УДК 003.26:004.056.55:621.39

КЛАССИФИКАЦИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ РАЗДЕЛЕНИЯ СЕКРЕТА

Евгений Василиу, Игорь Лимарь

В статье предложена классификация и обобщённый анализ наиболее известных схем разделения секрета на основе квантовых технологий. Классификация проведена по таким критериям, как физические принципы, на которых основаны соответствующие методы разделения секрета, и виды задач защиты информации, решаемых этими методами. Рассматриваются перспективные квантовые протоколы разделения секрета с учетом требований, предъявляемых современной квантовой криптографией, в частности – повышение информационной ёмкости протоколов путем использования квантовых систем большой размерности – кудитов. Наиболее перспективными являются квантовые методы разделения секрета на основе многочастичной сцепленности. Кратко рассмотрены некоторые отдельные задачи защиты информации с использованием методов квантового разделения секрета, в частности, совместно контролируемая передача квантового состояния удалённому получателю и гибридные протоколы – протоколы квантовой прямой безопасной связи с контролем над получением информации третьей доверенной стороной. Анализируется состояние современной экспериментальной базы по созданию систем квантового разделения секрета.

***Ключевые слова**: квантовая криптография, квантовое разделение секрета, классификация, кубит, многочастичная сцепленность.*

Введение и анализ предшествующих исследований. В настоящее время обеспечение информационной безопасности является важной и актуальной задачей. Одним из основных направлений противодействия техническим разведкам были и остаются теоретические и инженерно-прикладные исследования в области криптологии. Помимо множества прочих, в структуре ставящихся криптологической наукой целей и решаемых задач выделяется такой раздел, как «разделение секрета» (Secret Sharing) [1]. Суть данного организационно-технического решения заключается в том, что для осуществления управления теми или иными ресурсами в рамках определенной системы необходимо участие более чем одного субъекта. Так, например, во избежание фатальных последствий, управление национальными средствами ядерного поражения осуществляется более чем одним высшим военным должностным лицом, подсчёт голосов в ходе политических выборов, с целью взаимного контроля, осуществляется только совместно представителями противоборствующих партий и международными наблюдателями и т.д.

С другой стороны, одним из перспективных направлений криптологии в настоящее время является квантовая криптография [2], которая продемонстрировала свою привлекательность, в частности, для служб правительственной связи и кредитно-финансовых учреждений. Интенсивные исследования в данной области ведутся более двух десятилетий, что обусловлено появлением технической возможности промышленного серийного производства криптосистем, использующих специфические свойства объектов микромира. Схемы разделения секрета успешно разработаны также и в рамках квантовой криптографии.

С учетом значительного числа предложенных за последние полтора десятка лет в квантовой криптографии схем и протоколов разделения секрета важной задачей является их классификация. Это позволит при проведении последующих исследований существенно облегчить выбор направлений повышения стойкости квантовых схем разделения секрета к различным видам атак. Вместе с тем, до настоящего времени в литературе не был представлена классификация схем квантового разделения секрета, с учетом наукометрических данных, главным образом такого показателя, как количество цитирований публикации.

Наблюдающийся в последние 15–20 лет лавинообразный рост количества публикаций по квантовой криптографии в целом, и непосредственно по квантовому разделению секрета в частности, обуславливает, при построении соответствующей классификации, необходимость «вычленения» из весьма большого массива данных наиболее существенных научных работ по данной тематике. Очевидно, что количество цитирований является одним из важных критериев, по которому целесообразно осуществлять ранжирование публикаций и выделение наиболее ключевых из них.

Таким образом, **целью настоящего исследования** является систематизация и наиболее общий анализ предложенных на сегодняшний день в рамках квантовой криптографии схем и протоколов разделения секрета, в том числе, с

позиций и с применением подходов современной наукометрики.

Общая классификация квантовых схем разделения секрета. При осуществлении той или иной классификации в любой области исследований, как известно, всегда выбираются критерии и признаки, по которым такая классификация проводится. На основании анализа наиболее значимых публикаций, применительно к разновидностям технологий квантового разделения секрета целесообразно осуществлять классификацию по двум признакам: принципам физической реализации и характеру решаемых задач в рамках различных схем разделения секрета.

Если классифицировать схемы квантового разделения секрета по типам физической реализации, то к основным технологиям в рамках этой задачи (рис. 1) относятся: разделение секрета на основе многочастичной сцепленности [3-17], разделение секрета в режиме непрерывных переменных (использование квантовых систем с непрерывным спектром состояний) [18,19], разделение секрета, основанное на квантовой коррекции ошибок [20,21], разделение секрета без использования квантовой сцепленности [22-25] и разделения секрета с использованием квантовой сцепленности по параметру время [26].

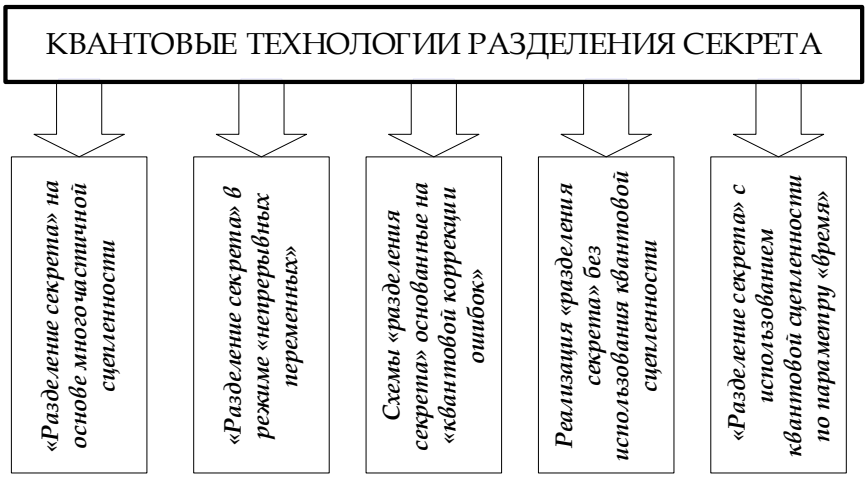

Рис. 1. Основные физические реализации квантовой технологии разделения секрета

Разделение секрета на основе многочастичной сцепленности. В рамках данного подхода реализуются следующие основные протоколы (рис. 2):

- протоколы семейства HBB99 [3-7];
- протокол с использованием состояний Белла и одночастичных измерений [8];
- протоколы с использованием «свопинга» – обмена перепутыванием [9-12];
- протоколы с использованием квантовых гейтов «контролируемое НЕ» и «преобразование Адамара» [13];
- протокол на основе алгоритма Гровера [14];
- протокол на основе перегруппировки порядка используемых квантовых частиц [15];
- протокол на основе квантовой сцепленности W-типа [16];
- протокол на основе ЭПР-пар и измерений в базисе Белла [17].

Впервые квантовое разделение секрета было предложено в 1999 году Hillery, Buzek и Berthiaume [3], в силу чего протокол получил наименование HBB99. Данное решение основано на использовании состояний Гринбергера – Хорна – Цайлингера (ГХЦ) и телепортации квантового состояния кубита. Как и в большинстве реализаций схем квантовой криптографии протокол HBB99 предполагает использование двух базисов. Передача фотонов осуществляется по открытому каналу. Эффективность в плане полезного использования фотонов составляет при полном отсутствии помех 50%. Данное обстоятельство обусловлено необходимостью соответствия измерительных базисов у различных субъектов разделения секрета, что происходит согласно распределению вероятности в половине случаев. Безопасность передачи данных по открытому каналу обеспечивается путем контроля на наличие прослушивающей стороны – так же, как и в протоколе BB84, несостоявшимся считается раунд, в котором процент ошибок превышает определенное установленное значение.

К этому же классу схем следует относить предложенное также в 1999 году решение на основе всего лишь двух связанных квантовой сцепленностью фотонов [4].

Рис. 2. Классификация квантовых протоколов разделения секрета на основе многочастичной сцепленности

Следует отметить, что успешное осуществление квантовой телепортации, которое помимо других приложений предложено для реализации квантового разделения секрета, требует при своей реализации соблюдения ряда условий. К одному из таких условий относятся аспекты, касающиеся характера запутанных состояний. Речь идёт о так называемых «максимально запутанных состояниях». Например, состояние пары кубитов, называемое ЭПР-парой или одним из состояний Белла:

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle - \left|10\right\rangle\right), \qquad (1)$$

является максимально запутанным. Максимально запутанными состояниями квантовой системы, состоящей из двух подсистем могут являться только чистые состояния, при этом для них частичные матрицы плотности должны быть пропорциональны единичной матрице.

При этом на начальном этапе исследования явления телепортации квантового состояния удавалось реализовывать данный процесс исключительно для случаев максимально запутанных состояний. В свою очередь, это создавало существенные трудности для реализации квантового разделения секрета, использующего телепортацию состояния. В силу этого, вскоре после анонсирования протокола HBB99 было проведено успешно завершившееся исследование [5], результатом которого стала возможность в рамках схемы квантового разделения секрета манипулировать с целью телепортации связанными квантовой сцепленностью частицами, состояние системы которых не является максимально запутанным.

Если изначально протокол HBB99 был предназначен для разделения секрета лишь между двумя участниками, то в работе [6] такая схема была расширена на произвольное количество сторон. Ключевым при этом было требование, согласно которому валидным считается такой раунд передачи, в котором количество участников, случайно выбравших одинаковый измерительный базис, является чётным.

Схема на основе пяти-кубитной квантовой сцепленности представлена в работе [7]. В данном решении путём использования сверхплотного кодирования удаётся достичь максимально возможной информационной ёмкости для 5-ти кубитного состояния. Как известно, такая предельно допустимая ёмкость определяется границей Холево.

Большого внимания исследователей заслужила схема разделения произвольного двухкубитного квантового состояния, предложенная Fu-Guo Deng с соавторами [8], которая основана на использовании ЭПР-пар. Характерной особенностью данного решения является задействование такой операции как «product measurement», представляющей собой измерения двух частиц в базисах *z* и *x*, т.е. измерение $\sigma_z \otimes \sigma_x$. При этом любой из N участников процедуры разделения секрета имеет возможность восстановить исход-

ное состояние. Разумеется, это представляется возможным лишь в кооперации с остальными членами группы, разделяющей секрет. В данной схеме имеет место последовательное применение двух локальных унитарных операций участником, уполномоченным получить исходное состояние. Каждому же из остальных членов группы, в ходе взаимодействия с уполномоченным агентом, у которого должно оказаться финальное восстановленное состояние, необходимо осуществить операцию «product measurement». Схема характеризуется высоким процентом эффективного использования квантовых частиц. В ходе реализации процедуры восстановления секрета также используется передача минимального (два бита) количества информации по классическому каналу.

Также весьма известной является предложенная в работе [9] схема, в которой квантовая сцепленность между частицами создается не путем непосредственного взаимодействия между ними, а опосредованно – путём так называемого свопинга (swapping) – обмена перепутыванием.

Обмен перепутыванием состоит в следующем. Для того, чтобы два объекта микромира были связаны квантовой сцепленностью между ними обязательно, хотя бы однажды должно произойти взаимодействие – процессы рассеяния, кулоновское взаимодействие, резонанс Ферми и т. д. Исключение в этом отношении составляют определенные системы фермионов при некоторых специальных условиях (в частности сверхнизкие температуры), однако в квантовой криптографии эти случаи не рассматриваются. Также квантовая сцепленность между частицами может формироваться путем осуществления взаимодействия, но без непосредственного контакта между ними – путем задействования частиц-посредников, с которыми, собственно и происходит тот или иной вид физического взаимодействия и которые впоследствии подвергаются процедуре проекционного «белловского» измерения. После передачи информации о результатах измерения в устройства где находятся частицы, они становятся связанными квантовой сцепленностью так, как если бы они непосредственно провзаимодействовали. Так если рассмотреть две пары связанных квантовой сцепленностью частиц – пару перепутанных частиц 1,2 и аналогичную пару перепутанных между собой частиц 3,4 (при этом частицы различный пар квантовой сцепленностью изначально не связаны), то:

$$\left|\Psi\right\rangle_{1234} = \left|\Psi^{-}\right\rangle_{12} \otimes \left|\Psi^{-}\right\rangle_{34}. \qquad (2)$$

В базисе белловских состояний состояние $\left|\Psi\right\rangle_{1234}$ записывается следующим образом:

$$\left|\Psi\right\rangle_{1234} = \left|\Psi^{+}\right\rangle_{14} \otimes \left|\Psi^{+}\right\rangle_{23} - \left|\Psi^{-}\right\rangle_{14} \otimes \left|\Psi^{-}\right\rangle_{23} - \left|\Phi^{+}\right\rangle_{14} \otimes \left|\Phi^{+}\right\rangle_{23} - \left|\Phi^{-}\right\rangle_{14} \otimes \left|\Phi^{-}\right\rangle_{23}. \qquad (3)$$

Теперь, если осуществить процедуру проекционного измерения частиц 2 и 3 в базисе Белла, то в перепутанном состоянии окажутся между собой частицы 1 и 4.

Помимо, собственно, реализованной в рамках данной конкретной схемы процедуры обмена перепутывания, в работе [9] также описано использование плотного кодирования, что существенно повышает эффективность протокола в плане передачи данных.

Реализация квантового разделения секрета на основе обмена перепутыванием также описана в другой публикации [10], где в качестве преимущества данного подхода продемонстрирована возможность произвольного выбора для решения задачи совместного реконструирования секрета тех или иных подмножеств участников из общего числа задействованных пользователей схемы, т.е. квантовая реализация (k, n) – пороговой схемы.

Использование обмена перепутыванием для осуществления процедуры разделения секрета описано и в работе [11]. Характерной особенностью исследования, изложенного в этой публикации, является рассмотрения аспектов реализации многомерных квантовых систем – кудитов, имеющих размерность гильбертова пространства более двух. Авторы данной работы справедливо указывают, что более высокая размерность гильбертова пространства при формировании конфигурации системы квантовых битов позволяет уменьшить количество кудитов. Это, в свою очередь, существенно упрощает инженерную реализацию прикладных задач, поскольку с увеличением количества квантовых битов связь и управление передачей информацией становятся более трудными.

Ещё одно известное решение по квантовому разделению секрета на основе обмена перепутыванием представлено в работе [12]. К его преимуществам относятся менее критичные требования в плане квантовых ресурсов, более удобная реализация за счет использования только двухкубитной сцепленности, а также приближающаяся

к 100% эффективность в силу почти полного использования передаваемых частиц.

Спецификой схемы квантового разделения секрета, представленной в работе [13], является поочередное формирование квантовой сцепленности и последующее её «распутывание» путём действия широко применяемых в квантовых вычислениях простых логических элементов – гейтов. Конкретно, в данном протоколе используются гейты «контролируемое НЕ» и «преобразование Адамара». Предложенный в работе [13] протокол предполагает, что запутанные состояния частиц, которые находятся у отправителя и получателя, выступают в роли несущей, с которой, в свою очередь, запутываются кубиты данных отправителя. Впоследствии эти информационные кубиты распутываются получателем путём воздействия соответствующими гейтами.

На одном из самых известных квантовых алгоритмов – так называемом алгоритме Гровера основана схема квантового разделения секрета, представленная в работе [14]. Суть алгоритма Гровера заключается в возможности осуществления поиска заданного значения в базе данных при помощи квантовых устройств полиномиально быстрее, чем это возможно сделать в классическом случае. Например, если в базе данных содержится N записей, то вместо в среднем $0,5 \cdot N$ обращений к базе в случае классического поиска, при использовании квантовых свойств для успешного нахождения нужного значения достаточно $\sqrt{N}$ обращений. Это достигается, в том числе, и за счет присущего квантовым системам принципа суперпозиции состояний. Конфигурация интерференционных характеристик квантовой системы выбирается такой, что в ходе поиска, который состоит из некоторого числа этапов, на каждом таком этапе связанные с искомым значением параметры усиливают друг друга. И хотя в протоколе [14] нет необходимости в существенном увеличении скорости поиска, особенности обработки квантовой информации, предоставляемые алгоритмом Гровера, позволяют весьма изящно реализовать определенные технические детали при реализации схемы квантового разделения секрета.

Ещё одним примером использования EPR-пар для реализации квантового разделения секрета является схема, описанная в работе [15]. Её характерной особенностью является перегруппировка порядка связанных квантовой сцепленностью частиц. Частицы, по сути, перетасовываются таким образом, что получатели без оглашения необходимой информации отправителем не имеют возможности определить, какие из частиц состоят друг с другом в EPR-паре. За счет этого обстоятельства обеспечивается защита от нечестных участников внутри самой схемы. Преимуществами данной схемы являются использование всех EPR-пар, что приближает эффективность к 100%, а также перенос сразу двух битов информации каждой парой за счет использования квантового сверхплотного кодирования. Кроме того, в качестве преимущества данного решения авторы указывают на существенное снижение объема передаваемой классической информации.

В работе [16] схема квантового разделения секрета основана на специфической разновидности квантовой сцепленности – так называемых перепутанных состояний W-типа. Характерной особенностью таких состояний является меньшая по сравнению с тривиальным видом квантовой сцепленности подверженность декогеренции – процессу потери системой квантовой когерентности из-за перепутывания составляющих её объектов микромира с окружением. При декогеренции происходит потеря наблюдателем информации о фазовых коэффициентах, в результате чего наблюдаемые чистые состояния в рамках системы переходят в смешанные. Предложенное же авторами в работе [16] решение позволяет уменьшить проявление декогеренции при реализации конкретных инженерных решений.

Последняя рассматриваемая нами схема разделения секрета на основе EPR-пар представлена протоколом [17], где в качестве перепутанных состояний выступают четыре (одно из четырёх возможных для каждого отдельного случая) состояния Белла. Конфигурация данной схемы сформирована таким образом, что путем последовательной передачи отдельных частиц из каждой EPR-пары и соответствующего применения унитарных операций, основанных на единичном операторе и матрицах Паули удаётся добиться ситуации, когда секрет может быть восстановлен лишь при совместном участии заданного количества сторон. Контроль прослушивания осуществляется измерением состояний специально предназначенных для этой процедуры фотонов и запросом определенной стороной полученных результатов.

Разделение секрета в режиме «непрерывных переменных». Немалый интерес вызвала также реализация разделения секрета, основанная на так называемых «непрерывных переменных» (continuous variable) [18]. Хорошо из-

вестно, что при рассмотрении некоторой физической величины, характеризующей квантовое состояние, принято говорить об определенном наборе значений, который она может принимать. При этом такой набор в квантовой механике (он также называется собственными значениями оператора) в большинстве случаев не представляет непрерывный ряд значений, а является так называемым «дискретным спектром». Однако в ряде случаев (в том числе путем искусственного создания определенных условий) удаётся наблюдать наличие непрерывного спектра собственных значений физической величины, измеряемой в квантовой системе. Использование схем на основе непрерывного спектра оправдало себя для многих решений в квантовой криптографии и, в частности, применительно к решениям по разделению секрета. Так, например, преимуществом реализации, описанной в работе [18], является возможность масштабирования схемы разделения секрета без, как правило, возникающей в таком случае необходимости повышения сложности технических средств инженерной реализации, сопряженной с увеличением количества различного рода оптических элементов.

В другой, также хорошо известной исследователям работе [19], представляющей собой развитие идеи реализации «разделения секрета» на основе непрерывного спектра собственных значений, указывается, что отсутствие необходимости повышения уровня использования квантовых ресурсов при построении такой схемы делает эту методику весьма перспективной для данной области криптографии. При этом исследование, описанное в работе [19], позиционирует квантовый ресурс, как единственно используемый в данном конкретном решении.

Схемы разделения секрета, основанные на квантовой коррекции ошибок. Практически одновременно с пионерской работой [3] было опубликовано альтернативное протоколу HBB99 решение на основе кутритов [20]. Авторы указанной публикации отмечают, что предложенная ими схема с тремя связанными квантовой сцепленность кутритами, по сути, подобна предложенным ранее решениям, целью которых является коррекция возникающих в ходе квантовых вычислений ошибок. Данная работа характеризуется превалированием в ходе изложения теоретических концептов над, собственно, описанием потенциальных возможностей практической реализации описываемой схемы. В этой связи следует заметить, что, несмотря на весьма значимое количество цитирований этого материала, по-видимому, существенного развития в плане предложений инженерно-организационной реализации подобные схемы не получили.

Еще большей теоретической направленностью характеризуется являющаяся в определенной мере развитием работы [20] статья Daniel Gottesman [21]. В данной работе также большое внимание уделяется концепции, согласно которой некоторые решения по разделению секрета тесным образом сопряжены с определенными аспектами квантовой коррекции ошибок.

Реализация разделения секрета без использования квантовой сцепленности. Известный интерес в рамках совершенствования схем разделения секрета представляют реализации на основе так называемых «product state» – частном случае так называемых «сепарабельных состояний».

Как известно, в квантовой теории информации сепарабельными называются состояния составных (состоящих из более чем одной подсистем) систем, для подсистем которых в рамках конкретной составной системы не наблюдается квантовой сцепленности. С точки зрения математического формализма это означает, что матрица плотности составной системы может быть представлена в виде:

$$\rho = \sum_k p_k \rho_k^A \otimes \rho_k^B , \qquad (4)$$

где ρ – матрица плотности составной системы, ρ_k^A и ρ_k^B – матрицы плотности первой и второй подсистем соответственно, представляющие собой ансамбли чистых состояний, а набор коэффициентов p удовлетворяет условию:

$$\sum_k p_k = 1. \qquad (5)$$

В свою очередь, «product state» – это состояние, когда в сумме (4) только один коэффициент p отличен от нуля. Очевидно, что в этом случае матрица плотности составной системы представима в виде:

$$\rho = \rho^A \otimes \rho^B . \qquad (6)$$

Описание схемы разделения секрета на основе «product state» было предложено в работе [22], авторы которой демонстрируют определенные преимущества такого подхода по сравнению с некоторыми ранее предложенными схемами, а именно: возможность инженерно-практической реализации для случаев с большим числом субъектов разделения секрета, а также эффективность использования частиц, которая приближается к 100 %.

Другим примером осуществления квантового «разделения секрета» без использования квантовой сцепленности является решение, предложенное в работе [23]. В отличие от предыдущей схемы отсутствие квантовой сцепленности в данном случае обусловлено не формированием «product state», а использованием полностью изолированных друг от друга единичных фотонов. В силу того, что частицы никак не взаимодействуют друг с другом, возникновение квантовой сцепленности исключено. Задача же решается последовательной передачей фотонов от одного участника к другому с применением некоторыми участниками специальных унитарных операций, воздействующих на частицы. Инженерная реализация, основанная на таком принципе, по ряду технических аспектов определенным образом облегчена в сравнении со схемами, использующими ГЦХ-состояния. Вместе с тем, буквально сразу же после публикации работы [23] в данном протоколе была выявлена подверженность атаке со стороны одного из участников разделения секрета. Потенциальная возможность эффективного изменения изначально предложенной схемы с целью ликвидировать указанный изъян, позволила добиться приемлемой с точки зрения криптографической стойкости конфигурации [24]. Обе эти публикации (с изложением изначальной и улучшенной схем) привлекли, согласно показателям цитируемости, значимое внимание среди специалистов, занимающимися исследованиями в области квантового разделению секрета.

Схема на основе единичных фотонов предложена также в работе [25]. Основным преимуществом данной реализации также, как и для схемы на основе «product state» [22] является 100% использование фотонов, что значимо снижает потребность в квантовых ресурсах.

Реализация разделения секрета с использованием квантовой сцепленности по параметру «время». Очень элегантным и, в то же время, достаточно известным является метод «разделения секрета», в основу которого положено использование квантовой сцепленности по параметру «время» [26] (рис. 3). Характерным в этой схеме является то, что в качестве базиса выступает не горизонтальная и диагональная поляризация фотонов, как практически во всех решениях по разделению секрета, а время прибытия фотона в интерферометре. Для этой цели используется широко применяемый в лабораторной практике интерферометр Маха-Цандера. При этом, однако, использовано оригинальное решение, в котором интерферометр выполнен на базе двух оптоволоконных линий связи. Одна из этих линий – короткое плечо интерферометра, имеет меньшую длину, чем вторая – длинное плечо. Фотон изначально поступает в разделитель пучка (луча) из которого выходят две указанных оптоволоконных линии. С определенной вероятностью, определяемой коэффициентами α и β, фотон «пройдёт» либо по короткому, либо по длинному плечу интерферометра. При этом разность длин плеч интерферометра выбрана такой, чтобы фотон не интерферировал сам с собой. В результате, в качестве базиса выступает множество $\{\text{long}, \text{short}\}$, где long – фотон прибыл по длинному пути, short – фотон прибыл по короткому пути. В итоге имеется кубит, описываемый как,

$$\alpha|long\rangle + \beta|short\rangle, \qquad (7)$$

то есть представляющий собой суперпозицию двух состояний фотона: «прибыл быстро» и «прибыл медленно». Далее, на выходе из интерферометра, фотон поступает в устройство формирования уже двух, связанных квантовой сцепленностью фотонов. Оно выполнено на основе нелинейного кристалла ($LiNbO_3$). При взаимодействии с узлами кристаллической решетки в результате спонтанного параметрического преобразования частоты «вниз» происходит спонтанный распад фотона на два, связанных между собой квантовой сцепленностью:

$$\alpha|short\rangle_s \otimes |short\rangle_i + \beta|long\rangle_s \otimes |long\rangle_i, \qquad (8)$$

где индексы s и i обозначают «сигнальный» (signal) и «незанятый» (idler) фотоны соответственно. Далее, каждый из образовавшейся пары связанных квантовой сцепленностью фотонов попадает на повёрнутый противоположным концом такой же интерферометр, в результате чего становится возможной интерференция состояний «long» и «short». И, наконец, путём выполнения определенных измерений и определенного протокола, в данной схеме становится возможным реализация процедуры разделения секрета. В качестве преимущества такого инженерного решения можно отметить отсутствие необходимости придерживаться определенной длины когерентности лазера накачки, а также возможность построения устройства без использования большого количества оптических схем.

Что же касается характера решаемых задач в рамках различных схем разделения секрета

(рис. 4), то наибольшее внимание исследователей уделяется вопросам совместного контроля телепортации квантового состояния, взаимного контроля при совместном осуществлении процедуры зашифрования–расшифрования, а также – разделения секрета при реализации квантовой прямой безопасной связи.

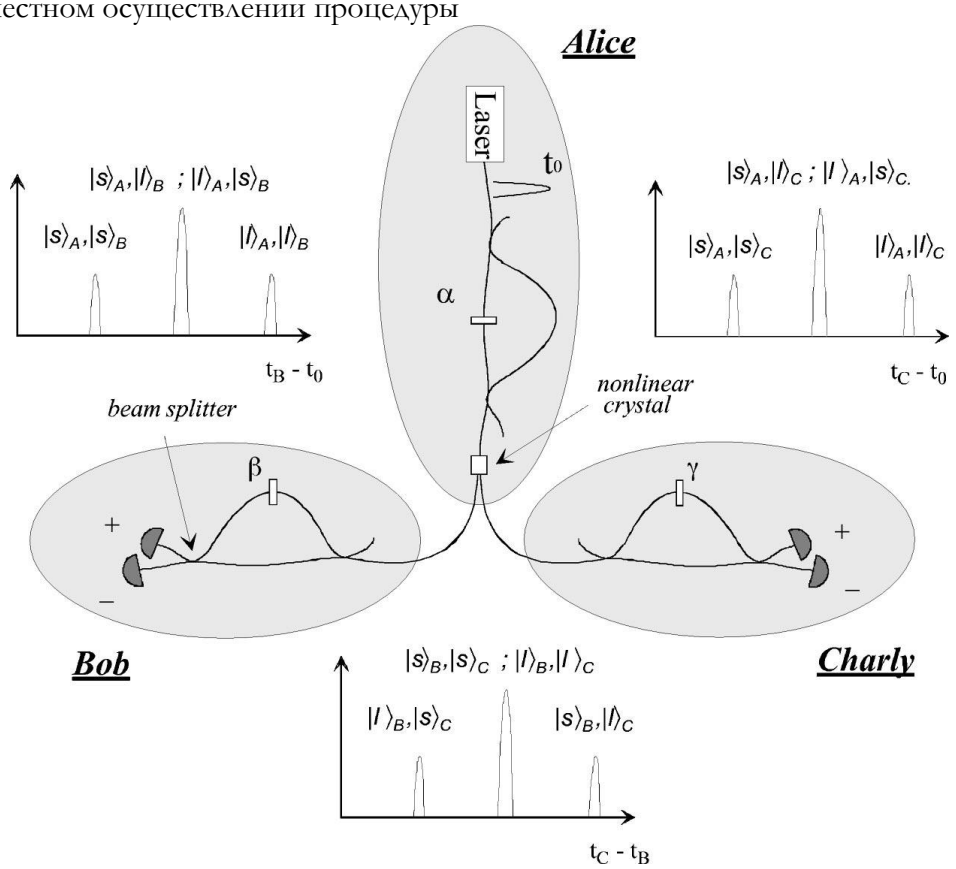

Рис. 3. Схема разделения секрета на основе интерферометров Маха-Цандера в оптоволоконном исполнении [26]

Совместно контролируемая передача квантового состояния удалённому получателю. Весьма полезным для решения ряда задач защищенной передачи данных и управления является метод, предложенный в работе [27]. В указанной публикации представлен способ телепортации мультикубитной квантовой информации от отправителя удалённому получателю под контролем нескольких доверенных участников в сети передачи данных. Продемонстрировано, что исходное состояние каждого кубита может быть восстановлено получателем тогда, когда все участники в сети сотрудничают. Если же хотя бы один из участников в сети по той или иной причине не задействован в коллективном контроле передачи, то получатель не имеет возможности в полном объеме восстановить передаваемую информацию. Авторы позиционируют данную методику как актуальную для реализации сетевой квантовой обработки информации и защищенной конференцсвязи.

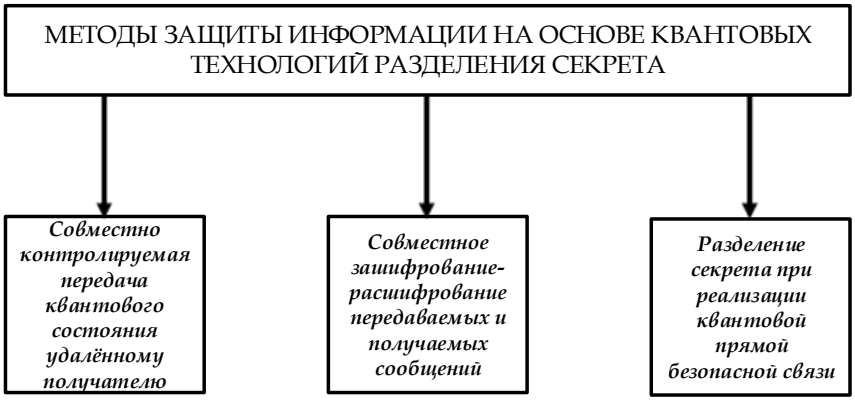

Рис. 4. Распространенные методы ЗИ на основе квантовой технологии разделения секрета

Своё развитие эта идея получила и в работе [28], которая получила большую известность и которая является одной из самых цитируемых публикаций по квантовому разделению секрета. Как и для ряда описанных выше схем, в качестве преимущества решения, предложенного в работе [28], авторы указывают высокую эффективность за счет использования в качестве носителей информации всех экземпляров передаваемых частиц.

На основе схемы, описанной в работе [28], впоследствии было разработано другое решение по осуществлению совместно контролируемой квантовой телепортации [29]. Его особенностью является использование в протоколе уже упомянутой выше операции «product measurement» [8]. За счет полного использования передаваемых по каналу связи частиц эффективность схемы приближается к 100%.

Совместное зашифрование - расшифрование передаваемых и получаемых сообщений. В публикации [30] решена проблема совместной криптозащиты. В случае, когда имеется два коллективных абонента, между которыми необходимо осуществлять конфиденциальную связь – например, два различных подразделения государственного учреждения, разделение секрета является незаменимым для ситуации, когда сотрудники должны совместно контролировать друг друга. При подготовке зашифрованного сообщения для передачи его в подразделение–получатель к процессу зашифрования привлекаются все уполномоченные для этого сотрудники подразделения–отправителя. Тогда в процессе расшифрования будут, соответственно, участвовать все уполномоченные сотрудники подразделения–отправителя. Отсутствие или бездействие хотя бы одного из уполномоченных сотрудников в отправляющем или принимающем подразделении сделает невозможным процесс зашифрования и рашифрования соответственно.

Разделение секрета при реализации квантовой прямой безопасной связи. Квантовая прямая безопасная связь – это один из основных видов защиты информации на основе квантовых технологий. Спецификой данного метода является отсутствие необходимости осуществлять криптографические преобразования, что в свою очередь, позволяет обходиться без процедуры распределения ключей шифрования.

Наряду со множеством предложенных к настоящему времени разновидностей протоколов квантовой прямой безопасной связи, в работе [31] был представлен вариант, предусматривающий использование в рамках реализации такого решения принципа разделения секрета. В этом случае успешное прочтение переданного отправителем сообщения возможно лишь тогда, когда имеется более чем один получатель, передача отправителем осуществляется этим нескольким получателем, и эти получатели должны совместно осуществить декодирование. Близким к данному принципу по своей сути является решение, предложенное в работе [32]. Здесь один из участников – лицо, желающее передать информацию посредством квантовой прямой безопасной связи таким образом, чтобы лицо, которому информация передаётся, имело возможность прочесть её исключительно в присутствии третьего лица, которому отправитель доверяет. Принципиально данная схема основана на распределении последовательностей кубитов из перепутанных ГЦХ-состояний между участниками протокола.

На рис. 5 представлена обобщенная схема наиболее известных на сегодняшний день методов и схем защиты информации, в основе которых лежит принцип квантового разделения секрета.

Перспективные направления исследований квантового разделения секрета. Значительно позже первых описанных в публикациях схем квантового разделения секрета было предложено решение на основе так называемых «graph state» [33]. Однако впоследствии в работе [34] была показана уязвимость такой схемы к определенно организованной атаке. В силу этого, хотя идея реализации квантового разделения секрета с использованием «graph state» и привлекла к себе внимание специалистов, очевидно, что необходимы дополнительные исследования с целью обеспечения стойкости протоколов такого класса.

Что же касается общих тенденций в области исследований по квантовому разделению секрета, то, как было отмечено во вводной части работы, в настоящее время основная масса публикаций посвящена усовершенствованию уже предложенных ранее базовых схем и повышению криптографической стойкости. Показательным в этом отношении примером является эволюция исследований стойкости протокола [35], который был предложен более 5-ти лет назад, положив начало серии публикаций, последние из которых выходили вплоть до недавнего времени [36, 37]. Работа [35] отражает некоторые характерные направления и подходы, которых придерживаются в настоящее время в рамках изысканий по повышению криптографической стойкости и инфор-

мационной ёмкости схем и протоколов квантового разделения секрета. В частности, одним из таких подходов является повышение размерности используемых в криптографических схемах квантовых систем – кудитов. То есть осуществляется переход от кубитов к кутритам и квантовым системам, имеющим ещё большую размерность. Это позволяет повысить информационную ёмкость реализуемых протоколов.

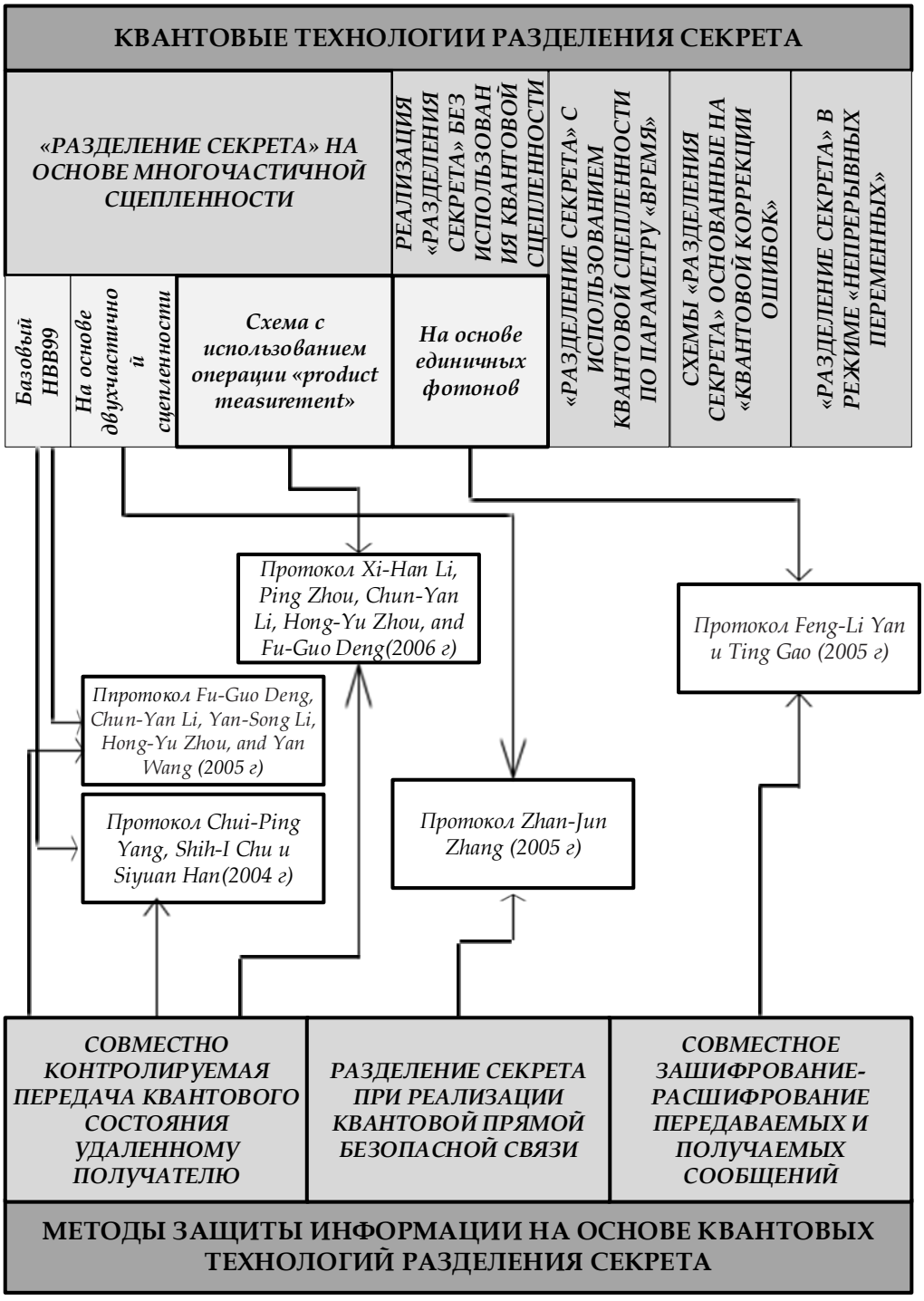

Рис. 5. Классификация некоторых методов защиты информации на основе квантового разделения секрета

Особый интерес представляют работы по созданию эффективных экспериментальных установок, реализующих квантовые схемы разделения секрета. Очевидно, что такие лабораторные исследования являются необходимым этапом на пути создания серийно производимых промышленностью криптосистем этого класса и потенциально в перспективе могут быть трансформированы в используемые на практике устройства. Одной из первых экспериментальных реализаций схемы разделения секрета на основе квантовой технологии является решение, описанное в

уже указанной выше работе [26], используемый здесь физический принцип – квантовая сцепленность по параметру «время». К наиболее интересным более поздним схемам, предложенным для экспериментальной реализации, относится установка, описанная интернациональным коллективом авторов (Германия, Швеция, Сингапур) [38], в которой осуществляется последовательное преобразование единичного кубита, последующее решение этих же исследователей уже на основе четырехфотонной сцепленности [39], разработка шведской части этой группы с использованием оптоволоконной техники [40], и, наконец, – новейшая лабораторная техника квантового разделения секрета недавно созданная в стенах Массачусетского технологического института [41].

Выводы. В работе выполнена систематизация и классификация современных методов разделения секрета на основе квантовых технологий. Детально рассмотрены все предложенные в литературе к настоящему времени основные схемы и протоколы в рамках предложенной в работе классификации на пять основных групп: разделение секрета на основе многочастичной сцепленности; разделение секрета в режиме непрерывных переменных; разделение секрета, основанное на квантовой коррекции ошибок; разделение секрета без использования квантовой сцепленности; разделение секрета с использованием квантовой сцепленности по параметру «время». Также кратко рассмотрены некоторые задачи, имеющие отношение к технологиям квантового разделения секрета, в частности, совместно контролируемая передача квантового состояния удалённому получателю и гибридные протоколы – протоколы квантовой прямой безопасной связи с контролем над получением информации третьей доверенной стороной. Далее обсуждаются некоторые экспериментальные реализации квантового разделения секрета и перспективы дальнейших исследований в этой области защиты информации.

В результате проведенного исследования выделены наиболее перспективные направления в области квантового разделения секрета, что позволяет эффективно определять дальнейшие направления исследований, в частности, для отечественного научного сообщества, так как в отечественной научной литературе публикации по этой тематике до настоящего времени практически отсутствовали.

ЛИТЕРАТУРА:

[1]. Shamir A. How to Share a Secret // Communications of the ACM.-1979.-V.22, issue 11.-P.612-613.

[2]. Scarani V. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev // Reviews of Modern Physics.-2009.-V.81, issue 3.-1301.

[3]. Hillery M. Quantum Secret Sharing / M. Hillery, V. Buzek, A. Berthiaume // Physical Review A.-1999.-V.59, issue 3.-P.1829-1834.

[4]. Karlsson A. Quantum Entanglement for Secret Sharing and Secret Splitting / A. Karlsson, M. Koashi, N. Imoto // Physical Review A.-1999.-V.59, issue 1.-P.162-168.

[5]. Bandyopadhyay S. Teleportation and secret sharing with pure entangled states // Physical Review A.-2000.-V.62, issue 1.- 012308.

[6]. Xiao L. Efficient Multiparty Quantum-Secret-Sharing Schemes / L. Xiao, G.L. Long, F.G. Deng, J.W. Pan // Physical Review A.-2004.-V.69, issue 5.-052307.

[7]. Muralidharan S. Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state / S. Muralidharan, P.K. Panigrahi // Physical Review A.-2008.-V.77, issue 3.- 032321.

[8]. Deng F.G. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs / F.G. Deng , X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou // Physical Review A.-2005.-V.72, issue 4.- 044301.

[9]. Zhang Z. Multiparty quantum secret sharing of classical messages based on entanglement swapping / Z. Zhang, Z. Man // Physical Review A.-2005.-V.72, issue 2.- 022303.

[10]. Li Y. Multiparty secret sharing of quantum information based on entanglement swapping / Y. Li, K. Zhang, K. Peng // Physics Letters A.-2004.-V. 324, issues 5-6.- P.420-424.

[11]. Karimipour V. Entanglement swapping of generalized cat states and secret sharing / V. Karimipour, A. Bahraminasab, S. Bagherinezhad // Physical Review A.-2002.-V.65, issue 4.- 042320.

[12]. Deng F.G. Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements / F.G. Deng, X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou // The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics.-2006.-V.39, issue 3.-P.459-464.

[13]. Bagherinezhad S. Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers / S. Bagherinezhad, V. Karimipour // Physical Review A.-2003.-V. 67, issue 4.-044302.

[14]. Hsu L.Y. Quantum secret-sharing protocol based on Grover's algorithm // Physical Review A.-2003.-V.68, issue 2.- 022306.

[15]. Deng F.G. An efficient quantum secret sharing scheme with Einstein–Podolsky–Rosen pairs / F.G. Deng, G.L. Long, H.Y. Zhou // Physics Letters A.-2005.-V. 340, issues 1-4.- P.43-50.

[16]. Zheng S.B. Splitting quantum information via W states // Physical Review A.-2006.-V.74, issue 5.-054303.

[17]. Deng F.G. Multiparty quantum secret splitting and quantum state sharing / F.G. Deng, X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou // Physics Letters A.-2006.-V. 354, issue 3.- P.190-195.

[18]. Lance A.M. Tripartite Quantum State Sharing / A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, P.K. Lam // Physical Review Letters.-2004.-V.92, issue 17.- 177903.

[19]. Lance A.M. Continuous-variable quantum-state sharing via quantum disentanglement / A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, T. Tyc, T.C. Ralph, P.K. Lam // Physical Review A.-2005.-V.71, issue 3.- 033814.

[20]. Cleve R. How to Share a Quantum Secret / R. Cleve, D. Gottesman, H. Lo // Physical Review Letters.-1999.-V.83, issue 3.-P.648-651.

[21]. Gottesman D. Theory of quantum secret sharing // Physical Review A.-2000.-V.61, issue 4.- 042311.

[22]. Guo G.P. Quantum secret sharing without entanglement / G.P. Guo, G.C. Guo // Physics Letters A.-2003.-V. 310, issue 4.- P.247-251.

[23]. Zhang Z. Multiparty quantum secret sharing / Z. Zhang, Y. Li, Z. Man // Physical Review A.-2005.-V.71, issue 4.-044301.

[24]. Deng F.G. Improving the security of multiparty quantum secret sharing against Trojan horse attack / F.G. Deng, X.H. Li, H.Y. Zhou, Z. Zhang // Physical Review A.-2005.-V.72, issue 4.- 044302.

[25]. Deng F.G. Bidirectional quantum secret sharing and secret splitting with polarized single photons / F.G. Deng, H.Y. Zhou, G.L. Long // Physics Letters A.-2005.-V. 337, issues 4-6.- P.329-334.

[26]. Tittel W. Experimental demonstration of quantum secret sharing / W. Tittel, H. Zbinden, N. Gisin // Physical Review A.-2001.-V.63, issue 4.- 042301.

[27]. Yang C.P. Efficient many-party controlled teleportation of multiqubit quantum information via entanglement / C.P. Yang, S.I. Chu, S. Han // Physical Review A.-2004.-V.70, issue 2.- 022329.

[28]. Deng F.G. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement / F.G. Deng, C.Y. Li, Y.S. Li, H.Y. Zhou, Y. Wang // Physical Review A.-2005.-V.72, issue 2.- 022338.

[29]. Li X.H. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state / X.H. Li, P. Zhou, C.Y. Li, H.Y. Zhou, F.G. Deng // Journal of Physics B: Atomic, Molecular and Optical Physics.-2006.-V.39, issue 8.-1975.

[30]. Yan F.L. Quantum secret sharing between multiparty and multiparty without entanglement / F.L. Yan, T. Gao // Physical Review A.-2005.-V.72, issue 1.-012304.

[31]. Zhang Z.J. Multiparty quantum secret sharing of secure direct communication // Physics Letters A.-2005.-V. 342, issues 1-2.- P.60-66.

[32]. Wang J. Multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state / J. Wang, Q. Zhang, C. Tang // Optics Communications.-2006.-V. 266, issue 2.-P.732-737.

[33]. Markham D. Graph states for quantum secret sharing / D. Markham, B.C. Sanders // Physical Review A.-2008.-V.78, issue 4.- 042309.

[34]. Hsu L.Y. Cryptanalysis of Quantum Secret Sharing Using Graph States / L.Y. Hsu, W.T. Yen // Chinese Journal of Physics.-2010.-V.48, issue 1.-P.138-142.

[35]. GAO Gan Multiparty Quantum Secret Sharing Using Two-Photon Three-Dimensional Bell States // Communications in Theoretical Physics.-2009.-V.52, issue 3.-P.421-424.

[36]. Song T.T. Participant Attack and Improvement to Multiparty Quantum Secret Sharing Based on GHZ States / T.T. Song, Q.Y. Wen, F. Gao, H. Chen // International Journal of Theoretical Physics.-2013.-V.52, issue 1.- P.293-301.

[37]. Tan X. Improved Three-Party Quantum Secret Sharing Based on Bell States / X. Tan, L. Jiang // International Journal of Theoretical Physics.-2013.-V.52, issue 10.- P.-3577-3585.

[38]. Schmid C. Experimental Single Qubit Quantum Secret Sharing / C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, H. Weinfurter // Physical Review Letters.-2005.-V.95, issue 23.-230505.

[39]. Gaertner S. Experimental Demonstration of Four-Party Quantum Secret Sharing / S. Gaertner, C. Kurtsiefer, M. Bourennane, H. Weinfurter // Physical Review Letters.-2007.-V.98, issue 2.-020503.

[40]. Bogdanski J. Experimental quantum secret sharing using telecommunication fiber / J. Bogdanski, N. Rafiei, M. Bourennane // Physical Review A.-2008.-V.78, issue 6.- 062307.

[41]. Bhatia P.S. Experimental tripartite quantum state sharing and perfect teleportation of the two-qubit photonic state using genuinely entangled multipartite states // Journal of the Optical Society of America B.-2014.-V.31, issue 1.-P.154-163.

REFERENCES

[1]. Shamir A. How to Share a Secret, Communications of the ACM., 1979., V.22, issue 11, P.612-613.

[2]. Scarani V. The security of practical quantum key distribution, V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, Reviews of Modern Physics, 2009, V.81, issue 3.-1301.

[3]. Hillery M. Quantum Secret Sharing, M. Hillery, V. Buzek, A. Berthiaume, Physical Review A., 1999, V.59, issue 3, P.1829-1834.

[4]. Karlsson A. Quantum Entanglement for Secret Sharing and Secret Splitting, A. Karlsson, M. Koashi, N. Imoto, Physical Review A., 1999., V.59, issue 1, P.162-168.

[5]. Bandyopadhyay S. Teleportation and secret sharing with pure entangled states, Physical Review A., 2000., V.62, issue 1.- 012308.

[6]. Xiao L. Efficient Multiparty Quantum-Secret-Sharing Schemes, L. Xiao, G.L. Long, F.G. Deng, J.W. Pan, Physical Review A., 2004, V.69, issue 5.- 052307.

[7]. Muralidharan S. Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state, S. Muralidharan, P.K. Panigrahi, Physical Review A., 2008.-V.77, issue 3.- 032321.

[8]. Deng F.G. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs, F.G. Deng , X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou, Physical Review A., 2005., V.72, issue 4.- 044301.

[9]. Zhang Z. Multiparty quantum secret sharing of classical messages based on entanglement swapping, Z. Zhang, Z. Man, Physical Review A., 2005., V.72, issue 2.- 022303.

[10]. Li Y. Multiparty secret sharing of quantum information based on entanglement swapping, Y. Li, K. Zhang, K. Peng, Physics Letters A., 2004., V. 324, issues 5-6.- P.420-424.

[11]. Karimipour V. Entanglement swapping of generalized cat states and secret sharing, V. Karimipour, A. Bahraminasab, S. Bagherinezhad, Physical Review A., 2002., V.65, issue 4.- 042320.

[12]. Deng F.G. Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements, F.G. Deng, X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou, The European Physical Journal D, Atomic, Molecular, Optical and Plasma Physics., 2006., V.39, issue 3.-P.459-464.

[13]. Bagherinezhad S. Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers, S. Bagherinezhad, V. Karimipour, Physical Review A., 2003., V. 67, issue 4.-044302.

[14]. Hsu L.Y. Quantum secret-sharing protocol based on Grover's algorithm, Physical Review A., 2003., V.68, issue 2.- 022306.

[15]. Deng F.G. An efficient quantum secret sharing scheme with Einstein–Podolsky–Rosen pairs, F.G. Deng, G.L. Long, H.Y. Zhou, Physics Letters A., 2005., V. 340, issues 1-4., P.43-50.

[16]. Zheng S.B. Splitting quantum information via W states, Physical Review A., 2006., V.74, issue 5.- 054303.

[17]. Deng F.G. Multiparty quantum secret splitting and quantum state sharing, F.G. Deng, X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou, Physics Letters A., 2006., V. 354, issue 3., P.190-195.

[18]. Lance A.M. Tripartite Quantum State Sharing, A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, P.K. Lam, Physical Review Letters., 2004., V.92, issue 17.- 177903.

[19]. Lance A.M. Continuous-variable quantum-state sharing via quantum disentanglement, A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, T. Tyc, T.C. Ralph, P.K. Lam, Physical Review A., 2005., V.71, issue 3.- 033814.

[20]. Cleve R. How to Share a Quantum Secret, R. Cleve, D. Gottesman, H. Lo, Physical Review Letters.- 1999., V.83, issue 3., P.648-651.

[21]. Gottesman D. Theory of quantum secret sharing, Physical Review A., 2000., V.61, issue 4.- 042311.

[22]. Guo G.P. Quantum secret sharing without entanglement, G.P. Guo, G.C. Guo, Physics Letters A., 2003.,V. 310, issue 4., P.247-251.

[23]. Zhang Z. Multiparty quantum secret sharing, Z. Zhang, Y. Li, Z. Man, Physical Review A., 2005., V.71, issue 4.-044301.

[24]. Deng F.G. Improving the security of multiparty quantum secret sharing against Trojan horse attack, F.G. Deng, X.H. Li, H.Y. Zhou, Z. Zhang, Physical Review A., 2005., V.72, issue 4.- 044302.

[25]. Deng F.G. Bidirectional quantum secret sharing and secret splitting with polarized single photons, F.G. Deng, H.Y. Zhou, G.L. Long, Physics Letters A., 2005., V. 337, issues 4-6., P.329-334.

[26]. Tittel W. Experimental demonstration of quantum secret sharing, W. Tittel, H. Zbinden, N. Gisin, Physical Review A., 2001., V.63, issue 4.- 042301.

[27]. Yang C.P. Efficient many-party controlled teleportation of multiqubit quantum information via entanglement, C.P. Yang, S.I. Chu, S. Han, Physical Review A., 2004., V.70, issue 2.- 022329.

[28]. Deng F.G. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement, F.G. Deng, C.Y. Li, Y.S. Li, H.Y. Zhou, Y. Wang, Physical Review A., 2005., V.72, issue 2.- 022338.

[29]. Li X.H. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state, X.H. Li, P. Zhou, C.Y. Li, H.Y. Zhou, F.G. Deng, Journal of Physics B: Atomic, Molecular and Optical Physics., 2006., V.39, issue 8.-1975.

[30]. Yan F.L. Quantum secret sharing between multiparty and multiparty without entanglement, F.L. Yan, T. Gao, Physical Review A., 2005., V.72, issue 1.- 012304.

[31]. Zhang Z.J. Multiparty quantum secret sharing of secure direct communication, Physics Letters A., 2005., V. 342, issues 1-2., P.60-66.

[32]. Wang J. Multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state, J. Wang, Q. Zhang, C. Tang, Optics Communications., 2006., V. 266, issue 2., P.732-737.

[33]. Markham D. Graph states for quantum secret sharing, D. Markham, B.C. Sanders, Physical Review A., 2008., V.78, issue 4.- 042309.

[34]. Hsu L.Y. Cryptanalysis of Quantum Secret Sharing Using Graph States, L.Y. Hsu, W.T. Yen, Chinese Journal of Physics., 2010., V.48, issue 1., P.138-142.

[35]. GAO Gan Multiparty Quantum Secret Sharing Using Two-Photon Three-Dimensional Bell States, Communications in Theoretical Physics., 2009., V.52, issue 3., P.421-424.
[36]. Song T.T. Participant Attack and Improvement to Multiparty Quantum Secret Sharing Based on GHZ States, T.T. Song, Q.Y. Wen, F. Gao, H. Chen, International Journal of Theoretical Physics., 2013., V.52, issue 1., P.293-301.
[37]. Tan X. Improved Three-Party Quantum Secret Sharing Based on Bell States, X. Tan, L. Jiang, International Journal of Theoretical Physics., 2013., V.52, issue 10., P.-3577-3585.
[38]. Schmid C. Experimental Single Qubit Quantum Secret Sharing, C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, H. Weinfurter, Physical Review Letters., 2005., V.95, issue 23.- 230505.
[39]. Gaertner S. Experimental Demonstration of Four-Party Quantum Secret Sharing, S. Gaertner, C. Kurtsiefer, M. Bourennane, H. Weinfurter, Physical Review Letters., 2007., V.98, issue 2.- 020503.
[40]. Bogdanski J. Experimental quantum secret sharing using telecommunication fiber, J. Bogdanski, N. Rafiei, M. Bourennane, Physical Review A., 2008., V.78, issue 6.- 062307.
[41]. Bhatia P.S. Experimental tripartite quantum state sharing and perfect teleportation of the two-qubit photonic state using genuinely entangled multipartite states, Journal of the Optical Society of America B., 2014.,V.31, issue 1., P.154-163.

КЛАСИФІКАЦІЯ КВАНТОВИХ ТЕХНОЛОГІЙ РОЗДІЛЕННЯ СЕКРЕТУ

У статті запропонована класифікація та узагальнений аналіз найбільш відомих схем розділення секрету на основі квантових технологій. Класифікація виконана за такими критеріями, як фізичні принципи, на яких базуються відповідні методи розділення секрету та види задач захисту інформації, що вирішуються цими методами. Розглядаються перспективні квантові протоколи розділення секрету з врахуванням вимог, що пред'являються сучасною квантовою криптографією, зокрема, – підвищення інформаційної місткості протоколів шляхом використання квантових систем великої розмірності – кудитів. Найбільш перспективними є квантові методи розділення секрету на основі багаточасткового переплутання. Стисло розглянуті деякі окремі задачі захисту інформації з використанням методів квантового розділення секрету, зокрема, – передавання, що спільно контролюється, квантового стану віддаленому отримувачу та гібридні протоколи – протоколи квантового прямого безпечного зв'язку з контролем над отриманням інформації третьою стороною. Аналізується стан сучасної експериментальної бази зі створення систем квантового розділення секрету.

Ключові слова: квантова криптографія, квантове розділення секрету, класифікація, кубіт, багаточасткове переплутання.

CLASSIFICATION OF QUANTUM TECHNOLOGIES OF A SECRET SHARING

In this paper the classification and the generalized analysis of the most known secret sharing schemes based on quantum technologies have been offered. The classification have been carried out by such criteria as physical principles, on which corresponding methods of secret sharing are based and kinds of tasks of information protection, which are being solved by these methods. Perspective quantum protocols of a secret sharing taking into account the requirements shown by modern quantum cryptography are considered, in particular, an increase of information capacity of protocols by using quantum systems of large dimension (qudits). The most perspective are quantum technologies of secret sharing based on multiparticle entanglement. The certain tasks of information protection with using quantum secret sharing are shortly considered, in particular, the many-party controlled teleportation of quantum state to the remote receiver and the protocols of quantum secure direct communication with the control of information receiving by the third confidential party. The status of modern experimental base on creation of systems of the quantum secret sharing is analyzed.

Keywords: quantum cryptography, quantum secret sharing, classification, qubit, multiparticle entanglement.

Василиу Евгений Викторович, доктор технических наук, доцент, директор Учебно-научного института Радио, телевидения и информационной безопасности Одесской национальной академии святи им. А.С. Попова.
E-mail: vasiliu@ua.fm
Василіу Євген Вікторович, доктор технічних наук, доцент, директор Навчально-наукового інституту Радіо, телебачення та інформаційної безпеки Одеської національної академії зв'язку ім. О.С. Попова.
Vasiliu Yevhen, Doctor of Science in Eng., Full Professor, Director of Educational and Research Institute of Radio, Television and Information Security of Odessa National Academy of Telecommunications n. a. O.S. Popov.

Лимарь Игорь Валериевич, аспирант Одесской национальной академии святи им. А.С. Попова.
E-mail: iv.limar@onu.edu.ua
Лимарь Ігор Валерійович, аспірант Одеської національної академії зв'язку ім. О.С. Попова.
Limar Igor, postgraduate of Odessa National Academy of Telecommunications n. a. O.S. Popov.