УДК 004.71:519.6

*Е.И. ВАСИЛЬЕВ, В.А. ФАЕРМАН*

# ДИСКРЕТНО-СОБЫТИЙНАЯ МОДЕЛЬ ОПТИЧЕСКОГО КАНАЛА СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

В статье предлагается дискретно-событийная модель простой системы квантового распределения ключей (КРК), реализующая протокол BB84 с поляризационным кодированием и построенная с применением раскрашенных сетей Петри. Манипулирование состояниями поляризации фотонов в физическом прототипе осуществляется с помощью пары устройств, состоящих из последовательно размещённых полуволновой и четвертьволновой пластин и поворотных механизмов. Для описания оптического канала используются исчисления Джонса. Модель системы КРК реализована в свободно распространяемой среде CPN Tools. С помощью разработанной модели исследованы влияния ошибки в позиционировании волновых пластин на вероятность ошибок в генерируемых сырых битовых последовательностях для нескольких различных целевых состояний линейной поляризации фотонов, передаваемых в оптический канал. В дальнейшем предполагается использование модели в качестве генератора реалистичных битовых последовательностей с ошибками для исследования алгоритмов постобработки, в частности согласования ключевого материала.

***Ключевые слова:*** *квантовое распределение ключей, оптический канал, сети Петри, имитационное моделирование, BB84.*

## Введение

В последние десятилетия всё большее значение в экономике, социальной и общественно-политической жизни имеют информационно-телекоммуникационные технологии. В [1] отмечается, что современный уровень цифровизации быта многих людей значительно превосходит смелые ожидания утопистов прошлого столетия. Дальнейшая цифровизация представляется неизбежной, а исследователи этого явления всё чаще отмечают связанные с ним вызовы и проблемы как социально-психологического, так и технического характера [2]. Одной из таких проблем является обеспечение безопасности данных, передаваемых в сеть и хранимых в ней.

Восприятие информационной безопасности телекоммуникационных процессов существенно изменилось в последние двадцать лет. Так, на заре появления первых стандартов беспроводных сетей, ориентированных на массового пользователя, защита информации рассматривалась исключительно как опция [3]. По этой причине меры криптографической защиты, вошедшие в стандарт WEP, оказались весьма ограниченными и неэффективными. Несмотря на то, что в последующие годы неоднократно была продемонстрирована несостоятельность WEP как средства обеспечения информационной безопасности [4], практические атаки, связанные с эксплуатацией его уязвимостей, сохраняли актуальность ещё более десяти лет. Основанный на этом опыте современный подход к разработке телекоммуникационных технологий и стандартов предполагает продолжительное теоретическое обсуждение любых потенциальных решений и документов в профессиональном сообществе [5].

Последний принцип имеет важное значение в создании перспективных телекоммуникационных систем, в особенности тех, которые не будут скомпрометированы с достижением так называемого «квантового превосходства». Известно, что современные телекоммуникационные технологии, практически на всех уровнях модели взаимодействия открытых систем, опираются на использование принципов асимметричной криптографии. Основной целью применения последней является получение обеими сторонами обмена секретного сеансового ключа, который используется в дальнейшем в рамках симметричной криптографической системы [6]. Безопасность асимметричных криптографических систем определяется односторонним характером производимых в них математических преобразований – получение секрета злоумышленником на основе передаваемых во вне данных может быть выполнено только за экспоненциальное время, что делает подобные атаки не реализуемыми практически. Однако, уже в течении продолжительного времени известны специальные алгоритмы (например, алгоритм Шора), способные с применением квантовых компьютеров выполнять такие операции за полиномиальное время [6, 7]. Несмотря на то, что наблюдаемый сегодня темп развития квантовых вычислений не представляет моментальный угрозы для современной телекоммуникационной инфраструктуры, эта перспектива подвергается серьёзному анализу на протяжении более чем 10 лет [8].

Наиболее готовым для масштабного внедрения ответом на появление квантовых компьютеров является технология квантового распределения ключей (КРК). Она предполагает передачу по специальному оптическому каналу информации, которая впоследствии используется сторонами обмена для производства секретного ключевого материала. Квантовая природа канала при этом, делает теоретически невозможным (или по крайней мере практически сложным) перехват передаваемых элементарных сообщений непосредственно в канале. Необходимо отметить, что экстремально низкий уровень оптических сигналов в канале (энергия импульсов должна быть сопоставима с энергией одиночного фотона) делает создание таких систем нетривиальным как в части обеспечения чувствительности используемого оборудования, так и в части постобработки принятых сторонами сырых данных.

Эта статья посвящена моделированию физического уровня системы КРК, представленного лазером, оптическим каналом и фотодетектором. Разработанная модель является дискретно-событийной и предназначена, преимущественно, для воссоздания сырой ключевой последовательности на принимающей стороне. Введение неидеальности в модели элементов оптического канала позволяет получать реалистичные сырые данные для исследования последующих этапов протоколов, в частности, согласования ключей.

## Физические основы квантового распределения ключей

Далее приводится упрощённое описание поляризационного принципа кодирования, используемого в некоторых системах КРК, которое не претендует ни на полноту, ни на общность.

Свет представляет собой поперечную электромагнитную волну. Поскольку направление вектора магнитного поля $\mathbf{H}(t, z)$ в любой момент времени $t = t_0$ и в произвольной точке пространства на пути распространения волны $z = z_0$ определяется направлением вектора электрического поля $\mathbf{E}(t, z)$, то для описания волны обычно используют только последний. При этом $\mathbf{E}(t, z)$ колеблется в плоскости перпендикулярной направлению $Oz$ распространения волны, следовательно, может быть представлен в виде суммы двух взаимно ортогональных компонент [9]

$$\mathrm{E}(t,z)=\begin{cases}\mathrm{E}_x(t,z),\\ \mathrm{E}_y(t,z),\\ 0.\end{cases} \tag{1}$$

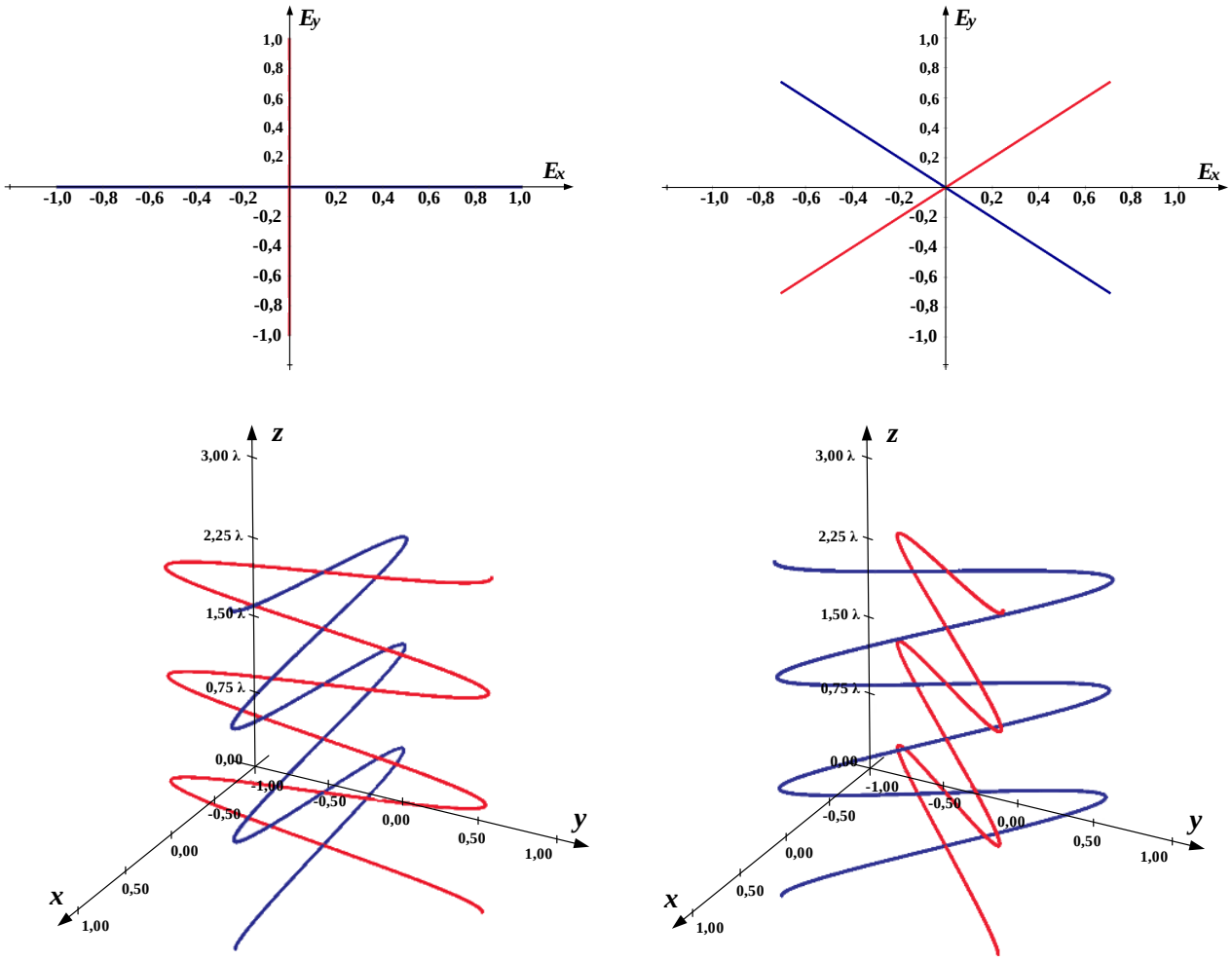
Рассматривая (1) применительно к конкретной точке пространства, например, $z = 0$, легко показать, что $\mathbf{E}(t)$ описывает некоторую траекторию в соответствующей плоскости. Характер этой траектории определяется компонентами $E_x(t)$ и $E_y(t)$ и соответствует поляризации волны. Для монохроматических волн, поляризация может быть линейной, круговой или эллиптической.

Для простоты, рассмотрим четыре определённых вида линейной поляризации (см. рис. 1):

- горизонтальную ($H$): $\mathbf{E_H}(t) = 1\cdot E_x(t) + 0\cdot E_y(t)$,
- вертикальную ($V$): $\mathbf{E_V}(t) = 0\cdot E_x(t) + 1\cdot E_y(t)$,
- диагональную ($D$): $\mathbf{E_D}(t) = 1/\sqrt{2}\cdot E_x(t) + 1/\sqrt{2}\cdot E_y(t)$,
- антидиагональную ($A$): $\mathbf{E_A}(t) = 1/\sqrt{2}\cdot E_x(t) - 1/\sqrt{2}\cdot E_y(t)$.

Полагая $E_x(t)$ и $E_y(t)$ численно равными легко показать, что пары состояний поляризации $H$ и $V$, а также $D$ и $A$ являются взаимно-ортогональными. Любой набор из двух ортогональных состояний поляризации является поляризационным базисом. Особенностью предложенных выше базисов является то, что они не ортогональны между собой.

Для изменения состояний поляризации используются оптические устройства, которые далее называются поляризаторами. Предполагается, что поляризаторы меняют поляризацию сигнала, не меняя его интенсивность. Напротив, поляризационные фильтры ослабляют сигнал, исключая из него компоненту, ортогональную оптической оси устройства.




(а) (б)

Рис. 1. Пример набора поляризационных базисов (линейных) в системах КРК с поляризационным кодированием: (а) базис *HV* (*H* – синим, *B* – красным); (б) базис *DA* (*D* – красным, *A* – синим)

Функциональная схема квантового канала представлена на рисунке 2 [10].

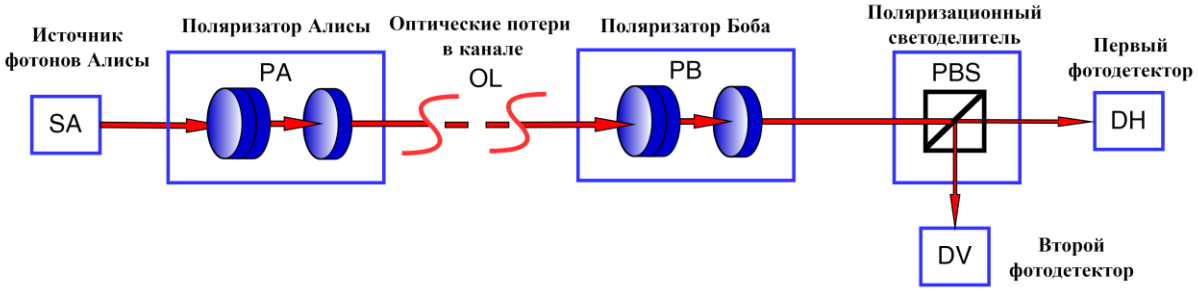



Рис. 2. Функциональная схема оптического канала простейшей системы КРК

Фотоисточник (SA) передающей стороны (Алисы) производит неполяризованный свет, который проходит через поляризатор (PA), имеющий одно из четырёх положений (*H*, *V*, *D*, *A*), соответствующих рассмотренным видам поляризации. Поляризатор (PB) принимающей стороны (Боба) имеет два положения (например, *H*, *D*) и предназначен для того, чтобы различать соответствующие ортогональные пары состояний (*H* и *V*, *D* и *A*). Поляризационный светоделитель (PBS) представляет собой пару поляризационных фильтров и раскладывает входящий сигнал на взаимно ортогональные компоненты, связанные с одним из базисов, например, *H* и *V*. Фотодетекторы (DH и DV) располагаются в соответствующих плечах фотоделителя. В случае если SA производит одиночные фотоны, а в оптическом канале отсутствуют какие-либо потери, то из фотодетекторов DH и DV непременно сработает один и только один.

Безопасность системы КРК следует из фундаментального для квантовой механики коллапса волновой функции. Последнее означает то, что третья сторона, находящаяся между Алисой и Бобом, не может определить состояние поляризации передаваемых по оптическому каналу фотонов, необратимо не искажая его в процессе. В свою очередь, при корректной и математически обоснованной реализации протокола распределения ключей, это гарантирует, что интерференция в канал извне будет замечена сторонами обмена [11].

В дальнейшем, все рассуждения приводятся для идеализированного однофотонного случая. Однако, исключая соображения безопасности, их можно адаптировать для описания системы, оперирующей оптическими импульсами.

## Исчисления Джонса

Для описания состояний поляризации и их трансформации поляризаторами используется математический аппарат, предложенный Р.К. Джонсом в 1941 году. Полагая, что волна является монохроматической с частотой $\omega_0$, (1) можно представить, как [9]

$$\mathbf{E}(t,z)=\begin{cases} E_x\cdot e^{i\cdot\varphi_x}\cdot e^{i\cdot\left(\frac{\omega_0}{c}\cdot z-\omega_0\cdot t\right)}, \\ E_y\cdot e^{i\cdot\varphi_y}\cdot e^{i\cdot\left(\frac{\omega_0}{c}\cdot z-\omega_0\cdot t\right)}. \end{cases}, \tag{2}$$

где $E_x$ , $E_y$ – коэффициенты определяющие интенсивность горизонтального и вертикального компонентов электрического поля; $\varphi_x$, $\varphi_y$ – начальные фазовые смещения соответствующих компонентов; $c$ – скорость света в вакууме. Третья координата (1) всегда остаётся неизменной и исключена из (2) для простоты записи [9].

Полагая для определённости $z = 0$ представим (2) в виде

$$\mathbf{E}(t)=\begin{cases} E_x\cdot e^{i\cdot\varphi_x}\cdot e^{-i\cdot\omega_0\cdot t}, \\ E_y\cdot e^{i\cdot\varphi_y}\cdot e^{-i\cdot\omega_0\cdot t}. \end{cases}. \tag{3}$$

Введём следующие обозначения $E_x = E_0\cdot\cos(\alpha)$, $E_y = E_0\cdot\sin(\alpha)$, $\varphi_0 = \varphi_x$, $\Delta\varphi = \varphi_x - \varphi_y$ и преобразуем (3) к виду

$$\mathbf{E}(t)=E_0\cdot e^{i\cdot(\varphi_0-\omega_0\cdot t)}\cdot\begin{pmatrix}\cos(\alpha)\\ \sin(\alpha)\cdot e^{i\cdot\Delta\varphi}\end{pmatrix}=E_0\cdot e^{i\cdot(\varphi_0-\omega_0\cdot t)}\cdot J(\alpha,\Delta\varphi), \tag{4}$$

где $E_0$ – интенсивность электрического поля; $\varphi_0$ – начальное фазовое смещение колебания в целом; $\Delta\varphi$ – фазовое смещение вертикального поляризационного компонента относительно горизонтального.

Векторный множитель $J(\alpha, \Delta\varphi)$ в (4) называют единичным вектором Джонса [9]. Поляризационное состояние сигнала в целом определяется исключительно данным компонентом. Следовательно, если моделирование оптического канала производится только с целью описания изменений состояния поляризации, то вместо сигналов вида (4) достаточно рассматривать только соответствующие векторы Джонса.

Описанные выше базисные поляризационные состояния в нотации Джонса будут иметь следующий вид: $|H\rangle = J_H = J(0,0)$, $|V\rangle = J_V = J(\pi / 2,0)$, $|D\rangle = J_D = J(\pi / 4,0)$, $|A\rangle = J_A = J(-\pi / 4,0)$.

Однако, необходимо отметить, что в качестве базисных, могут использоваться и произвольные состояния поляризации, если выполняются следующие условия относительно скалярных произведений их векторов Джонса

$$\langle V|H\rangle=\langle A|D\rangle=0,\ \ |\langle V|D\rangle|^2=|\langle H|D\rangle|^2=|\langle H|A\rangle|^2=|\langle V|A\rangle|^2=\frac{1}{2}. \tag{5}$$

Преобразование поляризации сигнала в оптическом канале сводится к умножению вектора Джонса на передаточную функцию оптического устройства. Передаточные функции представляют собой матрицы Джонса – комплекснозначные матрицы размерностью 2 на 2 [9].

## Протокол BB84

Протокол BB84 был предложен Бреннаром и Брассаром в 1984 году и оттуда получил своё название [11]. Согласно протоколу [10, 11], Алиса случайным образом переводит свой поляризатор в одно из 4 положений непосредственно перед отправкой в канал очередного фотона. Боб обычно использует тот же поляризатор, что и Алиса, но при этом переводит его в одно из 2 взаим-

но неортогональных положений. Так, если Боб переводит свой поляризатор в положение *H* (или *V*), то он получает возможность достоверно различать поляризационные состояния |*H*⟩ и |*V*⟩ переданного Алисой фотона. При этом, выбор между *H* и *V* не оказывает практического влияния, поскольку определяет только то, какой из двух фотодетекторов сработает при приёме |*H*⟩, а какой при приёме |*V*⟩. Аналогично, Боб может перевести свой поляризатор в положение *D* (или *A*) и получить возможность различать состояния |*D*⟩ и |*A*⟩ принятого фотона. Если положение поляризатора Боба не соответствует поляризации принятого фотона, то срабатывание любого из детекторов равновероятно, что следует из (5). Возможные ситуации, возникающие при передаче фотона сведены в таблицу 1.

Таблица 1

Возможные ситуации при передаче фотона в соответствии с BB84

| **Выбор Алисы** | **Выбор Боба** | **Принятое состояние** | **Принятый бит** | **Соответствие по базису** |
|---|---|---|---|---|
| \|*H*⟩ (0 в базисе *HV*) | *HV* | \|*H*⟩ | 0 | OK |
| | *DA* | \|*D*⟩ или \|*A*⟩ | 0 или 1 | X |
| \|*V*⟩ (1 в базисе *HV*) | *HV* | \|*V*⟩ | 1 | OK |
| | *DA* | \|*D*⟩ или \|*A*⟩ | 0 или 1 | X |
| \|*D*⟩ (0 в базисе *DA*) | *HV* | \|*H*⟩ или \|*V*⟩ | 0 или 1 | X |
| | *DA* | \|*D*⟩ | 0 | OK |
| \|*A*⟩ (1 в базисе *DA*) | *HV* | \|*H*⟩ или \|*V*⟩ | 0 или 1 | X |
| | *DA* | \|*A*⟩ | 1 | OK |

В дальнейшем, стороны обмениваются информацией об использованных базисах по открытому каналу [10-12]. С помощью этой информации, каждый из участников обмена, просеивает имеющуюся у него битовую последовательность для того, чтобы исключить значения, полученные при несоответствии выбора базисов. Просеянные значения используются в дальнейшем для получения ключевого материала. Появление злоумышленника в канале сделает возможной ситуацию, в которой при совпадении базисов у сторон будут отличаться принятые значения. Авторами протокола формально показано, что присутствие третьей стороны, способной скомпрометировать распределяемый ключ, может быть обнаружено даже в тех случаях, когда в канале возможны искажения и ошибки приёма [12].

## Модель поляризаторов

В качестве поляризаторов, для примера, выбрана комбинация из последовательно расположенных полуволновой и четвертьволновой пластин, предложенная в [13]. Такая реализация поляризаторов не является ни единственно возможной, ни простейшей. Однако, её отличительной особенностью является достижимость линейных, круговых и эллиптических поляризаций в канале.

Определим взаимноортогональные принципиальные состояния поляризации |*X*⟩ и |*Y*⟩, связанные с лабораторной системой координат и при этом непосредственно не связанные с базисами протокола BB84. Для определённости положим, что

$$|X\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |Y\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \qquad (5)$$

$$TF(\theta_1, \theta_2) = QW(\theta_2) \times HW(\theta_1)$$

Передаточная функция полуволновой пластины, оптическая ось которой повёрнута на угол θ относительно оси *Ox* в лабораторной системе координат описывается матрицей Джонса [9]

$$HW(\theta) = \begin{pmatrix} \cos(2\cdot\theta) & \sin(2\cdot\theta) \\ \sin(2\cdot\theta) & -\cos(2\cdot\theta) \end{pmatrix}. \qquad (6)$$

Аналогичным образом, описывается и четвертьволновая пластина [9]

$$QW(\theta) = \begin{pmatrix} \cos^2(\theta) + i\cdot\sin^2(\theta) & (1-i)\cdot\sin(\theta)\cdot\cos(\theta) \\ (1-i)\cdot\sin(\theta)\cdot\cos(\theta) & i\cdot\cos^2(\theta) + \sin^2(\theta) \end{pmatrix}. \qquad (7)$$

Поляризация $J_{OUT}$ сигнала на выходе поляризатора определяется как

$$J_{OUT} = QW(\theta_1) \times \left[ HW(\theta_2) \times J_{IN} \right].$$

### Модель в нотации раскрашенных сетей Петри

В качестве математической основы для модели выбраны раскрашенные сети Петри. Сети Петри представляют собой направленный двудольный ориентированный граф, вершины которого представлены переходами и позициями. Суть моделирования сводится к перемещению токенов между позициями через переходы. Каждое срабатывание перехода, то есть перемещение токена (или токенов) из исходной позиции (позиций) в конечную позицию (позиции) представляет собой дискретное событие. Структура графа, а именно связи между позициями и переходами, позволяют воссоздать условия появления тех или иных событий, а также воспроизвести требуемую их последовательность или, напротив, параллельность. Основным преимуществом моделирования с помощью сетей Петри обычно отмечают удобство для воспроизведения циклических и ветвящихся процессов в рамках дискретно-событийной модели. Другим преимуществом аппарата является то, что нотация сетей Петри принципиально имеет графическую интерпретацию и поэтому модель является в некоторой степени наглядной [14].

В раскрашенных сетях позиции ассоциированы с определёнными типами данных (палитрами), а токены – с конкретными значениями (цветами), соответствующими этим типам данных (то есть палитрам). Соответствующим образом, дискретное срабатывание перехода представляет собой определяемую на этапе построения модели функцию, которая применяется к значениям входных токенов и на их основе формируют значения выходных токенов [14]. Применение раскрашенных сетей Петри для моделирования оптического канала позволяет удобным описать циклический процесс передачи фотонов (представлены токенами, цвета которых принадлежат палитре, связанной с векторами Джонса в форме (4)). Оптические преобразования описываются на уровне переходов и сводятся к умножению вектора Джонса (значения в токене) на матрицу Джонса, задаваемую (6) или (7). При этом, значения целевых углов поворотов пластин передаётся в переход в качестве дополнительного аргумента. Общий вид модели, соответствующий композиции на рисунке 1, представлен на рисунке 3.

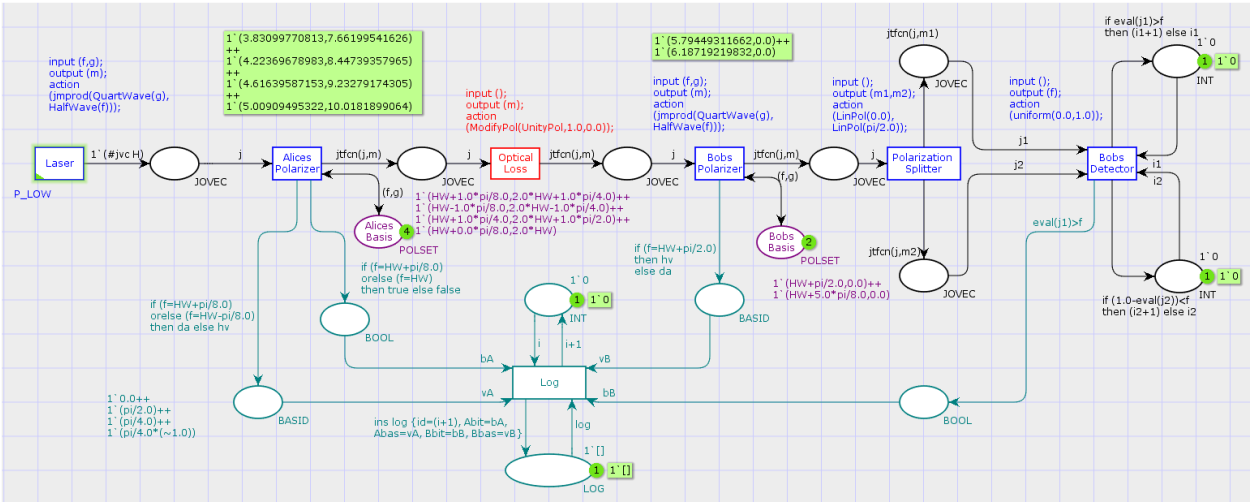



Рис. 3. Модель оптического канала в нотации раскрашенных сетей Петри

Переходы, выделенные синим цветом, соответствуют функциям основных устройств в оптическом канале, отмеченных на рисунке 1. Позиции, выделенные фиолетовым цветом, содержат уставки, относящиеся к углам поворота волновых пластин в поляризаторах Алисы и Боба. Базовая конфигурация моделируемого протокола BB84 предполагает, что каждая из уставок (положений поляризатора) выбирается случайным образом из заданного набора. Переход отмеченный красным может быть использован для внесения в модель вероятности потери фотона в оптической линии и не используется в исследовании, проводимом дальше. Фрагмент сети, отмеченный бирюзовым цветом, представляет собой надстройку, которая используется для логирования и последующего сбора статистики по результатам прогона модели.

## Исследование влияния ошибки в согласовании базисов поляризаторов на вероятность битовой ошибки

Согласно [15] источниками битовых ошибок в практических системах КРК выступает один из четырёх факторов: неидеальность источника или детектора одиночных фотонов, потери и искажения в квантовом канале, несоответствия в согласовании базисных положений поляризаторов между Алисой и Бобом. В дальнейшем воспроизводится численное исследование влияния последнего фактора, а именно ошибки в позиционировании фазовых пластин в поляризаторе одной из сторон, на битовые ошибки в принятой сырой битовой последовательности. Выбор этого фактора обусловлен, прежде всего, тем обстоятельством, что он может быть воспроизведён на физическом уровне с использованием программно-аппаратного учебного стенда имитации КРК, разработанного и производимого с участием нашего университета.

Для исследования влияния указанного фактора проведена серия вычислительных экспериментов, результаты которых сведены в таблицы далее. Для простоты, в качестве исходного набора базисов используются линейные поляризации, аналогичные представленным на рисунке 1 (для α = 0): $H = \begin{pmatrix}\cos(\alpha)\\ \sin(\alpha)\end{pmatrix}$, $V = \begin{pmatrix}-\sin(\alpha)\\ \cos(\alpha)\end{pmatrix}$, $D = 1/\sqrt{2}\begin{pmatrix}\cos(\alpha)-\sin(\alpha)\\ \sin(\alpha)+\cos(\alpha)\end{pmatrix}$, $A = 1/\sqrt{2}\begin{pmatrix}\cos(\alpha)+\sin(\alpha)\\ \sin(\alpha)-\cos(\alpha)\end{pmatrix}$.
Эксперименты характеризуются следующими условиями:

1. базисы сторон соответствуют с точностью до варьируемой величины ошибки в позиционировании полуволновой пластины на стороне Боба (в обоих базисах);
2. аналогично первому эксперименту, однако варьируемым параметром является не ошибка позиционирования пластины (остаётся фиксированной), а исходный поляризационный базис.

Результаты первого эксперимента представлены в таблице 2. Из таблицы видно, что ошибка Δφ в выборе пластин влияет на вероятность битовой ошибки (QBER) и на коррелированность между битами сырой ключевой последовательность у сторон обмена (CORR). Результаты, полученные для обратного направления поворота пластины, аналогичны данным в таблице. Таким образом, вероятность битовой ошибки и коррелированность ключевой последовательности определяется абсолютным значением |Δφ| ошибки согласования базисов.

Таблица 2

Возможные ситуации при передаче фотона в соответствии с BB84 (α = 0).

| Δφ, ° | CORR | QBER, % | Поляризатор Алисы $\theta_{1,A}$ $\theta_{2,A}$, ° | | | | Поляризатор Боба $\theta_{1,B}$ $\theta_{2,B}$, ° | |
|---|---|---|---|---|---|---|---|---|
| | | | *H* | *V* | *D* | *A* | *HV* | *DA* |
| 0 | 1,00 | 0 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 90 0 | 112,5 0 |
| 5 | 0,94 | 2,9 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 95 0 | 117,5 0 |
| 10 | 0,77 | 11,4 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 100 0 | 122,5 0 |
| 15 | 0,52 | 23,8 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 105 0 | 127,5 0 |
| 20 | 0,16 | 41,9 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 110 0 | 132,5 0 |
| 25 | –0,14 | 57,2 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 115 0 | 137,5 0 |
| 30 | –0,48 | 73,9 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 120 0 | 142,5 0 |
| 35 | –0,77 | 88,6 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 125 0 | 147,5 0 |
| 40 | –0,92 | 95,9 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 130 0 | 152,5 0 |
| 45 | –1,00 | 100 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 135 0 | 157,5 0 |

Результаты второго эксперимента представлены в таблице 3. Согласно данным моделирования, влияние выбранного базиса линейной поляризации на вероятность битовой ошибки не наблюдается. В отсутствии выраженного тренда, небольшие флуктуации в значениях объясняются относительно малым числом фотонов, передача которых моделировалась (3000 на каждый эксперимент).

Таблица 3

Возможные ситуации при передаче фотона в соответствии с BB84 ($\Delta\varphi = 22{,}5^{O}$).

| α, O | CORR | QBER, % | Поляризатор Алисы $\theta_{1,A}\ \theta_{2,A}$, O | | | | Поляризатор Боба $\theta_{1,B}\ \theta_{2,B}$, O | |
|---|---|---|---|---|---|---|---|---|
| | | | *H* | *V* | *D* | *A* | *HV* | *DA* |
| 0 | –0,03 | 51,5 | 0 0 | 45 90 | 22,5 45 | 337,5 315 | 112,5 0 | 135 0 |
| 10 | 0,05 | 47,7 | 10 20 | 55 110 | 32,5 65 | 347,5 335 | 122,5 0 | 145 0 |
| 20 | –0,01 | 50,1 | 20 40 | 65 130 | 42,5 85 | 357,5 355 | 132,5 0 | 155 0 |
| 30 | 0,01 | 49,7 | 30 60 | 75 150 | 52,5 105 | 7,5 15 | 142,5 0 | 165 0 |
| 40 | -0,01 | 50,5 | 40 80 | 85 170 | 62,5 125 | 17,5 35 | 152,5 0 | 175 0 |
| 50 | 0,03 | 48,5 | 50 100 | 95 190 | 72,5 145 | 27,5 55 | 162,5 0 | 185 0 |
| 60 | -0,01 | 50,2 | 60 120 | 105 210 | 82,5 165 | 37,5 75 | 172,5 0 | 195 0 |
| 70 | 0,01 | 49,8 | 70 140 | 115 230 | 92,5 185 | 47,5 95 | 182,5 0 | 205 0 |
| 80 | 0,02 | 49,2 | 80 160 | 125 250 | 102,5 205 | 57,5 105 | 192,5 0 | 215 0 |
| 90 | | 50,9 | 90 180 | 135 270 | 112,5 225 | 67,5 125 | 202,5 0 | 225 0 |

В целом, проделанные эксперименты с имитационной моделью, а также численный анализ с применением математических пакетов, позволяют сделать вывод о том, что в рамках протокола BB84 принимающая сторона, используя только информацию, передаваемую в рамках протокола по квантовому и вспомогательному каналам, не может сделать выводов об имеющем место рассогласовании базисов на основании статистической обработки получаемой информации.

## Выводы

Таким образом, предложенная дискретно-событийная модель, построенная с применением сетей Петри, была использована для изучения влияния неидеальности согласования поляризационных базисов на вероятность битовых ошибок. Последний приём, а именно внесение ошибок в позиционирование пластин, может использоваться для моделирования неидеальности реальных систем с применением физических учебных стендов-эмуляторов.

В дальнейшем планируется воспроизвести аналогичные эксперименты с использованием аппаратно-программного решения для имитации распределения ключей по протоколу BB84 с поляризационным кодированием, созданным совместно с кампанией Инфотекс в Томском государственном университете систем управления и радиоэлектроники.

Непосредственно предложенная модель будет использоваться для воссоздания реалистичного распределения битовых ошибок в рамках исследования методов постобработки сырого ключевого материала, в частности, для формализованного сравнения алгоритмов согласования ошибок. Последнее важно, поскольку является необходимым условием для оптимизации использования ресурсов систем КРК на этапе их широкого внедрения в существующую телекоммуникационную инфраструктуру [16].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Фролова С.М. Информационно-коммуникационных технологии в контексте современного развития общества. // Известия Саратовского университета. Философия. Психология. Педагогика. 2022. Т. 22. №. 3. С. 288-292.
2. Антилла Ю. Информационная безопасность как вызов современному обществу. // Вестник ЮУрГУ. 2022. Т. 14. №. 2. С. 65-70.
3. Shivaputrappa, V. IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability. // San Jose State University (CA). 2005. URL: http://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf.
4. Beck M., Tews E. Practical attacks against WEP and WPA. // Proceedings of the 2nd ACM Conference on Wireless Network Security, WiSec'09. Zurich, Switzerland, 2009. С. 79–85.
5. Vanhoef, M.; Ronen, E. Dragonblood: A Security Analysis of WPA3's SAE Handshake // Proceedings of the Real World Crypto 2020 and IEEE Symposium on Security & Privacy 2020. Vol. 2019. №. 383.
6. Aumasson J.P. The impact of quantum computing on cryptography. // Computer Fraud and Security. 2017. Iss. 6. P. 8-11.
7. Mina M.-Z., Simon E. Information Security in the Quantum Era. Threats to modern cryptography: Grover's algorithm. // Cryptology ePrint Archive. 2021. URL: https://eprint.iacr.org/2021/1662.
8. Ritik B., Eashan Jayant C., Ashutosh B., Kamlesh T., Sandeep D., Atul J. Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research. // ArXiv Preprint. 2022. URL: http://arxiv.org/abs/2202.02826.

9. Collet E. Field Guide to Polarization. SPIE Press. 2005. p. 148.
10. Bloom Y., Fields I., Maslennikov A., Rozenman G. Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation. // Physics (Switzerland). 2022. Vol. 4. Iss. 1. P. 104-123.
11. Sun S., Huang A. A Review of Security Evaluation of Practical Quantum Key Distribution System. // Entropy. 2022. Vol. 24. Iss. 2. P. 1-19.
12. Sabani M., Savvas I., Poulakis D., Makris G. Quantum Key Distribution: Basic Protocols and Threats. // ACM International Conference Proceeding Series. Vol. PCI-2022. 2022. P. 383-388.
13. Катамадзе К. Демонстрационный симулятор системы квантового распределения ключа. // Патент РФ №2795245. 2021. Бюл. №13.
14. Faerman V.A., Voevodin K.D., Avramchuk V.S. Case of discrete-event simulation of the simple sensor node with CPN Tools // Proceedings of 2022 International Siberian Conference on Control and Communications (SIBCON). IEEE, 2022.
15. Mailloux L.O., Morris J.D., Crimaila M.R., Hodson D.D., Colombi J.M., McLaughlin J.M., Holes J.A. A Modeling Framework for Studying Quantum Key Distribution System Implementation Nonidealities // IEEE Access. Vol. 3. 2015.
16. Шелупанов А.А., Евсютин О.О., Конев А.А., Костюченко Е.Ю., Кручинин Д.В., Никифоров Д.С.] Актуальные направления развития методов и средств защиты информации // Доклады ТУСУР. Том 20. № 3. 2017. С. 11-24.

**Васильев Егор Иванович**
Студент кафедры Безопасности
информационных систем,
Томский университет систем управления
и радиоэлектроники
634050, Россия, г. Томск, Ленина пр., д. 40
Эл. почта: egg.or.no@yandex.ru

**Фаерман Владимир Андреевич**
Старший преподаватель кафедры
Комплексной информационной безопасности
электронно-вычислительных систем,
Томский университет систем управления
и радиоэлектроники, член IEEE
634050, Россия, г. Томск, Ленина пр., д. 40
ORCID: 0000-0002-9643-0245
Тел.: +7-(923)-44-350-44
Эл. почта: fva@fb.tusur.ru

*E.I. VASILIEV, V.A. FAERMAN*

## DISCRETE-EVENT SIMULATION OF THE OPTICAL CHANNEL WITHIN QUANTUM KEY DISTRIBUTION SYSTEM

The article features a discrete-event simulation of a simple quantum key distribution (QKD) system that applies the BB84 protocol with polarization encoding. The model is built with colored Petri nets. The simulated physical prototype uses a pair of optical devices that are comprised of half-wave and quarter-wave phase retarders with mechanical rotators to alter the state of polarization of transmitted and received photons. Jones calculus is used to formalize and analyze polarization transforms within the optical channel. The QKD model is implemented with the free CPN Tools environment. We have used the proposed model to investigate the effects of inaccuracies in phase retarder angular positioning on quantum bit error rate. Those computational experiments are conducted for several reference positions of the retarders associated with the particular polarization states of the photons transmitted into the medium. In the future, this model will be used as a generator for realistic raw key sequences with errors to study and compare post-processing algorithms, such as error reconciliation methods.

***Keywords:*** *quantum key distribution, optical channel, Petri nets, simulation modeling, BB84.*

R E F E R E N C E S

1. Frolova S.M. Information and communication technologies in the context of modern development of society. *Izvestiya of Saratov University. Philosophy. Psychology. Pedagogy*. 2022. Vol. 22. Iss. 3. P. 288-292 (in Russian).
2. Antilla Ju. Information security challenge of modern society. *Bulletin of the South Ural State University*. 2022. Vol. 14. Iss. 2. P. 65-70 (in Russian).
3. Shivaputrappa, V. IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability. *San Jose, CA*. URL: http://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf. 2005.
4. Beck M., Tews E. Practical attacks against WEP and WPA. *Proceedings of the 2nd ACM Conference on Wireless Network Security, WiSec'09. Zurich, Switzerland*, 2009. P. 79–85.
5. Vanhoef, M.; Ronen, E. Dragonblood: A Security Analysis of WPA3's SAE Handshake. *Proceedings of the Real World Crypto 2020 and IEEE Symposium on Security & Privacy 2020*. Vol. 2019. No. 383.
6. Aumasson J.P. The impact of quantum computing on cryptography. *Computer Fraud and Security*. 2017. Iss. 6. P. 8-11.
7. Mina M.-Z., Simon E. Information Security in the Quantum Era. Threats to modern cryptography: Grover's algorithm. *Cryptology ePrint Archive*. 2021. URL: https://eprint.iacr.org/2021/1662.

8. Ritik B., Eashan Jayant C., Ashutosh B., Kamlesh T., Sandeep D., Atul J. Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research. *ArXiv Preprint*. 2022. URL: http://arxiv.org/abs/2202.02826.
9. Collet E. Field Guide to Polarization. *SPIE Press*. 2005. p. 148.
10. Bloom Y., Fields I., Maslennikov A., Rozenman G. Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation. *Physics (Switzerland)*. 2022. Vol. 4. Iss. 1. P. 104-123.
11. Sun S., Huang A. A Review of Security Evaluation of Practical Quantum Key Distribution System. *Entropy*. 2022. Vol. 24. Iss. 2. P. 1-19.
12. Sabani M., Savvas I., Poulakis D., Makris G. Quantum Key Distribution: Basic Protocols and Threats. *ACM International Conference Proceeding Series*. Vol. PCI-2022. 2022. P. 383-388.
13. Катамадзе К. Demonstrative Simulator of QKD System [Demonstracionnyj simuljator sistemy kvantovogo raspredelenija kljucha]. *Patent RU2795245*. 2021. Published 02.05.2023 in Bulletin No. 13.
14. Faerman V.A., Voevodin K.D., Avramchuk V.S. Case of discrete-event simulation of the simple sensor node with CPN Tools. *Proceedings of 2022 International Siberian Conference on Control and Communications (SIBCON)*. IEEE, 2022.
15. Mailloux L.O., Morris J.D., Crimaila M.R., Hodson D.D., Colombi J.M., McLaughlin J.M., Holes J.A. A Modeling Framework for Studying Quantum Key Distribution System Implementation Nonidealities. *IEEE Access*. Vol. 3. 2015.
16. Shelupanov A.A., Evsyutin O.O., Konev A.A., Kostyuchenko E.Yu., Kruchinin D.V., Nikiforov D.S. Current trends in methods and application for information security. [Aktual'nye napravlenija razvitija metodov i sredstv zashhity informacii]. *Doklady TUSUR*. Vol. 20. No. 3. 2017. P. 11-24. [in Russian]

**Egor I. Vasiliev**
Student, Department of Security of Information Systems,
Tomsk State University of Control Systems
and Radioelectronics,
40, Lenina ave., Tomsk, Russia, 634050,
E-mail: egg.or.no@yandex.ru

**Vladimir A. Faerman**
Senior Lecturer, Department of Complex
Information Security of Computer Systems,
Tomsk State University of Control Systems
and Radioelectronics, IEEE member
40, Lenina ave., Tomsk, Russia, 634050
ORCID: 0000-0002-9643-0245
Phone: +7 (391-3) 12-34-56
E-mail: fva@fb.tusur.ru