что это состояние не относится к состояниям, указанным в названии данного параграфа, пример 2.4.3 носит принципиальный характер и обращение внимания к нему в данном параграфе (под номером 1.5.8) представляется весьма полезным в свете облегчения и улучшения понимания последующих результатов, излагаемых в данном параграфе.

**Пример 1.5.8.** Рассмотрим следующее состояние квантовой системы ABC:

$$|\psi\rangle = \frac{|000\rangle + |101\rangle}{\sqrt{2}}.$$

Данное состояние не является несепарабельным состоянием. Это следует из критерия  $\mathbf{K}_3$ , (см. утверждение 1.3.17) и не представимо в виде тензорного произведения состояний меньшей размерности (см. утверждение 1.3.16).

Покажем, что с точностью до общих фазовых множителей, по модулю равных единице, для состояний квантовых подсистем AC и B справедливы соответственно равенства:

$$|\psi_{13}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

и

$$|\psi_2\rangle = |0\rangle.$$

Если будет проведено проективное измерение в базисе  $\{|0\rangle, |1\rangle\}$  над кубитом A квантовой системы ABC, то после проведения измерения квантовая

система ABC окажется в состоянии  $|000\rangle$  с вероятностью  $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$  (будем

считать это первым случаем для удобства последующих ссылок в рамках данного примера) или в состоянии  $|101\rangle$  с той же вероятностью  $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$  (это – второй случай).

Тогда кубиты А, В и С окажутся с точностью до общих фазовых множителей, по модулю равных 1, в первом случае - в состояниях  $|0\rangle$ ,  $|0\rangle$  и  $|0\rangle$ , а во втором случае - соответственно в состояниях  $|1\rangle$ ,  $|0\rangle$  и  $|1\rangle$ .

Полное множество ортогональных проекторов обсуждаемого измерения над кубитом А состоит из проекторов  $M_0$  и  $M_1$ , где

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

С другой стороны, обсуждаемое измерение над кубитом А является измерением над всей квантовой системой АВС с матрицами  $\tilde{M}_0$  и  $\tilde{M}_1$ , где

$$\tilde{M}_0 = M_0 \otimes I_2 \otimes I_2,$$

$$\tilde{M}_1 = M_1 \otimes I_2 \otimes I_2,$$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Это же измерение является также измерением над квантовой системой АСВ с теми же матрицами  $\tilde{M}_0$  и  $\tilde{M}_1$ . При этом, учитывая указанные выше состояния кубитов А, В, С (а именно  $|0\rangle$ ,  $|0\rangle$ ,  $|0\rangle$  или  $|1\rangle$ ,  $|0\rangle$ ,  $|1\rangle$ ), получаем, что после измерения квантовая система АСВ окажется в состоянии  $|000\rangle$  с вероятностью  $\frac{1}{2}$  или в состоянии  $|110\rangle$  с той же вероятностью  $\frac{1}{2}$ . Отсюда следует (с учетом того, что состояние квантовой системы АСВ является чистым состоянием), что до измерения квантовая система АСВ находится в состоянии

$$|\varphi\rangle = \alpha|000\rangle + \beta|110\rangle, \quad (1.5.9)$$

$$\text{где } \alpha \in \mathbb{C}, \beta \in \mathbb{C}, |\alpha|^2 = \frac{1}{2}, |\beta|^2 = \frac{1}{2}.$$

Покажем, что  $\alpha = \beta$ . Для этого положим

$$|a\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |b\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Тогда, учитывая, что

$$|0\rangle = \frac{|a\rangle + |b\rangle}{\sqrt{2}}, |1\rangle = \frac{|a\rangle - |b\rangle}{\sqrt{2}},$$

для состояния  $|\psi\rangle$  квантовой системы ABC имеем

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}} \left( \left( \frac{|a\rangle + |b\rangle}{\sqrt{2}} \right) |0\rangle \left( \frac{|a\rangle + |b\rangle}{\sqrt{2}} \right) + \left( \frac{|a\rangle - |b\rangle}{\sqrt{2}} \right) |0\rangle \left( \frac{|a\rangle - |b\rangle}{\sqrt{2}} \right) \right) = \\ &= \frac{1}{2\sqrt{2}} (|a0a\rangle + |a0b\rangle + |b0a\rangle + |b0b\rangle + |a0a\rangle - |a0b\rangle - |b0a\rangle + |b0b\rangle) = \\ &= \frac{1}{2\sqrt{2}} (2|a0a\rangle + 2|b0b\rangle) = \frac{|a0a\rangle + |b0b\rangle}{\sqrt{2}}. \end{aligned}$$

Далее, если будет проведено проективное измерение в базисе  $\{|a\rangle, |b\rangle\}$  над кубитом А квантовой системы ABC, то после проведения измерения квантовая система ABC окажется в состоянии  $|a0a\rangle$  с вероятностью  $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$  (это будем считать третьим случаем) или в состоянии  $|b0b\rangle$  с той же вероятностью  $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$  (это будем считать четвертым случаем). Тогда кубиты А, В и С окажутся с точностью до общих фазовых множителей, по модулю равных 1, в третьем случае – соответственно в состояниях  $|a\rangle, |0\rangle$  и  $|a\rangle$ , а в четвертом случае - соответственно в состояниях  $|b\rangle, |0\rangle$  и  $|b\rangle$ .

Полное множество ортогональных проекторов обсуждаемого измерения над кубитом А состоит из проекторов  $N_0$  и  $N_1$ , где

$$N_0 = |a\rangle\langle a|, N_1 = |b\rangle\langle b|.$$

С другой стороны, как и обсуждаемое ранее измерение над кубитом А является измерением над всей квантовой системой АВС с матрицами  $\tilde{N}_0$  и  $\tilde{N}_1$ , где

$$\tilde{N}_0 = N_0 \otimes I_2 \otimes I_2,$$

$$\tilde{N}_1 = N_1 \otimes I_2 \otimes I_2.$$

Это измерение является также измерением над квантовой системой АСВ в состоянии  $|\varphi\rangle$  (см. 1.5.9) с теми же матрицами  $\tilde{N}_0$  и  $\tilde{N}_1$ . При этом, учитывая указанные выше состояния кубитов А, В, С (а именно  $|a\rangle$ ,  $|0\rangle$ ,  $|a\rangle$  или  $|b\rangle$ ,  $|0\rangle$ ,  $|b\rangle$ ), получаем, что после измерения квантовая система АСВ окажется в состоянии  $|aa0\rangle$  с вероятностью  $\frac{1}{2}$  или в состоянии  $|bb0\rangle$  с той же вероятностью  $\frac{1}{2}$ . При этом переписав состояние  $|\varphi\rangle$  (см. 1.5.9) квантовой системы АСВ с учетом равенств

$$|0\rangle = \frac{|a\rangle + |b\rangle}{\sqrt{2}}, |1\rangle = \frac{|a\rangle - |b\rangle}{\sqrt{2}},$$

получаем

$$\begin{aligned} |\varphi\rangle &= \alpha|000\rangle + \beta|110\rangle = \\ &= \alpha \left( \left( \frac{|a\rangle + |b\rangle}{\sqrt{2}} \right) \left( \frac{|a\rangle + |b\rangle}{\sqrt{2}} \right) |0\rangle \right) + \beta \left( \left( \frac{|a\rangle - |b\rangle}{\sqrt{2}} \right) \left( \frac{|a\rangle - |b\rangle}{\sqrt{2}} \right) |0\rangle \right) = \\ &= \left( \frac{\alpha + \beta}{2} \right) |aa0\rangle + \left( \frac{\alpha - \beta}{2} \right) |ab0\rangle + \left( \frac{\alpha - \beta}{2} \right) |ba0\rangle + \left( \frac{\alpha + \beta}{2} \right) |bb0\rangle. \end{aligned}$$

Отсюда получаем:

$$\left| \frac{\alpha + \beta}{2} \right|^2 = \frac{1}{2}, \quad \left| \frac{\alpha - \beta}{2} \right|^2 = 0.$$

Из последнего равенства следует, что  $\alpha = \beta$ . Отсюда и из предпоследнего равенства вытекает, что существует число  $\theta \in \mathbf{R}$  такое, что

$$\alpha = \beta = \frac{1}{\sqrt{2}} e^{i\theta} = \frac{1}{\sqrt{2}} (\cos\theta + i \sin\theta),$$

где  $i = \sqrt{-1}$ . Тогда из (1.5.9) следует, что для состояния  $|\varphi\rangle$  квантовой системы АСВ справедлива цепочка равенств

$$\begin{aligned} |\varphi\rangle &= \alpha|000\rangle + \beta|110\rangle = \frac{1}{\sqrt{2}} e^{i\theta} |000\rangle + \frac{1}{\sqrt{2}} e^{i\theta} |110\rangle = \\ &= e^{i\theta} \left( \frac{|000\rangle + |110\rangle}{\sqrt{2}} \right), \end{aligned}$$

Последняя цепочка равенств означает, что квантовая система АСВ с точностью до общего фазового множителя, по модулю равного единице находится в состоянии

$$\left( \frac{|000\rangle + |110\rangle}{\sqrt{2}} \right) = \left( \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) |0\rangle.$$

Из последнего равенства следует, что с точностью до фазовых множителей, по модулю равных единице, квантовые подсистемы АС и В находятся соответственно в состояниях

$$|\psi_{13}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

и

$$|\psi_2\rangle = |0\rangle.$$

Рассуждения, аналогичные тем, которые были использованы в примере 1.5.8, можно применить и в случае состояния

$$|\psi\rangle = \frac{|0t_{12\dots m}1\rangle - |1t_{12\dots m}0\rangle}{\sqrt{2}} \quad (1.5.10)$$

квантовой системы  $AA_1A_2 \dots A_mB$ , состоящей из  $m+2$  кубитов  $A, A_1, A_2, \dots, A_m, B$ , где  $m \in \mathbf{N}$ ,  $|t_{12\dots m}\rangle$  - некоторое состояние квантовой подсистемы  $A_1A_2 \dots A_m$ . В этом случае можно показать, что подсистемы  $AB$  и  $A_1A_2 \dots A_m$  с точностью до общих фазовых множителей, по модулю равных единице, находятся соответственно в состояниях

$$|\psi_{AB}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (1.5.11)$$

и

$$|t_{12\dots m}\rangle.$$

Далее сформулируем и представим доказательство теоремы, непосредственным следствием которой являются указанные выше описания состояний квантовых подсистем  $AB$  и  $A_1A_2 \dots A_m$ .

**Теорема 1.5.12.** Пусть квантовая система  $AA_1A_2 \dots A_mB$ , состоящая из  $m+2$  кубитов  $A, A_1, A_2, \dots, A_m, B$  находится в состоянии  $|\psi\rangle$ , заданном равенством (1.5.10). Тогда с точностью до общего фазового множителя, по модулю равного единице, состояние  $|\varphi\rangle$  квантовой системы  $ABA_1A_2 \dots A_m$  определяется равенством

$$|\varphi\rangle = \frac{|01t_{12\dots m}\rangle - |10t_{12\dots m}\rangle}{\sqrt{2}}. \quad (1.5.13)$$

**Доказательство.** Если будет проведено проективное измерение в базисе  $\{|0\rangle, |1\rangle\}$  над кубитом  $A$  квантовой системы  $AA_1A_2 \dots A_mB$ , то после проведения измерения квантовая система  $AA_1A_2 \dots A_mB$  окажется в состоянии

$|0t_{12\dots m}1\rangle$  с вероятностью  $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$  (это будем считать первым случаем

для удобства последующих ссылок в рамках данного доказательства) или в

состоянии  $|1t_{12\dots m}0\rangle$  с той же вероятностью  $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$  (это – второй случай).

Тогда кубит  $A$ , квантовая подсистема  $A_1A_2 \dots A_m$  и кубит  $B$  окажутся с точностью до общих фазовых множителей, по модулю равных 1, в первом случае - в состояниях  $|0\rangle$ ,  $|t_{12\dots m}\rangle$  и  $|1\rangle$ , а во втором случае - соответственно в состояниях  $|1\rangle$ ,  $|t_{12\dots m}\rangle$  и  $|0\rangle$ .

Полное множество ортогональных проекторов обсуждаемого измерения над кубитом  $A$  состоит из проекторов  $M_0$  и  $M_1$ , где

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

С другой стороны, обсуждаемое измерение над кубитом  $A$  является измерением над всей квантовой системой  $AA_1A_2 \dots A_mB$  с матрицами  $\tilde{M}_0$  и  $\tilde{M}_1$ , где

$$\tilde{M}_0 = M_0 \otimes \underbrace{I_2 \otimes I_2 \otimes \dots \otimes I_2}_{m+1 \text{ раз}},$$

$$\tilde{M}_1 = M_1 \otimes \underbrace{I_2 \otimes I_2 \otimes \dots \otimes I_2}_{m+1 \text{ раз}}.$$

Это же измерение является также измерением над квантовой системой  $ABA_1A_2 \dots A_m$  с теми же матрицами  $\tilde{M}_0$  и  $\tilde{M}_1$ . При этом, учитывая выше указанные состояния квантовых подсистем  $A$ ,  $A_1A_2 \dots A_m$ ,  $B$ , (а именно  $|0\rangle$ ,  $|t_{12\dots m}\rangle$ ,  $|1\rangle$  или  $|1\rangle$ ,  $|t_{12\dots m}\rangle$ ,  $|0\rangle$ ), получаем, что после измерения квантовая система  $ABA_1A_2 \dots A_m$  окажется в состоянии  $|01t_{12\dots m}\rangle$  с вероятностью  $\frac{1}{2}$  или в состоянии  $|10t_{12\dots m}\rangle$  с той же вероятностью  $\frac{1}{2}$ . Отсюда следует (с учетом того, что состояние квантовой системы  $ABA_1A_2 \dots A_m$  является чистым состоянием), что до измерения квантовая система  $ABA_1A_2 \dots A_m$  находится в состоянии

$$|\varphi\rangle = \alpha|01t_{12\dots m}\rangle + \beta|10t_{12\dots m}\rangle, \quad (1.5.14)$$

$$\text{где } \alpha \in \mathbb{C}, \beta \in \mathbb{C}, |\alpha|^2 = \frac{1}{2}, |\beta|^2 = \frac{1}{2}.$$

Покажем, что  $\alpha = -\beta$ . Для этого положим

$$|a\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |b\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Тогда, учитывая, что

$$|0\rangle = \frac{|a\rangle + |b\rangle}{\sqrt{2}}, \quad |1\rangle = \frac{|a\rangle - |b\rangle}{\sqrt{2}},$$

для состояния  $|\psi\rangle$  квантовой системы  $AA_1A_2 \dots A_mB$  имеем

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}} \\ &\left( \left( \frac{|a\rangle + |b\rangle}{\sqrt{2}} \right) |t_{12\dots m}\rangle \left( \frac{|a\rangle - |b\rangle}{\sqrt{2}} \right) - \left( \frac{|a\rangle - |b\rangle}{\sqrt{2}} \right) |t_{12\dots m}\rangle \left( \frac{|a\rangle + |b\rangle}{\sqrt{2}} \right) \right) = \\ &= \frac{1}{2\sqrt{2}} (|at_{12\dots m}a\rangle - |at_{12\dots m}b\rangle + |bt_{12\dots m}a\rangle - |bt_{12\dots m}b\rangle - \\ &- |at_{12\dots m}a\rangle - |at_{12\dots m}b\rangle + |bt_{12\dots m}a\rangle + |bt_{12\dots m}b\rangle) = \\ &= \frac{1}{2\sqrt{2}} (-2|at_{12\dots m}b\rangle + 2|bt_{12\dots m}a\rangle) = \\ &= \frac{-|at_{12\dots m}b\rangle + |bt_{12\dots m}a\rangle}{\sqrt{2}}. \end{aligned}$$

Далее, если будет проведено проективное измерение в базисе  $\{|a\rangle, |b\rangle\}$  над кубитом  $A$  квантовой системы  $AA_1A_2 \dots A_mB$ , то после проведения измерения квантовая система  $AA_1A_2 \dots A_mB$  окажется в состоянии  $|at_{12\dots m}b\rangle$  с

вероятностью  $\left(-\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$  (это будем считать третьим случаем) или в

состоянии  $|\mathbf{b}t_{12\dots m}\mathbf{a}\rangle$  с той же вероятностью  $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$  (это будем считать четвертым случаем). Тогда квантовые подсистемы  $A, A_1A_2 \dots A_m$  и  $B$  окажутся с точностью до общих фазовых множителей, по модулю равных 1, в третьем случае – соответственно в состояниях  $|\mathbf{a}\rangle, |t_{12\dots m}\rangle$  и  $|\mathbf{b}\rangle$ , а в четвертом случае – соответственно в состояниях  $|\mathbf{b}\rangle, |t_{12\dots m}\rangle$  и  $|\mathbf{a}\rangle$ .

Полное множество ортогональных проекторов обсуждаемого измерения над кубитом  $A$  состоит из проекторов  $N_0$  и  $N_1$ , где

$$N_0 = |\mathbf{a}\rangle\langle\mathbf{a}|, N_1 = |\mathbf{b}\rangle\langle\mathbf{b}|.$$

С другой стороны, как и выше обсуждаемое измерение над кубитом  $A$  является измерением над всей квантовой системой  $AA_1A_2 \dots A_mB$  с матрицами  $\tilde{N}_0$  и  $\tilde{N}_1$ , где

$$\tilde{N}_0 = N_0 \otimes \underbrace{I_2 \otimes I_2 \otimes \dots \otimes I_2}_{m+1 \text{ раз}},$$

$$\tilde{N}_1 = N_1 \otimes \underbrace{I_2 \otimes I_2 \otimes \dots \otimes I_2}_{m+1 \text{ раз}}.$$

Это же измерение является также измерением над квантовой системой  $ABA_1A_2 \dots A_m$  в состоянии  $|\varphi\rangle$  (см. 1.5.14) с теми же матрицами  $\tilde{N}_0$  и  $\tilde{N}_1$ .

При этом, учитывая выше указанные состояния квантовых подсистемы  $A, A_1A_2 \dots A_m, B$  (а именно -  $|\mathbf{a}\rangle, |t_{12\dots m}\rangle, |\mathbf{b}\rangle$  или  $|\mathbf{b}\rangle, |t_{12\dots m}\rangle, |\mathbf{a}\rangle$ ), получаем, что после измерения квантовая система  $ABA_1A_2 \dots A_m$  окажется в состоянии

$|\mathbf{a}b t_{12\dots m}\rangle$  с вероятностью  $\frac{1}{2}$  или в состоянии  $|\mathbf{b}a t_{12\dots m}\rangle$  с той же вероятностью

$\frac{1}{2}$ . При этом переписав состояние  $|\varphi\rangle$  квантовой системы  $ABA_1A_2 \dots A_m$  с

учетом равенств

$$|0\rangle = \frac{|a\rangle + |b\rangle}{\sqrt{2}}, \quad |1\rangle = \frac{|a\rangle - |b\rangle}{\sqrt{2}},$$

получаем

$$\begin{aligned} |\varphi\rangle &= \alpha|01t_{12\dots m}\rangle + \beta|10t_{12\dots m}\rangle = \\ &= \alpha\left(\left(\frac{|a\rangle + |b\rangle}{\sqrt{2}}\right)\left(\frac{|a\rangle - |b\rangle}{\sqrt{2}}\right)|t_{12\dots m}\rangle\right) + \beta\left(\left(\frac{|a\rangle - |b\rangle}{\sqrt{2}}\right)\left(\frac{|a\rangle + |b\rangle}{\sqrt{2}}\right)|t_{12\dots m}\rangle\right) \\ &= \left(\frac{\alpha + \beta}{2}\right)|aat_{12\dots m}\rangle + \left(\frac{-\alpha + \beta}{2}\right)|abt_{12\dots m}\rangle + \left(\frac{\alpha - \beta}{2}\right)|bat_{12\dots m}\rangle - \left(\frac{\alpha + \beta}{2}\right)|bbt_{12\dots m}\rangle \end{aligned}$$

Отсюда и из непосредственно предыдущего получаем:

$$\left|\frac{\alpha - \beta}{2}\right|^2 = \frac{1}{2}, \quad \left|\frac{\alpha + \beta}{2}\right|^2 = 0.$$

Из последнего равенства следует, что  $\alpha = -\beta$ . Отсюда и из предпоследнего равенства следует, что существует число  $\theta \in \mathbf{R}$  такое, что

$$\alpha = \frac{1}{\sqrt{2}} e^{i\theta} = \frac{1}{\sqrt{2}} (\cos\theta + i \cdot \sin\theta),$$

$$\beta = -\alpha = e^{i\pi} \alpha = \frac{1}{\sqrt{2}} e^{i(\theta + \pi)} = \frac{1}{\sqrt{2}} (\cos(\theta + \pi) + i \cdot \sin(\theta + \pi))?$$

где  $i = \sqrt{-1}$ . Тогда из (1.5.14) следует, что для состояния  $|\varphi\rangle$

квантовой системы  $ABA_1A_2 \dots A_m$  справедлива цепочка равенств

$$\begin{aligned} |\varphi\rangle &= \alpha|01t_{12\dots m}\rangle + \beta|10t_{12\dots m}\rangle = \frac{1}{\sqrt{2}} e^{i\theta} |01t_{12\dots m}\rangle + \frac{1}{\sqrt{2}} e^{i(\theta + \pi)} |10t_{12\dots m}\rangle \\ &= e^{i\theta} \left( \frac{|01t_{12\dots m}\rangle + e^{i\pi} |10t_{12\dots m}\rangle}{\sqrt{2}} \right) = e^{i\theta} \left( \frac{|01t_{12\dots m}\rangle - |10t_{12\dots m}\rangle}{\sqrt{2}} \right), \end{aligned}$$

что означает, что квантовая система  $ABA_1A_2 \dots A_m$  с точностью до общего фазового множителя, по модулю равного единице находится в состоянии

$$\left( \frac{|01t_{12\dots m}\rangle - |10t_{12\dots m}\rangle}{\sqrt{2}} \right)$$

Теорема доказана.

**Утверждение 1.5.15.** Пусть квантовая система  $AA_1A_2 \dots A_mB$ , состоящая из  $m+2$  кубитов  $A, A_1, A_2, \dots, A_m, B$  находится в состоянии  $|\psi\rangle$ , заданном равенством (1.5.10). Тогда подсистемы  $AB$  и  $A_1A_2 \dots A_m$  квантовой системы  $AA_1A_2 \dots A_mB$  с точностью до общих фазовых множителей, по модулю равных единице, находятся соответственно в состояниях

$$|\psi_{AB}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad \text{и} \quad |t_{12\dots m}\rangle.$$

**Доказательство.** Пусть квантовая система  $AA_1A_2 \dots A_mB$ , состоящая из  $m+2$  кубитов  $A, A_1, A_2, \dots, A_m, B$  находится в состоянии  $|\psi\rangle$ , заданном равенством (1.5.10). Тогда из теоремы 1.5.12 следует, что квантовая система  $ABA_1A_2 \dots A_m$  с точностью до общего фазового множителя, по модулю равного единице находится в состоянии

$$\left( \frac{|01t_{12\dots m}\rangle - |10t_{12\dots m}\rangle}{\sqrt{2}} \right).$$

Отсюда и из равенства

$$\left( \frac{|01t_{12\dots m}\rangle - |10t_{12\dots m}\rangle}{\sqrt{2}} \right) = \left( \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right) |t_{12\dots m}\rangle$$

вытекает справедливость следствия 1.5.15.

Теорема 1.5.12 служит математической основой алгоритма дистанционной регенерации состояний носителей-кубитов для формирования ключевой информации криптографической системы **АКМ2017**, представленной далее в главе 3.

По результатам исследований, представленных в главе 1, можно сделать следующие выводы.

1. Под термином *классическая информация* в контексте целей настоящей диссертации понимается информация в ее традиционном смысле. Единицей классической информации является *бит*.

2. Состояние квантовой системы представляет особого рода информационный ресурс, содержащий сведения о статистике всевозможных измерений над данной квантовой системой. С этих позиций информация, содержащаяся в квантовом состоянии, имеет качественные отличия от классической информации и поэтому для нее применяют специальный термин *квантовая информация*. Единицей квантовой информации является *кубит*.

3. Физического прибора (инструмента) в самом широком смысле этого понятия, позволяющего осуществить клонирование кубита в произвольном неизвестном состоянии **не существует**. Более того, **не существует** физического прибора (инструментальных средств), позволяющего клонировать кубит в неизвестном состоянии, принадлежащем известному множеству состояний, содержащему не менее чем два неортогональных состояния.

4. Для любых двух ортогональных состояний  $|\psi_1\rangle$  и  $|\psi_2\rangle$  **существует** физический прибор (инструмент), позволяющий осуществить клонирование кубита в неизвестном состоянии  $|\psi\rangle \in \{|\psi_1\rangle, |\psi_2\rangle\}$ . При этом, если состояния  $|\psi_1\rangle$  и  $|\psi_2\rangle$  известны, то **можно построить** квантовый логический элемент, позволяющий клонировать квантовую информацию, представленную кубитами, состояние каждого из которых неизвестно, но принадлежит множеству  $\{|\psi_1\rangle, |\psi_2\rangle\}$ .

5. Свойство, установленное в теореме о *невозможности клонирования*, представляет собой одно из главных различий между квантовой

и классической информацией [66]. Оно является новым квантовым ресурсом, эффективно применяемым в квантовой криптографии при построении квантовых криптографических систем генерации и распределения ключей (квантовые криптографические протоколы BB84 [88], B92 [89], SARG04 [105] и др. [49], [63]). В Главе 3 настоящей диссертации этот вопрос рассмотрен более подробно.

6. **Несепарабельные или запутанные состояния** квантовых систем относятся к ряду основных объектов и ресурсов современных квантовых технологий хранения, обработки и передачи информации, не имеющих классических аналогов. В настоящее время уже экспериментально подтверждена техническая возможность искусственного создания и сохранения несепарабельных квантовых состояний в формах, пригодных для решения прикладных задач криптографии. Теоретические расчеты «времени жизни» несепарабельных квантовых состояний, реализованных с использованием спинов ядер атомов некоторых химических элементов, дают результат - около 3000000 лет [63].

7. Существуют корректные математические определения понятий сепарабельности и несепарабельности состояний многокубитных квантовых систем, учитывающие сложную специфику связей составных компонент многокубитных квантовых систем и адекватно в математической форме отражающие их физическую реакцию на процессы всевозможных измерений [24]. В случае двухкубитных состояний определения понятий сепарабельности и несепарабельности совпадают с ранее известными [71], [77].

8. Из двухкубитных состояний Белла только состояние спиновый синглет обладает тем свойством, что результаты измерений компоненты спина вдоль произвольной оси над каждым из кубитов двухкубитной квантовой системы будут противоположными.

Существуют эффективные для практических применений и вычислительно несложные критерии для определения несепарабельности состояний двухкубитных, трехкубитных и четырехкубитных квантовых

систем [24]. Однако надо отметить, что для решения задачи бинарной классификации состояний (сепарабельные или несепарабельные) квантовой системы из  $n$  кубитов (где  $n$  – натуральное число,  $n > 1$ ) число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, равно  $2^{n-1} - 1$ . Тогда как при решении задачи выяснения неразложимости (или разложимости) состояния квантовой системы в тензорное произведение состояний меньшей размерности число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, равно  $n-1$  [24]. Таким образом, с ростом числа  $n$  кубитов, число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, при решении задачи выяснения неразложимости (или разложимости) состояний  $n$ -кубитных квантовых систем в тензорное произведение состояний меньшей размерности, растет **линейно**. При этом число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, при решении задачи бинарной классификации состояний (сепарабельные или несепарабельные)  $n$ -кубитных квантовых систем, растет **экспоненциально** с ростом  $n$ . Поэтому актуальна задача исследования и выявления эффективно проверяемых (на наличие или отсутствие) достаточных признаков несепарабельности для состояний многокубитных квантовых систем. Некоторые варианты решения указанной задачи осуществлены в рамках диссертационных исследований, проведенных автором данной работы. Полученные результаты приводятся в главе 2.

## ГЛАВА 2. ДОСТАТОЧНЫЕ ПРИЗНАКИ НЕСЕПАРАБЕЛЬНОСТИ СОСТОЯНИЙ МНОГОКУБИТНЫХ КВАНТОВЫХ СИСТЕМ

В связи с отмеченным выше экспоненциальным ростом вычислительной сложности решения задачи о бинарной классификации состояний многокубитных квантовых систем (то есть, задачи определения к какому из двух классов – классу сепарабельных состояний или классу несепарабельных состояний – принадлежит заданное многокубитное состояние) представляют интерес эффективно проверяемые признаки многокубитного состояния, по которым можно определить несепарабельно это состояние или нет. Выявление таких признаков может быть предметом отдельных будущих исследований. Однако в общем случае (т. е. при условии, что число кубитов  $n$  произвольное натуральное число) некоторые достаточные признаки несепарабельности состояний квантовой системы из  $n$  кубитов могут быть установлены через изучение соответствующих этим состояниям булевых масок или нумераторов ([24], [59], [60], [61]). Глава 2 посвящена исследованиям этого направления, на основе аналитического аппарата булевых масок. Автором предложено использование нумераторов весов состояний многокубитных квантовых систем для получения некоторых достаточных признаков несепарабельности и разработана процедура редукции булевой функции, которая предоставляет возможность алгоритмического решения задачи о неразложимости квантовых состояний в тензорное произведение состояний меньшей размерности.

## § 2.1. Булевы маски состояний квантовых систем

В данном параграфе вводятся основные определения и представляются результаты исследования некоторых свойств булевых масок состояний квантовой системы. На булеву маску распространяются определения разного типа понятий сепарабельности и несепарабельности, аналогичные для квантовых состояний. Формулируется и доказывается утверждение о том, что из несепарабельности любого типа для булевой маски состояния многокубитной квантовой системы следует несепарабельность того же типа для самого состояния. Обратное в общем случае неверно, то есть из несепарабельности состояния многокубитной квантовой системы не следует несепарабельность его булевой маски. В подтверждение этого вывода приводится пример несепарабельного состояния двухкубитной квантовой системы, булева маска которого является сепарабельной.

Вначале сформулируем необходимые для дальнейшего определения.

**Определение 2.1.1.** Вектор  $V_\psi = (b_0, b_1, \dots, b_{2^n-1})^T \in \mathbb{C}^{2^n}$  называется **булевой маской** состояния  $|\psi\rangle = (a_0, a_1, \dots, a_{2^n-1})^T \in \mathbb{C}^{2^n}$  (здесь  $T$  – знак транспонирования)  $n$ -кубитной квантовой системы  $A_1 A_2 \dots A_n$ , если для любого  $k \in \{0, 1, \dots, 2^n-1\}$  справедливо равенство

$$b_k = \begin{cases} 0, & \text{если } a_k = 0; \\ 1, & \text{в противном случае.} \end{cases}$$

Для булевых масок определения разного типа сепарабельности и несепарабельности во многом аналогичны соответствующим определениям 2.4.4, 2.4.8 – 2.4.11 из параграфа 2.4 работы [24] для состояний квантовых систем. Напомним некоторые обозначения, введенные в параграфе 2.4 работы [24]:  $S_n$  – симметрическая группа подстановок [38] на множестве  $\{1, 2, \dots, n\}$ ;  $M_n^{(t)}$  – множество разбиений натурального числа  $n$  на  $t$  слагаемых (здесь

понятие разбиения отличается от понятия разбиения в [83]), где  $t \in \{2, 3, \dots, n\}$ , то есть  $M_n^{(t)}$  - множество упорядоченных наборов натуральных чисел  $(k_1, k_2, \dots, k_t)$ , таких, что справедливо равенство

$$k_1 + k_2 + \dots + k_t = n.$$

**Определение 2.1.2.** Пусть  $s \in S_n$ ,  $m_{n,t}^{(j)} \in M_n^{(t)}$ ,  $m_{n,t}^{(j)} = (k_1, k_2, \dots, k_t)$ ,  $j \in \{1, 2, \dots, |M_n^{(t)}|\}$ ,  $|M_n^{(t)}|$  - мощность множества  $M_n^{(t)}$ ,  $t \in \{2, 3, \dots, n\}$ .

Булева маска  $V_\Psi$  состояния  $|\Psi\rangle$   $n$ -кубитной квантовой системы  $A_1 A_2 \dots A_n$  называется  $(s; m_{n,t}^{(j)})$  – **сепарабельной булевой маской**, если для булевой маски  $V_{\Psi^{(s)}}$  состояния  $|\Psi^{(s)}\rangle$  квантовой системы

$$A_{s(1)} A_{s(2)} \dots A_{s(k_1)} A_{s(k_1+1)} \dots A_{s(k_1+k_2)} A_{s(k_1+k_2+1)} \dots A_{s(k_1+k_2+\dots+k_{t-1})} \\ A_{s(k_1+k_2+\dots+k_{t-1}+1)} \dots A_{s(n)} \quad (2.1.3)$$

справедливо равенство

$$V_{\Psi^{(s)}} = (c_{10}, c_{11}, \dots, c_{1(2^{k_1}-1)})^T \otimes (c_{20}, c_{21}, \dots, c_{2(2^{k_2}-1)})^T \otimes \dots \\ \dots \otimes (c_{t0}, c_{t1}, \dots, c_{t(2^{k_t}-1)})^T, \quad (2.1.4)$$

где  $c_{qr^{(q)}} \in \{0; 1\}$ ,  $q \in \{1, 2, \dots, t\}$ ,  $r^{(q)} \in \{0, 1, \dots, 2^{k_q}-1\}$ .

**Определение 2.1.5.** Булева маска  $V_\Psi$  состояния  $|\Psi\rangle$   $n$ -кубитной квантовой системы  $A_1 A_2 \dots A_n$  называется  $(s; *)$  – **сепарабельной булевой маской**, если найдется разбиение  $m_{n,t}^{(j)} \in M_n^{(t)}$ , такое, что булева маска  $V_\Psi$  является  $(s; m_{n,t}^{(j)})$  – сепарабельной булевой маской.

**Определение 2.1.6.** Булева маска  $V_\Psi$  состояния  $|\Psi\rangle$   $n$ -кубитной квантовой системы  $A_1 A_2 \dots A_n$  называется  $(*; m_{n,t}^{(j)})$  – **сепарабельной булевой маской**, если найдется подстановка  $s \in S_n$ , такая, что булева маска  $V_\Psi$  является  $(s; m_{n,t}^{(j)})$  – сепарабельной булевой маской.

**Определение 2.1.7.** Булева маска  $V_\psi$  состояния  $|\psi\rangle$   $n$ -кубитной квантовой системы  $A_1A_2\dots A_n$  называется  $t$  – **сепарабельной булевой маской**, если найдутся подстановка  $s \in \mathbf{S}_n$  и разбиение  $m_{n,t}^{(j)} \in M_n^{(t)}$ , такие, что булева маска  $V_\psi$  является  $(s; m_{n,t}^{(j)})$  – сепарабельной булевой маской, где  $t \in \{2, 3, \dots, n\}$ .

**Определение 2.1.8.** Булева маска  $V_\psi$  состояния  $|\psi\rangle$   $n$ -кубитной квантовой системы  $A_1A_2\dots A_n$  называется **сепарабельной булевой маской**, если найдется число  $t \in \{2, 3, \dots, n\}$ , такое, что  $V_\psi$  является  $t$  – сепарабельной булевой маской.

**Определение 2.1.9.** Булева маска  $V_\psi$  состояния  $|\psi\rangle$   $n$ -кубитной квантовой системы  $A_1A_2\dots A_n$  называется  $(s; m_{n,t}^{(j)})$  – **несепарабельной булевой маской** (соответственно  $(s; *)$  – **несепарабельной**,  $(*; m_{n,t}^{(j)})$  – **несепарабельной**,  $t$  – **несепарабельной**, **несепарабельной**), если она не является  $(s; m_{n,t}^{(j)})$  – сепарабельной булевой маской (соответственно не является  $s; *$  – сепарабельной,  $(*; m_{n,t}^{(j)})$  – сепарабельной,  $t$  – сепарабельной, сепарабельной).

Автором сформулировано и доказано следующее утверждение.

**Утверждение 2.1.10.** Если булева маска  $V_\psi$  состояния  $|\psi\rangle$   $n$ -кубитной квантовой системы  $A_1A_2\dots A_n$  является  $(s; m_{n,t}^{(j)})$  – несепарабельной булевой маской (или  $(s; *)$  – несепарабельной, или  $(*; m_{n,t}^{(j)})$  – несепарабельной, или  $t$  – несепарабельной, или несепарабельной), то состояния  $|\psi\rangle$  является  $(s; m_{n,t}^{(j)})$  – несепарабельным состоянием (соответственно  $(s; *)$  – несепарабельным,  $(*; m_{n,t}^{(j)})$  – сепарабельным,  $t$  – несепарабельным, несепарабельным).

Доказательство Утверждения 2.1.10 приведем в этом параграфе ниже. Пока же обратим внимание на то, что обращение утверждения 2.1.10 в общем случае неверно, то есть в общем случае несепарабельность булевой маски

состояния не является необходимым условием для несепарабельности самого состояния. Это видно, в частности, из следующего примера.

**Пример 2.1.11.** Рассмотрим двухкубитное состояние

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle.$$

Так как

$$ad - bc = \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \cdot \left(-\frac{1}{2}\right) = \frac{1}{2} \neq 0,$$

то данное состояние является несепарабельным состоянием в соответствии с утверждением 2.2.8. Однако его булева маска

$$V_\psi = |00\rangle + |01\rangle + |10\rangle + |11\rangle$$

является сепарабельной булевой маской, так как справедливо равенство

$$V_\psi = (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle),$$

где  $|0\rangle + |1\rangle$  - булева маска однокубитного состояния  $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ .

Приведем теперь доказательство утверждения 2.1.10.

**Доказательство.** Утверждение 2.1.10 состоит из нескольких частей. Все они доказываются примерно одинаково. Поэтому ограничимся доказательством той части утверждения, в которой утверждается, что из несепарабельности булевой маски  $V_\psi$  состояния  $|\psi\rangle$  следует несепарабельность самого состояния  $|\psi\rangle$ .

Докажем методом от противного. Допустим, что булева маска  $V_\psi$  состояния  $|\psi\rangle$  несепарабельна, а само состояние  $|\psi\rangle$  является сепарабельным состоянием.

Из сепарабельности состояния  $|\psi\rangle$  следует, что найдется подстановка  $s \in \mathbf{S}_n$  такая, что для состояния  $|\psi^{(s)}\rangle$  квантовой системы (2.1.3) справедливо равенство

$$|\psi^{(s)}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle, \tag{2.1.12}$$

где

$$|\Psi_1\rangle = (a_{10}, a_{11}, \dots, a_{1(2^{t_1}-1)})^T \quad (2.1.13)$$

- состояние квантовой системы из  $t_1$  кубитов;

$$|\Psi_2\rangle = (a_{20}, a_{21}, \dots, a_{2(2^{t_2}-1)})^T \quad (2.1.14)$$

- состояние квантовой системы из  $t_2$  кубитов;

$t_1$  и  $t_2$  – некоторые натуральные числа, такие, что справедливо равенство  $t_1+t_2=n$ ;

координаты состояний  $|\Psi_1\rangle$  и  $|\Psi_2\rangle$  удовлетворяют условиям

$$a_{qr^{(q)}} \in \mathbb{C}, r^{(q)} \in \{0, 1, \dots, 2^{t_q}-1\}, q \in \{1, 2\},$$

$$\sum_{r^{(q)}=0}^{2^{t_q}-1} |a_{qr^{(q)}}|^2 = 1.$$

Из равенств (2.1.12) – (2.1.14) следует, что каждая координата состояния  $|\Psi^{(s)}\rangle$  равна произведению соответствующей координаты состояния  $|\Psi_1\rangle$  и соответствующей координаты состояния  $|\Psi_2\rangle$ . При этом координата состояния  $|\Psi^{(s)}\rangle$  не равна нулю тогда и только тогда, когда не равны нулю сомножители в произведении. Отсюда следует, что для булевой маски  $V_{\Psi^{(s)}}$  состояния  $|\Psi^{(s)}\rangle$  справедливо равенство

$$V_{\Psi^{(s)}} = V_{\Psi_1} \otimes V_{\Psi_2},$$

где  $V_{\Psi_1}$  и  $V_{\Psi_2}$  - булевы маски состояний  $|\Psi_1\rangle$  и  $|\Psi_2\rangle$  соответственно.

Отсюда и из определения 2.1.8 следует, что булева маска  $V_{\Psi}$  является сепарабельной булевой маской, что противоречит исходному предположению о несепарабельности  $V_{\Psi}$ . Следовательно, предположение о сепарабельности состояния  $|\Psi\rangle$  неверно, то есть  $|\Psi\rangle$  является несепарабельным состоянием. Доказательство завершено.

При переходе от векторов состояний к их булевым маскам часть

информации обычно теряется. Также может быть потеряна информация и при переходе от булевых масок к их нумераторам. Тем не менее, используя непосредственно булевы маски или булевы функции, ими определяемые, как и их нумераторы, удастся получить содержательные результаты о несепарабельности состояний многокубитных квантовых систем. Соответствующие результаты о нумераторах представлены в нижеследующем параграфе 2.2. Результаты с использованием булевых функций представлены далее в параграфе 2.3.

## § 2.2. Нумераторы весов состояний квантовых систем

Напомним (см. § 1.1), что состоянием квантовой системы из  $n$  ( $n \geq 1$ ) кубитов является любой нормированный вектор  $|\psi\rangle$ , принадлежащий  $n$ -ой тензорной степени  $\mathbf{C}^{2^n}$  гильбертова пространства  $\mathbf{C}^2$ , то есть  $2^n$ -мерного гильбертова пространства  $\mathbf{C}^{2^n} = \mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \dots \otimes \mathbf{C}^2$  над полем комплексных чисел  $\mathbf{C}$ , где  $\otimes$  - знак операции тензорного произведения [36], [37], [70].

Этот вектор  $|\psi\rangle$ , представляется в виде **суперпозиции (линейной комбинации)**:

$$|\psi\rangle = \alpha_0 \underbrace{|000\dots 00\rangle}_n + \alpha_1 |000\dots 01\rangle + \alpha_2 |000\dots 10\rangle + \dots + \alpha_{2^n-1} |111\dots 11\rangle, \quad (2.2.1)$$

где

$$\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_{2^n-1} \in \mathbf{C}, \quad |\alpha_0|^2 + |\alpha_1|^2 + \dots + |\alpha_{2^n-1}|^2 = 1, \quad (2.2.2)$$

$$\begin{aligned} |\varphi_1 \varphi_2 \varphi_3 \dots \varphi_{n-1} \varphi_n\rangle &= |\varphi_1\rangle |\varphi_2\rangle |\varphi_3\rangle \dots |\varphi_{n-1}\rangle |\varphi_n\rangle = \\ &= |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes |\varphi_3\rangle \otimes \dots \otimes |\varphi_{n-1}\rangle \otimes |\varphi_n\rangle, \end{aligned} \quad (2.2.3)$$

$$\varphi_m \in \{0; 1\}, \quad m = \overline{1, n},$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Векторы  $\underbrace{|000\dots 00\rangle}_n, |000\dots 01\rangle, \dots, |111\dots 11\rangle$  называются **состояниями**

**вычислительного базиса** в случае квантовой системы из  $n$  кубитов. Они составляют ортонормированный базис гильбертова пространства  $\mathbf{C}^{2^n}$ .

Вычислительный базис квантовой системы из  $n$  кубитов обозначим через  $B_n$ , то есть

$$B_n = \{ \underbrace{|000\dots 00\rangle}_n, |000\dots 01\rangle, \dots, |111\dots 11\rangle \} \quad (2.2.4)$$

**Определение 2.2.5.** Пусть  $|\phi\rangle = |\varphi_1 \varphi_2 \varphi_3 \dots \varphi_{n-1} \varphi_n\rangle$  - произвольное

состояние из вычислительного базиса, где  $\varphi_m \in \{0; 1\}$ ,  $m = \overline{1, n}$ . Число отличных от нуля элементов в конечной последовательности  $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$  длины  $n$  называется **весом** (весом Хэмминга) состояния  $|\phi\rangle$  и обозначается  $\text{wt}(|\phi\rangle)$ .

**Определение 2.2.6.** Нумератором весов состояния  $|\psi\rangle$  квантовой системы из  $n$  кубитов, заданного равенством (2.2.1), называется многочлен

$$N_{|\psi\rangle}(x, y) = \sum_{k=0}^n \eta_k(|\psi\rangle) x^k y^{n-k},$$

от двух формальных переменных  $x$  и  $y$ , где  $\eta_k(|\psi\rangle)$  – число состояний веса  $k$  из вычислительного базиса  $B_n$ , входящих с ненулевыми коэффициентами в правую часть равенства (2.2.1).

**Определение 2.2.7.** Характеристической функцией состояния  $|\psi\rangle$  квантовой системы из  $n$  кубитов, заданного равенством (2.2.1), называется функция  $\chi_{|\psi\rangle}(|\phi\rangle)$  с областью определения  $B_n$  и множеством значений  $\{0; 1\}$ , такая, что для любого состояния  $|\phi\rangle \in B_n$  справедливо равенство  $\chi_{|\psi\rangle}(|\phi\rangle) = 1$ , если состояние  $|\phi\rangle$  входит с ненулевым коэффициентом в равенство (2.2.1), и справедливо равенство  $\chi_{|\psi\rangle}(|\phi\rangle) = 0$  – в противном случае.

Справедливы следующие утверждения.

**Утверждение 2.2.8.** Для нумератора весов  $N_{|\psi\rangle}(x, y)$  состояния  $|\psi\rangle$  справедливо равенство

$$N_{|\psi\rangle}(x, y) = \sum_{|\phi\rangle \in B_n} \chi_{|\psi\rangle}(|\phi\rangle) x^{\text{wt}(|\phi\rangle)} y^{n-\text{wt}(|\phi\rangle)}.$$

**Утверждение 2.2.9.** Пусть для состояния  $|\psi\rangle$  квантовой системы из  $n$  кубитов выполняется равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle,$$

где  $|\psi_1\rangle$  – состояние квантовой системы из  $n_1$  кубитов,  $|\psi_2\rangle$  – состояние

квантовой системы из  $n_2 = n - n_1$  кубитов;  $n_1, n_2$  – натуральные числа. Тогда для любого состояния  $|\phi\rangle = |\phi_1\phi_2\phi_3\dots\phi_{n-1}\phi_n\rangle \in B_n$  справедливо равенство

$$\chi_{|\psi\rangle}(|\phi\rangle) = \chi_{|\psi_1\rangle}(|\phi_1\rangle) \cdot \chi_{|\psi_2\rangle}(|\phi_2\rangle),$$

где  $|\phi_1\rangle = |\phi_1\phi_2\dots\phi_{n_1}\rangle \in B_{n_1}$ ,  $|\phi_2\rangle = |\phi_{n_1+1}\phi_{n_1+2}\dots\phi_n\rangle \in B_{n_2}$ ;  $\chi_{|\psi_1\rangle}, \chi_{|\psi_2\rangle}$  –

характеристические функции состояний  $|\psi_1\rangle$  и  $|\psi_2\rangle$  соответственно.

**Утверждение 2.2.10.** Пусть для состояния  $|\psi\rangle$  квантовой системы из  $n$  кубитов выполняется равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle,$$

где  $|\psi_1\rangle$  – состояние квантовой системы из  $n_1$  кубитов,  $|\psi_2\rangle$  – состояние квантовой системы из  $n_2 = n - n_1$  кубитов;  $n_1, n_2$  – натуральные числа. Тогда

для нумератора весов  $N_{|\psi\rangle}(x, y)$  состояния  $|\psi\rangle$  справедливо равенство

$$N_{|\psi\rangle}(x, y) = N_{|\psi_1\rangle}(x, y) \cdot N_{|\psi_2\rangle}(x, y),$$

где  $N_{|\psi_1\rangle}(x, y)$  и  $N_{|\psi_2\rangle}(x, y)$  – нумераторы весов состояний  $|\psi_1\rangle$  и  $|\psi_2\rangle$  соответственно.

Из утверждения 2.2.10 вытекает следующее

**Следствие 2.2.11.** Если нумератор весов  $N_{|\psi\rangle}(x, y)$  состояния  $|\psi\rangle$  квантовой системы из  $n$  кубитов не раскладывается в произведение нумераторов двух состояний меньшей размерности, чем размерность исходного состояния, то состояние  $|\psi\rangle$  является несепарабельным состоянием.

Доказательства утверждений 2.2.8, 2.2.9 и 2.2.10 приведем далее в настоящем параграфе. Теперь же заметим, что в виде следствия 2.2.11 получилось достаточное условие для эффективного выявления несепарабельных состояний квантовых систем. Однако надо не забывать, что это условие включает в себя и ситуацию, когда нумератор весов  $N_{|\psi\rangle}(x, y)$

может быть разложен только в произведение двух многочленов от переменных  $(x, y)$ , хотя бы один из которых не является нумератором весов некоторого квантового состояния. В этом случае исходное состояние также является несепарабельным. Приведем иллюстрирующий пример.

**Пример 2.2.12.** Пусть

$$|\psi\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}.$$

Известно, что состояние  $|\psi\rangle$  несепарабельное состояние (это, в частности, следует из утверждения 2.2.8).

Непосредственно из определения 2.2.6 нумератора весов  $N_{|\psi\rangle}(x, y)$  состояния  $|\psi\rangle$  получаем

$$N_{|\psi\rangle}(x, y) = 2xy.$$

Хотя нумератор весов  $N_{|\psi\rangle}(x, y)$  разложим на множители, его возможные делители  $2x$  и  $2y$  не могут являться нумераторами какого-либо состояния квантовой системы из одного кубита.

Из Утверждения 2.2.10 вытекает и более жесткое достаточное условие для несепарабельности квантового состояния. Оно представлено в формулируемом ниже следствии 2.2.13.

**Следствие 2.2.13.** Если нумератор весов  $N_{|\psi\rangle}(x, y)$  состояния  $|\psi\rangle$  квантовой системы из  $n$  кубитов является неприводимым многочленом над кольцом целых чисел от двух переменных  $(x, y)$ , то состояние  $|\psi\rangle$  является несепарабельным состоянием.

Далее последовательно проведем доказательства сформулированных выше утверждений 2.2.8, 2.2.9 и 2.2.10.

**Доказательство** утверждения 2.2.8. По определению 2.2.6 имеем

$$N_{|\psi\rangle}(x, y) = \sum_{k=0}^n \eta_k(|\psi\rangle) x^k y^{n-k}. \quad (2.2.14)$$

Для величины  $\eta_k(|\psi\rangle)$  справедливо равенство

$$\eta_k(|\Psi\rangle) = \sum_{|\phi\rangle \in B_n, \text{wt}(|\phi\rangle)=k} \chi_{|\Psi\rangle}(|\phi\rangle) \quad (2.2.15)$$

для любого  $k \in \{0, 1, \dots, n\}$ .

Подставив правую часть равенства (2.2.15) вместо  $\eta_k(|\Psi\rangle)$  в правую часть равенства (2.2.14), получаем

$$\begin{aligned} N_{|\Psi\rangle}(x, y) &= \sum_{k=0}^n \left( \sum_{|\phi\rangle \in B_n, \text{wt}(|\phi\rangle)=k} \chi_{|\Psi\rangle}(|\phi\rangle) \right) x^k y^{n-k} = \\ &= \sum_{k=0}^n \left( \sum_{|\phi\rangle \in B_n, \text{wt}(|\phi\rangle)=k} \chi_{|\Psi\rangle}(|\phi\rangle) x^{\text{wt}(|\phi\rangle)} y^{n-\text{wt}(|\phi\rangle)} \right). \end{aligned}$$

Отсюда, учитывая свойство коммутативности операции сложения многочленов и то, что значения весов всех состояний из вычислительного базиса  $B_n$  полностью исчерпываются значениями от 0 до  $n$ , получаем

$$N_{|\Psi\rangle}(x, y) = \sum_{|\phi\rangle \in B_n} \chi_{|\Psi\rangle}(|\phi\rangle) x^{\text{wt}(|\phi\rangle)} y^{n-\text{wt}(|\phi\rangle)}.$$

Утверждение 2.2.8 доказано.

**Доказательство** утверждения 2.2.9. Пусть выполняется равенство

$$|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle.$$

Выпишем по аналогии с (2.2.1) выражения для представлений состояний  $|\Psi\rangle$ ,  $|\Psi_1\rangle$  и  $|\Psi_2\rangle$  в соответствующих им вычислительных базисах:

$$|\Psi\rangle = \alpha_0 \underbrace{|000\dots 00\rangle}_n + \alpha_1 |000\dots 01\rangle + \alpha_2 |000\dots 10\rangle + \dots + \alpha_{2^n-1} |111\dots 11\rangle,$$

$$|\Psi_1\rangle = \alpha_{10} \underbrace{|000\dots 00\rangle}_{n_1} + \alpha_{11} |000\dots 01\rangle + \alpha_{12} |000\dots 10\rangle + \dots + \alpha_{1(2^{n_1}-1)} |111\dots 11\rangle$$

$$|\Psi_2\rangle = \alpha_{20} \underbrace{|000\dots 00\rangle}_{n_2} + \alpha_{21} |000\dots 01\rangle + \alpha_{22} |000\dots 10\rangle + \dots + \alpha_{2(2^{n_2}-1)} |111\dots 11\rangle.$$

Подставив правые части этих равенств в выражение

$$|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$$

вместо состояний  $|\Psi\rangle$ ,  $|\Psi_1\rangle$  и  $|\Psi_2\rangle$  соответственно, после этого

выполнив операцию тензорного произведения в левой части этого равенства и затем приравняв коэффициенты перед одинаковыми состояниями вычислительного базиса  $B_n$  в левой и правой частях результирующего выражения, получим равенство

$$\alpha_t = \alpha_{1t_1} \cdot \alpha_{2t_2}, \quad (2.2.16)$$

для коэффициентов перед каждым состоянием  $|\phi\rangle = |\varphi_1\varphi_2\varphi_3\dots\varphi_{n-1}\varphi_n\rangle \in$

$B_n$ , где

$$t = 2^{n-1}\varphi_1 + 2^{n-2}\varphi_2 + \dots + 2^0\varphi_n,$$

$$t_1 = 2^{n_1-1}\varphi_1 + 2^{n_1-2}\varphi_2 + \dots + 2^0\varphi_{n_1},$$

$$t_2 = 2^{n_2-1}\varphi_{n_1+1} + 2^{n_2-2}\varphi_{n_1+2} + \dots + 2^0\varphi_n,$$

$\alpha_t$  - коэффициент в (2.2.16) перед состоянием  $|\phi\rangle = |\varphi_1\varphi_2\varphi_3\dots\varphi_{n-1}\varphi_n\rangle \in B_n$

$\alpha_{1t_1}$  - коэффициент в (2.2.17) перед состоянием  $|\phi_1\rangle = |\varphi_1\varphi_2\dots\varphi_{n_1}\rangle \in B_{n_1}$ ,

$\alpha_{2t_2}$  - коэффициент в (2.2.18) перед состоянием  $|\phi_2\rangle = |\varphi_{n_1+1}\varphi_{n_1+2}\dots\varphi_n\rangle$

$\in B_{n_2}$ .

Из (2.2.16) получаем, что коэффициент  $\alpha_t$  не равен нулю тогда и только тогда, когда не равен нулю каждый из коэффициентов  $\alpha_{1t_1}$  и  $\alpha_{2t_2}$ .

Рассмотрим случай, когда  $\alpha_t \neq 0$ , В этом случае из определения 2.2.7 следует, что  $\chi_{|\psi\rangle}(|\phi\rangle) = 1$ . Одновременно с этим из неравенства  $\alpha_t \neq 0$  в соответствии с (2.2.16) следует справедливость неравенств  $\alpha_{1t_1} \neq 0$  и  $\alpha_{2t_2} \neq 0$ , которые, в свою очередь, по определению 2.2.7 влекут за собой соответственно справедливость равенств  $\chi_{|\psi_1\rangle}(|\phi_1\rangle) = 1$  и  $\chi_{|\psi_2\rangle}(|\phi_2\rangle) = 1$ . Следовательно, в этом случае равенство  $\chi_{|\psi\rangle}(|\phi\rangle) = \chi_{|\psi_1\rangle}(|\phi_1\rangle) \cdot \chi_{|\psi_2\rangle}(|\phi_2\rangle)$  выполнено.

Рассмотрим случай, когда  $\alpha_t = 0$ , В этом случае из определения

2.2.7 следует, что  $\chi_{|\psi\rangle}(|\phi\rangle) = 0$ . Одновременно с этим из равенства  $\alpha_t = 0$  в соответствии с (2.2.16) следует справедливость хотя бы одного из равенств  $\alpha_{1t_1} = 0$  или  $\alpha_{2t_2} = 0$ , что, в свою очередь, влечет за собой по определению 2.2.7 справедливость хотя бы одного из равенств  $\chi_{|\psi_1\rangle}(|\phi_1\rangle) = 0$  и  $\chi_{|\psi_2\rangle}(|\phi_2\rangle) = 0$ .

Следовательно, и в этом случае равенство

$$\chi_{|\psi\rangle}(|\phi\rangle) = \chi_{|\psi_1\rangle}(|\phi_1\rangle) \cdot \chi_{|\psi_2\rangle}(|\phi_2\rangle)$$

выполнено.

Таким образом, равенство  $\chi_{|\psi\rangle}(|\phi\rangle) = \chi_{|\psi_1\rangle}(|\phi_1\rangle) \cdot \chi_{|\psi_2\rangle}(|\phi_2\rangle)$

справедливо для всех возможных значений входящих в него характеристических функций. Утверждение 2.2.9 доказано.

**Доказательство** утверждения 2.2.10. Пусть выполняется равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle.$$

Тогда из утверждения 2.2.9 следует, что для любого состояния

$|\phi\rangle = |\phi_1\phi_2\phi_3\dots\phi_{n-1}\phi_n\rangle \in B_n$  справедливо равенство

$$\chi_{|\psi\rangle}(|\phi\rangle) = \chi_{|\psi_1\rangle}(|\phi_1\rangle) \cdot \chi_{|\psi_2\rangle}(|\phi_2\rangle),$$

где  $|\phi_1\rangle = |\phi_1\phi_2\dots\phi_{n_1}\rangle \in B_{n_1}$ ,  $|\phi_2\rangle = |\phi_{n_1+1}\phi_{n_1+2}\dots\phi_n\rangle \in B_{n_2}$

Из утверждения 2.2.8 для нумератора весов состояния  $|\psi\rangle$  имеем

$$N_{|\psi\rangle}(x, y) = \sum_{|\phi\rangle \in B_n} \chi_{|\psi\rangle}(|\phi\rangle) x^{\text{wt}(|\phi\rangle)} y^{n-\text{wt}(|\phi\rangle)}$$

Заменив  $\chi_{|\psi\rangle}(|\phi\rangle)$  под знаком суммы в правой части этого равенства на правую часть  $\chi_{|\psi_1\rangle}(|\phi_1\rangle) \cdot \chi_{|\psi_2\rangle}(|\phi_2\rangle)$  предыдущего равенства, получим

$$N_{|\psi\rangle}(x, y) = \sum_{|\phi\rangle \in B_n} (\chi_{|\psi_1\rangle}(|\phi_1\rangle) \cdot \chi_{|\psi_2\rangle}(|\phi_2\rangle)) x^{\text{wt}(|\phi\rangle)} y^{n-\text{wt}(|\phi\rangle)}$$

Учитывая равенства

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle,$$

$$n = n_1 + n_2$$

и

$$\text{wt}(|\phi\rangle) = \text{wt}(|\phi_1\rangle) + \text{wt}(|\phi_2\rangle),$$

получаем

$$\begin{aligned} N_{|\psi\rangle}(x, y) &= \\ &= \sum_{(|\phi_1\rangle \otimes |\phi_2\rangle) \in B_n} (\chi_{|\psi_1\rangle}(|\phi_1\rangle) \chi_{|\psi_2\rangle}(|\phi_2\rangle)) x^{(\text{wt}(|\phi_1\rangle) + \text{wt}(|\phi_2\rangle))} y^{(n_1 + n_2) - (\text{wt}(|\phi_1\rangle) + \text{wt}(|\phi_2\rangle))} = \\ &= \sum_{(|\phi_1\rangle \otimes |\phi_2\rangle) \in B_n} (\chi_{|\psi_1\rangle}(|\phi_1\rangle) x^{\text{wt}(|\phi_1\rangle)} y^{n_1 - \text{wt}(|\phi_1\rangle)}) \times \\ &\quad \times (\chi_{|\psi_2\rangle}(|\phi_2\rangle) x^{\text{wt}(|\phi_2\rangle)} y^{n_2 - \text{wt}(|\phi_2\rangle)}) = \\ &= \left( \sum_{|\phi_1\rangle \in B_{n_1}} \chi_{|\psi_1\rangle}(|\phi_1\rangle) x^{\text{wt}(|\phi_1\rangle)} y^{n_1 - \text{wt}(|\phi_1\rangle)} \right) \times \\ &\quad \times \left( \sum_{|\phi_2\rangle \in B_{n_2}} \chi_{|\psi_2\rangle}(|\phi_2\rangle) x^{\text{wt}(|\phi_2\rangle)} y^{n_2 - \text{wt}(|\phi_2\rangle)} \right). \end{aligned}$$

Отсюда и из утверждения 2.2.8 получаем искомое равенство

$$N_{|\psi\rangle}(x, y) = N_{|\psi_1\rangle}(x, y) \cdot N_{|\psi_2\rangle}(x, y).$$

Утверждение 2.2.10 доказано.

Неразложимость нумератора может следовать и из того, что его значение для некоторых целых  $x$  и  $y$  равно простому числу. В то же время, вопрос о разложимости нумератора в общем случае является непростой алгебраической задачей. В следующем параграфе для решения вопроса о разложимости булевой маски приводится построенный автором алгоритм редукции булевой функции.

### § 2.3. Алгоритм определения неразложимости состояния квантовой системы в тензорное произведение состояний меньшей размерности с использованием редукций булевых функций

Существует другой способ описания квантовых систем, - не через векторы состояний, а посредством операторов плотности. Поведение квантовой подсистемы, входящей как часть в некоторую квантовую систему с известным оператором плотности, принято описывать с помощью редуцированного оператора плотности. Точно также и для булевых масок состояний можно ввести в рассмотрение булеву маску оператора плотности и вычисление редуцированного оператора. В этом случае, поскольку матрица булевой маски оператора плотности чистого состояния полностью определяется произвольной строкой (или столбцом) этой матрицы, то операция, аналогичная редукции по подсистеме для квантового состояния, становится операцией над соответствующей булевой функцией. Эта операция, которую мы будем называть «редукцией булевой функции», имеет ряд свойств, имеющих отношение к вопросу о неразложимости состояния квантовой системы в тензорное произведение состояний меньшей размерности. Результатам исследования этих свойств и посвящён настоящий параграф.

Введём в рассмотрение несколько определений.

**Определение 2.3.1.** Пусть  $|\psi\rangle = (a_0, a_1, \dots, a_{2^n-1})^T \in \mathbf{C}^{2^n}$  (здесь  $T$  – знак транспонирования) состояние  $n$ -кубитной квантовой системы, а  $B_\psi = (b_0, b_1, \dots, b_{2^n-1})^T$  – булева маска состояния  $|\psi\rangle$  (см. определение 2.1.1).

Определим булеву функцию  $f_\psi(x_1, x_2, \dots, x_n)$ , положив для каждого  $j \in \{0, 1, \dots, 2^n-1\}$

$$f_\psi(x_1, x_2, \dots, x_n) = b_j$$

при условии, что справедливо равенство

$$2^{n-1} \cdot x_1 + 2^{n-2} \cdot x_2 + \dots + 2^0 \cdot x_n = j.$$

Определенную таким образом функцию  $f_\psi(x_1, x_2, \dots, x_n)$  назовем **булевой функцией** состояния  $|\psi\rangle$ .

Очевидно, что булева маска  $B_\psi$  состояния  $|\psi\rangle$  является столбцом значений в таблице истинности [26] булевой функции  $f_\psi(x_1, x_2, \dots, x_n)$  состояния  $|\psi\rangle$ .

Если для состояния  $|\psi\rangle$  справедливо равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle,$$

то, принимая во внимание определение 2.1.1, можно отметить, что для булевых масок  $B_\psi$ ,  $B_{\psi_1}$  и  $B_{\psi_2}$ , справедливо равенство

$$B_\psi = B_{\psi_1} \otimes B_{\psi_2}. \quad (2.3.2)$$

Тогда существует натуральное число  $m$  такое, что  $1 \leq k \leq n-1$  и булевы функции  $f_{\psi_1}$  и  $f_{\psi_2}$  соответственно состояний  $|\psi_1\rangle$  и  $|\psi_2\rangle$  зависят от непересекающихся множеств переменных  $\{x_1, x_2, \dots, x_k\}$  и  $\{x_{k+1}, x_{k+2}, \dots, x_n\}$ , причем справедливо равенство

$$f_\psi(x_1, x_2, \dots, x_n) = f_{\psi_1}(x_1, x_2, \dots, x_k) \cdot f_{\psi_2}(x_{k+1}, x_{k+2}, \dots, x_n) \quad (2.3.3)$$

Таким образом, получаем, что справедливо следующее утверждение.

**Утверждение 2.3.4.** Если квантовое состояние  $|\psi\rangle$  представляется в виде тензорного произведения квантовых состояний  $|\psi_1\rangle$  и  $|\psi_2\rangle$ , то булева функция  $f_\psi(x_1, x_2, \dots, x_n)$  равна конъюнкции (произведению) булевых функций  $f_{\psi_1}(x_1, x_2, \dots, x_k)$  и  $f_{\psi_2}(x_{k+1}, x_{k+2}, \dots, x_n)$  соответственно состояний  $|\psi_1\rangle$  и  $|\psi_2\rangle$ .

Исследуем вопрос о представимости булевой функции в виде конъюнкции двух булевых функций от различных переменных.

Пусть далее в данном параграфе  $(i_1, i_2, \dots, i_n)$  – перестановка чисел  $1, 2, \dots, n$ , такая, что

$$1 \leq i_1 < i_2 < \dots < i_k \leq n$$

и

$$1 \leq i_{k+1} < i_{k+2} < \dots < i_n \leq n,$$

где  $k, n \in \mathbf{N}$ ,  $n > 1$  и  $1 \leq k \leq n-1$ .

**Определение 2.3.5.** Пусть  $f(x_1, x_2, \dots, x_n)$  – произвольная булева функция от переменных  $x_1, x_2, \dots, x_n$ . **Редукцией** булевой функции  $f(x_1, x_2, \dots, x_n)$  по переменным  $X_{i_1}, X_{i_2}, \dots, X_{i_k}$  называется булева функция  $f'_{x_{i_1} \dots x_{i_k}}(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n})$  заданная равенством

$$f'_{x_{i_1} \dots x_{i_k}}(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}) = \bigvee_{(x_{i_1}, \dots, x_{i_k}) \in \{0,1\}^k} f(x_1, x_2, \dots, x_n),$$

где  $\vee$  – знак операции дизъюнкция.

Таким образом,  $f'_{x_{i_1} \dots x_{i_k}}(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n})$  – новая булева функция, зависящая от  $m=n-k$  переменных  $X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}$ .

Справедливо следующее утверждение.

**Утверждение 2.3.6.** Пусть булева функция  $f(x_1, x_2, \dots, x_n)$  от  $n=m+k$  переменных  $x_1, x_2, \dots, x_n$  отлична от тождественного нуля и представляется в виде

$$f(x_1, x_2, \dots, x_n) = g(X_{i_1}, X_{i_2}, \dots, X_{i_k}) \cdot h(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}) \quad (2.3.7)$$

для некоторых функций  $g$  и  $h$ . Тогда выполняются равенства

$$h(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}) = f'_{x_{i_1} \dots x_{i_k}}(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}) \quad (2.3.8)$$

и

$$g(X_{i_1}, X_{i_2}, \dots, X_{i_k}) = f'_{x_{i_{k+1}} \dots x_{i_n}}(X_{i_1}, X_{i_2}, \dots, X_{i_k}). \quad (2.3.9)$$

**Доказательство.** Действительно, поскольку булева функция  $f(x_1, x_2, \dots, x_n)$  не является тождественным нулем, то из (2.3.7) следует, что

существует такой двоичный набор  $(X_1^{(0)}, X_2^{(0)}, \dots, X_n^{(0)})$ , что справедливы равенства

$$g(X_{i_1}^{(0)}, X_{i_2}^{(0)}, \dots, X_{i_k}^{(0)}) = 1 \quad (2.3.10)$$

и

$$h(X_{i_{k+1}}^{(0)}, X_{i_{k+2}}^{(0)}, \dots, X_{i_n}^{(0)}) = 1. \quad (2.3.11)$$

Из определения 2.3.5, равенств (2.3.7) и (2.3.10) получаем

$$\begin{aligned} f'_{X_{i_1} \dots X_{i_k}}(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}) &= \bigvee_{(x_{i_1}, \dots, x_{i_k}) \in \{0,1\}^k} f(x_1, x_2, \dots, x_n) = \\ &= \bigvee_{(x_{i_1}, \dots, x_{i_k}) \in \{0,1\}^k} g(X_{i_1}, X_{i_2}, \dots, X_{i_k}) \cdot h(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}) = \\ &= h(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}) \cdot \left( \bigvee_{(x_{i_1}, \dots, x_{i_k}) \in \{0,1\}^k} g(X_{i_1}, X_{i_2}, \dots, X_{i_k}) \right) = \\ &= h(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}), \end{aligned}$$

то есть доказана справедливость равенства (2.3.8).

Аналогично, из определения 2.3.5, равенств (2.3.7) и (2.3.11) вытекает справедливость равенства (2.3.9). Утверждение доказано.

**Замечание 2.3.12.** Утверждение 2.3.6 в обратную сторону, вообще говоря, неверно. В частности, конъюнкция

$$f'_{X_{i_1} \dots X_{i_k}}(X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}) \cdot f'_{X_{i_{k+1}} \dots X_{i_n}}(X_{i_1}, X_{i_2}, \dots, X_{i_k})$$

не совпадает с  $f(x_1, x_2, \dots, x_n)$  ни при какой непересекающейся паре подмножеств  $\{X_{i_1}, X_{i_2}, \dots, X_{i_k}\}$  и  $\{X_{i_{k+1}}, X_{i_{k+2}}, \dots, X_{i_n}\}$  различных переменных из множества  $\{x_1, x_2, \dots, x_n\}$ , если  $f(x_1, x_2, \dots, x_n)$  не представляется в виде конъюнкции двух булевых функций от непустых непересекающихся множеств переменных. Простейшим примером такой функции является функция

$$f(x_1, x_2) = x_1 \oplus x_2,$$

где  $\oplus$  - знак операции суммирования по модулю 2. Здесь  $n=2$ ,

$$f'_{x_1}(x_2) = x_2 \vee (x_2 \oplus 1) = 1 \text{ и } f'_{x_2}(x_1) = x_1 \vee (x_1 \oplus 1) = 1.$$

Очевидно, что  $f'_{x_1}(x_2) \cdot f'_{x_2}(x_1) \neq f(x_1, x_2)$ .

Доказанное выше утверждение позволяет изучать вопрос о разложимости исходного квантового состояния в тензорное произведение состояний меньшей размерности (чем размерность исходного квантового состояния) при помощи булевой функции исходного квантового состояния и рассмотрения определенных редукций данной булевой функции. Это можно осуществить следующим образом:

1. Для булевой функции  $f_{\psi}(x_1, x_2, \dots, x_n)$  состояние  $|\psi\rangle$   $n$ -кубитной квантовой системы последовательно строятся ее редукции

$$f'_{\psi_{x_1 \dots x_k}}(x_{k+1}, x_{k+2}, \dots, x_n) \text{ и } f'_{\psi_{x_{k+1} \dots x_n}}(x_1, x_2, \dots, x_k)$$

для каждого  $k = \overline{1, n-1}$ . Для каждого  $k = \overline{1, n-1}$  осуществляется проверка равенства

$$f_{\psi}(x_1, x_2, \dots, x_n) = f'_{\psi_{x_1 \dots x_k}}(x_{k+1}, x_{k+2}, \dots, x_n) \cdot f'_{\psi_{x_{k+1} \dots x_n}}(x_1, x_2, \dots, x_k).$$

2. Если в процессе поиска равенство

$$f_{\psi}(x_1, x_2, \dots, x_n) = f'_{\psi_{x_1 \dots x_k}}(x_{k+1}, x_{k+2}, \dots, x_n) \cdot f'_{\psi_{x_{k+1} \dots x_n}}(x_1, x_2, \dots, x_k)$$

не выполнилось ни для каких  $k = \overline{1, n-1}$ , то, в соответствии с утверждениями 2.3.4 и 2.3.6, можно сделать вывод о неразложимости исходного квантового состояния  $|\psi\rangle$  в тензорное произведение состояний меньшей размерности.

3. В случае, если для некоторого  $k \in \{1, 2, \dots, n-1\}$  получилось тождественное равенство

$$f_{\psi}(x_1, x_2, \dots, x_n) = f'_{\psi_{x_1 \dots x_k}}(x_{k+1}, x_{k+2}, \dots, x_n) \cdot f'_{\psi_{x_{k+1} \dots x_n}}(x_1, x_2, \dots, x_k),$$

то вопрос о разложимости изучаемого квантового состояния  $|\psi\rangle$  продолжает оставаться открытым.

## Выводы по главе 2

По результатам исследований, представленных в главе 2, можно сделать следующие выводы.

1. Если булева маска состояния квантовой системы, состоящей из  $n$  кубитов (где  $n \in \mathbf{N}$ ), является несепарабельной, то само состояние также является несепарабельным.

2. Выяснение вопроса несепарабельности для булевой маски состояния квантовой системы является менее трудоемкой в вычислительном плане задачей, чем для самого состояния. Поэтому подход, основанный на использовании булевых масок для определения несепарабельности состояний квантовых систем, оказывается эффективным подходом в решении задачи бинарной классификации состояний для случаев, когда булевы маски несепарабельны.

3. Если нумератор весов состояния квантовой системы, состоящей из  $n$  кубитов (где  $n \in \mathbf{N}$ ), не равен произведению нумераторов весов состояний квантовых систем с числом кубитов меньшим, чем  $n$ , то это состояние является несепарабельным.

4. Если нумератор весов состояния квантовой системы, состоящей из  $n$  кубитов (где  $n \in \mathbf{N}$ ), является неприводимым многочленом над кольцом целых чисел, то это состояние является несепарабельным.

5. Нумераторы весов состояний квантовых систем позволяют получить эффективные достаточные условия несепарабельности этих состояний.

6. Если отличная от нуля булева функция от  $n$  переменных не представима в виде произведения двух своих редукций, то состояние  $n$ -кубитной квантовой системы, булева маска которого совпадает с вектором значений данной булевой функции, неразложимо в тензорное произведение состояний меньшей размерности.

7. На основе использования редуций булевых функций разработан и представлен эффективный алгоритм, позволяющий определить неразложимость состояние квантовой системы в тензорное произведение состояний меньшей размерности в случае непредставимости соответствующей булевой функции состояния в виде конъюнкции ее некоторых редуций.

В следующей главе будет показано, как несепарабельные квантовые состояния используются в современных протоколах квантовой криптографии.

### ГЛАВА 3. КВАНТОВЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

Развитие квантовых криптографических систем стимулируется двумя задачами. Во-первых, это устранение «человеческого фактора» из жизненного цикла криптографических ключей для традиционных систем шифровальной связи. Во-вторых, это противодействие методам криптоанализа, использующим квантовые компьютеры. Решение этих задач основывается на задействовании физических ресурсов, предоставляемых квантовой механикой.

В соответствии с заявленной темой диссертации, в настоящей главе представлены как некоторые известные квантовые криптографические системы, так и новая, разработанная автором в рамках диссертационных исследований теоретически стойкая квантовая криптографическая система **АКМ2017**. Проанализированы и выявлены качественные свойства квантовой криптографической системы **АКМ2017**, которыми в принципе не обладают ни классические криптографические системы, ни известные ранее системы квантовой криптографии. Математически обосновано сохранение свойства идеальной стойкости для квантовой криптографической системы **АКМ2017** при компрометации квантовых шифрблокнотов. Разработан и представлен алгоритм дистанционной регенерации носителей-кубитов использованных квантовых шифровальных блокнотов квантовой криптографической системы **АКМ2017** в состоянии, позволяющие повторное использование данных квантовых шифровальных блокнотов. Этот алгоритм позволяет существенно повысить надежность шифрованной связи. Такая возможность отсутствует в известных классических и квантовых криптографических системах.

При получении результатов главы 3 существенно использован материал глав 1 и 2.

### **§ 3.1. Квантовые криптографические системы на основе ресурса невозможности клонирования неизвестного квантового состояния**

К квантовым криптографическим системам на основе ресурса невозможности клонирования неизвестного квантового состояния (см. параграф 1.1) относятся криптографические системы BB84 [88], B92 [89] и различные их модификации и обобщения, например, SARG04 [105]. Этот ресурс используется для формирования принципиально не компрометируемого канала передачи информации, которая служит для выработки криптографического ключа. Приводимые далее краткие описания некоторых из них, а именно BB84 и B92, иллюстрируют общие черты таких протоколов. Общим для них является использование ГСЧ, следовательно, необходимость применения процедуры согласования результатов измерений, и отслеживание статистики ошибок для обнаружения атак на канал.

#### **Протокол BB84**

В 1984 году Беннет (фирма IBM) и Brassard (Монреальский университет) предположили, что квантовые состояния фотонов могут быть использованы в криптографии для получения надежно защищенного канала [88]. Они предложили простую схему квантового распределения ключей, названную ими BB84. Эта схема использует квантовый канал, по которому два пользователя **A** и **B** обмениваются сообщениями, передавая их в виде поляризованных фотонов, и в результате формируют общий секретный ключ.

Квантовый канал может представлять собой, например, просто волоконнооптическую линию в совокупности с оконечными устройствами, которые дают возможность генерировать и передавать отдельные фотоны, а также производить некоторые измерения их состояний.

Противник в случае перехвата может попытаться производить измерение этих фотонов, но он не может сделать это, не внося в них искажений. Пользователи **A** и **B** используют открытый классический канал

для обсуждения и сравнения сигналов, передаваемых по квантовому каналу, проверяя их на возможность перехвата. Если не выявлено деструктивное воздействие на квантовый канал, пользователи могут извлечь из полученных данных информацию, которая надежно распределена, случайна и секретна, несмотря на преднамеренные технические ухищрения и вычислительные возможности, которыми располагает противник.

Основные шаги протокола BB84 можно описать следующим образом.

Пользователь **A** имеет два двоичных генератора случайных чисел ГСЧ1 и ГСЧ2.

Пользователь **A** с помощью генератора случайных чисел ГСЧ1 формирует случайную последовательность двоичных битов  $\alpha$ . В процессе формирования общего с **B** секретного ключа, пользователь **A** посылает пользователю **B** данную последовательность, кодируя каждый бит в квантовом состоянии фотона. При этом у него есть возможность закодировать каждый двоичный бит одним из двух возможных способов, в одном из двух различных ортонормированных базисах. Нормальном базисе «+», где двоичный ноль кодируется горизонтальной поляризацией фотона «0»  $\rightarrow |-\rangle$  ( $|0\rangle$ ), а двоичная единица – вертикальной «1»  $\rightarrow |/\rangle$  ( $|1\rangle$ ), или в диагональном базисе «х», где двоичный ноль кодируется леводиагональной поляризацией фотона «0»  $\rightarrow | \setminus \rangle$  ( $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ ), а двоичная единица – праводиагональной «1»  $\rightarrow |/\rangle$  ( $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ ). Конкретный вид базиса выбирается для каждого элемента последовательности с помощью ГСЧ2, при этом двоичному нулю, сгенерированному с помощью ГСЧ2, соответствует нормальный базис «+», а единице – диагональный «х». Таким образом, получается последовательность фотонов  $\tilde{\alpha}$  с произвольной ( $0^0$ ,  $90^0$  или  $45^0$ ,  $135^0$ ) поляризацией, которую пользователь **A** пошагово (потактно) посылает пользователю **B** по квантовому (оптическому) каналу связи.

Пользователь **В** имеет один двоичный генератор случайных чисел ГСЧЗ. Пользователь **В** измеряет состояния фотонов (получаемых от **А** по квантовому каналу), выбирая на каждом шаге один из возможных базисов, в зависимости от значения бита получаемого им с помощью ГСЧЗ. При этом двоичному нулю (сгенерированному с помощью ГСЧЗ) соответствует нормальный базис «+», а единице – диагональный «х».

Измерение состояния фотона пользователем **В** приводит к тому, что если для определения вида поляризации фотона им (пользователем **В**) был выбран тот же базис что и при его (фотона) кодировании пользователем **А**, то пользователь **В** с вероятностью 1 определит правильное значение поляризации, если же базис был выбран пользователем **В** неверно, то в качестве результата его измерения будет выступать один из векторов выбранного им базиса с вероятностью  $\frac{1}{2}$ . В результате пользователь **В** получает последовательность  $\beta$ .

После того, как все биты переданы, пользователь **В** сообщает пользователю **А** по открытому классическому каналу, какие базисы он использовал для измерения (раскодирования) фотонов при приеме. После этого пользователь **А** сообщает получателю по тому же открытому классическому каналу, какие базисы пользователь **В** выбрал правильно. Биты, полученные при совпавших измерениях, стороны будут использовать в качестве ключа, все остальные будут отброшены.

В среднем пользователи **А** и **В** будут иметь примерно 50% совпадений базисов, т.е. для ключа будет использована примерно половина передаваемых битов. Примерно в половине случаев пользователь **В** будет использовать ложные базисы.

Всякое подслушивание в квантовом канале увеличивает число ошибок передачи, что легко может быть обнаружено легальными пользователями, если они сравнят по открытому каналу некоторое количество контрольных битов ключа. В этом случае легальные пользователи прекращают сеанс

закрытой связи, и ключ объявляется недействительным.

## Протокол B92

В 1992 году Беннет (фирма IBM) предложил другую схему, отличную от схемы BB84, квантового распределения ключей, названную им B92 [89]. Эта схема также использует:

- квантовый канал, по которому пользователь **A** передает поляризованные в зависимости от значения некоторого параметра  $\alpha$  фотоны пользователю **B**;
- открытый канал, по которому пользователь **B** сообщает пользователю **A** значения некоторого параметра  $\beta$ , который формируется пользователем **B** после каждого своего измерения.

Пользователь **A** имеет двоичный генератор случайных чисел ГСЧ1, с помощью которого он генерирует очередной один бит  $\alpha$  для формирования одного бита ключа.

Если  $\alpha=0$ , то по квантовому каналу связи пользователю **B** направляется фотон с поляризацией "–", то есть фотон в состоянии

$$|\psi\rangle = |0\rangle.$$

Если  $\alpha=1$ , то по квантовому каналу связи пользователю **B** направляется фотон с поляризацией "/", то есть фотон в состоянии

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Пользователь **B** имеет двоичный генератор случайных чисел ГСЧ2, с помощью которого он генерирует очередной один бит  $\tilde{\alpha}$  для выбора базиса для измерения состояния очередного фотона, получаемого им от пользователя **A** по квантовому каналу. При этом двоичному нулю (т.е.  $\tilde{\alpha}=0$ ) соответствует нормальный базис «+», а единице (т.е.  $\tilde{\alpha}=1$ ) – диагональный базис «х». Если при измерении в выбранном базисе получилась «1», то этот бит бракуется. Если получился «0», то в качестве бита ключа пользователь **A** принимает значение  $\alpha$ , а пользователь **B** число  $1-\tilde{\alpha}$ .

### § 3.2. Квантовые криптографические системы на основе двух ресурсов: невозможности клонирования неизвестного квантового состояния и несепарабельности

Примером квантовой криптографической системы, основанной на двух квантовых ресурсах (невозможности клонирования и несепарабельности (см. параграфы 1.1, 1.2 и 1.3 главы 1)) является E91 [96]. Приведем ее краткое описание.

#### Протокол E91

Протокол E91 [95] отличается от протоколов BB84 [88], B92 [89], SARG04 [105] тем, что биты ключа получаются из фундаментально случайного процесса, основанного на свойствах запутанных квантовых состояний.

Основные шаги протокола E91 можно описать следующим образом.

Центр (допускается, что он может совпадать с одним из пользователей) генерирует  $N$  пар фотонов в состоянии Белла  $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$  (которое может быть записано и в другом виде  $\frac{|S_1 S_1\rangle + |S_2 S_2\rangle}{\sqrt{2}}$ , где  $S_1 = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ ,  $S_2 = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ ) и посылает их пользователям **A** и **B**, которые независимо измеряют полученные ими фотоны в случайно выбранных (с помощью генераторов случайных двоичных чисел ГСЧ1 и ГСЧ2 соответственно) каждым из абонентов базисах (нормальном - «+» или диагональном – «х»).

При этом, если в результате измерения были получены состояния  $|-\rangle$  или  $|\backslash\rangle$ , то принимается решение, что значение двоичного бита в соответствующем такте равно 0, если же в результате измерения были получены состояния  $|\parallel\rangle$  или  $|/\rangle$ , то принимается решение, что значение двоичного бита в соответствующем такте равно 1. После этого абоненты обмениваются друг с другом информацией об использованных ими для

измерения базисах по открытому классическому каналу. При этом в качестве элементов общего ключа принимаются биты, выработанные в тех тактах, в которых пользователи **A** и **B** использовали для измерения одинаковые базисы, т.к. при совпадении измерительных базисов пользователи гарантированно получают одинаковые значения измеряемых параметров, вследствие того, что измеряемые ими пары фотонов находятся в несепарабельном состоянии Белла.

Главным преимуществом квантовой криптографической системы E91 перед криптографическими системами, основанными только на ресурсе невозможности клонирования (такими, например, как BB84, B92, SARG04 и т.д.) является то, что ключевая последовательность (гамма) генерируется на основе фундаментально случайного процесса, основанного на свойствах квантового ресурса несепарабельности двухкубитного состояния. Считается, что ключевой материал, сгенерированный на основе классических подходов к формированию и применению случайных процессов по своим криптографическим качествам уступает ключевому материалу, сгенерированному на основе квантовых носителей «истинной» случайности (таких, например, как состояния Белла). На этом вопросе более подробно остановимся в параграфе 3.3. Отметим, что для протокола E91 также значима угроза компрометации ключевого материала, для борьбы с которой применяют тест Белла.

### § 3.3. Квантовая криптографическая система АКМ2017 на основе ресурса несепарабельности состояния спиновый синглет

Из представленных в первых двух параграфах примеров видно, что современные квантовые криптографические системы уязвимы к компрометации ключевого материала. Для борьбы с компрометацией (для обнаружения вмешательства нарушителя в квантовый канал) учитывается статистика ошибок, либо применяется тест Белла. Это означает, что до окончания всех проверок нельзя воспользоваться сформированным ключом. Представленная в настоящем параграфе квантовая криптографическая система АКМ2017 свободна от этого недостатка и обладает ещё целым рядом уникальных свойств, перечисленных далее.

Пусть сгенерировано достаточное число  $N \in \mathbf{N}$  пар кубитов  $A_i B_i$  (где  $i = \overline{1, N}$ ) в состоянии Белла  $|\Psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ , называемым (по историческим причинам) **спиновым синглетом** [61], где  $\mathbf{N}$  – множество натуральных чисел. Кубиты массива пар  $\{A_i B_i \mid i = \overline{1, N}\}$  разделены так, что массив кубитов  $\{A_i \mid i = \overline{1, N}\}$  составляет исходящий шифрблокнот Алисы, а массив кубитов  $\{B_i \mid i = \overline{1, N}\}$  составляет входящий шифрблокнот Боба. Алиса и Боб разделены в пространстве, то есть, проще говоря, живут далеко друг от друга. Может ли быть решена следующая задача?

Алиса должна передать Бобу сообщение, имеющее в двоичном виде представление

$$m = m_1, m_2, \dots, m_L,$$

длины  $L \leq N$  бит, зашифровав его с использованием своего исходящего блокнота, а Боб должен получить и расшифровать сообщение с использованием своего входящего блокнота. При этом предполагается, что Алиса и Боб располагают дополнительно еще общедоступным (открытым) классическим каналам связи.

Ответ: да. Для подтверждения истинности этого ответа изложим

решение данной задачи.

Алиса выбирает случайным образом (например, используя подходящий генератор случайных чисел) единичный вектор  $v = (v_1, v_2, v_3)$  – (то есть вектор  $v$  является нормированным вектором [62]) в трехмерном пространстве над полем действительных чисел  $\mathbf{R}$ .

Вектор  $v$  является **сеансовым (разовым) ключом** и используется для зашифрования только **одного** данного сообщения.

Вектор  $v$  будет передан Бобу после завершения процесса зашифрования сообщения  $m$  вместе с зашифрованным сообщением (например, по предварительной договоренности в начале криптограммы перед зашифрованным сообщением) по классическому каналу.

Будем полагать, что Алиса осуществляет зашифрование сообщения  $m$  последовательно по одному биту.

Для зашифрования двоичного символа  $m_i$ , где  $i = \overline{1, L}$ , Алиса осуществляет следующие действия:

1. выполняет измерение наблюдаемой  $v \cdot \sigma$  для кубита  $A_i$  и в зависимости от результата измерения «1» или «-1» полагает значение  $i$ -го знака  $\gamma_i$  двоичной гаммы

$$\gamma = \gamma_1, \gamma_2, \dots, \gamma_L$$

равным 0 или 1 соответственно;

2. вычисляет значение  $i$ -го знака  $s_i$  криптограммы (зашифрованного сообщения)

$$s = s_1, s_2, \dots, s_L$$

через равенство

$$s_i = m_i \oplus \gamma_i,$$

где  $\oplus$  - знак операции сложения по модулю 2,  $i = \overline{1, L}$ .

3. выполняет измерение наблюдаемой  $\sigma_3 = \sigma_z = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  для кубита  $A_i$  и получает результат измерения «1» или «-1»; если получен результат «1», то кубит  $A_i$  оставляется в том состоянии (то есть в состоянии

$|0\rangle$ ), в котором он оказался после измерения; если же получен результат «-1» (то есть состояние кубита  $A_i$  после измерения  $-|1\rangle$ ), то к кубиту  $A_i$  применяется элемент  $\sigma_1 = \sigma_x = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , после чего он окажется в состоянии  $|0\rangle$ .

Так как биты сообщения  $m$  зашифровываются независимо, то возможно распараллеливание процесса зашифрования без ограничений.

После завершения процесса зашифрования сообщения  $m$  Алиса передает Бобу пару  $(v, s)$  (то есть криптограмму) по открытому классическому каналу связи.

Получив криптограмму  $(v, s)$ , Боб выполняет процедуру расшифрования.

Для расшифрования двоичного символа  $s_i$ , где  $i = \overline{1, L}$ , Боб осуществляет следующие действия:

1. выполняет измерение наблюдаемой  $v \cdot \sigma$  для кубита  $B_i$  и получает результат измерения «1» или «-1», противоположный в соответствии с утверждением 1.5.20 (пункт а) с результатом, полученным Алисой при зашифровании знака  $m_i$ ; далее Боб, в зависимости от полученного результата измерения «1» или «-1», полагает значение  $i$ -го знака  $\gamma_i$  двоичной гаммы

$$\gamma = \gamma_1, \gamma_2, \dots, \gamma_L$$

равным 1 или 0 соответственно (напомним, что у Алисы знак гаммы был равен 0 при получении результата ее измерения «1», а при результате измерения «-1») знак гаммы был равен 1);

2. вычисляет значение  $i$ -го знака  $m_i$  сообщения

$$m = m_1, m_2, \dots, m_L$$

через равенство

$$m_i = s_i \oplus \gamma_i,$$

где  $\oplus$  - знак операции сложения по модулю 2;

3. выполняет измерение наблюдаемой  $\sigma_z = \sigma_z = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  для кубита  $V_i$  и получает результат измерения «1» или «-1»; если получен результат «1», то кубит  $V_i$  оставляется в том состоянии (то есть в состоянии  $|0\rangle$ ), в котором он оказался после измерения; если же получен результат «-1» (то есть состояние кубита  $V_i$  после измерения  $-|1\rangle$ ), то к кубиту  $V_i$  применяется элемент  $\sigma_x = \sigma_x = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , после чего он окажется в состоянии  $|0\rangle$ .

Так как биты сообщения  $m$  расшифровываются независимо, то возможно распараллеливание процесса расшифровки без ограничений.

Еще раз отметим, что в изложенном описании квантовой криптографической системы использовалось то, что **знаки двоичных гамм, сформированных и Алисой и Бобом совпадают**. Это следует из пункта а) утверждения 1.4.20.

Описанную квантовую криптографическую система называется квантовая криптографическая система **АКМ2017** ([25]).

Вначале обсудим преимущества квантовой криптографической системы **АКМ2017** по сравнению с известными системами, такими как BB84, E91, B92, SARG и т. д.:

1. исключена процедура определения значения гаммы путем проведения измерений (детектирования) в разных случайным образом выбираемых базисах, что исключает необходимость дополнительной передачи информации о выбранных базисах измерений (детекторах) по открытому классическому каналу связи;

2. для **АКМ2017** ключевой материал (гамма) не накапливается у абонентов, а формируется при проведении процессов зашифрования и расшифрования;

3. у **АКМ2017** более экономичный расход ключевого материала в том смысле, что для генерации  $n$  знаков гаммы в известных квантовых криптографических системах необходимо передать с помощью квантового

канала в среднем от  $2n$  посылок (фотонов или других частиц); каждому абоненту; этот показатель обеспечения ключевыми носителями в случае **АКМ2017** в два раза меньше и режим обеспечения ключевыми носителями имеет принципиальные отличия;

4. для квантовой криптографической системы **АКМ2017** существует принципиальная возможность с использованием операции *свопинг* (подкачка) дистанционной (например, используя космические спутники связи, аналогичные известным китайским спутникам квантовой связи) регенерации несепарабельных состояний (спиновых синглетов) использованных пар кубитов и, тем самым, повысить надежность шифрованной связи; для известных квантовых криптографических систем такая возможность отсутствует;

5. более высокий уровень стойкости при компрометации ключевых носителей.

Теперь обратимся к преимуществам квантовой криптографической системы **АКМ2017** по сравнению с классическими криптографическими системами.

Сравнивать **АКМ2017** с асимметричными криптографическими системами или с симметричными криптографическими системами с ограниченным ключом (не являющимися теоретически стойкими) не имеет смысла. Это обусловлено тем, что **АКМ2017** является совершенной криптографической системой [27], [44], [80]. А перечисленные криптографические системы не являются совершенными шифрами [27], [44], [80], что влечет их уязвимость, например, при «силовой» атаке типа «тотальный перебор ключа», который реален, как предполагают, при применении в целях дешифрования квантовых компьютеров [48], [53].

Совершенство [27], [28], [44], [80] криптографической системы **АКМ2017** следует из того, что по сути дела – это совершенная криптографическая система «одноразовый шифр-блокнот» (криптографическая система Гилберта Вернама) [80], [81] с улучшенными

шифровальными блокнотами на основе использования квантового ресурса несепарабельности двухкубитного состояния спиновый синглет. Эти улучшения влекут за собой принципиально новые полезные качества, отсутствующие у криптографической системы «одноразовый шифр-блокнот». Прежде чем обсудить эти новые качества приведем краткое описание криптографической системы «одноразовый шифр-блокнот» [27], [28], [44], [80], [81].

Алгоритм шифрования Вернама (то есть криптографическая система «одноразовый шифр-блокнот») заключается в том, что представленная в двоичном коде последовательность открытого текста побитово складывается по модулю 2 с ключом (называемым гаммой в российской криптографической литературе) – случайной двоичной последовательностью. Случайный набор символов ключа, написанных на листах бумаги и сброшюрованных в виде блокнота, используется только один раз и только для зашифрования одного сообщения. Отсюда, очевидно, и название шифра - «одноразовый шифрблокнот». Закончив шифровать сообщение, отправитель уничтожает использованные страницы блокнота. В свою очередь получатель, используя другой, точно такой же блокнот, осуществляет расшифрование. Расшифровав сообщение, он уничтожает соответствующие страницы блокнота. Итак, для зашифрования каждого нового сообщения используются новые двоичные символы ключа и их количество совпадает с длиной шифруемого сообщения.

Гилберт Вернам не представил строгих доказательств того, что предложенный им шифр обладает высокими криптографическими качествами. Строгое математическое обоснование теоретической стойкости шифра Вернама осуществил К. Шеннон, опубликовавший в 1949 году основные положения теоретической криптографии [80].

Перехват сообщения, зашифрованного с помощью шифра «одноразовый шифрблокнот», не содержит для криптоаналитика противника никакой информации, если ключ ему неизвестен и этот ключ обладает хорошими вероятностно-статистическими качествами (то есть является, в определенном

смысле, совершенно случайным). Кроме этого, как было сказано выше, количество двоичных символов ключа, используемых для шифрования сообщения, совпадает с длиной шифруемого сообщения. Это означает, что использование шифра «одноразовый шифрблокнот» для защиты больших объемов информации требует огромных издержек, связанных с производством, распределением, хранением и уничтожением ключевых материалов. Таким образом, критичной для практических применений компонентой шифра «одноразовый шифрблокнот» является его система управления ключевой информацией, под которой понимается система, включающая в себя производство, распределение, хранение, использование и уничтожение ключевых материалов [27], [68].

Кроме того, компрометация шифровальных блокнотов приводит к несанкционированному полному доступу к защищаемой информации. То есть при компрометации шифровальных блокнотов стойкость криптографической системы «одноразовый шифрблокнот» - нулевая (образно говоря), а в случае криптографической системы **АКМ2017**, как будет показано в дальнейшем, ситуация намного лучше. Это одно из принципиальных новых преимуществ, присущих **АКМ2017**. Есть и другие. Не претендуя на исчерпывающую полноту (так как будущие исследования могут расширить и уточнить положительные свойства **АКМ2017**) укажем на следующие преимущества криптографической системы **АКМ2017** по сравнению с классической криптографической системой «одноразовый шифрблокнот».

1) В случае **АКМ2017** ключевая последовательность (гамма) генерируется на основе фундаментально случайного процесса, основанного на свойствах квантового ресурса несепарабельности двухкубитного состояния спиновый синглет, здесь, как говорит известный физик Николя Жизан, «истинная» случайность [43]. В случае «одноразовый шифрблокнот» используются ГСЧ, основанные на классических подходах к исследованию случайных процессов [31], [32], [54].

2) В случае **АКМ2017** появляется еще одна степень усиления стойкости,

отсутствующая в случае криптографической системы «одноразовый шифрблокнот» - это сеансовый ключ в виде единичного вектора  $v = (v_1, v_2, v_3)$  – в трехмерном пространстве над полем действительных чисел  $\mathbf{R}$ ; эта степень усиления стойкости выражается в следующем: при компрометации ключевых блокнотов стойкость криптографической системы «одноразовый шифрблокнот» становится, образно говоря, нулевой. В случае **АКМ2017** ситуация более благоприятная, в том плане, что стойкость в определенном смысле сохраняется.

3) Как было отмечено выше, для квантовой криптографической системы **АКМ2017** существует принципиальная возможность, с использованием операции *свопинг* (подкачка) [49], дистанционной регенерации носителей-кубитов использованных квантовых шифровальных блокнотов в состояние, пригодное для повторного использования данных квантовых шифровальных блокнотов. Тем самым, удаётся повысить надежность шифрованной связи. Для криптографической системы «одноразовый шифрблокнот» такая возможность отсутствует.

На первой из перечисленных выше позиций остановимся более подробно в этом параграфе. Положения пунктов 2 и 3 более подробно рассмотрим в отдельных параграфах 3.4 и 3.5.

Ранее было отмечено, в случае **АКМ2017** ключевая последовательность (гамма) генерируется на основе фундаментально случайного процесса, основанного на свойствах квантового ресурса несепарабельности двухкубитного состояния спиновый синглет. В случае же криптографической системы «одноразовый шифрблокнот» используются методы формирования шифровальных блокнотов, основанные на классических подходах к исследованию случайных процессов. Считается, что ключевой материал, представленный в таких шифровальных блокнотах по своим криптографическим качествам уступает ключевому материалу, сгенерированному на основе квантовых носителей «истинной» случайности.

К их числу относятся, например, состояния Белла и, в частности, спиновый синглет.

В классической физике считается, что результат любого измерения предопределен, что он в известном смысле записан в физическом состоянии системы, подвергающейся измерению [45], [58], [73]. Вероятности «появляются» только из-за того, что экспериментатору (наблюдателю и т.п., то есть субъекту проводящему измерение) *точное физическое состояние неизвестно*. Эта неизвестность приводит к необходимости использовать статистические методы и вероятностный расчет в соответствии с аксиомами Колмогорова [31], [32], [54]. Что касается псевдослучайных последовательностей, генерируемых компьютерами, то здесь генерируемые числовые последовательности таковы, что отношение между одним псевдослучайным числом и следующим заранее предопределено соответствующим правилом (полное отсутствие случайности), которое достаточно сложно для того, чтобы его можно было предугадать.

В квантовой физике результат измерения не предопределен никаким субъективным фактором, даже если *точное физическое состояние вполне известно*. В физическом состоянии системы, над которой производится измерение, записана лишь «предрасположенность» (более точно амплитуда) к проявлению того или иного возможного результата измерения. Эта предрасположенность не удовлетворяет [43] аксиомам Колмогорова ([31], [32], [54]). Вероятность каждого из двух значений результата первого однокубитного измерения, над каждой квантовой системой из двух кубитов в состоянии спиновый синглет, составляющих в совокупности два массива исходящий и входящий шифрблокнот криптографической системы **АКМ2017**, должна быть равна 0,5. И возможные отклонения никак не связаны с отсутствием субъективных знаний о природе процесса, а определяются лишь точностью применяемых приборов как для формирования и хранения двухкубитных квантовых систем в состоянии спиновый синглет в виде двух разных массивов - исходящий и входящий шифрблокноты, так и точностью

приборов, используемых для измерения. Если даже допустить, что применяемые приборы идеальны, все равно результат измерения случаен и ничем не предопределен. Невозможно убрать случайность путем совершенствования приборов [43].

Истинность случайности ключевого материала в **АКМ2017** объясняется, прежде всего, отсутствием «даже в принципе» субъективного фактора – неполноты знаний о задействованных процессах. Деструктивное влияние этого субъективного фактора в классической физике допускается как наличие случайности – не истинной случайности, которую можно нивелировать путем устранения неполноты необходимых знаний [43].

Теоретическая стойкость шифра Вернама достигается только если ключ представляет собой случайную равновероятную последовательность. Последнее, а значит и теоретическая стойкость, есть «врождённое» свойство квантовой криптографической системы **АКМ2017**.

### § 3.4. Сеансовый ключ квантовой криптографической системы АКМ2017 как еще одна степень усиления криптографической стойкости

Как следует из описания криптографической системы АКМ2017, представленного в параграфе 3.3, сеансовым ключом (синхропосылкой) является единичный вектор  $v = (v_1, v_2, v_3)$  в трехмерном пространстве над полем действительных чисел  $\mathbf{R}$ , выбираемый Алисой (стороной, реализующей процесс зашифрования) случайным образом, используя подходящий генератор случайных чисел. Вектор  $v$  передается в открытом (общедоступном) виде Бобу после завершения процесса зашифрования сообщения  $m$  вместе с зашифрованным сообщением (например, по предварительной договоренности в начале криптограммы перед зашифрованным сообщением) по классическому каналу.

Как и криптографическая система Вернама (то есть криптографическая система «одноразовый шифр-блокнот»), криптографическая система АКМ2017 является совершенным шифром. Однако в плане стойкости при компрометации шифрблокнотов они принципиально отличаются.

В криптографической системе Вернама компрометация исходящего или входящего шифрблокнота противником (субъектом, чей доступ к открытому тексту и ключам является несанкционированным) дает ему возможность полного доступа к открытому тексту. То есть полное отсутствие стойкости после компрометации исходящего или входящего шифрблокнота.

В случае с криптографической системой АКМ2017 ситуация принципиально иная по сравнению с криптографической системой Вернама. Именно наличие сеансового ключа придает криптографической системе АКМ2017 новое качество стойкости при компрометации шифровальных блокнотов, отсутствующее у криптографической системы Вернама. Конечно при этом (то есть при компрометации) стойкость криптографической системы АКМ2017 понижается. Она перестает удовлетворять условиям **теоретически стойкого** (совершенного) шифра. Однако ее **идеальная стойкость**

сохраняется. Для доказательства последнего утверждения напомним, следуя [27], [28], [57], [74], [75], [76], [80], необходимые определения из криптографии.

Пусть  $X$ ,  $K$ ,  $Y$  – конечные множества, называемые множеством открытых текстов, множеством ключей и множеством шифрованных текстов (криптограмм) соответственно;  $|X| > 1$ ,  $|K| > 1$ ;

$E_k: X \rightarrow Y$  – правило зашифрования на ключе  $k \in K$ ,  $E_k(X)$   
 $= \{E_k(x): x \in X\}$ ,  $E = \{E_k: k \in K\}$ ;

$D_k: E_k(X) \rightarrow X$  – правило расшифрования на ключе  $k \in K$ ,  $D$   
 $= \{D_k: k \in K\}$ .

**Криптографической системой** или **шифром** называется совокупность

$$\Sigma_A = (X, K, Y, E, D),$$

введенных выше множеств, которые удовлетворяют следующим условиям:

1) для любых  $x \in X$  и  $k \in K$  выполняется равенство

$$D_k(E_k(x)) = x;$$

2)  $Y = \bigcup_{k \in K} E_k(X)$ .

Часто каждое  $k \in K$  представляется в виде  $k = (k_z, k_p)$ , где  $k_z$  – ключ зашифрования,  $k_p$  – ключ расшифрования. Тогда  $E_k$  понимается как отображение  $E_{k_z}$ , а  $D_k$  – как отображение  $D_{k_p}$ . В этом случае, если для любых  $k = (k_z, k_p) \in K$  выполняется равенство  $k_z = k_p$  то криптографическая система  $\Sigma_A$  называется **симметричной криптографической системой**; если же для любых  $k = (k_z, k_p) \in K$  выполняется неравенство  $k_z \neq k_p$  то криптографическая система  $\Sigma_A$  называется **асимметричной криптографической системой**. Далее будем рассматривать только симметричные криптографические системы.

Неформально, **криптографическая система** или **шифр** – это совокупность множеств возможных открытых текстов (то, что

зашифровывается), возможных ключей (то есть сменных элементов, с помощью чего осуществляется процедура зашифрования), возможных шифрованных текстов (то, что является результатом зашифрования), правил зашифрования и правил расшифрования.

По сути, данное определение вводит математическую модель, отражающую основные свойства реальных шифров. В силу этого, как правило, реальный шифр и его математическую модель принято отождествлять. При этом по отношению к совокупности  $\Sigma_A = (X, K, Y, E, D)$  используют также понятие **алгебраическая модель шифра**.

**Вероятностной моделью шифра** называется совокупность

$$\Sigma_B = (X, K, Y, E, D, P(X), P(K)),$$

где  $X, K, Y, E, D$  – множества, введенные выше, а  $P(X) = \{p_X(x): x \in X\}$  и  $P(K) = \{p_K(k): k \in K\}$  – вероятностные распределения на множествах  $X$  и  $K$  соответственно, называемые **априорными распределениями вероятностей** на множестве открытых текстов  $X$  и множестве ключей  $K$ . При этом предполагается, что распределения  $P(X)$  и  $P(K)$  независимы и для любых  $x \in X$  и  $k \in K$  для **априорных вероятностей**  $p_X(x)$ ,  $p_K(k)$  выполняется неравенства  $p_X(x) > 0$ ,  $p_K(k) > 0$ .

На основе заданных априорных распределений вероятностей  $P(X)$ ,  $P(K)$  и условия их независимости однозначно вычисляются распределения на множестве шифрованных текстов  $Y$ , а также соответствующие условные распределения:

$$p_Y(y) = \sum_{\{(x,k) \in X \times K: E_k(x)=y\}} p_X(x) \cdot p_K(k),$$

$$p_{Y/X}(y/x) = \sum_{\{k \in K: E_k(x)=y\}} p_K(k),$$

$$p_{Y/K}(y/k) = \sum_{\{x \in X: E_k(x)=y\}} p_X(x),$$

$$p_{X/Y}(x/y) = p_{Y/X}(y/x) \frac{p_X(x)}{p_Y(y)},$$

$$p_{K/Y}(k/y) = p_{Y/K}(y/k) \frac{p_K(k)}{p_Y(y)}.$$

Для любых  $x \in X$  и  $y \in Y$  условная вероятность  $p_{X/Y}(x/y)$  называется

**апостериорной вероятностью** открытого текста  $x$  при условии заданного шифрованного текста  $y$ .

По отношению к  $\Sigma_B$  также в зависимости от контекста часто используются понятия **криптографическая система** или **шифр**.

Криптографическая система

$$\Sigma_B = (X, K, Y, E, D, P(X), P(K))$$

называется **теоретически стойкой (совершенной или совершенно стойкой)** криптографической системой, если при любых  $x \in X$  и  $y \in Y$  выполняется равенство

$$p_{X/Y}(x/y) = p_X(x).$$

Другими словами, в совершенной (теоретически стойкой) криптографической системе апостериорные вероятности открытых текстов совпадают с их априорными вероятностями. Таким образом, теоретическая стойкость криптографической системы означает статистическую независимость открытых и шифрованных текстов. Иначе говоря, при использовании теоретически стойкой криптографической системы распределение вероятностей на множестве открытых текстов  $X$  после перехвата криптограммы  $y \in Y$  (апостериорное распределение вероятностей) не отличается от распределения вероятностей  $P(X)$  до получения перехваченной криптограммы  $y \in Y$  (от априорного распределения вероятностей).

Криптографическая система называется **идеально стойкой** криптографической системой [74], [75], [76], [80], если невозможно определить однозначно открытый текст при известном шифрованном тексте сколь угодно большой длины.

Примером идеально стойкой криптографической системы служит любая теоретически стойкая криптографическая система. Обратное неверно, то есть не всякая идеально стойкая криптографическая система является теоретически стойкой.

Получение криптоаналитиком (противником) открытого текста по

шифрованному тексту (предполагается, что ключ расшифрования криптоаналитику неизвестен) называется **дешифрованием**.

**Вернемся теперь к доказательству выше декларированного утверждения, что криптографическая система АКМ2017 остается идеально стойкой криптографической системой после компрометации ее исходящего или входящего шифрблокнота.** Как и в параграфе 3.3 Алиса – сторона, выполняющая зашифрование сообщения и передающая полученную криптограмму Бобу по открытым (общедоступным) каналам связи: Боб – сторона, принимающая криптограмму и осуществляющая его расшифрование. Кроме этих персонажей введем еще Еву, осуществляющую действия по компрометации шифрблокнотов и пытающуюся дешифровать перехваченную в канале связи криптограмму.

Для определенности полагаем, что действия Евы по компрометации шифрблокнотов заключаются в проведении измерений в вычислительном базисе  $\{|0\rangle, |1\rangle\}$  над каждым кубитом из массива, составляющего исходящий шифрблокнот Алисы или входящий шифрблокнот Боба.

Так как в криптографической системе АКМ2017 все кубиты, составляющие массивы шифрблокнотов, после их использования по назначению переводятся в состояние  $|0\rangle$ , то содержательными являются только те действия Евы по компрометации, которые осуществлены до использования шифрблокнотов по назначению. При этом неважно какой из блокнотов – исходящий шифрблокнот Алисы или входящий блокнот Боба подвергался компрометации. И тот и другой случай дают Еве одинаково полную информацию о состояниях из базиса  $\{|0\rangle, |1\rangle\}$ , в которых находятся кубиты из шифровальных блокнотов Алисы и Боба после действий Евы по компрометации. Поэтому для определенности будем полагать, что Ева, перехватив криптограмму, отправленную Алисой Бобу, пытается ее дешифровать на основе информации, полученной при компрометации шифрблокнота Алисы. По этой информации Ева однозначно может разделить

двоичные символы шифрованного текста (криптограммы) на два множества  $M_0$  и  $M_1$ :

в множестве  $M_0$  – все двоичные символы шифрованного текста, полученные с использованием гаммы, сгенерированной путем измерения Алисой кубита, находящегося в состоянии  $|0\rangle$  (после выполнения Евой действий по компрометации);

в множестве –  $M_1$  все двоичные символы шифрованного текста, полученные с использованием гаммы, сгенерированной путем измерения Алисы кубита, находящегося в состоянии  $|1\rangle$  (после выполнения Евой действий по компрометации).

Рассмотрим множество  $M_0$ . Зададимся вопросом, **что Еве может быть известно о вероятностных свойствах гаммы, использованной Алисой при формировании множества  $M_0$ ?**

После перехвата криптограммы Еве становится доступным сеансовый ключ  $v = (v_1, v_2, v_3)$  – единичный вектор (то есть вектор  $v$  является нормированным вектором [62]) в трехмерном пространстве над полем действительных чисел  $\mathbf{R}$ . Гамму, использованную для формирования элементов множества  $M_0$ , Алиса получила путем измерения наблюдаемой  $v \cdot \sigma$  над кубитом, находящимся в состоянии  $|0\rangle$ , где

$$v \cdot \sigma = v_1 \sigma_1 + v_2 \sigma_2 + v_3 \sigma_3$$

$\sigma_1, \sigma_2, \sigma_3$  – вентили Паули;

Тогда, как следует из пункта в) утверждения 1.5.20, можно сделать вывод о том, что Еве известно распределение знаков гаммы, использованной Алисой при формировании множества  $M_0$ . Точнее, Еве известно, что гамма сгенерирована по схеме простого источника без памяти с вероятностями нуля и единицы

$$p_0 = P(0) = \frac{1+v_3}{2}, \quad (3.4.1)$$

и

$$q_0 = 1 - p_0 = P(1) = \frac{1 - v_3}{2}. \quad (3.4.2)$$

Аналогично, рассмотрев множество  $M_1$  и задавшись вопросом, **что Еве может быть известно о вероятностных свойствах гаммы, использованной Алисой при формировании множества  $M_1$** , можно сделать вывод о том, что Еве известно распределение знаков гаммы, использованной Алисой при формировании множества  $M_1$ . Точнее, Еве известно, что гамма сгенерирована по схеме простого источника без памяти с вероятностями нуля и единицы

$$p_1 = P(0) = \frac{1 - v_3}{2}, \quad (3.4.3)$$

и

$$q_1 = 1 - p_1 = P(1) = \frac{1 + v_3}{2}. \quad (3.4.4)$$

Выше указанные источники имеют одну и ту же энтропию

$$H(v_3) = - \left( \frac{1 + v_3}{2} \log_2 \frac{1 + v_3}{2} + \frac{1 - v_3}{2} \log_2 \frac{1 - v_3}{2} \right).$$

Далее обратимся к асимптотическим методам теории информации [80], точнее к некоторой качественной интерпретации теоремы Шеннона о кодировании при отсутствии шума [10], [28], [35], [42], [63], [66], [72]. В соответствии с с потребностями решаемых задач в данной работе, займемся рассмотрением только случая двоичного источника сообщений, который генерирует 0 и 1 потактно по схеме независимых испытаний, соответственно, с вероятностями  $p$  и  $q$ , где  $p \geq 0$ ,  $q \geq 0$ ,  $p + q = 1$ .

Теорема Шеннона о кодировании при отсутствии шума отвечает на следующий вопрос: какие минимальные ресурсы необходимы для того, чтобы сохранять информацию, получаемую из источника, так, чтобы впоследствии можно было ее восстановить?

Оказывается, что для хранения двоичной вектор-строки длины  $\ell$  требуется (в среднем)  $\ell H(X)$  битов, где  $X$  – случайная величина, принимающая значения 0 и 1 с вероятностями  $p$  и  $q$  соответственно;  $H(X)$  – энтропия случайной величины  $X$  (называемая также энтропией источника),  $H(X) = - (p \log_2 p + q \log_2 q)$ . Этот результат известен как теорема Шеннона о кодировании при отсутствии шума. В связи с задачами нашей работы полезно

понять основную идею Шеннона, на которой базируется эта теорема. Она заключается в следующем.

При достаточно больших значениях натурального числа  $\ell$  все сообщения, т. е. двоичные векторы-строки длины  $\ell$ , генерируемые источником, можно разбить на два класса: первый класс  $K_{1\ell}$  – это класс типичных векторов-строк, содержащих примерно  $\ell p$  нулей и примерно  $\ell q$  единиц; второй класс  $K_{2\ell}$  – это класс атипичных векторов-строк, то есть тех векторов-строк, которые не попали в класс  $K_{1\ell}$ . Вероятность того, что сгенерированное источником сообщение длины  $\ell$  атипично, т.е. принадлежит классу  $K_{2\ell}$ , асимптотически (т.е. в пределе при  $\ell \rightarrow \infty$ ) мала. Таким образом, атипичные векторы-строки генерируются источником редко, в отличие от типичных, так как при больших значениях  $\ell$  с большой вероятностью доля символов 0 на выходе источника будет равна  $p$ , а доля символов 1 будет равна  $q$ , что согласуется с определением типичных векторов-строк. Вероятность генерации источником любой одной типичной вектор-строки примерно равна  $p^{\ell p} \cdot q^{\ell q}$ . Значение логарифма по основанию 2 от этой величины равно  $(-\ell H(X))$ . Следовательно, вероятность генерации источником любой одной типичной вектор-строки примерно равна  $2^{-\ell H(X)}$ . Поскольку полная вероятность всех типичных векторов-строк длины  $\ell$  не может быть больше единицы, то количество типичных двоичных векторов-строк не может быть больше  $2^{\ell H(X)}$ . Идея Шеннона заключается в том, что кодированию с целью сжатия должны подвергаться только сообщения из класса  $K_{1\ell}$ . Отсюда следует довольно простая схема сжатия данных на выходе источника сообщений. Если источником сгенерировано сообщение, относящееся к классу  $K_{2\ell}$ , то оно считается ошибкой и игнорируется. При больших значениях числа  $\ell$  это случается редко, как указано выше. Если же сгенерировано сообщение из класса  $K_{1\ell}$ , то оно сжимается в соответствии с предварительно выбранной схемой кодирования путем его замены на

двоичную вектор-строку из  $\ell H(X)$  битов. Поскольку существует не более  $2^{\ell H(X)}$  типичных сообщений длины  $\ell$ , то для их кодирования (с возможностью последующего однозначного декодирования) двоичных векторов-строк длины  $\ell H(X)$  достаточно; более того, установлено, что число  $\ell H(X)$  невозможно уменьшить, то есть, всех двоичных векторов-строк фиксированной длины, меньшей, чем  $\ell H(X)$ , не хватает для кодирования всех типичных сообщений длины  $\ell$ . При больших значениях  $\ell$  данная схема сжатия работает корректно (то есть, без ошибок) с вероятностью, приближающейся к единице [10], [42], [66], [72], [80].

Таким образом, чтобы передать, по существу, всю информацию, переносимую вектор-строкой из  $\ell$  битов, достаточно выбрать двоичный блоковый код  $B$ , присваивающий кодовое слово длины  $\ell H(X)$  битов каждой типичной вектор-строке из  $\ell$  битов. Этот блоковый равномерный код  $B$  имеет  $2^{\ell H(X)}$  слов одинаковой длины  $\ell H(X)$  битов, появляющихся с одинаковой вероятностью  $2^{-\ell H(X)}$  и называется оптимальным блоковым равномерным кодом [10], [42], [66], [72], [80]. Поскольку  $0 \leq H(X) \leq 1$  при  $0 \leq p \leq 1$  и  $H(X) = 1$  только при  $p=0,5$ , то оптимальный блоковый код  $B$  сжимает сообщение при любом  $p \neq 0,5$ . В силу того, что вероятность каждого слова в коде  $B$  равна  $2^{-\ell H(X)}$ , можно полагать, что каждое кодовое слово генерируется в течение  $\ell H(X)$  тактов источником сообщений, который генерирует 0 и 1 потактно по схеме независимых испытаний с одной и той же вероятностью 0,5 [72].

Отсюда, возвращаясь к нашей задаче, можно указать, что число возможных вариантов гаммы, использованной для формирования элементов множеств  $M_0$  и  $M_1$  равно  $2^{n_0 H(v_3)}$  и  $2^{n_1 H(v_3)}$  соответственно, где  $n_0$  и  $n_1$  – достаточно большие числа, равные мощностям множеств  $M_0$  и  $M_1$ , число  $n_0 + n_1$  равно длине  $n$  криптограммы. При этом каждый вариант гаммы для  $M_0$  имеет одну и ту же вероятность  $2^{-n_0 H(v_3)}$ .

Аналогично, каждый вариант гаммы для  $M_1$  имеет одну и ту же вероятность  $2^{-n_1 H(v_3)}$ .

Отсюда следует, что потенциальное число различных возможных вариантов гаммы Алисы для зашифрования всей криптограммы равно  $2^{nH(v_3)}$  при достаточно большом значении  $n$ , где, напомним,  $n$  - длина криптограммы. При этом каждый вариант гаммы имеет одну и ту же вероятность  $2^{-nH(v_3)}$ . Поэтому для Евы открытый текст доступен в количестве вариантов, равном  $2^{nH(v_3)}$  и отсутствует критерий выбора среди них истинного открытого текста. Таким образом, криптографическая система **АКМ2017** является **идеально стойкой** криптографической системой, так как при ее применении невозможно определить однозначно открытый текст при известном зашифрованном тексте сколь угодно большой длины. И это обусловлено наличием сеансового ключа, введение и применение которого возможно в связи с уникальными свойствами квантового состояния **спиновый синглет**, на основе которого построена криптографическая система **АКМ2017**.

### § 3.5. Восстановление состояний носителей-кубитов для формирования ключевой информации в криптографической системе АКМ2017

Из описания криптографической системы АКМ2017, представленного в параграфе 3.3, следует, что носители-кубиты для формирования ключевой информации после их использования не уничтожаются, а в обязательном порядке устанавливаются в состоянии  $|0\rangle$ . Возникает вопрос – **существует ли принципиальная возможность их восстановления в состоянии, пригодном для повторного использования?**

Ответ положительный. Восстановление пар носителей-кубитов для формирования ключевой информации в состоянии спиновый синглет можно осуществить дистанционно с использованием внешнего источника пар запутанных фотонов (например, бифотонов [69]) в состоянии спиновый синглет (например, с использованием спутников, подобных тем, что построены в китайско-европейском проекте 2013-2017 гг. [50]) с помощью процедуры, близкой к процедуре «свопинг» - перенос перепутывания [49]. Схематично процедура состоит из двух частей и для одной использованной пары носителей кубитов А и В в состоянии  $|0\rangle$  выглядит следующим образом.

Часть 1. В начале у Алисы и у Боба два кубита А и В, каждый из которых находится в состоянии  $|0\rangle$ .

Алиса и Боб удалены в пространстве друг от друга и они самостоятельно и заблаговременно используя по одному дополнительному кубиту  $A_1$  и  $B_1$  в состоянии также  $|0\rangle$  создают соответственно пары  $A_1A$  (пара кубитов Алисы) и  $B_1B$  (пара кубитов Боба), каждая из которых находится в состоянии Белла

$$|\Psi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Приведем пошагово соответствующий алгоритм действий на примере Алисы.

На входе алгоритма два кубита  $A_1A$  в состоянии  $|\Psi_0^{(2)}\rangle = |00\rangle$ .

**Шаг 1.** Алиса пропускает кубит  $A_1$  через элемент Адамара  $H$  [63], что равносильно применению к состоянию  $|\Psi_0^{(2)}\rangle$  линейного преобразования с матрицей  $H \otimes I_2$ , где  $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ ,  $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $\otimes$  - знак тензорного произведения. В результате квантовая система  $A_1A$  переходит в состояние  $|\Psi_1^{(2)}\rangle$ , задаваемое равенством:

$$|\Psi_1^{(2)}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

**Шаг 2.** Алиса пропускает свои кубиты  $A_1$  и  $A$  через элемент CNOT [63]. Это равносильно тому, что к состоянию  $|\Psi_1^{(2)}\rangle$  применяется линейное преобразование с матрицей CNOT, где  $\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ . В результате получается состояние  $|\Psi_2^{(2)}\rangle$  квантовой системы  $A_1A$ , задаваемое равенством:

$$|\Psi_2^{(2)}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Psi_{00}\rangle.$$

Аналогично, Боб также создает пару кубитов в состоянии  $B_1B$  в состоянии

$$|\Psi_2^{(2)}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Psi_{00}\rangle.$$

**Часть 2.** Внешний источник генерирует два кубита (например, два запутанных фотона)  $A_2B_2$  в состоянии Белла спиновый синглет

$$|\Psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

и направляет кубит  $A_2$  Алисе и кубит  $B_2$  Бобу.

Приведем пошагово соответствующий алгоритм действий вначале на примере Алисы, а затем на примере Боба. Не имеет принципиального значения очередность действий Алисы и Боба. Для определенности положим, что **Алиса** действует первой.

На входе алгоритма четыре кубита  $B_2A_2A_1A$  в состоянии

$$\begin{aligned} |\psi_0^{(4)}\rangle &= \frac{|10\rangle - |01\rangle}{\sqrt{2}} \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \\ &= \frac{1}{2} (|1000\rangle + |1011\rangle - |0100\rangle - |0111\rangle). \end{aligned}$$

**Шаг 1.** Алиса пропускает свои кубиты  $A_2$  и  $A_1$  через элемент CNOT [63].

Это равносильно тому, что к состоянию  $|\psi_0^{(4)}\rangle$  применяется линейное преобразование с матрицей  $I_2 \otimes \text{CNOT} \otimes I_2$ , где  $\otimes$  - знак тензорного

произведения,  $\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ ,  $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . В результате получается

состояние  $|\psi_1^{(4)}\rangle$  квантовой системы  $B_2A_2A_1A$ , задаваемое равенством:

$$|\psi_1^{(4)}\rangle = \frac{1}{2} (|1000\rangle + |1011\rangle - |0110\rangle - |0101\rangle).$$

**Шаг 2.** Алиса пропускает свой кубит  $A_2$  через элемент Адамара H [63],

что равносильно применению к состоянию  $|\psi_1^{(4)}\rangle$  линейного преобразования

с матрицей  $I_2 \otimes H \otimes I_2 \otimes I_2$ , где  $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ . В результате квантовая система

$B_2A_2A_1A$ , переходит в состояние  $|\psi_2^{(4)}\rangle$ , задаваемое равенством:

$$\begin{aligned} |\psi_2^{(4)}\rangle &= \\ &= \frac{1}{2} (|1\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle |0\rangle + |1\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}} |1\rangle |1\rangle - |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} |1\rangle |0\rangle - \end{aligned}$$

$$|0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} |0\rangle |1\rangle),$$

что, перегруппировав члены, можно переписать следующим образом

$$\begin{aligned} |\psi_2^{(4)}\rangle &= \\ &= \frac{1}{2\sqrt{2}} (|1\rangle|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|1\rangle|1\rangle + |1\rangle|1\rangle|1\rangle|1\rangle - \\ &- |0\rangle|0\rangle|1\rangle|0\rangle + |0\rangle|1\rangle|1\rangle|0\rangle - |0\rangle|0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle|1\rangle) = \\ &= \frac{1}{2} \left( -\frac{1}{\sqrt{2}} (|0\rangle|00\rangle|1\rangle - |1\rangle|00\rangle|0\rangle) - \frac{1}{\sqrt{2}} (|0\rangle|01\rangle|0\rangle - |1\rangle|01\rangle|1\rangle) \right) + \\ &+ \frac{1}{\sqrt{2}} (|0\rangle|10\rangle|1\rangle + |1\rangle|10\rangle|0\rangle) + \frac{1}{\sqrt{2}} (|0\rangle|11\rangle|0\rangle + |1\rangle|11\rangle|1\rangle). \end{aligned}$$

**Шаг 3.** Алиса проводит измерение над своими двумя кубитами  $A_2$  и  $A_1$  в вычислительном базисе из векторов  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  и  $|11\rangle$  [63]. В результате этого измерения квантовая система из четырех кубитов  $B_2A_2A_1A$  может иметь следующие свои состояния и состояния своих подсистем:

с вероятностью  $\frac{1}{4}$  квантовая система  $B_2A_2A_1A$  - в состоянии

$$\frac{1}{\sqrt{2}} (|0\rangle|00\rangle|1\rangle - |1\rangle|00\rangle|0\rangle)$$

и при этом подсистема из двух кубитов  $A_2A_1$  - в состоянии  $|00\rangle$ , а подсистема из двух кубитов  $B_2A$  - в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

(это следует из результатов, представленных в параграфе 1.5; далее такая ссылка предполагается по умолчанию);

с вероятностью  $\frac{1}{4}$  квантовая система  $B_2A_2A_1A$  - в состоянии

$$\frac{1}{\sqrt{2}}(|0\rangle|01\rangle|0\rangle - |1\rangle|01\rangle|1\rangle)$$

и при этом подсистема из двух кубитов  $A_2A_1$  - в состоянии  $|01\rangle$ , а подсистема из двух кубитов  $B_2A$  - в состоянии Белла

$$|\psi_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}};$$

с вероятностью  $\frac{1}{4}$  квантовая система  $B_2A_2A_1A$  - в состоянии

$$\frac{1}{\sqrt{2}}(|0\rangle|10\rangle|1\rangle + |1\rangle|10\rangle|0\rangle)$$

и при этом подсистема из двух кубитов  $A_2A_1$  - в состоянии  $|10\rangle$ , а подсистема из двух кубитов  $B_2A$  - в состоянии Белла

$$|\psi_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}};$$

с вероятностью  $\frac{1}{4}$  квантовая система  $B_2A_2A_1A$  - в состоянии

$$\frac{1}{\sqrt{2}}(|0\rangle|11\rangle|0\rangle + |1\rangle|11\rangle|1\rangle)$$

и при этом подсистема из двух кубитов  $A_2A_1$  в состоянии  $|11\rangle$ , а подсистема из двух кубитов  $B_2A$  в состоянии Белла

$$|\psi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

**Шаг 4** Если на шаге 3 в результате измерения Алисы два кубита  $A_2A_1$  оказались в состоянии  $|00\rangle$ , то Алиса не делает ничего. Кубиты  $B_2A$  находятся в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}};$$

Если на шаге 3 в результате измерения Алисы два кубита  $A_2A_1$  оказались в состоянии  $|01\rangle$ , то Алиса пропускает кубит  $A$  через элемент Паули

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . В результате этого кубиты  $B_2A$  окажутся в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Если на шаге 3 в результате измерения Алисы два кубита  $A_2A_1$  оказались в состоянии  $|10\rangle$ , то Алиса пропускает кубит  $A$  через элемент Паули  $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ . В результате этого кубиты  $B_2A$  окажутся с точностью до общего сомножителя  $(-1)$  в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Если на шаге 3 в результате измерения Алисы два кубита  $A_2A_1$  оказались в состоянии  $|11\rangle$ , то Алиса пропускает кубит  $A$  сперва через элемент Паули  $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ , а затем через элемент Паули  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . В результате этого кубиты  $B_2A$  окажутся с точностью до общего сомножителя  $(-1)$  в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Теперь приведем пошагово соответствующий алгоритм действий **Боба**.

На входе алгоритма четыре кубита  $AB_2B_1B$  в состоянии в состоянии

$$\begin{aligned} |\psi_0^{(4)}\rangle &= \frac{|10\rangle - |01\rangle}{\sqrt{2}} \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \\ &= \frac{1}{2} (|1000\rangle + |1011\rangle - |0100\rangle - |0111\rangle). \end{aligned}$$

**Шаг 1.** Боб пропускает свои кубиты  $B_2$  и  $B_1$  через элемент CNOT [63].

Это равносильно тому, что к состоянию  $|\psi_0^{(4)}\rangle$  применяется линейное преобразование с матрицей  $I_2 \otimes \text{CNOT} \otimes I_2$ , где  $\otimes$  - знак тензорного

произведения,  $\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ ,  $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . В результате получается

состояние  $|\psi_1^{(4)}\rangle$  квантовой системы  $AB_2B_1B$  задаваемое равенством:

$$|\psi_1^{(4)}\rangle = \frac{1}{2} (|1000\rangle + |1011\rangle - |0110\rangle - |0101\rangle).$$

**Шаг 2.** Боб пропускает свой кубит  $B_2$  через элемент Адамара  $H$  [63], что равносильно применению к состоянию  $|\psi_1^{(4)}\rangle$  линейного преобразования с матрицей  $I_2 \otimes H \otimes I_2 \otimes I_2$ , где  $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ . В результате квантовая система

$AB_2B_1B$ , переходит в состояние  $|\psi_2^{(4)}\rangle$ , задаваемое равенством:

$$\begin{aligned} |\psi_2^{(4)}\rangle = & \\ = & \frac{1}{2} (|1\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle |0\rangle + |1\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}} |1\rangle |1\rangle - |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} |1\rangle |0\rangle - \\ & |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} |0\rangle |1\rangle), \end{aligned}$$

что, перегруппировав члены, можно переписать следующим образом

$$\begin{aligned} |\psi_2^{(4)}\rangle = & \\ = & \frac{1}{2\sqrt{2}} (|1\rangle |0\rangle |0\rangle |0\rangle + |1\rangle |1\rangle |0\rangle |0\rangle + |1\rangle |0\rangle |1\rangle |1\rangle + |1\rangle |1\rangle |1\rangle |1\rangle - \\ & - |0\rangle |0\rangle |1\rangle |0\rangle + |0\rangle |1\rangle |1\rangle |0\rangle - |0\rangle |0\rangle |0\rangle |1\rangle + |0\rangle |1\rangle |0\rangle |1\rangle) = \\ = & \frac{1}{2} (-\frac{1}{\sqrt{2}} (|0\rangle |00\rangle |1\rangle - |1\rangle |00\rangle |0\rangle) - \frac{1}{\sqrt{2}} (|0\rangle |01\rangle |0\rangle - |1\rangle |01\rangle |1\rangle)) + \\ & + \frac{1}{\sqrt{2}} (|0\rangle |10\rangle |1\rangle + |1\rangle |10\rangle |0\rangle) + \frac{1}{\sqrt{2}} (|0\rangle |11\rangle |0\rangle + |1\rangle |11\rangle |1\rangle). \end{aligned}$$

**Шаг 3.** Боб проводит измерение над своими двумя кубитами  $V_2$  и  $V_1$  в вычислительном базисе из векторов  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  и  $|11\rangle$  [63]. В результате этого измерения квантовая система из четырех кубитов  $AV_2V_1V$  может иметь следующие свои состояния и состояния своих подсистем:

с вероятностью  $\frac{1}{4}$  квантовая система  $AV_2V_1V$  - в состоянии

$$\frac{1}{\sqrt{2}}(|0\rangle|00\rangle|1\rangle - |1\rangle|00\rangle|0\rangle)$$

и при этом подсистема из двух кубитов  $V_2V_1$  - в состоянии  $|00\rangle$ , а подсистема из двух кубитов  $AV$  - в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}};$$

с вероятностью  $\frac{1}{4}$  квантовая система  $AV_2V_1V$  - в состоянии

$$\frac{1}{\sqrt{2}}(|0\rangle|01\rangle|0\rangle - |1\rangle|01\rangle|1\rangle)$$

и при этом подсистема из двух кубитов  $V_2V_1$  - в состоянии  $|01\rangle$ , а подсистема из двух кубитов  $AV$  - в состоянии Белла

$$|\psi_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}};$$

с вероятностью  $\frac{1}{4}$  квантовая система  $AV_2V_1V$  - в состоянии

$$\frac{1}{\sqrt{2}}(|0\rangle|10\rangle|1\rangle + |1\rangle|10\rangle|0\rangle)$$

и при этом подсистема из двух кубитов  $V_2V_1$  - в состоянии  $|10\rangle$ , а подсистема из двух кубитов  $AV$  - в состоянии Белла

$$|\psi_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}};$$

с вероятностью  $\frac{1}{4}$  квантовая система  $AB_2V_1V$  - в состоянии

$$\frac{1}{\sqrt{2}}(|0\rangle|11\rangle|0\rangle + |1\rangle|11\rangle|1\rangle)$$

и при этом подсистема из двух кубитов  $V_2V_1$  в состоянии  $|11\rangle$ , а подсистема из двух кубитов  $AB$  в состоянии Белла

$$|\psi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

**Шаг 4** Если на шаге 3 в результате измерения Боба два кубита  $V_2V_1$  оказались в состоянии  $|00\rangle$ , то Боб не делает ничего. Кубиты  $AB$  находятся в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}};$$

Если на шаге 3 в результате измерения Боба два кубита  $V_2V_1$  оказались в состоянии  $|01\rangle$ , то Боб пропускает кубит  $V$  через элемент Паули  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . В результате этого кубиты  $AB$  окажутся в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Если на шаге 3 в результате измерения Боба два кубита  $V_2V_1$  оказались в состоянии  $|10\rangle$ , то Боб пропускает кубит  $V$  через элемент Паули  $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ . В результате этого кубиты  $AB$  окажутся с точностью до общего множителя (-1) в состоянии Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Если на шаге 3 в результате измерения Боба два кубита  $V_2V_1$  оказались в состоянии  $|11\rangle$ , то Боб пропускает кубит  $V$  сперва через элемент Паули  $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ , а затем через элемент Паули  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . В результате этого кубиты  $AB$  окажутся с точностью до общего множителя (-1) в состоянии

Белла спиновый синглет

$$|\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Итак, квантовая система АВ из кубитов Алисы и Боба установлены в необходимое состояние спиновый синглет и готовы к использования для генерации одного бита ключа криптографической системы **АКМ2017**.

## Выводы по главе 3

1. Квантовый ресурс, заключающийся «в невозможности клонирования неизвестных квантовых состояний и эквивалентной ей невозможности идеального различения неортогональных квантовых состояний» при своем использовании для построения квантовых криптографических систем, требует применения классических генераторов случайных числовых последовательностей. Поэтому генерируемая в этом случае гамма случайна в классическом смысле («кажущаяся» случайность, основанная на отсутствии полного знания об используемых объектах и процессах) и не является «истинно» случайной.

2. Квантовые криптографические системы BB84, B92, SARG04 и различные их обобщения и модификации (основанные на ресурсе невозможности клонирования неизвестных квантовых состояний и эквивалентной ей невозможности идеального различения неортогональных квантовых состояний) по качеству вырабатываемого ключевого материала уступают протоколу E91. Это обусловлено тем, что, хотя в E91 для генерации используется также процедура случайной выборки на основе классического генератора случайных числовых последовательностей, но из последовательности, сформированной на основе «истинной» случайности путем измерений над двухкубитной (точнее двухфотонной) квантовой системой, находящейся в одном из несепарабельных состояний Белла.

3. Разработана совершенно стойкая квантовая криптографическая система **AKM2017** с использованием несепарабельного двухкубитного состояния спиновый синглет. Квантовая криптографическая система **AKM2017** обладает рядом качественных свойств, которые невозможны в принципе для классических криптографических систем, а некоторые из них невозможны и для известных квантовых криптографических систем, даже таких, как E91. Указанные качественные свойства – преимущества следующие:

в квантовой криптографической системе **АКМ2017** ключевая последовательность (гамма) генерируется на основе фундаментально случайного процесса, основанного на свойствах квантового ресурса несепарабельности двухкубитного состояния спиновый синглет, здесь, как говорит известный физик Николя Жизан, «истинная» случайность [43]; а в случае криптографической системой «одноразовый шифрблокнот» используются методы формирования шифровальных блокнотов, основанные на классических подходах к исследованию случайных процессов (данное преимущество в известной степени имеется и у известной квантовой криптографической системы E91);

в квантовой криптографической системе **АКМ2017** появляется еще одна степень усиления стойкости, отсутствующая у всех известных криптографических систем, в том числе и у квантовых, - это дополнительный сеансовый ключ в виде единичного вектора  $v = (v_1, v_2, v_3)$  – в трехмерном пространстве над полем действительных чисел  $\mathbf{R}$ ; эта степень усиления стойкости выражается в следующем: при компрометации ключевых блокнотов стойкость всех криптографических систем становится, образно говоря, нулевой; а в случае **АКМ2017** ситуация более благоприятная, в том плане, что стойкость в определенном смысле сохраняется, то есть сохраняется свойство идеальной стойкости;

для квантовой криптографической системы **АКМ2017** существует принципиальная возможность с использованием операции *свопинг* (подкачка) дистанционной регенерации носителей-кубитов использованных квантовых шифровальных блокнотов квантовой криптографической системы **АКМ2017** и, тем самым, повысить надежность шифрованной связи; а для всех других известных криптографических систем такая возможность отсутствует.

## ЗАКЛЮЧЕНИЕ

Разработанная в рамках диссертационного исследования криптографическая система **АКМ2017** не имеет аналогов, является теоретически стойкой и не теряет свойство идеальной стойкости даже при компрометации своих квантовых шифровальных блокнотов. Программно-аппаратные комплексы шифрованной связи, построенные с применением данной криптографической системы, будут обладать такой высокой надежностью, которая в принципе не может быть достигнута на парке классических криптографических систем и известных квантовых криптографических систем, отличных от **АКМ2017**. Указанная надежность основана, в первую очередь, на присущей для квантовой криптографической системы **АКМ2017** возможности дистанционной регенерации использованных квантовых носителей ключевого материала криптографической системы.

Полученные в диссертации результаты обладают научной новизной. В частности, новыми научными результатами являются:

- 1) достаточные признаки несепарабельности многокубитных состояний (по которым можно определить несепарабельные они или нет), основанные на использовании аналитического аппарата булевых масок и нумераторов весов;
- 2) решение задачи бинарной классификации квантовых состояний (то есть, задачи определения к какому из двух классов – классу сепарабельных состояний или классу несепарабельных состояний – принадлежит заданное многокубитное состояние) через вычисление всех возможных **редукций** булевых функций, векторы значений которых являются булевыми масками квантовых состояний;
- 3) выявление класса состояний многокубитных квантовых систем, во многом по своим свойствам, аналогичных двухкубитному состоянию спиновый синглет;
- 4) разработанная в рамках диссертационных исследований квантовая криптографическая система **АКМ2017** и математическое обоснование ее

теоретической стойкости;

5) выявление и математическое обоснование того, что квантовая криптографическая система **АКМ2017** сохраняет идеальную стойкость при компрометации носителей ключевого материала; данное свойство в принципе невозможно для всех классических криптографических систем и известных квантовых криптографических систем, отличных от **АКМ2017**;

б) выявление и математическое обоснование того, что для квантовой криптографической системы **АКМ2017** существует возможность дистанционной регенерации использованных квантовых носителей ключевого материала криптографической системы; данное свойство в принципе невозможно для всех классических криптографических систем и известных квантовых криптографических систем, отличных от **АКМ2017**;

7) алгоритм дистанционной регенерации использованных квантовых носителей ключевого материала криптографической системы.

К направлениям дальнейших исследований можно отнести:

- исследование и расширение возможности применения квантовой криптографической системы **АКМ2017** для обеспечения защиты информации для конференц-связи путем дистанционного объединения шифровальных блокнотов;

- экспериментальные исследования по разработке технологий создания квантовых систем, состоящих из «долгоживущих» в несепарабельных состояниях массивных частиц (объектов).

## СПИСОК ЛИТЕРАТУРЫ

1. Алиев Ф.К., Бородин А.М., Клюев А.В. К вопросу о сепарабельности трехкубитных квантовых систем. Обзорение прикладной и промышленной математики, т.16, выпуск 4, - М.: Изд-во "ТВП", 2009.
2. Алиев Ф.К., Бородин А.М., Клюев А.В. О состояниях с максимальной мерой несепарабельности двухкубитных квантовых систем. Обзорение прикладной и промышленной математики, т.16, выпуск 4, - М.: Изд-во "ТВП", 2009.
3. Алиев Ф.К., Бородин А.М., Клюев А.В. К вопросу о сепарабельности состояний многокубитных квантовых систем. Обзорение прикладной и промышленной математики, т.17, выпуск 5 - М.: Изд-во "ТВП", 2010.
4. Алиев Ф.К., Бородин А.М. О возможности применения квантового механизма телепортации для представления произвольной двоичной последовательности в виде суммы двух случайных равновероятных двоичных последовательностей. Обзорение прикладной и промышленной математики, т.17, выпуск 5 - М.: Изд-во "ТВП", 2010.
5. Алиев Ф.К., Бородин А.М., Корольков А.В. О связи свойств несепарабельности состояния многокубитной квантовой системы и его булевой проекции. Материалы 11 научно-технической конференции. Секция №13. - М., 2011.
6. Алиев Ф.К., Бородин А.М. Достаточные условия несепарабельности состояний трехкубитной квантовой системы. Материалы 11 научно-технической конференции. Секция №13. - М., 2011.
7. Алиев Ф.К. О состояниях квантовой системы из двух частиц со спиновым числом  $\frac{1}{2}$  и разными гиромангнитными отношениями. Материалы 11 Научно-технической конференции по криптографии. Секция «Проблемы квантовой криптографии». М.: 2011.
8. Алиев Ф.К. О новом способе передачи информации. Материалы 11 научно-технической конференции. Секция №13. - М., 2011.

9. Алиев Ф.К., Бородин А.М., Вассенков А.В., Матвеев Е.А. О несепарабельных состояниях многочастичных квантовых систем, - В сборнике научных трудов по итогам работы 6 – 7 Всероссийских научно-технических конференций школы-семинара «Информационная безопасность – актуальная проблема современности». – Краснодар: ФВАС (г. Краснодар), 2013. – Т.1. – С. 77 - 80.
10. Алиев Ф.К., Зайцева А.В., Костенюк И.В., Сенцов А.Г., Шеремет И.А. Оптимальный и субоптимальный энтропийные стеганографические алгоритмы защиты сообщений, сгенерированных двоичным источником без памяти // Известия Института инженерной физики, 2013. № 4(30). С. 2-9.
11. Алиев Ф.К., Бородин А.М., Вассенков А.В., Матвеев Е.А., Царьков А.Н., Шеремет И.А. О способе дистанционного изменения меры несепарабельности квантовых систем и возможности его применения в области связи // Известия Института инженерной физики, 2014. № 3(33). С. 30-38.
12. Алиев Ф.К., Бородин А.М., Вассенков А.В., Матвеев Е.А., Царьков А.Н., Шеремет И.А. ATF-технология связи, основанная на использовании ресурса несепарабельных состояний квантовых систем // Научные технологии, 2015. № 1. С. 65-78.
13. Алиев Ф.К., Матвеев Е.А., Шеремет И.А. Критерий несепарабельности состояния трехкубитной квантовой системы. Материалы 12 научно-технической конференции по криптографии. Секция №12. - М., 2016.
14. Алиев Ф.К., Бородин А.М., Матвеев Е.А., Шеремет И.А. Двухкубитные состояния А.В. Ключева, - В сборнике научных трудов по итогам работы 12 – 13 Всероссийских научно-технических конференций школы-семинара «Информационная безопасность – актуальная проблема современности». – Краснодар, 2016. – Т.1. – С. 77 – 81.

15. Алиев Ф.К., Бородин А.М., Матвеев Е.А., Шеремет И.А. О количественной характеристике ресурса несепарабельности многокубитных квантовых систем,- В сборнике научных трудов по итогам работы 12 – 13 Всероссийских научно-технических конференций школы-семинара «Информационная безопасность – актуальная проблема современности». – Краснодар, 2016. – Т.1. – С. 31 – 35.
16. Алиев Ф.К., Матвеев Е.А., Шеремет И.А. О характеристиках критерия принятия решения в АТФ-технологии связи, - В сборнике научных трудов по итогам работы 12 – 13 Всероссийских научно-технических конференций школы-семинара «Информационная безопасность – актуальная проблема современности». – Краснодар, 2016. – Т.1. – С. 8 – 9.
17. Алиев Ф.К., Матвеев Е.А., Шеремет И.А. К вопросу о бинарной классификации состояний спиновых квантовых систем, - В сборнике научных трудов по итогам работы 12 – 13 Всероссийских научно-технических конференций школы-семинара «Информационная безопасность – актуальная проблема современности». – Краснодар, 2016. – Т.1. – С. 89 – 92.
18. Алиев Ф.К., Бец М.О, Киселенко В.А., Матвеев Е.А., Орлов С. С. Квантовая криптографическая система АКМ2017. Сборник докладов 9-го межведомственного семинара «Системы и средства защиты информации» - Пенза, 2017.
19. Алиев Ф.К., Бец М.О, Киселенко В.А., Матвеев Е.А., Орлов С. С. О теоретической и идеальной стойкости квантовой криптографической системы АКМ2017. Сборник докладов 9-го межведомственного семинара «Системы и средства защиты информации» - Пенза, 2017.
20. Алиев Ф.К., Бец М.О, Киселенко В.А., Матвеев Е.А., Орлов С. С. О повторном использовании носителей ключевой информации квантовой криптографической системы АКМ2017. Сборник докладов 9-го

межведомственного семинара «Системы и средства защиты информации» - Пенза, 2017.

21. Алиев Ф.К., Зайцева А.В., Киселенко В.А., Матвеев Е.А., Орлов С.С., Шеремет И.А. Об усиленном квантовом варианте криптографической системы Вернама., - В сборнике научных трудов по итогам работы 14 – 15 Всероссийских научно-технических конференций школы-семинара «Информационная безопасность – актуальная проблема современности». – Краснодар, 2017.
22. Алиев Ф.К., Зайцева А.В., Киселенко В.А., Матвеев Е.А., Орлов С.С., Шеремет И.А. О стойкости усиленного квантового варианта криптографической системы Вернама при известных параметрах гипотетически допускаемой компрометации, - В сборнике научных трудов по итогам работы 14 – 15 Всероссийских научно-технических конференций школы-семинара «Информационная безопасность – актуальная проблема современности». – Краснодар, 2017.
23. Алиев Ф.К., Зайцева А.В., Киселенко В.А., Матвеев Е.А., Орлов С.С., Шеремет И.А. О возможности восстановления состояний носителей сменных элементов усиленного квантового варианта криптографической системы Вернама, - В сборнике научных трудов по итогам работы 14 – 15 Всероссийских научно-технических конференций школы-семинара «Информационная безопасность – актуальная проблема современности». – Краснодар, 2017.
24. Алиев Ф.К., Корольков А.В., Матвеев Е.А. Несепарабельные состояния многокубитных квантовых систем. Монография / Под ред. Ф.К. Алиева. – М.: Радиотехника. 2017. – 320 с.
25. Алиев Ф.К., Корольков А.В., Матвеев Е.А., Орлов С.С., Шеремет И.А. Квантовая криптографическая система АКМ2017 на основе ресурса несепарабельности состояния спиновый синглет. //Системы высокой доступности, №4. т.14, 2018.

26. Алиев Ф.К., Юров И.А. Курс лекций по математической логике и теории алгоритмов. М.: МИФИ, 2003. – 198 с.
27. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2005. – 480 с.
28. Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Р, 2002. – 512с.
29. Баумастер Д., Эжерт А., Цайлингер А. Физика квантовой информации. – М.: Постмаркет, 2002. – 376 с.
30. Берман Г.П., Дулен Г.Д., Майньери Р., Цифринович В.И. Введение в квантовые компьютеры. – М.-Ижевск: НИЦ «Регулярная и хаотическая динамика»; 2004. – 188 с.
31. Боровков А.А. Теория вероятностей. –М.: Наука, 1976. – 352 с.
32. Боровков А.А. Математическая статистика. – М.: Наука, 1984. – 472 с.
33. Будкер Д., Кимбелл Д., ДеМилье Д. Атомная физика. Освоение через задачи/ Пер. с англ. – М.: ФИЗМАТЛИТ, 2009. - 400 с.
34. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежда и реальность. – М.-Ижевск: НИЦ «Регулярная и хаотическая динамика»; 2004. – 320 с.
35. Вернер М. Основы кодирования. – М.: Техносфера, 2006. – 288 с.
36. Воеводин В.В., Кузнецов Ю.А. Матрицы и вычисления. – М.: Наука, - 1984. – 320 с.
37. Гантмахер Ф.Р. Теория матриц. – 4-е изд. – М.: Наука, - 1988. – 560 с.
38. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. Т. 1, 2. – М.: Гелиос-АРВ, - 2003. – 336 с., 416 с.
39. Гринштейн Дж., Зайонц А. Квантовый вызов. Современные исследования оснований квантовой механики. – М.: ИД «Интеллект», 2008. – 400 с.
40. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 05 декабря 2016 г.

41. Дориченко С.А., Яценко В.В. 25 этюдов о шифрах. М.: ТЕИС, 1994. 69с.
42. Духин А.А. Теория информации. – М.: Гелиос АРВ, 2007. – 248 с.
43. Жизан Н. Квантовая случайность. Пер. с англ. – М.: Альпина нон-фикшн, 2016. – 202 с.
44. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. – М.: Гелиос АРВ, 2005. – 192 с.
45. Иванов М.Г. Как понимать квантовую механику. – М.- Ижевск: НИЦ «Регулярная и хаотическая динамика», 2012. – 516 с.
46. Ивченко Г.И., Медведев Ю.И. Математическая статистика. – М. «ЛИБРОКОМ», 2014. – 352 с.
47. Имре Ш., Балаж Ф. Квантовые вычисления и связь. Инженерный подход. - М.: ФИЗМАТЛИТ, 2008. – 320 с.
48. Квантовый компьютер. [Электронный ресурс]. ([ru.wikipedia.org](http://ru.wikipedia.org)).
49. Килин С.Я. и др. Квантовая криптография: идеи и практика. –Минск: Беларус. наука, 2007. – 391 с.
50. Китайский спутник Мо Цзы. [Электронный ресурс]. ([yandex.ru](http://yandex.ru)).
51. Клышко Д.Н. Фотоны и нелинейная оптика. – М.: Наука, 1980 – 302 с.
52. Клышко Д.Н. Физические основы квантовой электроники. – М.: Наука, 1986 – 280 с.
53. Кокин А.А. Твердотельные квантовые компьютеры на ядерных спинах. – М.-Ижевск: Институт компьютерных исследований, 2004. – 204 с.
54. Коралов Л.Б., Синай Я.Г. Теория вероятностей и случайные процессы. – М.: МЦНМО, 2013. – 408 с.
55. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. - М.: Наука, - 1984 – 833 с.
56. Кудрявцев Л.Д. Курс математического анализа. Т 1, 2. – М.: Высшая школа, - 1981. - 687 с., 584 с.
57. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2016. – 473 с.

58. Матвеев А.Н. Атомная физика: учебное пособие для вузов. – М.: Издательство «Мир и Образование», 2007. – 432 с.
59. Матвеев Е.А. Об изучении несепарабельности квантовых состояний с использованием их булевых масок. Сборник докладов 6-го межведомственного семинара «Системы и средства защиты информации» - Пенза, 2014. – С. 30 - 33.
60. Матвеев Е.А. Об изучении несепарабельности квантовых состояний с использованием нумераторов весов двоичных кодов. Сборник докладов 6-го межведомственного семинара «Системы и средства защиты информации» - Пенза, 2014. – С. 34 - 37.
61. Матвеев Е.А. Нумераторы весов состояний квантовых систем. Материалы 12 научно-технической конференции. Секция №12. - М., 2016.
62. Матвеев Е.А. Протокол восстановления состояний носителей-кубитов для формирования ключевой информации квантовой криптографической системы АКМ2017. //Системы высокой доступности, 2018. №4. – С. 73 - 78.
63. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир, 2006. – 824 с.
64. Прасолов В.В. Задачи и теоремы линейной алгебры. – М.: МЦНМО, 2015. – 576 с.
65. Перри Р. Элементарное введение в квантовые вычисления. Пер. с англ. Учебное пособие. – Долгопрудный: «Интеллект», 2015. – 208 с.
66. Прескилл Дж. Квантовая информация и квантовые вычисления. Том 1. – М. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2008. – 464с.
67. Приоритетные проблемы научных исследований в области обеспечения информационной безопасности Российской Федерации (утверждена Исполняющим обязанности Секретаря Совета Безопасности Российской Федерации, председателя научного совета

при Совете Безопасности Российской Федерации 7 марта 2008 г.).  
[Электронный ресурс]. (<http://www.scrf.gov.ru/documents/6/93.html>).

68. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРВ, 2002. – 432 с.
69. Самарцев В.В. Коррелированные фотоны и их применение. – М.: ФИЗМАТЛИТ, 2014. – 168 с.
70. Сокольников И.С. Тензорный анализ. – М.: КомКнига, 2007. – 376 с.
71. Стиб В.-Х., Харди Й. Задачи и их решения в квантовых вычислениях и квантовой теории информации. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2007. - 296 с.
72. Стратонович Р.Л. Теория информации. – М.: «Сов. радио», 1975. – 424с.
73. Фейнман Ричард Ф., Лейтон Роберт Б., Сэндс Мэтью Фейнмановские лекции по физике: Вып. 8, 9: Квантовая механика: учебное пособие. – М.: Издательство ЛКИ, 2008. 528 с.
74. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.
75. Фомичев В.М. Методы дискретной математики в криптологии. – М.: ДИАЛОГ-МИФИ, 2010. – 424 с.
76. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Част.1, Математические аспекты. – М.: Издательство Юрайт, 2016. – 200 с. Часть 2, Системные и прикладные аспекты. – М.: Издательство Юрайт, 2016. – 245 с.
77. Холево А.С. Квантовые системы, каналы, информация. М.: МЦНМО, 2010. -328 с.
78. Хренников А.Ю. Введение в квантовую теорию информации. – М.: ФИЗМАТЛИТ, 2008. – 284 с.
79. Чернявский А.Ю. Минимум энтропии измерений как вычислимая мера запутанности многочастичных квантовых состояний. Канд. дисс. – М.: Физико-технологический институт РАН, 2010. – 130 с.

80. Шеннон К. Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – 869 с.
81. Шнаер Б. Прикладная криптография. – М.: ТРИУМФ, 2003 г. – 816 с.
82. Шляйх В.П. Квантовая оптика в фазовом пространстве/ Пер. с англ. – М.: ФИЗМАТЛИТ, 2005- 760 с.
83. Эндрюс Г. Теория разбиений/ Пер. с англ. –М.: Наука, 1982. - 256 с.
84. Aliev F.K., Borodin A.M., Vassenkov A.V., Matveev E.A., Tzarkov A.N., Sheremet I.A. ATF-technology of communication based on using the resource of entangled states of quantum systems// *Electromagnetic Waves and Electronic Systems*. 2015. V.20, № 3. P. 60-72.
85. Aspect A., Grangier Ph. and Roger G. *Phys. Rev. Lett.* 49, 91 (1982)
86. Aspect A., Dalibard J. and Roger G. *Phys. Rev. Lett.* 49, 1804 (1982)
87. Bell J.S. *Physics* 1 195 (1964)
88. Bennet C.H., Brassard G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175-179, IEEE, New York, 1984, Bangalore, India, December 1984.
89. Bennet C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21): 3121 – 3124, 1992.
90. Bennet C.H., Brassard G., Cre'peau C., Jozsa R., Peres A., Wootters W.K. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channel// *Phys. Rev. Lett.*, 1993, v. 70, № 13, pp 1895-1899.
91. Bennet C.H., Bernstein H.J., Popescu S., Schumacher B. *Phys. Rev. A* 53, 2046 (1996)
92. Bennet C.H., Divincenco, Smolin J.A., Wootters W.K. *Phys. Rev. A* 54, 3824 (1996)
93. Dieks D. Communication by EPR devices. . *Phys. Lett. A*, 92(6): 271-272, 1982.
94. Dur W., Vidal G., Cirac J.I. *Phys. Rev. A* 62, 062314 (2000).

95. Einstein A., Podolsky B., Rosen N. Phys. Rev. 47 777 (1935)
96. Ekert A.K. Quantum cryptography based on Bells theorem. Phys. Rev. Lett. 67(6) (1991)
97. Hanson R. end ...Unconditional quantum teleportation between distant solid-state qubits, arXiv: 1404.4369v3 [quant-ph] 3Jun 2014.
98. Hanson R. end ... Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km, arXiv: 1508.05949v1 [quant-ph] 24 Aug 2015.
99. Hill S., Wootters W.K. Phys. Rev. Lett. 78, 5022 (1997)
100. Meyer D., Wallach N. Global entanglement in multiparticle systems // Journal of Mathematical Physics. 2002. Vol. 43/ P. 4273.
101. Neumann P., Mizuochi N., Rempp F., Hemmer P., Watanabe H., Yamasaki S., Jacques V., Gaebel T., Jelezko F., Wrachtrup J. Multipartite entanglement among single spins in diamond, Science 320, 1326 (2008)
102. Nielsen M. Quantum Information Theory. Ph. D. thesis, University of New Mexico, 1998.
103. O'Connor K.M., Wootters W.K. Entangled Rings. Department of Physics, Williams College, Williamstown, MA 01267, USA, 2000.
104. Rungta P., Buzer V., Caves C.M., Hillery M., Milburn G.J. Universal state inversion and concurrence in arbitrary dimensions. Phys. Rev. A 64, 042315 (2001).
105. Scarani V., Achin A., Ribordy G., Gisin N. Quantum Cryptography Protocols RRobust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. Phys. Rev. Lett. 92(5) (2004)
106. Schmidt E. Zur theorie der linearen und nichtlinearen integralgleichungen. Math. Annalen., 63: 433-476, 1906.
107. Schrodinger E. Naturwissenschaften 23 807, 823, 844 (1935)
108. Wootters W.K., Zurek W.H. A single quantum cannot be cloned. Nature, 299: 802-803, 1982.

109. Wootters W.K. Entanglement of Formation of an Arbitrary State of Two Qubits. Department of Physics, Williams College, Williamstown MA 01267, USA, 1997.
110. Wootters W.K. Entangled chains. Department of Physics, Williams College, Williamstown MA 01267, USA, 2003.
111. Greenberger D.M., Horne M.A., Shimony A. and Zeilinger A. Bell's theorem without inequalities. Amer. J. Phys. Vol. 58. Pp 1131-1143, 1990.
112. Pan J.-W., Bouwmeester D., Daniell H., Wiefurter H. and Zeilinger A. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. Nature. Vol. 403. Pp. 515-519, 2000.
113. Е. А. Матвеев, С. Е. Игошина, А. А. Карманов. Квантовый фазовый переход как основа для практической реализации АТФ технологии связи. // Программная инженерия, 2019, Том 10, №7-8, С.305 – 310
114. Матвеев Е.А. Квантовый телеграф. // Программная инженерия, 2019, Том 10, №7-8, С.317 – 323.
115. Bennet C.H., Brassard G., Mermin N.D. Quantum cryptography without Bell's theorem. Phys. Rev. Lett. 68 (1992).

## ПРИЛОЖЕНИЕ А

### Тензорный ранг

Пусть  $\mathbf{V}$  и  $\mathbf{W}$  – конечномерные векторные пространства над полем комплексных чисел  $\mathbb{C}$ . Тогда тензорное произведение  $\mathbf{V} \otimes \mathbf{W}$  пространств  $\mathbf{V}$  и  $\mathbf{W}$  является векторным пространством над полем комплексных чисел  $\mathbb{C}$  и состоит из линейных комбинаций элементов вида  $v \otimes w$ , где  $v \otimes w$  – тензорное произведение векторов  $v$  и  $w$ ,  $v \in \mathbf{V}$ ,  $w \in \mathbf{W}$ . Но не всякий элемент пространства  $\mathbf{V} \otimes \mathbf{W}$  можно представить в виде  $v \otimes w$ , где  $v \in \mathbf{V}$ ,  $w \in \mathbf{W}$ .

Следуя [64] сформулируем определение.

**Определение А1.** Тензорным рангом элемента  $u \in \mathbf{V} \otimes \mathbf{W}$  называется наименьшее число  $k$ , для которого

$$u = v_1 \otimes w_1 + v_2 \otimes w_2 + \dots + v_k \otimes w_k,$$

где  $v_i \in \mathbf{V}$ ,  $w_i \in \mathbf{W}$ ,  $i \in \{1, 2, \dots, k\}$ . Тензорный ранг элемента  $u \in \mathbf{V} \otimes \mathbf{W}$  обозначается  $\text{rank}(u)$  или кратко  $\text{rk}(u)$ .

Напомним определения минора и ранга матрицы [64].

**Определение А2.** Пусть дана матрица

$$M = M_{ts} = \begin{pmatrix} m_{11} & \dots & m_{1s} \\ \vdots & \ddots & \vdots \\ m_{t1} & \dots & m_{ts} \end{pmatrix} = (m_{ij})$$

размера  $t \times s$  над полем комплексных чисел  $\mathbb{C}$ , где  $t \in \mathbb{N}$ ,  $s \in \mathbb{N}$ ,  $\mathbb{N}$  – множество натуральных чисел.

Пусть число  $p \in \mathbb{N}$  такое, что выполняется двойное нестрогое неравенство  $1 \leq p \leq \min(t, s)$ .

**Минором**  $p$ -го порядка матрицы  $A$  называется определитель матрицы размера  $p \times p$ , элементы которой стоят на пересечениях любых  $p$  строк и  $p$  столбцов матрицы  $A$ .

Ненулевой минор максимального порядка называют **базисным минором**, а его порядок называют **рангом** матрицы  $A$ . Ранг матрицы  $A$  обозначим  $r(A)$ .

Справедлива следующая теорема [64].

**Теорема А3.** Пусть для элемента  $u \in V \otimes W$  выполняется равенство

$$u = \sum m_{ij} (e_i \otimes \varepsilon_j),$$

где  $\{e_i\}$  и  $\{\varepsilon_j\}$  – базисы пространств  $V$  и  $W$  соответственно,  $m_{ij} \in \mathbb{C}$ . Тогда

$$\text{rk}(u) = r(M),$$

где  $\text{rk}(u)$  – тензорный ранг элемента  $u$ ,  $r(M)$  – ранг матрицы  $M = (m_{ij})$ .

## ПРИЛОЖЕНИЕ Б

### Критерий несепарабельности состояний двухкубитных квантовых систем

В вычислительном базисе из векторов  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  произвольное двухкубитное состояние  $|\psi\rangle$  можно представить в следующем общем виде:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \quad (\text{Б.1})$$

где  $a, b, c, d \in \mathbb{C}$ ,  $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$ .

**Утверждение Б.2 (критерий  $K_2$ ).** Двухкубитное состояние  $|\psi\rangle$ , представленное равенством (Б.1), является несепарабельным состоянием тогда и только тогда, когда выполняется неравенство  $ad - bc \neq 0$ .

**Доказательство.** Данное утверждение равносильно утверждению о том, что состояние  $|\psi\rangle$  является сепарабельным состоянием тогда и только тогда, когда выполняется равенство  $ad - bc = 0$ . Поэтому достаточно доказать последнее утверждение.

Заметим, что для состояния двухкубитной квантовой системы свойство его сепарабельности эквивалентно его разложимости в тензорное произведение состояний однокубитных квантовых систем. Поэтому в соответствии с определением 1.3.3 и определением А1 состояние  $|\psi\rangle$  является сепарабельным состоянием тогда и только тогда, когда для его тензорного ранга  $\text{rk}(|\psi\rangle)$  выполняется равенство

$$\text{rk}(|\psi\rangle) = 1.$$

Из теоремы А3 следует, что предыдущее равенство справедливо тогда и только тогда, когда ранг  $r(M)$  матрицы  $M$ , определяемой равенством

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

равен 1. Так как состояние  $|\psi\rangle$  имеет норму, равную 1, то хотя бы одно

из чисел  $a, b, c, d$  отлично от нуля. Поэтому для ранга  $r(M)$  матрицы  $M$  справедливо нестрогое неравенство

$$1 \leq r(M) \leq 2.$$

Следовательно,  $r(M) = 1$  тогда и только тогда, когда все миноры 2-го порядка матрицы  $M$  равны нулю. Отсюда и из того, что у матрицы  $M$  только один минор 2-го порядка, а именно  $ad-bc$ , получаем выполнимость условия  $ab-bc=0$ .

## ПРИЛОЖЕНИЕ В

### О разложимости состояний трехкубитных квантовых систем в тензорное произведение состояний меньшей размерности

В вычислительном базисе из векторов  $|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$  произвольное трехкубитное состояние можно представить в следующем общем виде:

$$|\psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle, \quad (\text{B.1})$$

где  $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbf{C}$ ,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1. \quad (\text{B.2})$$

Для состояния  $|\psi\rangle \in \mathbf{C}^8$ , заданного равенством (B.1), определим величины  $Z_1, Z_2, Z_3, Z_4, Z_5, Z_6$  и  $Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$ , положив

$$\begin{aligned} Z_1 &= a_0 a_5 - a_1 a_4, Z_2 = a_0 a_6 - a_2 a_4, Z_3 = a_0 a_7 - a_3 a_4, \\ Z_4 &= a_1 a_6 - a_2 a_5, Z_5 = a_1 a_7 - a_3 a_5, Z_6 = a_2 a_7 - a_3 a_6, \end{aligned} \quad (\text{B.3})$$

$$Y_1 = a_0 a_3 - a_1 a_2, Y_2 = a_0 a_5 - a_1 a_4, Y_3 = a_0 a_7 - a_1 a_6,$$

$$Y_4 = a_2 a_5 - a_3 a_4, Y_5 = a_2 a_7 - a_3 a_6, Y_6 = a_4 a_7 - a_5 a_6.$$

Имеет место следующее утверждение.

**Утверждение В.4.** а) Для чистого состояния  $|\psi\rangle$  трехкубитной квантовой системы ABC справедливо равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_{23}\rangle,$$

где  $|\psi_1\rangle \in \mathbf{C}^2$ ,  $|\psi_{23}\rangle \in \mathbf{C}^4$ ,  $|\psi_1\rangle$ - чистое состояние однокубитной квантовой системы A,  $|\psi_{23}\rangle$ - чистое состояние двухкубитной квантовой системы BC, тогда и только тогда, когда справедлива цепочка равенств

$$Z_1 = Z_2 = Z_3 = Z_4 = Z_5 = Z_6 = 0.$$

б) Для чистого состояния  $|\psi\rangle$  трехкубитной квантовой системы ABC справедливо равенство

$$|\psi\rangle = |\psi_{12}\rangle \otimes |\psi_3\rangle,$$

где  $|\psi_{12}\rangle \in \mathbf{C}^4$ ,  $|\psi_3\rangle \in \mathbf{C}^2$ ,  $|\psi_{12}\rangle$  - чистое состояние двухкубитной квантовой системы AB,  $|\psi_3\rangle$  - чистое состояние однокубитной квантовой системы C, тогда и только тогда, когда справедлива цепочка равенств

$$Y_1 = Y_2 = Y_3 = Y_4 = Y_5 = Y_6 = 0.$$

**Доказательство.** Докажем пункт (а).

Из определения A1 следует, что справедливость равенства

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_{23}\rangle,$$

где  $|\psi_1\rangle \in \mathbf{C}^2$ ,  $|\psi_{23}\rangle \in \mathbf{C}^4$ ,  $|\psi_1\rangle$  - чистое состояние однокубитной квантовой системы A,  $|\psi_{23}\rangle$  - чистое состояние двухкубитной квантовой системы BC, означает, что тензорный ранг  $\text{rk}(|\psi\rangle)$  состояния  $|\psi\rangle$  равен 1. Последнее в соответствии с теоремой A3 равносильно справедливости равенства

$$r(M) = 1,$$

где  $r(M)$  ранг матрицы

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \end{pmatrix}.$$

Так как состояние  $|\psi\rangle$  имеет норму, равную 1 (см. (B.2)), то хотя бы одно из чисел  $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbf{C}$  отлично от нуля. Поэтому для ранга  $r(M)$  матрицы M справедливо нестрогое неравенство

$$1 \leq r(M) \leq 2.$$

Следовательно,  $r(M) = 1$  тогда и только тогда, когда все миноры 2-го порядка матрицы M равны нулю. Отсюда и из того, что у матрицы M все миноры 2-го порядка исчерпываются величинами  $Z_1, Z_2, Z_3, Z_4, Z_5$  и  $Z_6$ , получаем, что равенство  $r(M) = 1$  справедливо тогда и только тогда, когда

выполняется цепочка равенств  $Z_1 = Z_2 = Z_3 = Z_4 = Z_5 = Z_6 = 0$ . Пункт (а) утверждения В.4 доказан.

Докажем пункт (б).

Из определения А1 следует, что справедливость равенства

$$|\Psi\rangle = |\Psi_{12}\rangle \otimes |\Psi_3\rangle,$$

где  $|\Psi_{12}\rangle \in \mathbf{C}^4$ ,  $|\Psi_3\rangle \in \mathbf{C}^2$ ,  $|\Psi_{12}\rangle$  - чистое состояние двухкубитной квантовой системы АВ,  $|\Psi_3\rangle$  - чистое состояние однокубитной квантовой системы С, означает, что тензорный ранг  $\text{rk}(|\Psi\rangle)$  состояния  $|\Psi\rangle$  равен 1. Последнее в соответствии с теоремой А3 равносильно справедливости равенства

$$r(M) = 1,$$

где  $r(M)$  ранг матрицы

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \\ m_{31} & m_{32} \\ m_{41} & m_{42} \end{pmatrix} = \begin{pmatrix} a_0 & a_1 \\ a_2 & a_3 \\ a_4 & a_5 \\ a_6 & a_7 \end{pmatrix}.$$

Так как состояние  $|\Psi\rangle$  имеет норму, равную 1 (см. (В.2)), то хотя бы одно из чисел  $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbf{C}$  отлично от нуля. Поэтому для ранга  $r(M)$  матрицы М справедливо нестрогое неравенство

$$1 \leq r(M) \leq 2.$$

Следовательно,  $r(M) = 1$  тогда и только тогда, когда все миноры 2-го порядка матрицы М равны нулю. Отсюда и из того, что у матрицы М все миноры 2-го порядка исчерпываются величинами  $Y_1, Y_2, Y_3, Y_4, Y_5$  и  $Y_6$ , получаем, что равенство  $r(M) = 1$  справедливо тогда и только тогда, когда выполняется цепочка равенств  $Y_1 = Y_2 = Y_3 = Y_4 = Y_5 = Y_6 = 0$ . Пункт (б) утверждения В.4 доказан и тем самым утверждение В.4 доказано.

Непосредственно из утверждения В.4 вытекает следствие В.5.

**Следствие В.5.** Чистое состояние  $|\Psi\rangle$  трехкубитной квантовой системы АВС не представимо в виде тензорного произведения состояний меньших

размерностей тогда и только тогда, когда в каждом из наборов величин  $V_0 = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6\}$  и  $V_1 = \{Y_1, Y_2, Y_3, Y_4, Y_5, Y\}$  имеется величина, не равная нулю.

## ПРИЛОЖЕНИЕ Г

### Критерий несепарабельности состояний трехкубитных квантовых систем

Рассмотрим квантовую систему  $A_1A_2A_3$  из трех кубитов  $A_1, A_2, A_3$ . Симметрическая группа подстановок  $S_3$  состоит из следующих подстановок:

$$s_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, s_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Пусть  $|\psi\rangle \in \mathbf{C}^{2^3}$  - произвольное состояние 3-кубитной квантовой системы  $A_1A_2A_3$ . Состояние  $|\psi\rangle$  можно представить в виде

$$\begin{aligned} |\psi\rangle &= \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \dots + \alpha_7|111\rangle = \\ &= \sum_{\phi=0}^7 \alpha_\phi |\phi\rangle = \sum_{\phi=0}^7 \alpha_\phi |\varphi_1\varphi_2\varphi_3\rangle \end{aligned} \quad (\text{Г.1})$$

где

$$\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_7 \in \mathbf{C}, |\alpha_0|^2 + |\alpha_1|^2 + \dots + |\alpha_7|^2 = 1;$$

$$\phi \in \{0, 1, \dots, 7\}, \phi = \phi_1 \cdot 2^2 + \phi_2 \cdot 2^1 + \phi_3 \cdot 2^0, \phi_m \in \{0; 1\}, m = \overline{1, 3};$$

$$|\phi\rangle = |\varphi_1\varphi_2\varphi_3\rangle = |\phi_1\rangle |\phi_2\rangle |\phi_3\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes |\phi_3\rangle.$$

Тогда для любой подстановки  $s = \begin{pmatrix} 1 & 2 & 3 \\ s(1) & s(2) & s(3) \end{pmatrix} \in S_3$  через  $|\psi^{(s)}\rangle$

обозначим состояние

$$|\psi^{(s)}\rangle = \sum_{\phi=0}^7 \alpha_\phi |\varphi_{s(1)}\varphi_{s(2)}\varphi_{s(3)}\rangle. \quad (\text{Г.2})$$

квантовой системы  $A_{s(1)}A_{s(2)}A_{s(3)}$ , в которой кубиты рассматриваются в порядке, определяемом перестановкой  $(s(1), s(2), s(3))$  чисел 1, 2, 3.

Положим в определении 1.3.3 из параграфа 1.3 данной работы число кубитов  $n=3$ . В результате имеем следующее определение.

**Определение Г.3.** Состояние  $|\psi\rangle$  3-кубитной квантовой системы

$A_1A_2A_3$  называется **сепарабельным состоянием**, если найдется подстановка  $s \in S_3$ , такая, что состояние  $|\psi^{(s)}\rangle$  квантовой системы  $A_{s(1)} A_{s(2)} A_{s(3)}$  разлагается в тензорное произведение состояний размерности меньшей, чем  $2^3$ .

Состояние  $|\psi\rangle$  3-кубитной квантовой системы  $A_1A_2A_3$  называется **несепарабельным состоянием**, если оно не является сепарабельным состоянием.

Как и в приложении В (а также см. 1.3.13 и 1.3.14 в параграфе 1.3 данной работы), положим

$$V_0 = \{a_0 a_5 - a_1 a_4, a_0 a_6 - a_2 a_4, a_0 a_7 - a_3 a_4, \\ a_1 a_6 - a_2 a_5, a_1 a_7 - a_3 a_5, a_2 a_7 - a_3 a_6\}, \quad (\text{Г.4})$$

$$V_1 = \{a_0 a_3 - a_1 a_2, a_0 a_5 - a_1 a_4, a_0 a_7 - a_1 a_6, \\ a_2 a_5 - a_3 a_4, a_2 a_7 - a_3 a_6, a_4 a_7 - a_5 a_6\}. \quad (\text{Г.5})$$

Кроме этого еще положим (см. 1.3.15 в параграфе 1.3 данной работы)

$$V_2 = \{a_0 a_3 - a_1 a_2, a_0 a_6 - a_2 a_4, a_0 a_7 - a_2 a_5, \\ a_1 a_6 - a_3 a_4, a_1 a_7 - a_3 a_5, a_4 a_7 - a_5 a_6\}, \quad (\text{Г.6})$$

Справедливо следующее утверждение.

**Утверждение Г.7 (критерий  $K_3$ ).** Состояние  $|\psi\rangle$  трехкубитной квантовой системы  $A_1A_2A_3$ , представленное равенством (Г.1), является несепарабельным состоянием тогда и только тогда, когда для любого  $i \in \{0, 1, 2\}$  в наборе  $V_i$  имеется хотя бы одна величина, неравная нулю.

**Доказательство.** Из определения Г.3 следует, что состояние  $|\psi\rangle$  является несепарабельным состоянием тогда и только тогда, когда состояния  $|\psi^{(s_0)}\rangle, |\psi^{(s_1)}\rangle, |\psi^{(s_2)}\rangle, |\psi^{(s_3)}\rangle, |\psi^{(s_4)}\rangle, |\psi^{(s_5)}\rangle$  неразложимы в тензорное произведение состояний размерности меньшей 8.

Пользуясь следствием В.5 утверждения В.4 (см. приложение В) и учитывая равенство  $|\psi^{(s_0)}\rangle = |\psi\rangle$ , получаем, что состояние  $|\psi^{(s_0)}\rangle$  неразложимо в тензорное произведение состояний размерности меньшей 8

тогда и только тогда, когда в каждом из наборов величин  $V_0$  и  $V_1$  имеется величина, не равная нулю. Для учета подстановки  $s_0$  введем обозначения  $V_0^{(s_0)} = V_0$  и  $V_1^{(s_0)} = V_1$ .

Аналогично, для каждого состояния  $|\psi^{(s_k)}\rangle$  (где  $k=\overline{1,5}$ ), используя следствие В.5 утверждения В.4 (см. приложение В) и учитывая перестановку коэффициентов в представлении (Г.2) состояния  $|\psi^{(s_k)}\rangle$  по сравнению с представлением (Г.1) состояния  $|\psi\rangle$ , получаем, что состояние  $|\psi^{(s_k)}\rangle$  неразложимо в тензорное произведение состояний размерности меньшей 8 тогда и только тогда, когда в каждом из наборов величин  $V_0^{(s_k)}$  и  $V_1^{(s_k)}$  имеется величина, не равная нулю. Наборы  $V_0^{(s_k)}$  и  $V_1^{(s_k)}$  определяются по наборам  $V_0$  и  $V_1$  с учетом перестановки коэффициентов в представлении (Г.2) состояния  $|\psi^{(s_k)}\rangle$  по сравнению с представлением (Г.1) состояния  $|\psi\rangle$ .

В результате имеем, что состояние  $|\psi\rangle$  является несепарабельным состоянием тогда и только тогда, когда имеется величина, не равная нулю, в каждом (совпадающем с точностью до знаков отдельных величин с одним из наборов  $V_0$ ,  $V_1$  и  $V_2$ ) из следующих наборов величин:

$$V_0^{(s_0)} = \{a_0 a_5 - a_1 a_4, a_0 a_6 - a_2 a_4, a_0 a_7 - a_3 a_4, \\ a_1 a_6 - a_2 a_5, a_1 a_7 - a_3 a_5, a_2 a_7 - a_3 a_6\} \text{ (совпадает с } V_0),$$

$$V_1^{(s_0)} = \{a_0 a_3 - a_1 a_2, a_0 a_5 - a_1 a_4, a_0 a_7 - a_1 a_6, \\ a_2 a_5 - a_3 a_4, a_2 a_7 - a_3 a_6, a_4 a_7 - a_5 a_6\} \text{ (совпадает с } V_1);$$

$$V_0^{(s_1)} = \{a_0 a_3 - a_1 a_2, a_0 a_6 - a_2 a_4, a_0 a_7 - a_2 a_5, \\ a_1 a_6 - a_3 a_4, a_1 a_7 - a_3 a_5, a_4 a_7 - a_5 a_6\} \text{ (совпадает с } V_2),$$

$$V_1^{(s_1)} = \{a_0 a_3 - a_1 a_2, a_0 a_5 - a_1 a_4, a_0 a_7 - a_1 a_6,$$

$\underline{a_4 a_3 - a_5 a_2}$ ,  $a_2 a_7 - a_3 a_6$ ,  $a_4 a_7 - a_5 a_6$  } (совпадает с  $V_1$  с точностью до знака подчеркнутой величины);

$$V_0^{(s_2)} = \{ a_0 a_3 - a_1 a_2, a_0 a_5 - a_1 a_4, a_0 a_7 - a_1 a_6,$$

$\underline{a_3 a_4 - a_2 a_5}$ ,  $a_2 a_7 - a_3 a_6$ ,  $a_4 a_7 - a_5 a_6$  } (совпадает с  $V_1$  с точностью до знака подчеркнутой величины),

$$V_1^{(s_2)} = \{ a_0 a_5 - a_1 a_4, a_0 a_6 - a_2 a_4, a_0 a_7 - a_3 a_4,$$

$\underline{a_2 a_5 - a_6 a_1}$ ,  $a_1 a_7 - a_3 a_5$ ,  $a_2 a_7 - a_3 a_6$  } (совпадает с  $V_0$  с точностью до знака подчеркнутой величины);

$$V_0^{(s_3)} = \{ a_0 a_5 - a_1 a_4, a_0 a_6 - a_2 a_4, a_0 a_7 - a_3 a_4,$$

$\underline{a_2 a_5 - a_6 a_1}$ ,  $a_1 a_7 - a_3 a_5$ ,  $a_2 a_7 - a_3 a_6$  } (совпадает с  $V_0$  с точностью до знака подчеркнутой величины),

$$V_1^{(s_3)} = \{ a_0 a_3 - a_1 a_2, a_0 a_6 - a_2 a_4, a_0 a_7 - a_2 a_5,$$

$a_1 a_6 - a_3 a_4$ ,  $a_1 a_7 - a_3 a_5$ ,  $a_4 a_7 - a_5 a_6$  } (совпадает с  $V_2$ );

$$V_0^{(s_4)} = \{ a_0 a_3 - a_1 a_2, a_0 a_6 - a_2 a_4, a_0 a_7 - a_2 a_5,$$

$a_1 a_6 - a_3 a_4$ ,  $a_1 a_7 - a_3 a_5$ ,  $a_4 a_7 - a_5 a_6$  } (совпадает с  $V_2$ ),

$$V_1^{(s_4)} = \{ a_0 a_5 - a_1 a_4, a_0 a_6 - a_2 a_4, a_0 a_7 - a_3 a_4,$$

$a_1 a_6 - a_2 a_5$ ,  $a_1 a_7 - a_3 a_5$ ,  $a_2 a_7 - a_3 a_6$  } (совпадает с  $V_0$ );

$$V_0^{(s_5)} = \{ a_0 a_3 - a_1 a_2, a_0 a_5 - a_1 a_4, a_0 a_7 - a_1 a_6,$$

$a_2 a_5 - a_3 a_4$ ,  $a_2 a_7 - a_3 a_6$ ,  $a_4 a_7 - a_5 a_6$  } (совпадает с  $V_1$ ),

$$V_1^{(s_5)} = \{ a_0 a_3 - a_1 a_2, a_0 a_6 - a_2 a_4, a_0 a_7 - a_2 a_5,$$

$\underline{a_3 a_4 - a_1 a_6}$ ,  $a_1 a_7 - a_3 a_5$ ,  $a_4 a_7 - a_5 a_6$  } (совпадает с  $V_2$  с точностью до знака подчеркнутой величины). Утверждение доказано.

## ПРИЛОЖЕНИЕ Д

### О понятии секретности в связи с квантовой криптографической системой АКМ2017

Напомним, следуя [63], что понимается под **квантовым распределением ключей (КРК)** и **секретностью КРК**. КРК является протоколом, посредством которого биты ключа для симметричной криптографической системы могут быть созданы в процессе коммуникации двух сторон (в соответствующей специальной литературе для определенности этими двумя сторонами полагаются Алиса и Боб) по *открытому (общедоступному)* каналу. Предполагается, что при этом по *открытому* каналу передаются и классическая информация, и кубиты, необходимые для реализации процесса КРК. В состояниях кубитов закодированы биты распределяемого ключа. Полученный в результате выполнения процесса КРК ключ Алиса и Боб используют для обеспечения шифрованной связи с применением соответствующей симметричной криптографической системы.

Ева - третий персонаж. Она пытается в процессе КРК между Алисой и Бобом, их «подслушать» в целях несанкционированного (незаконного) получения информации об общем ключе Алисы и Боба.

В самом общем случае КРК, Алиса приготавливает каждый передаваемый по *открытому* каналу кубит в состоянии  $\rho_X$ , где  $X = k$  с вероятностью  $p_k$ ,  $k \in \{1, 2, \dots, n\}$ ,  $p_1 + p_2 + \dots + p_n = 1$  (например, для протокола BB84  $n = 4$ ). Боб проводит измерение над полученными кубитами, состояния которых могут отличаться от того, что было сделано Алисой из-за шумов в канале или «подслушивания» Евы. Результаты измерений, проводимых Бобом, полагаются как реализации некоторой случайной величины  $Y$ . Взаимную информацию  $H(X:Y) = H(X) + H(Y) - H(X,Y)$  случайных величин  $X$  и  $Y$  называют взаимной информацией Боба с Алисой и обозначают  $H_{\text{Боб : Алиса}}$ .

Аналогично, результаты «подслушивания» Евы трактуются как реализации некоторой случайной величины  $Z$ . Взаимную информацию  $H(X:Z)$

$= H(X)+H(Z)-H(X,Z)$  случайных величин  $X$  и  $Z$  называют взаимной информацией Евы с Алисой и обозначают  $H_{\text{Ева} : \text{Алиса}}$ .

Определяется величина  $\mathcal{R}$  через равенство

$$\mathcal{R} = \sup(H_{\text{Боб} : \text{Алиса}} - H_{\text{Ева} : \text{Алиса}})$$

как гарантированная **секретность** канала, где супремум берется по всем стратегиям, которые Алиса и Боб могут применить при использовании этого канала. Известна нижняя граница для **секретности**  $\mathcal{R}$ , как **квантовая когерентная информация** канала [63]. Но даже она не достигается известными протоколами BB84, B92, E91 и др. [63].

В настоящее время основное требование к протоколу КРК состоит в том, что при передаче кубитов по *открытому* каналу частота появления ошибок должна быть меньше определенного порога. Безопасность (или секретность) получающегося в результате ключа гарантируется свойствами квантовой информации и, следовательно, обусловлена только фундаментальными законами физики [63]. Проверая переданные Алисой кубиты на предмет их нарушения, Алиса и Боб получают верхнюю оценку любого шума и «подслушивания», которые имеют место в их канале связи [49], [63].

Понятие **секретности** в выше приведенных значениях **не имеет никакого отношения** к квантовой криптографической системе **АКМ2017** по той простой причине, что при формировании ключа зашифрования никаких передач кубитов по открытым (общедоступным) каналам **не осуществляется**.

Но вместе с тем, в данной диссертационной работе (см. параграф 3.5) предлагается протокол дистанционного восстановления состояний носителей-кубитов для формирования ключевой информации квантовой криптографической системы. **АКМ2017**. В этом случае, а также в случае формирование носителей ключевой информации третьим лицом Натаном (в общем случае отличным от Евы и, возможно, недоверенным), могут иметь место попытки сформировать пары кубитов - носителей ключевой информации в состояниях, запутанных с состояниями квантовых систем,

доступных Натану или какому-либо другому нарушителю для последующих собственных измерений в целях получения информации о ключе.

Эффективную нейтрализацию Алисой и Бобом такой угрозы (такой атаки) можно осуществить с помощью совместного проведения теста с использованием в качестве вектора сеансового ключа сначала вектора  $v = (0, 0, 1)$ , а затем  $v = (1, 0, 0)$ . Этот тест аналогичен предложенному в работе [115], который используется для доказательства высказанного А.Экертом предположения [96], что квантовые криптографические протоколы на перепутанных состояниях безопасны по отношению к атакам, в которых вместо истинного источника пар кубитов в состоянии спиновой синглет используется источник с тремя или более кубитами в несепарабельном состоянии, из которых два кубита посылаются Алисе и Бобу, а остальные позволяют за счет имеющихся корреляций с подсистемами извлечь информацию о ключе и при этом не обнаружить себя.

Чистое состояние квантовой системы из трех или более кубитов, сгенерированной таким источником, можно представить в следующем виде:

$$|\psi\rangle = a|00\rangle \otimes |A\rangle + b|01\rangle \otimes |B\rangle + c|10\rangle \otimes |C\rangle + d|11\rangle \otimes |D\rangle, \quad (\text{Д.1})$$

где  $a, b, c, d \in \mathbf{C}$ ,  $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$ , состояния  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  представляют базисные состояния квантовой системы из кубитов Алисы и Боба, а  $|A\rangle, |B\rangle, |C\rangle, |D\rangle$  - некие состояния квантовой системы, доступной Натану или какому-либо другому нарушителю для последующих собственных измерений в целях получения информации о ключе. В указанной выше работе [115] доказано, что единственной возможностью для Натана не быть обнаруженным – это генерировать состояния вида

$$|\psi\rangle = \left( \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right) \otimes |C\rangle. \quad (\text{Д.2})$$

В любом другом случае состояния квантовой системы Натана будут запутаны с состояниями квантовой системы Алисы и Боба, что может быть обнаружено при соответствующих измерениях, проводимых Алисой и Бобом.

Но в (Д.2) состояние  $|C\rangle$  является полностью декоррелированным по отношению к состоянию спиновой синглет  $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$ . Следовательно, измерения, производимые Натаном над состоянием  $|C\rangle$ , не дают никакой информации о состоянии кубитов Алисы и Боба.