17

Квантовое распределение ключей с временным кодированием tb-кубитов

© А.С. Задорин

Томский государственный университет систем управления и радиоэлектроники,
634050 Томск, Россия

e-mail: Anatoly.Zadorin@gmail.com

Поступила в редакцию 16.11.2017 г.
В окончательной редакции 22.05.2018 г.

Показана возможность реализации системы квантового распределения ключей (СКРК) с использованием временного кодирования tb-кубитов (time-bin qubit), приготавливаемых и измеряемых с помощью разбалансированных интерферометров Маха-Цендера. Показано, что для исключения четкой априорной идентификации tb-кубитов с равными базами их кодирование символами 0 и 1 может осуществляться за счет задержки одного из них на половину тактового интервала (ТИ). Показано, что однозначность измерений кутритов в данном алгоритме основывается на способности квантовых частиц в β-состояниях к интерференции амплитуд вероятностей в портах интерферометров системы, а также на отсутствии коллизий сигнальных состояний кутритов в смежных ТИ. Описан способ организации контроля таких коллизий в том числе за счет кубитов, приготавливаемых из квази-однофотонных когерентных лазерных состояний.

DOI: 10.21883/OS.2018.09.46561.265-17

Введение

Развитие технологий квантовых вычислений во многом определяется прогрессом в разработке новых квантовых алгоритмов, успехами в адаптации их к различным форматам данных и существующей схемотехнике квантовых вентилей. Наглядным примером здесь могут служить разнообразные технологии построения систем квантового распределения ключей (СКРК), основанные на использовании квантовых процессоров, осуществляющих ряд логических операций над последовательностью кубитов $|\psi_i\rangle$. Иерархическая структура алгоритмов работы процессоров СКРК, как и других телекоммуникационных протоколов, содержит ряд уровней, объединенных в общий стек протоколов. Физический уровень в данной иерархии представлен протоколом генерации первичного ключа, включающим процедуры приготовления, измерения и обработки кубитов $|\psi_i\rangle$. Среди большого разнообразия алгоритмов генерации первичного ключа можно выделить несколько наиболее часто используемых базовых протоколов СКРК [1–4]. К их числу относятся такие классические протоколы, как BB84 1984 г. Ч. Беннета и Ж. Брассаро, B92 Ч. Беннета 1992 г. [5] и др., реализуемые в двух основных форматах кодирования — поляризационном и фазовом [1–6].

Наиболее простым в реализации оказывается вариант поляризационного кодирования $|\psi_i\rangle$. К сожалению, в оптоволоконных (ОВ) каналах связи поляризационные кубиты (ПК) испытывают сильную декогеренцию, т.е. быстро разрушаются вследствие поляризационной дисперсии ОВ. По этой причине основой большинства протоколов генерации первичного ключа в СКРК с ОВ в настоящее время является фазовое кодирование кубитов [1–4]. Практическое использование данного метода затрудняется сложностью контроля состояния поляризации, а также случайных фазовых сдвигов в квантовом канале (КК) СКРК. Применение в СКРК автокомпенсационных схем лишь частично решает эту проблему. Так, система plug-and-play [6] позволяет устранить поляризационные искажения оптических сигналов за счет их двойного прохода по квантовому каналу с промежуточным отражением от зеркал Фарадея, однако вносит свои ограничения. К ним относятся снижение квантового битрейта, защищенной длины КК и др. [7].

В данной связи актуальной задачей развития технологической базы СКРК является отыскание и исследование альтернативных способов кодирования $|\psi_i\rangle$. В качестве одного из них можно рассматривать способ построения однокубитовых логических процессоров СКРК на основе временного кодирования tb-кубитов, ранее предложенный в [8] для построения первичного протокола BB84. Целью настоящей работы является обсуждение возможностей дальнейшего развития указанного подхода.

Техника приготовления и измерения tb-кубитов

В настоящее время схемотехника приготовления и измерения tb-кубитов хорошо разработана для систем КРК с фазовым кодированием [1–6]. Квантовый процессор этих систем содержит некоторый набор логических квантовых вентилей, распределенных между удаленными пользователями А и Б (ПА, ПБ), соединенными квантовым (ККС) и классическим каналами связи. Наиболее широкоиспользуемым в этих системах вентилем является разбалансированный интерферометр Маха-

Цендера (ИМЦ), объединяющий несколько логических устройств: однокубитовые квантовые вентили Адамара, сдвигающий и фазовращающий вентили, реализованные в виде ОВ-линий задержки на время Δ и регулятора фазы α в плечах интерферометра [4,9]. В данной системе трансформация исходного когерентного состояния $|\psi_0\rangle$ квазиодиночного фотона в состояние $|\psi\rangle$ на выходе ИМЦ будет определяться последовательным произведением соответствующих унитарных операторов **H**, **P** и **D** указанных квантовых вентилей. Для отыскания связи кет-векторов $|\psi_0\rangle$ и $|\psi_4\rangle$ вычислительный базис кубита и операторов **H**, **P** и **D** удобно совместить с номерами портов интерферометра $|0\rangle$, $|1\rangle$, $|3\rangle$ и $|4\rangle$. В указанных координатах реакция ИМЦ $|\psi_4\rangle$, например, на возбуждение $|\psi_0\rangle = |0\rangle$, т.е. посылку фотона в порт $|0\rangle$, будет описываться соотношением [9],

$$|\psi\rangle = \frac{1}{2}\left[e^{j\alpha_0}D + e^{j\alpha_1}\right]|3\rangle + \frac{1}{2}\left[e^{j\alpha_0}D - e^{j\alpha_1}\right]|4\rangle, \quad (1)$$

где D, α_0, α_1 — унитарный оператор сдвига, описывающий относительное временное смещение одиночных фотонов на время Δ, а также соответствующие фазовые сдвиги в плечах интерферометра.

Из последнего соотношения следует, что в портах $|3\rangle$ и $|4\rangle$ разбалансированного ИМЦ $|\psi\rangle$ представляется суперпозицией двух разделенных промежутком времени Δ состояний. Обозначим данные состояния кет-векторами $|\alpha\rangle$ и $|\beta\rangle$ и используем их для образования нового двумерного ортогонального динамического вычислительного базиса указанных квантовых объектов $|\psi_i\rangle$:

$$|\psi_i\rangle = \langle i|\psi\rangle = \xi_{i\alpha}|\alpha\rangle + \xi_{i\beta}|\beta\rangle, \quad (2)$$

где $i = 3, 4$; $\xi_{j\alpha}$, $\xi_{i\beta}$ — комплексные амплитуды вероятности состояний $|\alpha\rangle$ и $|\beta\rangle$ объекта $|\psi_i\rangle$ в портах $|3\rangle$ и $|4\rangle$ соответственно. В литературе суперпозиция (2) называется time-bin qubit [9]. Ниже она обозначается как временной или tb-кубит. Временной сдвиг Δ между базисными состояниями $|\alpha\rangle$ и $|\beta\rangle$ будем называть базой ИМЦ.

Измерение временных кубитов $|\psi_i\rangle$ осуществляется с помощью второго интерферометра Б, аналогичного рассмотренному выше ИМЦ-А. Результат расчета кет-вектора $|\psi_4\rangle$ в системе из двух последовательно включенных интерферометров несложно получить путем замены состояния $|\psi_0\rangle = |0\rangle$ на входе ИМЦ-Б на соотношение (2). При этом следует учесть различие матриц **P** фазовращающих вентилей интерферометров. Эти различия в дальнейшем будем помечать нижними индексами фазовых переменных А и Б, например как $\alpha_{\text{А}0}$ или $\alpha_{\text{Б}1}$. Кроме этого, обозначим операторы сдвига интерферометров как $D_\text{А}$ и $D_\text{Б}$. В результате можно показать, что отклик $|\psi\rangle$ системы интерферометров, соединенных каналом из одного оптического волокна, на возбуждение $|\psi_0\rangle = |0\rangle$ имеет вид [9],

$$\begin{aligned}|\psi\rangle = \frac{e^{j\alpha_{qc0}}}{4}\Big[&e^{j(\alpha_{\text{Б}0}+\alpha_{\text{А}0})}D_\text{Б}D_\text{А} + (e^{j(\alpha_{\text{Б}0}+\alpha_{\text{А}1}}D_\text{Б} \\ &+ e^{j(\alpha_{\text{Б}1}+\alpha_{\text{А}0}}D_\text{А}) + e^{j(\alpha_{\text{Б}1}+\alpha_{\text{А}1})}\Big]|3\rangle \\ &+ \frac{e^{j\alpha_{qc0}}}{4}[e^{j(\alpha_{\text{Б}0}+\alpha_{\text{А}0})}D_\text{Б}D_\text{А}) + (e^{j(\alpha_{\text{Б}0}+\alpha_{\text{А}1})}D_\text{Б} \\ &- e^{j(\alpha_{\text{Б}1}+\alpha_{\text{А}0})}D_\text{А}) - e^{j(\alpha_{\text{Б}1}+\alpha_{\text{А}1})}]|4\rangle. \end{aligned} \quad (3)$$

Из (3) следует, что в каждом из портов $|3\rangle$ и $|4\rangle$ ИМЦ-Б объект $|\psi_4\rangle$ в общем случае представлен суперпозицией из четырех динамических состояний. Одно из них является состоянием с нулевой задержкой ($D = 1$), реализуемым на оптической траектории $\text{К}_\text{А}-\text{К}_\text{Б}$, еще два состояния с однократной задержкой ($D = D_\text{А}, D_\text{Б}$), реализуемые на траекториях $\text{Д}_\text{А}-\text{К}_\text{Б}$ и $\text{К}_\text{А}-\text{Д}_\text{Б}$, а также одно состояние с двукратной задержкой ($D = D_\text{А} \cdot D_\text{Б}$) на траектории $\text{Д}_\text{А}-\text{Д}_\text{Б}$. При равных базах интерферометров, когда $D_\text{А} = D_\text{Б}$, размерность вектора $|\psi\rangle$ снижается до 3, т.е. $|\psi\rangle$ обращается в кутрит $|\varphi\rangle$, представленный тремя линейно независимыми динамическими состояниями, разнесенными по времени друг от друга на базовую задержку ИМЦ Δ. Выберем указанные состояния в качестве базисных векторов объекта $|\varphi\rangle$ и обозначим как $|\alpha\rangle$, $|\beta\rangle$ и $|\gamma\rangle$. Далее, находим проекции $|\psi\rangle$ на векторы $|3\rangle$ и $|4\rangle$, определяющие вероятности регистрации фотона в выходных портах второго ИМЦ-Б,

$$|\varphi_i\rangle = \langle i|]psi\rangle = \xi_{i\alpha}|\alpha\rangle + \xi_{i\beta}|\beta\rangle + \xi_{i\gamma}|\gamma\rangle, \quad (4)$$

где $i = 3, 4$; $\xi_{i\alpha}$, $\xi_{i\beta}$, $\xi_{i\gamma}$ — комплексные амплитуды вероятности состояний $|\alpha\rangle$, $|\beta\rangle$ и $|\gamma\rangle$ кутрита $|\varphi_i\rangle$ в портах $|3\rangle$ и $|4\rangle$ соответственно.

Отметим, что состояние $|\beta\rangle$ является наиболее важным информационным состоянием кутрита (4), в котором у квантовой частицы появляется возможность интерферировать сама с собой в форме интерференции амплитуд вероятностей [11]. В этом случае при сдвиге фазы на траекториях $\text{Д}_\text{А}-\text{К}_\text{Б}$ и $\text{К}_\text{А}-\text{Д}_\text{Б}$, равном ϕ, вероятности регистрации одиночных фотонов в портах $|3\rangle$ и $|4\rangle$ ИМЦ-Б будут [2]

$$P_1 \sim \cos^2(\phi/2) \;\text{ и }\; P_2 \sim \sin^2(\phi/2). \quad (5)$$

Соотношения (4), (5) являются формальной основой техники фазового кодирования и измерения кубитов $|\psi_i\rangle$ в ИМЦ, характерной особенностью которой является фиксированное положение векторов $|\alpha\rangle$, $|\beta\rangle$ и $|\gamma\rangle$ относительно границ тактового интервала. Естественная для данных квантовых объектов динамическая степень свободы здесь остается не востребованной. Ниже рассмотрим способ ее использования для расширения функциональных возможностей фазового кодирования tb-кубитов и построения на его основе протокола СКРК.

Временное кодирование tb-кубитов

При временном кодировании каждый из двоичных символов связывается с различным положением или конфигурацией (относительными сдвигами базисных состояний в (2) и (3)) сигнального квантового объекта на i-м тактовом интервале T_i (ТИ). Для $|\psi_i\rangle$ и $|\varphi_i\rangle$ в качестве сигнальных признаков можно использовать базу Δ ИМЦ и временную задержку τ, измеряемую относительно начала ТИ. В дальнейшем изменения динамической структуры $|\psi_i\rangle$ и $|\varphi_i\rangle$, связанные с передаваемыми символами 0 и 1, будем описывать зависимостью указанных объектов от дискретного параметра $l = 0, 1$ как $|\psi_i(l)$ и $|\varphi_i(l)\rangle$.

Основными критериями корректного выбора Δ и τ в СКРК для каждой конфигурации состояний $|\alpha\rangle$, $|\beta\rangle$ и $|\gamma\rangle$ объектов $|\psi_i(l)\rangle$ и $|\varphi_i(l)\rangle$ являются условия выполнения теоремы о запрете клонировния [1,2], исключающие возможность четкой априорной идентификации указанных объектов с альтернативными символами l. При отыскании этих условий следует иметь в виду, что представление $|\psi_i(l)\rangle$ и $|\varphi_i(l)\rangle$ в виде суперпозиции базисных состояний (2) сохраняется лишь до акта измерения. В момент измерения волновая функция кубита с вероятностью, определяемой комплексной амплитудой ξ_{ij}, переходит в одно из базисных состояний [1,2,11].

Возможными конфигурациями tb-объектов $|\psi_i(l)\rangle$ и $|\varphi_i(l)\rangle$, удовлетворяющими указанным условиям, представляются структуры на рис. 1. На этом рисунке внутри каждого i-го ТИ штриховкой обозначены тайм-слоты (ТС) $\Delta t_i(0)$ и $\Delta t_i(1)$, представляющие собой сигнальные интервалы, в которых возможна локализация квази-одиночных фотонов из базисных состояний $|\alpha\rangle$, $|\beta\rangle$ и $|\gamma\rangle$ объектов $\psi(l)\rangle$ и $|\varphi(l)\rangle$. Из рисунка видно, что основной особенностью данных динамических структур является то, что ТС тактовых интервалов раз- решены для появления в них нескольких различных состояний tb-кубитов и кутритов $|\psi_i(l)\rangle$ и $|\varphi_i(l)\rangle$ из смежных ТИ. Такое наложение tb-объектов является признаком их динамической неортогональности и может служить основой для построения соответствующего протокола СКРК. Препятствием для этого является наличие в тайм-слоте $\Delta t_i(l)$ разрешенных состояний равновероятных квантовых объектов, ассоциированных с альтернативными символами 0 и 1 ключевого кода.

Такое ограничение относится, например, к кубитам $|\psi(0)\rangle$ и $|\psi(1)\rangle$, которые на рис. 1 характеризуются одинаковыми базами $\Delta = T/2$ и различаются лишь задержкой $\tau = \Delta = T/2$ относительно границы ТИ. Из рисунка видно, что в показанных структурах $|\psi_i(l)\rangle$ одиночный фотон может находиться в середине или по краям ТИ, в тайм-слотах $\Delta t_i(0)$, $\Delta t_i(1)$ или $\Delta t_{i+1}(0)$. При этом если $|\xi_{i\alpha}| = |\xi_{i\beta}|$, то вероятности регистрации фотона в состояниях 0 и 1 в каждом из указанных ТС совпадают. В данных условиях четкое разделение в измеряемой последовательности $|\psi_i(l)\rangle$ кубитов на $|\psi(0)\rangle$ и $|\psi(1)\rangle$ не представляется возможным.

$P(\|\varphi_i(l)\rangle)$	$t = \Delta t_i(0)$		$t = \Delta t_i(1)$	
	порт $\|3\rangle$	порт $\|4\rangle$	порт $\|3\rangle$	порт $\|4\rangle$
$P(\|\alpha_i(0)\rangle)$	0.125	0.125	0	0
$P(\|\gamma_{i-1}(0)\rangle)$	0.125	0.125	0	0
$P(\|\beta_i(0)\rangle)$	0	0	0	0.5
$P(\|\alpha_i(1)\rangle)$	0	0	0.125	0.125
$P(\|\gamma_{i-1}(1)\rangle)$	0	0	0.125	0.125
$P(\|\beta_{i-1}(1)\rangle)$	0	0.5	0	0

Воспользуемся данными рис. 1 для исследования возможности построения протокола СКРК на основе обработки tb-кутритов. В данном случае в каждом ТС $\Delta t_i(l)$ разрешенным оказывается любое из трех состояний кутрита (4). При этом, во-первых, в силу вырожденности β-состояния $|\varphi_i(l)\rangle$ вероятность его регистрации равна сумме соответствующих вероятностей α- и γ-состояний, и, во-вторых, переносимый им кодовый символ всегда альтернативен символу, связанному с остальными векторами кутрита (4). Это значит, что в общем случае ПБ не в состоянии надежно разделить кодовые состояния $|\psi_i(l)\rangle$.

Для того чтобы исключить вероятность появления в ТС $\Delta t_i(l)$ состояний tb-кутрита с различными кодовыми символами, можно воспользоваться упомянутой ранее способностью квантовой частицы в β-состояниях к интерференции амплитуд вероятностей [11]. С этой целью в состав одного или обоих интерферометров ИМЦ-А, Б на рис. 2 вводятся фазовращающие вентили, обеспечивающие фазовые сдвиги $\phi_\text{А}$ и $\phi_\text{Б}$ оптического сигнала в их плечах так, чтобы суммарный сдвиг был равен π, т. е.

$$\phi_\text{А} + \phi_\text{Б} = \pi. \tag{6}$$

Подставим (6) в (5) полагая, что $|\xi_{i\alpha}| = |\xi_{i\beta}|$. Заключаем, что при посылке кубита $|\psi_i(l)\rangle$ в порт $|0\rangle$ ИМЦ-Б вследствие квантовой интерференции β-состояний tb-кутрита вероятности их регистрации в портах $|3\rangle$ и $|4\rangle$ (сигнальном и контрольном) ИМЦ-Б будут равны 0 и 0.5 соответственно. Вероятности $P(|\varphi_i(l)\rangle)$ для указанных и других состояний $|\varphi_i(l)\rangle$ в обоих портах ИМЦ-Б и тайм-слотах $\Delta t_i(l)$ i-го ТИ для $|\xi_{i\alpha}| = |\xi_{i\beta}|$ приведены в таблице. В соответствии с этими данными, а также рис. 1, в условиях (6) в сигнальном порте $|3\rangle$ интерферометра Б разрешенными оказываются только α- и γ-состояния tb-кутритов, локализованные в смежных $(i-1)$-м и i-м ТИ, но связанные с одинаковыми кодовыми символами $l = 0, 1$. Последнее означает возможность надежного разделения предаваемых символов.

Действительно, согласно изложенному, регистрация одиночного фотона в порте $|3\rangle$ ИМЦ-Б в момент ТС $\Delta t_i(0)$ означает передачу по квантовому каналу в $(i-1)$-м или i-м ТИ символа 0, а регистрация в момент ТС $\Delta t_i(1)$ — символа 1 (на рис. 1 эти состояния кутритов $|\varphi_i(l)\rangle$ обведены пунктирной линией). Важно подчеркнуть, что динамическая неортогональность

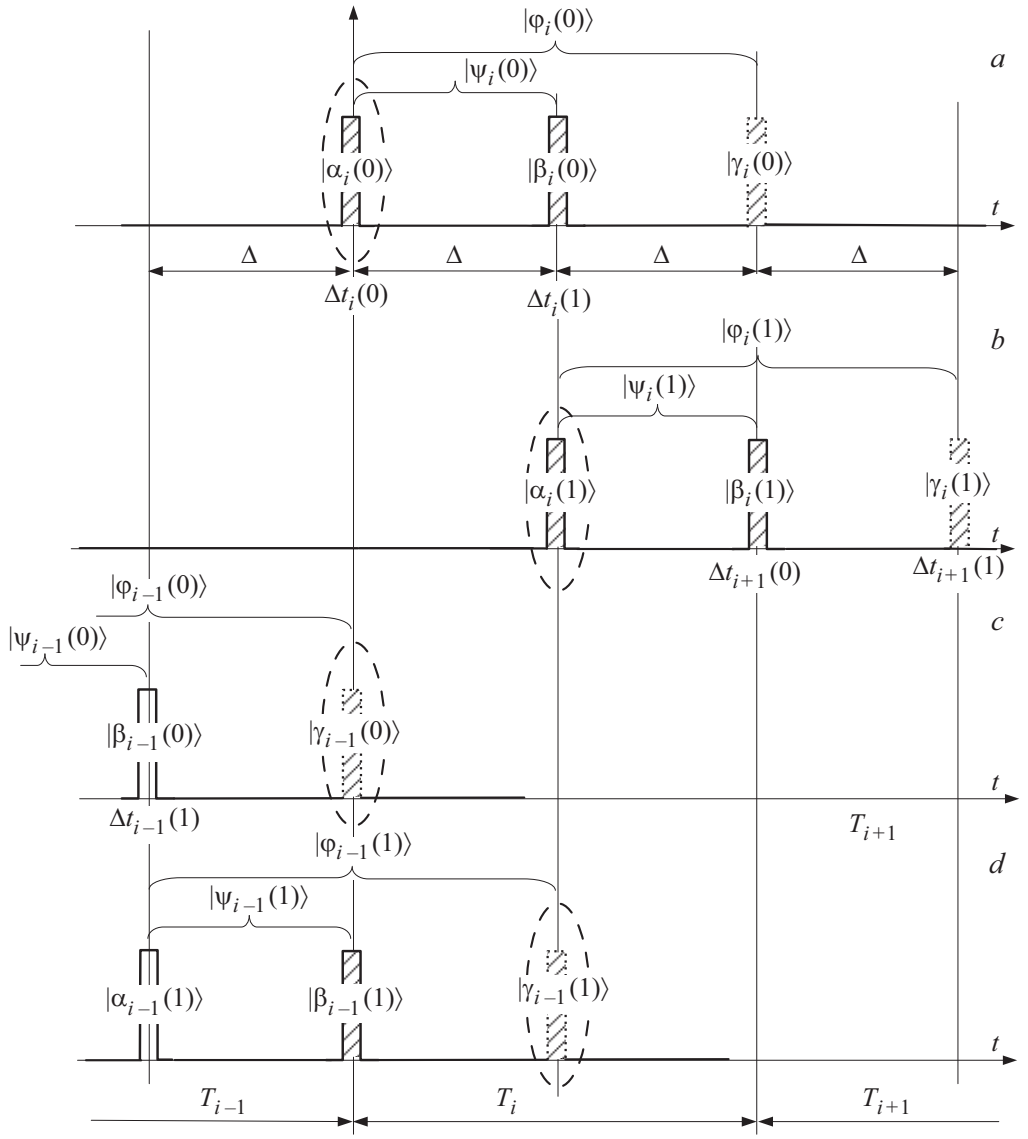

Рис. 1. Кодовые состояния кубитов $|\psi_i(l)\rangle$ и кутритов $|\varphi_i(l)\rangle$ при различных временных сдвигах относительно границ i-го ТИ (*a*) $|\psi_i(0)\rangle$, $|\varphi_i(0)\rangle$; (*b*) $|\psi_i(1)\rangle$, $|\varphi_i(1)\rangle$; (*c*) $|\psi_{i-1}(0)\rangle$, $|\varphi_{i-1}(0)$; (*d*) $|\psi_{i-1}(1)\rangle$, $|\varphi_{i-1}(1)\rangle$.

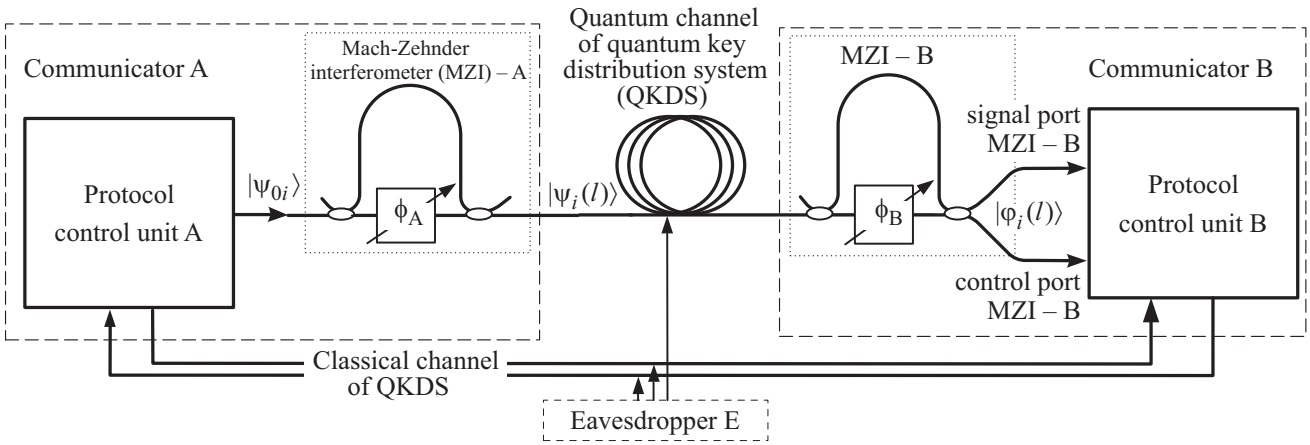

Рис. 2. Структурная схема СКРК с временным кодированием tb-кубитов.

состояний объектов $|\varphi_i(l)\rangle$ здесь проявляется не в неопределенности значения символа l, а в его номере в последовательности $|\varphi_i(l)\rangle$. В рассматриваемом протоколе эту неопределенность и предлагается использовать для обеспечения основной защиты СКРК от попыток клонирования одиночных фотонов в квантовом канале нелегитимным пользователем (агентом E (AE)).

Механизм защиты здесь может быть аналогичен, например, механизму защиты протокола B92 [1,2,6]. С этой целью на стороне ПА формируется случайная двоичная последовательность $\mathbf{m}_\mathrm{A}$ с числом элементов, равным числу тактовых интервалов во фрейме СКРК. Каждый элемент $\mathbf{m}_\mathrm{A}$ содержит два поля — поле номера элемента i и поле кодового символа $m_{\mathrm{A}i}$. Элементы $m_{\mathrm{A}i}$ ПА использует для случайной смены значений кодовых символов l в i-х ТИ последовательности кубитов $|\psi_i(l)\rangle$, приготовляемых в вычислительных базисах по рис. 1, т. е.

$$|\psi_i(l)\rangle = |\psi_i(m_{\mathrm{A}i})\rangle. \qquad (7)$$

Для исключения неоднозначных измерений последовательности $|\psi_i(l)\rangle$ при формировании $\mathbf{m}_\mathrm{A}$ стороной А не допускается возникновение коллизий, т. е наложений нескольких состояний кубитов из соседних тактовых интервалов в любом из его тайм-слотов. С этой целью поля кодовых символов в $\mathbf{m}_\mathrm{A}$ перемежаются случайным числом из нескольких (от $1-2$) холостых полей, исключающих какую-либо регулярность в чередовании $|\psi_i(l)\rangle$ по параметру l. Такие вставки практически легко осуществимы, например, путем приготовления состояний $|\psi_0\rangle$ за счет ослабления лазерных импульсов до уровня, характеризуемого заданным средним числом фотонов в ТС $m \approx 0.1$ [1–7]. В данном случае вероятность обнаружить n фотонов в состоянии $|\psi_0\rangle$ описывается пуассоновской статистикой, параметр m которой определяет среднее число ($\sim m^{-1}$) холостых полей между активными состояниями $|\psi_0\rangle$.

Сторона Б, анализируя далее состояния $|\psi_i(l)\rangle$ и $|\varphi_i(l)\rangle$, пытается определить некоторые элементы $\mathbf{m}_\mathrm{A}$ с целью создания на их основе ключевых кодовых последовательностей $\mathbf{k}_{\mathrm{AБ}}$. В условиях (6) и в отсутствие шумов эти попытки ПБ основаны на упомянутой выше возможности безошибочного определения кодового символа l в зарегистрированном кутрите (рис. 1). Таким образом, проблема отыскания ПБ элементов $\mathbf{m}_{\mathrm{A}i}$ оказывается связанной только с восстановлением нумерации полей $m_{\mathrm{A}i}$. Для решения этой задачи ПБ формирует у себя собственную случайную двоичную последовательность $\mathbf{m}_\mathrm{Б}$ с числом элементов, равным $\mathbf{m}_\mathrm{A}$, которая используется им для принятия решения о том, к какому $(i-1)$-му или i-му ТИ относится зарегистрированный в порте $|3\rangle$ ИМЦ-Б кутрит $|\varphi_i(l)\rangle$, или, иначе, какой номер i в последовательности $\mathbf{m}_\mathrm{A}$ имеет принятый в j-м ТИ кодовый символ l. Решение ПБ о принятии той или иной гипотезы относительно номераi можно представить, например, так:

$$i = j - 1 + m_{\mathrm{Б}j}, \qquad (8)$$

где $m_{\mathrm{Б}j}$ — значение j-го двоичного символа (0 или 1) последовательности $\mathbf{m}_\mathrm{Б}$.

В силу стохастичности $\mathbf{m}_\mathrm{Б}$ данное решение приблизительно в половине случаев будет давать неправильный результат. В этой связи для использования восстановленных стороной Б фрагментов $\mathbf{m}_\mathrm{A}$ в качестве ключевых последовательности $\mathbf{k}_{\mathrm{AБ}}$ необходимо в каждом i-м ТИ предусмотреть процедуру устранения ошибок в решениях (8) (проверку состоятельности гипотез (8)), которая может производиться следующим образом. При регистрации в сигнальном порте $|3\rangle$ ИМЦ-Б j-го ТИ состояния пользователь Б по классическому каналу СКРК (рис. 2) сообщает стороне А текущее значение элемента $m_{\mathrm{Б}j}$ в формуле (8), не раскрывая при этом значение самого кодового символа l. В ответ ПА подтверждает или не подтверждает правильность такого решения. Указанная квитанция является основанием для включения ПБ очередных элементов $m_{\mathrm{A}i}$ в качестве элементов $\mathbf{k}_{\mathrm{AБ}}$. На стороне А элементы $\mathbf{k}_{\mathrm{AБ}}$ создаются из $\mathbf{m}_\mathrm{A}$ за счет исключения из нее неактивных ТИ, т. е. тактовых интервалов, в которых не зарегистрированы α- или γ-состояния tb-кутритов в сигнальном порте $|3\rangle$ ИМЦ-Б. Исключаются также и поля ТИ, если зарегистрированные в них сигналы не прошли указанной выше проверки состоятельности.

В соответствии с приведенным описанием ключевая последовательность $\mathbf{k}_{\mathrm{AБ}}$ в рассматриваемом протоколе представляет собой согласованный сторонами набор фрагментов последовательности $\mathbf{m}_\mathrm{A}$, элементы которой состоят из поля номера элемента N_i и собственно кодового символа l_i. Совокупность всех значений l_i в $\mathbf{k}_{\mathrm{AБ}}$ представляет собой генерируемый системой секретный код. Последовательность же N_i секретной не является. Она вместе с приведенной в таблице статистикой распределений состояний кутритов $|\varphi_i(l)\rangle$ по портам ИМЦ-Б и тайм-слотам $\Delta t_i(l)$ ТИ представляет защитную информацию системы, предназначенную для детектирования попыток AE клонирования tb-кубитов в канале СКРК. Рассмотрим возможности использования этой информации при различных сценариях поведения AE.

Прежде всего отметим бесперспективность попыток AE подмены α- или β-состояний кубитов одиночными фотонами $|\psi_0\rangle$ и последующего анализа движения квитанций ПА в классическом канале с целью определения согласованных легитимными сторонами элементов $\mathbf{k}_{\mathrm{AБ}}$. Такое нарушение целостности $|\psi_i(l)\rangle$ приведет к разрушению интерференции амплитуд вероятностей этих квантовых объектов и, как следствие, наложению альтернативных символов в сигнальном порте ИМЦ-Б. Согласно данным таблицы, в этом случае в обоих портах этого интерферометра соответствующие вероятности будут одинаковы, т. е. $P(|\alpha(0,1)\rangle) + P(|\gamma(0,1)\rangle) \approx P(|\beta(1,0)\rangle)$.

Последнее означает недопустимо высокий уровень системного показателя — коэффициента квантовых ошибок Q-BER.

Проанализируем далее возможности АЕ клонирования кубитов $|\psi_i(l)\rangle$ в квантовом канале СКРК (рис. 2). Для этой цели АЕ может использовать аппаратуру, аналогичную упомянутой выше аппаратуре легитимных пользователей. При такой попытке сторона АЕ, как и законный пользователь Б, столкнется с необходимостью принятия решения типа (8) относительно номера ТИ, в котором должен быть приготовлен фальшивый кубит $|\psi_i(l)$, взамен зарегистрированного им $|\psi_i(l)$. Как рассматриваемый, так и другие известные протоколы СКРК исключает для АЕ возможность такой проверки. Поэтому неизбежные в таком случае ошибки в полях номера элемента N_i формируемой на сторонах А и Б ключевой последовательности $\mathbf{k}_{\text{АБ}}$, связанные с появлением в канале СКРК кубитов $|\psi_i(l)\rangle$, позволяют детектировать указанную активность АЕ.

Заключение

Приведенное выше обсуждение указывает на возможность построения алгоритма временного кодирования tb-кубитов, а также соответствующих однокубитовых логических процессоров СКРК на этой основе. Показано, что однозначность измерений кутритов в данном алгоритме основывается на способности квантовых частиц в β-состояниях к интерференции амплитуд вероятностей в портах интерферометров системы, а также отсутствии коллизий сигнальных состояний кутритов в смежных ТИ. Описан способ организации контроля таких коллизий в том числе за счет кубитов, приготавливаемых из квазиоднофотонных когерентных лазерных состояний.

Следует отметить, что за рамками обсуждения остались такие вопросы, как оценка допустимого уровня коэффициента квантовых ошибок Q-BER и $B_{\text{К}}$ — скорости формирования $\mathbf{k}_{\text{АБ}}$ (битрейт), значения которых также используются для детектирования несанкционированных вторжений АЕ в систему [1–8]. По мнению автора, данные вопросы заслуживают отдельного обсуждения.

Список литературы

[1] *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир, 2008. 824 с.
[2] *Имре Ш., Балаж Ф.* Квантовые вычисления и связь. Инженерный подход. М.: Физматлит, 2008. 320 с.
[3] *Кулик С.П., Молотков С.Н., Маккавеев А.П.* // Письма в ЖЭТФ, 2007. Т. 85. № 6. С. 354–359.
[4] *Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю.* Квантовая криптография. Учебно-методическое пособие. М.: МаксПресс, 2011. 112 с.
[5] *Zbinden H., Gautier J.D., Gisin N., Huttner B., Muller A., Tittel W.* // Electron. Lett. 1997. V. 33. P. 586–588.
[6] *Bennett C.H.* // Phys. Rev. Lett. 1992. V. 68. P. 3121.
[7] *Румянцев К.Е., Плёнкин А.П.* // Радиотехника. 2015. Т. № 2. С. 125–134.
[8] *Задорин А.С., Махорин Д.А.* // Изв. вузов. Физика. 2016. Т. 59. № 3. С. 24–29.
[9] *Задорин А.С., Махорин Д.А.* // Доклады ТУСУРа. 2015. Т. 37. № 3. С. 145–149.
[10] *Gisin N., Ribordy G., Wolfgang T.* // Rev. Mod. Phys. 2002. V. 74. P. 145–195.
[11] *Дирак П.* Принципы квантовой механики. М.: Наука, 1979. 480 с.