Письма в ЖЭТФ, том 112, вып. 6, с. 401 – 411

О новой атаке на квантовое распределение ключей: совместные измерения с определенным исходом зондирующих состояний и PNS атака на информационные состояния

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии Российской Федерации, 121552 Москва, Россия

Центр квантовых технологий, МГУ им. М. В. Ломоносова, 119899 Москва, Россия

Поступила в редакцию 11 августа 2020 г.
После переработки 15 августа 2020 г.
Принята к публикации 16 августа 2020 г.

Предложена новая атака на квантовое распределение ключей, основанная на совместных квантовых измерениях с определенным исходом отраженных зондирующих состояний от модулятора интенсивности и PNS измерениях (Photon Number Splitting – неразрушающие измерения числа фотонов) информационных состояний в квантовом канале связи. Данная атака не изменяет относительной статистики фотоотсчетов состояний с разным числом фотонов, не производит ошибок на приемной стороне, поэтому не детектируется ни одним из известных методов, включая модифицированный Decoy State метод. Атака приводит только к дополнительным потерям в линии связи, за которыми не "следит" Decoy State метод. Дана оценка привносимых потерь в зависимости от интенсивности отраженных зондирующих состояний. Критический уровень потерь зависит от конкретной физической реализации системы квантовой криптографии, которая определяет верхнюю границу интенсивности отраженных зондирующих состояний. Знание данной границы принципиально необходимо для обеспечения секретности ключей. Тот факт, что атака не приводит к ошибкам на приемной стороне и не изменяет относительной статистики фотоотсчетов, а приводит только к дополнительным потерям, которые зависят от интенсивности, соответственно различимости отраженных зондирующих состояний, *не означает*, что данная атака переводит системы квантовой криптографии из разряда криптографических систем, где секретность ключей гарантируется фундаментальными законами квантовой механики, в разряд систем, где секретность гарантируется техническими ограничениями. Даже при наличии побочных каналов утечки информации секретность ключей по-прежнему гарантируется фундаментальными ограничениями квантовой механики на различимость состояний. Низкий уровень различимости ("интенсивности") квантовых состояний в побочных каналах, естественно, достигается техническими средствами.

DOI: 10.31857/S123456782018010X

1. Введение. Методы несакционированного съема информации развиваются по мере развития способов передачи и защиты информации. В классической области носителями информации являются электромагнитные сигналы, которые передаются либо через открытое пространство, по кабельным или волоконным линиям связи. Несанкционированный съем информации для классических сигналов возможен как с кабельных линий связи, так и с волоконно-оптических линий.

Для получения информации не обязательно иметь непосредственный доступ к самой линии связи, поскольку работа передающей и приемной аппаратуры приводит к побочному электромагнитному излучению, которое может детектироваться. Детектирование побочного электромагнитного излучения может приводить к компроментации работы электронного криптографического оборудования. Различные типы интерфейсов между отдельными модулями аппаратуры также приводят к компроментирующему побочному излучению.

Существуют и другие побочные каналы утечки информации: электромагнитное излучение, оптическое излучение (электромагнитное в оптическом диапазоне), акустические каналы, ультразвуковые, механические и пр., которые могут приводить к утеч-

[1)]e-mail: sergei.molotkov@gmail.com

ке информации без непосредственного доступа к источнику информации. Большой набор методов и экспериментальных устройств, существующих в данной области, обычно широко не освещается. Некоторые аспекты детектирования побочных сигналов в классических криптографических системах, а также исторические примеры см., например, в [1–7].

Понижение уровня оптического сигнала до однофотонного уровня приводит к тому, что сигнал становится квантовым, и это приводит к принципиально качественно новой ситуации. В отличии от интенсивного классического оптического сигнала, передаваемого по волоконной линии связи, попытки подслушать – измерить неизвестное состояние в линии связи приводят к возмущению квантового состояния и ошибкам на приемной стороне [8]. По этой причине любое вторжение в квантовый канал связи детектируется, что гарантируется фундаментальными законами квантового мира. Более того, фундаментальные ограничения квантовой механики позволяют связать наблюдаемый уровень возмущения квантовых состояний (уровень ошибок) на приемной стороне с верхней границей утечки информации [9–11]. Собственно, на этом и строится квантовая криптография – квантовое распределение секретных ключей.

В этом смысле, системы квантовой криптографии защищены от атак непосредственно на линию связи. Более того, считается, что линия связи непосредственно доступна для активного прослушивания – вторжения.

На сегодняшний день касательно атак на квантовые состояния в квантовой линии связи – попыток съема передаваемой ключевой информации достигнуто достаточно глубокое понимание. Существуют методы учета не строгой однофотонности источника квантовых состояний, потерь в линии связи, не единичной квантовой эффективности однофотонных детекторов и пр. Относительно атак на квантовый канал связи можно говорить, что квантовая криптография обеспечивает безусловную секретность ключей, которая базируется только на фундаментальных законах квантовой механики.

Системы квантовой криптографии представляют собой достаточно сложные и насыщенные активными волоконными компонентами устройства – фазовыми модуляторами, модуляторами интенсивности, контроллерами поляризации, управляющей электроникой с различными внешними и внутренними интерфейсами. Работа электроники и электронно-управляемых активных волоконных элементов приводит к побочному излучению, которое несет на себе информацию о передаваемых ключах.

В квантовой криптографии ситуация еще более деликатная, чем в классических криптографических системах. Системы квантовой криптографии являются открытыми системами, в том смысле, что кроме детектирования побочного излучения, подслушиватель может активно зондировать через волоконную линию связи состояние волоконных элементов (фазовых модуляторов, модуляторов интенсивности, контроллеров поляризации и пр.), которые дают информацию о передаваемых ключах.

Без понимания и учета утечки информации по побочным каналам невозможно всерьез говорить о секретности ключей в реальных системах квантовой криптографии.

Еще одно принципиальное отличие побочных каналов в квантовой криптографии от побочных каналов в классических системах состоит в том, что невозможно рассматривать состояния в побочных каналах классическим образом. Подслушиватель может совместно измерять информационные квантовые состояния и состояния в побочных каналах, что требует полного квантового рассмотрения.

На сегодняшний день полный набор методов учета атак на аппаратуру и учет побочных каналов утечки находится в стадии активного исследования. В отличии от классических криптографических систем исследование утечки информации по побочных каналам началось совсем недавно [12–20].

В реальных системах источник информационных состояний представляет собой ослабленные когерентные состояния с пуассоновской статистикой по числу фотонов, и не является строго однофотонным. Секретный ключ набирается только из однофотонной компоненты когерентных состояний. Информация, заключенная в многофотонных компонентах состояний с числом фотонов $k > 1$, консервативно в пользу Евы, считается ей известной. Доля однофотонной компоненты на приемной стороне оценивается модифицированным Decoy State методом (см. детали в [21–23]). Без побочных каналов утечки информации самой общей атакой на однофотонную компоненту состояний является унитарная атака. Для протокола BB84 такую оптимальную атаку можно построить явно [24, 25].

Поскольку многофотонные компоненты состояний "отдаются" (считаются известными) подслушивателю, то дальнейшая задача сводится к построению атаки на однофотонную компоненту с учетом побочных каналов утечки.

Принципиально важно для Decoy State метода, что не имея дополнительной информации, подслушиватель не знает, из какого состояния и с каким средним числом фотонов произошла компонента с данным числом фотонов k. Искажение однофотонной компоненты в посылках, относящихся к когерентным состояниям с разной интенсивностью, приводит к искажению относительного наблюдаемого полного темпа отсчетов – статистики на приемной стороне для посылок, в которых посылались состояния с разной интенсивностью. Изменение относительного полного темпа отсчетов позволяет оценить долю однофотонной компоненты и ошибку в ней на приемной стороне.

Все сказанное справедливо до тех пор, пока у подслушивателя нет дополнительной информации о том, какое состояние и с какой интенсивностью (средним числом фотонов) посылалось в квантовый канал связи в каждой посылке.

При наличии побочных сигналов, предположения, на которых базируется Decoy State метод, нарушаются. При активном зондировании состояния модулятора интенсивности, подслушиватель получает дополнительную информацию об интенсивности передаваемого состояния.

Измерения над отраженными от модулятора интенсивности зондирующими состояниями дают дополнительную информацию об интенсивности передаваемого состояния в каждой посылке. Возможны измерения двух типов.

1) Измерение, минимизирующее ошибку различения отраженных состояний.

2) Измерения с определенным исходом – Unambiguous Measurements (UM).

Измерения первого типа позволяют различить квантовые состояния, но с некоторой вероятностью ошибки. Измерения второго типа различают состояния с определенностью, если получен *conclusive* исход. При неопределенном исходе, обычно обозначаемым "?", ничего о состоянии сказать нельзя. При различении N состояний, измерение первого типа имеет N исходов. Измерение второго типа имеет $N+1$ исход, N определенных, и один "?" – неопределенный. Отметим, что для существования UM измерений необходимым и достаточным условием является линейная независимость набора N состояний [26–33], что выполнено для отраженных состояний (см. ниже).

Атака на распределяемые ключи в случае измерений первого типа детектируется Decoy State методом, поскольку изменяет пуассоновскую статистику отсчетов. Однако стандартный Decoy State метод [21–23] требует радикального изменения, что было сделано в работах [17, 18].

В данной работе будет предъявлена новая атака, которая сводится к активному зондированию модулятора интенсивности, UM измерений отраженных состояний и PNS атака с неразрушающим измерением числа фотонов в информационных состояниях в квантовом канале, которая до сих пор, насколько нам известно, не рассматривалась.

При такой атаке подслушиватель *знает весь ключ*, не производит ошибок на приемной стороне, не изменяет пуассоновской статистики фотоотсчетов на приемной стороне в посылках, отвечающих когерентным состояниям с разной интенсивностью (средним числом фотонов).

Данная атака принципиально не детектируется Decoy State методом, поскольку не меняет наблюдаемой относительной статистики отсчетов на приемной стороне состояний с разной интенсивностью. Атака приводит лишь к снижению общего темпа фотоотсчетов, т.е. приводит лишь к увеличению наблюдаемых потерь без изменения статистики отсчетов в фоковских компонентах состояний с разным числом фотонов.

Важно отметить, что полные потери в линии связи в Decoy State методе явно не фигурируют [17, 21–23], т.е. за общими потерями не нужно следить в стандартном [21–23] и модифицированном Decoy State методе [17, 18].

Поскольку предлагаемая атака приводит лишь к дополнительным потерям – снижению темпа отсчетов на приемной стороне и не производит ошибок, и не нарушает статистики отсчетов, то важно знать, к какому уровню потерь приводит такая атака.

Точнее говоря, атака не детектируется известными методами, но является эффективной – не детектируемой, если уровень потерь, производимый атакой будет не менее некоторой величины.

Цель работы – оценить критический наблюдаемый уровень потерь – снижение темпа фотоотсчетов, при котором такая атака становится возможной.

2. Описание атаки. Идея атаки достаточно проста. В системах квантовой криптографии с фазовым кодированием на передающей стороне используются активные элементы – фазовый модулятор и модулятор интенсивности. Если известно состояние фазового модулятора, то известен передаваемый бит ключа. Если известно состояние модулятора интенсивности, то известна интенсивность когерентного состояния (и среднего числа фотонов) в нем. Если подслушивателю достоверно известно состояние обоих активных элементов, то подслушиватель знает весь передаваемый ключ.

Поскольку системы квантовой криптографии являются открытыми системами, то подслушиватель, кроме доступа к квантовому каналу связи, может активно зондировать через волоконную линию связи состояние активных элементов, посылая зондирующее излучение, и затем измеряя отраженное состояние.

Степень различимости отраженных состояний от активных элементов передающей станции зависит от интенсивности отраженных состояний. Интенсивные – классические состояния достоверно различимы. Если интенсивность информационных состояний, выходящих из передающей станции, контролируется передатчиком, то интенсивность отраженных состояний контролируется подслушивателем. Чем более интенсивные зондирующие состояния посылает подслушиватель, тем более интенсивными будут отраженные зондирующие состояния.

Для того, чтобы знать верхнюю границу интенсивности отраженных состояний, нужно знать верхнюю границу по интенсивности входных зондирующих состояний. Такая граница по интенсивности диктуется плавлением оптического волокна [34–36]. Иначе говоря, интенсивность входных состояний не может быть больше предела, при котором волокно плавится [34–36].

Верхняя граница интенсивности отраженных состояний при известной верхней границе интенсивности входных состояний может регулироваться использованием оптических изоляторов, которые ослабляют выходные отраженные состояния до нужного уровня. Данный уровень будем считать известным. Данный уровень будет определять вероятность различимости выходных зондирующих состояний.

Ниже будем иметь в виду применение к протоколу BB84, как наиболее распространенному. Фазовый модулятор может быть в 4-х состояниях, отвечающих значениям $x = 0$ и $x = 1$ в прямом базисе $b = +$ и сопряженном $b = \times$. Обозначим отраженные от фазового модулятора состояния, отвечающие 4-м значениям $|\psi_{x_b}\rangle_{PM}$.

В Decoy State методе [17, 23] обычно используются состояния с тремя разными интенсивностями (средним числом фотонов) μ, ν_1, ν_2, которые отвечают трем разным состояниям модулятора интенсивности. Отраженные от модулятора интенсивности состояния для трех значений интенсивности (среднего числа фотонов) $\xi = \mu, \nu_1, \nu_2$, $|\psi_\xi\rangle_{MI}$ обозначим $|\psi_{x_b}\rangle_{PM}$. Всего имеется 12 отраженных состояний в побочном канале активного зондирования

$$|\psi_{x_b\xi}\rangle_{PMMI} = |\psi_{x_b}\rangle_{PM} \otimes |\psi_\xi\rangle_{MI}. \tag{1}$$

Если в качестве входных зондирующих состояний на практике используется когерентное состояние, то после отражения от активного оптического элемента на выходе в линию связи будет когерентное состояние со сдвинутой фазой, зависящей от состояния активного элемента, и другой интенсивностью. В пользу Евы считаем отраженные состояния чистыми, поскольку они имеют большую различимость. В этих предположениях можно представить отраженные состояния как

$$\begin{gathered}|\alpha_{x_b\xi}\rangle_{PMMI} = |\alpha_{x_b}\rangle_{PM} \otimes |\alpha_\xi\rangle_{MI},\\ x_b = \{0+, 1+, 0\times, 1\times\},\ \xi = \{\mu, \nu_1, \nu_2\}.\end{gathered} \tag{2}$$

2.1. Непосредственное различение состояний в побочном канале. Первая стратегия сводится к различению непосредственно 12-ти отраженных (1), (2) зондирующих состояний при помощи UM измерений. Однако такая стратегия не является наилучшей изза малой вероятности определенного исхода при UM измерениях, поскольку требует различения 12-ти состояний.

Такая стратегия приводит к вероятности определенного исхода порядка $\Pr_{OK} \approx \mu_{\max}^{11}$, где $\mu_{\max} = \max_{x_b,\xi}\{|\alpha_{x_b,\xi}|^2\}$ – максимальное среднее число фотонов в отраженных состояниях.

Считаем, что использование оптических изоляторов, среднее число фотонов в отраженных состояниях не превышает среднего числа фотонов $\mu \approx 0.2{-}0.5$ в информационных состояниях, $\mu_{\max} < \max_\xi\{\xi\} = \mu$. При такой атаке вероятность успешного различения интенсивности передаваемых информационных состояний и значений бита ключа оказывается ничтожной, соответственно в таком виде атака приводит к слишком большим потерям. Более эффективной будет следующая стратегия.

2.2. Измерение интенсивности отраженных от модулятора интенсивности состояний и PNS атака на информационные состояния в квантовом канале. Напомним, что цель Евы узнать передаваемый бит, не произвести ошибок, и не быть обнаруженной Decoy State методом. Для последнего Ева должна знать интенсивность состояния в каждой посылке, что передается μ, ν_1, ν_2.

Атака:

Ева при помощи UM измерений различает состояния $|\alpha_\mu\rangle_{MI}$, $|\alpha_{\nu_1}\rangle_{MI}$ и $|\alpha_{\nu_2}\rangle_{MI}$. Если исход измерения неопределенный, посылка блокируется.

Если исход определенный, то известно состояние: или $|\alpha_\mu\rangle_{MI}$, или $|\alpha_{\nu_1}\rangle_{MI}$, или $|\alpha_{\nu_2}\rangle_{MI}$. Затем производятся неразрушающие измерения числа фотонов в информационных состояниях – PNS атака. Если обнаружены посылки с числом фотонов $k < 3$, то посылка блокируется. Если в информационных состояниях обнаружено число фотонов $k \geq 3$, то проводятся UM измерения над информационным состоянием.

Необходимым и достаточным условием для существования UM измерений является линейная независимость состояний [31]. В протоколе BB84 при фазовом кодировании, если базис неизвестен, то необходимо различать 4-е состояния. В посылках с 3-мя фотонами 4-е состояния имеют вид:

$$|\Phi_k^x\rangle = \sqrt{\frac{3!}{2^3}} \sum_{m=0}^{3} e^{i\varphi_x m} \frac{|m\rangle_1 \otimes |k-m\rangle_2}{\sqrt{m!(k-m)!}}, \qquad (3)$$

т.е. 4-е состояния (3) становятся линейно независимыми, начиная с 3-х фотонных посылок.

Действительно, базисные векторы в фоковском подпространстве с 3-мя фотонами ($k = 3$) в двух временных окнах есть

$$|3\rangle_1|0\rangle_2, \quad |2\rangle_1|1\rangle_2, \quad |1\rangle_1|2\rangle_2, \quad |0\rangle_1|3\rangle_2.$$

Информационных состояний при $k = 3$ в двух базисах также имеется 3 вектора (см. ф-лу (3))

$$\text{basis} + \begin{cases} 0+ \to & \frac{1}{\sqrt{3!}}|3\rangle_1|0\rangle_2 + \frac{1}{\sqrt{2!}}|2\rangle_1|1\rangle_2 + \frac{1}{\sqrt{2!}}|1\rangle_1|2\rangle_2 + \frac{1}{\sqrt{3!}}|0\rangle_1|3\rangle_2 \\ \\ 1+ \to & \frac{1}{\sqrt{3!}}|3\rangle_1|0\rangle_2 + \frac{1}{\sqrt{2!}}|2\rangle_1|1\rangle_2 - \frac{1}{\sqrt{2!}}|1\rangle_1|2\rangle_2 - \frac{1}{\sqrt{3!}}|0\rangle_1|3\rangle_2 \end{cases},$$

$$\text{basis} \times \begin{cases} 0\times \to & \frac{1}{\sqrt{3!}}|3\rangle_1|0\rangle_2 + \frac{i}{\sqrt{2!}}|2\rangle_1|1\rangle_2 - \frac{1}{\sqrt{2!}}|1\rangle_1|2\rangle_2 - \frac{i}{\sqrt{3!}}|0\rangle_1|3\rangle_2 \\ \\ 1\times \to & \frac{1}{\sqrt{3!}}|3\rangle_1|0\rangle_2 - \frac{i}{\sqrt{2!}}|2\rangle_1|1\rangle_2 - \frac{1}{\sqrt{2!}}|1\rangle_1|2\rangle_2 + \frac{i}{\sqrt{3!}}|0\rangle_1|3\rangle_2 \end{cases}.$$

Для однофотонной компоненты состояний фоковское подпространство является двумерным, информационных состояний по-прежнему 4-е, поэтому они линейно зависимы. Размерность подпространства с 2-мя фотонами равна 3, состояний 4-е, и они линейно зависимы. По этой причине измерения с определенным исходом над информационными состояниями возможны только, начиная с трехфотонной компоненты состояний.

Вероятность $\Pr_\xi(k \geq 3)$, $\xi = \mu, \nu_1, \nu_2$ присутствия в квантовом канале посылок с тремя и более фотонами зависит от интенсивности информационного когерентного состояния – среднего числа фотонов в нем μ, ν_1, ν_2, имеем

$$\Pr_\xi(k \geq 3) = e^{-2\xi} \sum_{k=3}^{\infty} \frac{(2\xi)^k}{k!} \leq (\xi)^3. \qquad (4)$$

Для того, чтобы знать передваемый бит ключа, Ева должна иметь посылки с числом фотонов $k \geq 3$ для посылок с любой интенсивностью, поэтому вероятность успеха определяется минимальной вероятностью обнаружить три и более фотонов в посылках с разным средним числом фотонов $\xi = \mu, \nu_1, \nu_2$. Для минимальной вероятности, учитывая иерархию интенсивностей $\mu > \nu_1 > \nu_2$, находим

$$\Pr_{\min}(k \geq 3) = \min_{\xi=(\mu,\nu_1,\nu_2)} \left\{ e^{-2\xi} \sum_{k=3}^{\infty} \frac{(2\xi)^k}{k!} \right\} \leq (\nu_2)^3. \qquad (5)$$

После проведения UM измерений над 3-х фотонными состояниями Ева знает передаваемый бит. Если исход UM измерений над информационными состояниями неопределенный, то посылка блокируется.

PNS атака с последующими UM измерениями информационных состояний и отбрасыванием неопределенных исходов, без знания к какой посылке и с каким средним числом фотонов относится трехфотонное состояние, приведет к искажению статистики фотоотсчетов в посылках с разным средним числом фотонов μ, ν_1, ν_2, что будет обнаружено Decoy State методом.

Однако у Евы в распоряжении имеются отраженные от модулятора интенсивности состояния. UM измерение данных состояний, при определенном исходе после PNS атаки и UM измерений над информационными состояниями, позволяют Еве, при определенном исходе над отраженными состояниями, знать как

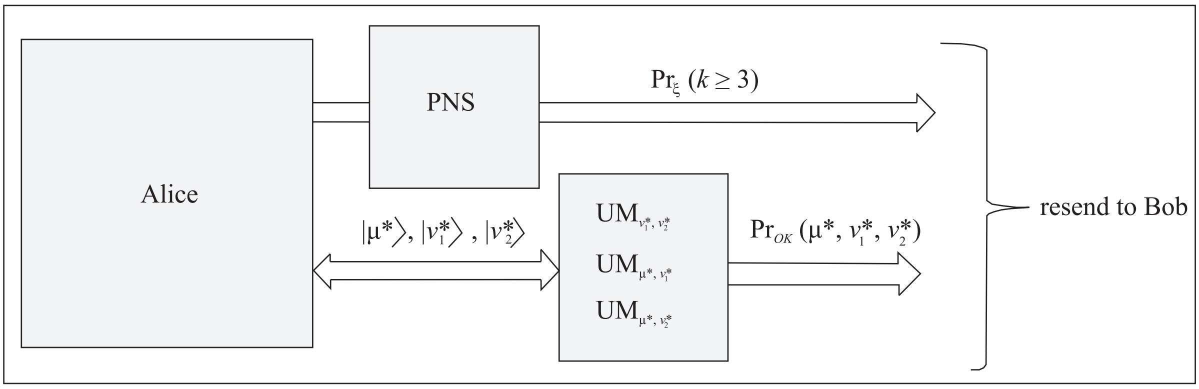

Рис. 1. Схематическое изображение атаки с UM измерениями отраженных состояний и PNS измерениями информационных состояний

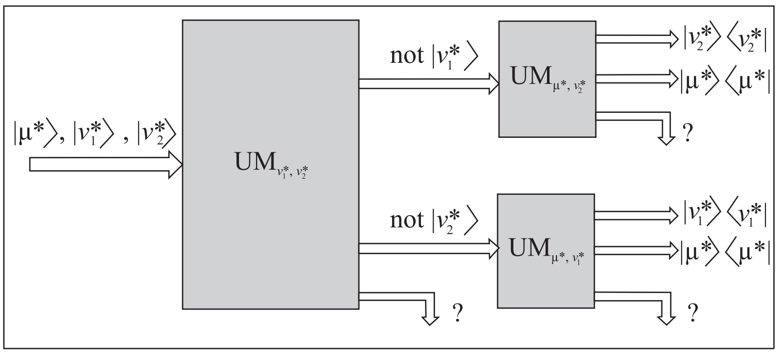

Рис. 2. Схематическое изображение второго каскада измерений с определенным исходом

информационный бит, так и значение интенсивности в данной посылке – μ, ν_1, ν_2.

В итоге, при двух последовательных определенных исходах Ева знает все о передаваемых состояниях – значение бита ключа и значение μ, ν_1, ν_2. Все остальные посылки, где был неопределенный исход, либо при PNS и UM измерениях над информационными состояниями, либо над отраженными от модулятора интенсивности, блокируются.

Сделаем теперь оценку минимальной вероятности определенного исхода при различении состояний, отраженных от модулятора интенсивности. Оптимальные UM измерения для двух чистых состояний известны [29–31]. Имеется ряд результатов для различения более чем двух чистых и смешанных состояний. Для получения конкретных числовых значений требуется знать точную структуру квантовых состояний и использовать численную минимизацию.

Для оценки порядка величины вероятности определенных исходов, соответственно, потерь, к которым приводит данная атака, удобнее воспользоваться точными аналитическими результатами для различения двух состояний, а для различения трех состояний воспользоваться каскадными измерениями с определенным исходом, где на каждом шаге различается пара состояний (см. рис. 1). При этом не придется прибегать к численной минимизации.

2.3. Каскадные измерения зондирующих состояний. При различении трех состояний, отраженных от модулятора интенсивности, которые для краткости обозначим $|\mu^*\rangle$, $|\nu_1^*\rangle$, $|\nu_2^*\rangle$, каскадные UM измерения содержат два шага. На первом шаге различается пара состояний $|\nu_1^*\rangle$, $|\nu_2^*\rangle$, точнее при одном из двух определенных исходов, исключается третье состояние. Например, исключение на первом шаге состояния $|\nu_1^*\rangle$ приводит к тому, что после такого исхода измерения остаются неразличенными состояния $|\mu^*\rangle$ и $|\nu_1^*\rangle$. При исключении на первом шаге состояния $|\nu_2^*\rangle$, определенными остаются состояния $|\mu^*\rangle$, и $|\nu_2^*\rangle$, которые различаются на втором шаге UM измерений (см. рис. 2). На втором шаге UM измерений различаются две данные пары состояний (рис. 2) $|\mu^*\rangle$ и $|\nu_1^*\rangle$, либо $|\mu^*\rangle$ и $|\nu_2^*\rangle$.

На первом шаге выполняется измерение $\mathrm{UM}_{\nu_1*,\nu_2^*}$ (рис. 2), которое дается разложением единицы

$$I = \mathcal{P}^{\perp}_{\nu_1^*} + \mathcal{P}^{\perp}_{\nu_2^*} + \mathcal{P}^{?}_{\nu_1^*,\nu_2^*}, \tag{6}$$

где

$$\mathcal{P}^{\perp}_{\nu_1^*} = \frac{I - |\nu_1^*\rangle\langle\nu_1^*|}{1 + |\langle\nu_1^*|\nu_2^*\rangle|}, \quad \mathcal{P}^{\perp}_{\nu_2^*} = \frac{I - |\nu_2^*\rangle\langle\nu_2^*|}{1 + |\langle\nu_1^*|\nu_2^*\rangle|}, \quad \mathcal{P}^{?}_{\nu_1^*,\nu_2^*} = I - \mathcal{P}^{\perp}_{\nu_1^*} - \mathcal{P}^{\perp}_{\nu_2^*}, \tag{7}$$

где I – единичный оператор. Операторно-значные меры в (6), (7) $\mathcal{P}^{\perp}_{\nu_1^*}$ и $\mathcal{P}^{\perp}_{\nu_2^*}$ с точностью до нормировки являются проекторами, в том смысле, что $(\mathcal{P}^{\perp}_{\nu_1^*,\nu_1^*})^2 \propto \mathcal{P}^{\perp}_{\nu_2^*,\nu_2^*}$, это потребуется далее.

Вероятности определенного исхода и состояния на выходе на первом каскаде имеют вид

$$\mathrm{UM}_{\nu_1^*,\nu_2^*}\left\{\begin{array}{l} \text{not } |\nu_1^*\rangle \to \left\{\begin{array}{ll} \Pr(|\nu_2^*\rangle|\text{not } |\nu_1^*\rangle) = 1 - |\langle\nu_2^*|\nu_1^*\rangle|, & \text{output state } |\nu_2^*\rangle\langle\nu_2| \\ \Pr(|\mu^*\rangle|\text{not } |\nu_1^*\rangle) = \frac{1-|\langle\mu^*|\nu_1^*\rangle|}{1+|\langle\nu_2^*|\nu_1^*\rangle|}, & \text{output state } |\mu^*\rangle\langle\mu^*| \end{array}\right\} \to \mathrm{UM}_{\mu^*,\nu_2^*} \\ \\ \text{not } |\nu_2^*\rangle \to \left\{\begin{array}{ll} \Pr(|\nu_1^*\rangle|\text{not } |\nu_2^*\rangle) = 1 - |\langle\nu_2^*|\nu_1^*\rangle|, & \text{output state } |\nu_1^*\rangle\langle\nu_1^*| \\ \Pr(|\mu^*\rangle|\text{not } |\nu_2^*\rangle) = \frac{1-|\langle\mu^*|\nu_2^*\rangle|}{1+|\langle\nu_2^*|\nu_1^*\rangle|}, & \text{output state } |\mu^*\rangle\langle\mu^*| \end{array}\right\} \to \mathrm{UM}_{\mu^*,\nu_1^*} \end{array}\right. . \tag{8}$$

Вероятность определенного исхода на первом шаге, с учетом (8), не более

$$\Pr^{(1)}_{OK} \le \min\left\{\Pr(|\mu^*\rangle|\text{not } |\nu_1^*\rangle), \Pr(|\nu_1^*\rangle|\text{not } |\nu_2^*\rangle), \Pr(|\nu_2^*\rangle|\text{not } |\nu_1^*\rangle)\right\}. \tag{9}$$

Второй каскад измерений с определенным исходом (рис. 2) выбирается в зависимости от исхода на первом шаге. Выбирается одно из двух измерений, каждое из которых дается своим разложением единицы. При исходе на первом шаге (not $|\nu_1^*\rangle$) на втором каскаде выбирается измерение $\mathrm{UM}_{\mu^*,\nu_2^*}$ (рис. 2)

$$I = \mathcal{P}^{\perp}_{\mu^*} + \mathcal{P}^{\perp}_{\nu_2^*} + \mathcal{P}^{?}_{\mu^*,\nu_2^*}, \tag{10}$$

где

$$\mathcal{P}^{\perp}_{\mu^*} = \frac{I - |\mu^*\rangle\langle\mu^*|}{1 + |\langle\mu^*|\nu_2^*\rangle|}, \quad \mathcal{P}^{\perp}_{\nu_2^*} = \frac{I - |\nu_2^*\rangle\langle\nu_2^*|}{1 + |\langle\mu^*|\nu_2^*\rangle|}, \quad \mathcal{P}^{?}_{\mu^*,\nu_2^*} = I - \mathcal{P}^{\perp}_{\mu^*} - \mathcal{P}^{\perp}_{\nu_2^*}, \tag{11}$$

$$\mathrm{UM}_{\mu^*,\nu_2^*}\left\{\begin{array}{lll} \text{not } |\mu^*\rangle \to & \Pr(|\nu_2^*\rangle|\text{not } |\mu^*\rangle) = 1 - |\langle\mu^*|\nu_2^*\rangle|, & \text{output state } |\nu_2^*\rangle\langle\nu_2^*| \\ \text{not } |\nu_2^*\rangle \to & \Pr(|\mu^*\rangle|\text{not } |\nu_2^*\rangle) = 1 - |\langle\mu^*|\nu_2^*\rangle|, & \text{output state } |\mu^*\rangle\langle\mu^*| \end{array}\right. . \tag{12}$$

При исходе на первом шаге (not $|\nu_2^*\rangle$) на втором каскаде выбирается измерение $\mathrm{UM}_{\mu*,\nu_1^*}$ (рис. 2)

$$I = \mathcal{P}^{\perp}_{\mu^*} + \mathcal{P}^{\perp}_{\nu_1^*} + \mathcal{P}^{?}_{\mu^*,\nu_1^*}, \tag{13}$$

где

$$\mathcal{P}^{\perp}_{\mu^*} = \frac{I - |\mu^*\rangle\langle\mu^*|}{1 + |\langle\mu^*|\nu_1^*\rangle|}, \quad \mathcal{P}^{\perp}_{\nu_1^*} = \frac{I - |\nu_1^*\rangle\langle\nu_1^*|}{1 + |\langle\mu^*|\nu_1^*\rangle|}, \quad \mathcal{P}^{?}_{\mu^*,\nu_1^*} = I - \mathcal{P}^{\perp}_{\mu^*} - \mathcal{P}^{\perp}_{\nu_1^*}, \tag{14}$$

$$\mathrm{UM}_{\mu^*,\nu_1^*}\left\{\begin{array}{lll} \text{not } |\mu^*\rangle \to & \Pr(|\nu_1^*\rangle|\text{not } |\mu^*\rangle) = 1 - |\langle\nu_1^*|\mu^*\rangle|, & \text{output state } |\nu_1^*\rangle\langle\nu_1^*| \\ \text{not } |\nu_1^*\rangle \to & \Pr(|\mu^*\rangle|\text{not } |\nu_1^*\rangle) = 1 - |\langle\nu_1^*|\mu^*\rangle|, & \text{output state } |\mu^*\rangle\langle\mu^*| \end{array}\right. . \tag{15}$$

Вероятность определенного исхода на втором шаге, с учетом (10)–(15), не более

$$\Pr^{(2)}_{OK} \le \min\left\{\Pr(|\mu^*\rangle|\text{not } |\nu_1^*\rangle), \Pr(|\nu_1^*\rangle|\text{not } |\mu^*\rangle), \Pr(|\mu^*\rangle|\text{not } |\nu_2^*\rangle), \Pr(|\nu_2^*\rangle|\text{not } |\mu^*\rangle)\right\}. \tag{16}$$

В итоге вероятность определенного исхода в двух каскадах при измерении отраженных состояний от модулятора интенсивности не более

$$\Pr_{OK}(\min) = \Pr^{(1)}_{OK} \cdot \Pr^{(2)}_{OK}. \tag{17}$$

Считая отраженные состояния когерентными различными фазами и средним числом фотонов $\xi, \xi' \ll \ll 1$, для скалярных произведений в (8), (12), (15) получаем $1 - |\langle\xi|\xi'\rangle|^2 = 1 - e^{-|\xi-\xi'|^2} \le |\xi - \xi'|$, где

ξ, ξ' принимают значения μ^*, ν_1^*, ν_2^*.[2)] Учитывая естественную иерархию интенсивностей отраженных состояний, т.е. считая, что $\mu^* > \nu_1^* > \nu_2^*$, для оценки получаем

$$\mathrm{Pr}_{OK}(\min) \le \mu^* \nu_1^* (\nu_2^*)^2. \quad (18)$$

2.4. Финальная стадия атаки – перепосыл состояний на приемную станцию. В посылках, где получены определенные исходы над отраженными состояниями и информационными состояниями в квантовом канале связи, Ева знает как информационный бит, так и с каким средним числом фотонов было состояние в данной посылке.

Все посылки с совместным определенным исходом разбиваются на три множества. Одно множество посылок, где посылались состояния со средним числом фотонов μ, второе множество посылок с ν_1 и третье с ν_2. Во всех этих посылках Еве также известен передаваемый бит ключа.

Как Ева может использовать данную атаку, чтобы не произвести ошибок на приемной стороне и не изменить относительную статистику фотоотсчетов в посылках с разным средним числом фотонов?

Нужно напомнить следующий факт, если когерентное состояние со средним числом фотонов ξ проходит через канал связи с коэффициентом прохождения T, соответственно с потерями $1-T$, то непосредственно на входе приемной стороны будут состояния

$$\rho^x(\xi) \to \rho^x(\xi T) = e^{-2\xi T} \sum_{k=0}^{\infty} \frac{(2\xi T)^k}{k!} |\Phi_k^x\rangle\langle\Phi_k^x|, \quad (19)$$

здесь T – коэффициент прохождения через канал связи ($T = 10^{-\frac{\delta L}{10}}$, L – длина линии связи, δ – коэффициент удельных потерь). Соответственно, вероятность компонент состояний с ненулевым числом фотонов *на входе станции Боба* есть

$$Q(\xi T) = e^{-2\xi T} \sum_{k=1}^{\infty} \frac{(2\xi T)^k}{k!} = 1 - e^{-2\xi T}. \quad (20)$$

Иначе говоря, формула (20) дает вероятность достижения входа приемной стороны Боба каждой компонентой $|\Phi_k^x\rangle\langle\Phi_k^x|$ с числом фотонов k без искажений после прохождения канала с потерями. Вероятность достижения приемной стороны компоненты состояния $|\Phi_k^x\rangle\langle\Phi_k^x|$ с $k = 0, 1 \ldots$ фотонами есть

$$e^{-2\xi T} \frac{(2\xi T)^k}{k!}. \quad (21)$$

[2)] Не путать обозначения когерентных состояний $|\xi\rangle$ со средним значением числа фотонов ξ.

Пусть T_μ, T_{ν_1}, T_{ν_2} – прозрачности канала, при которых выполнены равенства

$$\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_\mu(k \ge 3) = Q(\mu T_\mu) \approx 2\mu T, \quad (22)$$

$$\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_{\nu_1}(k \ge 3) = Q(\nu_1 T_{\nu_1}) \approx 2\nu_1 T, \quad (23)$$

$$\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_{\nu_2}(k \ge 3) = Q(\nu_2 T_{\nu_2}) \approx 2\nu_2 T. \quad (24)$$

Фомулы дают вероятность совместного определенного исхода для различения состояния и с каким средним числом фотонов произошла данная посылка и вероятности определения передаваемого бита ключа. Неформально, это доля посылок со средним числом фотонов при разных $\xi = \mu, \nu_1, \nu_2$, в которых Ева знает все про данные посылки.

Далее выберем минимальный коэффициент прохождения из T_ξ в (22)–(24)

$$T_{\min} = \min_{\xi \in \{\mu, \nu_1, \nu_2\}} \{T_\xi\} =$$
$$= \min_{\xi \in \{\mu, \nu_1, \nu_2\}} \left\{ \frac{1}{\xi} Q^{-1} \left(\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_\xi(k \ge 3) \right) \right\}, \quad (25)$$

здесь $Q^{-1}(\ldots)$ – обратная функция к $Q(\ldots)$.

Пусть для определенности это будет $\xi = \nu_2$, тогда

$$\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_\mu(k \ge 3) \ge Q(\mu T_{\min}), \quad (26)$$
$$\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_{\nu_1}(k \ge 3) \ge Q(\nu_1 T_{\min}),$$
$$\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_{\nu_2}(k \ge 3) = Q(\nu_2 T_{\min}).$$

Неформально (26) определяет размеры множеств посылок с μ, ν_1 и ν_2, в которых Ева знает все – среднее число фотонов и передаваемый бит ключа.

Если $\xi = \mu$, то в доле посылок

$$\frac{Q(\mu T_{\min})}{\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_\mu(k \ge 3)}, \quad (27)$$

с совместным определенным исходом Ева *подает непосредственно на вход станции Боба* (см. рис. 1), состояния

$$|\Phi_k^x\rangle_{BB}\langle\Phi_k^x| \quad (28)$$

с нужными вероятностями

$$e^{-2\mu T_{\min}} \frac{(2\mu T_{\min})^k}{k!}, \quad k \ge 1. \quad (29)$$

А в доле посылок

$$1 - \frac{Q(\mu T_{\min})}{\mathrm{Pr}_{OK}(\min) \cdot \mathrm{P}_\mu(k \ge 3)} \quad (30)$$

ничего не передает Бобу (см. рис. 1), даже если получен совместный определенный исход. Говоря другими словами, часть посылок с совместным определенным исходом в (22) и (23) является избыточной.

Размер множества посылок с совместным определенным исходом для посылок с μ больше, чем требуется для удовлетворения неравенств (26).

Аналогично Ева поступает для посылок с ν_1, где получен совместный определенный исход. В посылках с ν_2 на вход приемной станции Ева доставляет все посылки с совместным определенным исходом.

В итоге, *на входе станции Боба* при любом $\xi = \mu, \nu_1, \nu_2$ возникают состояния, которые даются матрицами плотности

$$\rho^x(\xi T_{\min}) = e^{-2\xi T_{\min}} \sum_{k=0}^{\infty} \frac{(2\xi T_{\min})^k}{k!} |\Phi_k^x\rangle_{BB}\langle\Phi_k^x|, \\ \xi = \mu, \nu_1, \nu_2. \quad (31)$$

Состояния на входе приемной станции выглядят так, как, если бы неискаженные состояния прошли через канал с прозрачностью $T_{\min}$. При этом относительная и внутренняя пуассоновская статистика состояний по числу фотонов и сами фоковские состояния остаются неискаженными, и все состояния выглядят как, если бы они прошли через один и тот же идеальный канал с потерями $1 - T_{\min}$. В итоге на входе приемной станции Боб видит неискаженные состояния с неискаженной внутренней и относительной пуассоновской статистикой для состояний с разными ξ. Напомним, что Decoy State метод не следит за потерями, поэтому такая атака не детектируется Decoy State методом.

2.5. Некоторые численные оценки. Сделаем численные оценки потерь, к которым приводит данная атака. Наблюдаемые потери зависят от среднего числа фотонов в отраженных зондирующих состояниях от модулятора интенсивности. Пусть среднее число фотонов в отраженных состояниях, когда состояние модулятора интенсивности отвечает посылкам информационных состояний со средним числом фотонов μ равно $\mu^* = 0.1$. Соответственно для информационных посылок с ν_1 и ν_2 есть $\nu_1^* = 0.01$, $\nu_2^* = 0.01$. С учетом полученных выше формул (24), (27), для коэффициента прохождения T_{Eve} (коэффициент потерь $1 - T_{Eve}$) при такой атаке, получаем

$$\mathrm{Pr}_{OK}(\min) \cdot \mathrm{Pr}_{\min}(k \geq 3) \leq \nu_2 T_{\mathrm{Eve}}, \\ T_{\mathrm{Eve}} \leq \mu^* \nu_1^* \nu_2^* \approx 10^{-5}. \quad (32)$$

Напомним, что при стандартных потерях в одномодовом волокне $\delta = 0.2$ Дб/км, при длине линии $L = 100$ км, вероятность прохождения линии связи составляет $T_{100} = 10^{-\frac{\delta L}{10}} = 10^{-2}$, что на три порядка больше, чем при такой атаке и используемой для оценок интенсивности отраженных зондирующих состояний. Чем меньше интенсивность отраженных состояний, тем больше будут вносимые потери при такой атаке. Обеспечить низкую интенсивность отраженных зондирующих состояний можно использованием односторонних оптических изоляторов на выходе из передающей станции. Коэффициент ослабления оптических изоляторов будет определяться конкретной технической реализацией системы квантовой криптографии.

3. Заключение. Системы квантовой криптографии были предложены для квантового распределения ключей, секретность которых гарантируется фундаментальными запретами квантовой механики на различимость квантовых состояний. Более точно, запрет на копирование неизвестного квантового состояния (*no cloning* теорема [37]) запрещает создать копию неизвестного квантового состояния *с вероятностью единица*, что является элегантной переформулировкой фундаментальных соотношений неопределенностей Гайзенберга–Робертсона [38, 39]. Применительно к квантовой криптографии, этот запрет означает, что подслушиватель не может сделать копию информационного состояния (соответственно, любое число копий, если можно было бы сделать хоть одну) для своих измерений при подслушивании. Соотношения неопределенностей Гайзенберга–Робертсона есть выражение математического факта, что пара некоммутирующих наблюдаемых (эрмитовых операторов) не может иметь общей системы собственных векторов, поэтому любые вторжения в квантовый канал связи неизбежно будут приводить к ошибкам на приемной стороне.

Следующий фундаментальный факт состоит в том, что квантовая теория позволяет получить верхнюю фундаментальную границу утечки информации к подслушивателю при данной наблюдаемой ошибке на приемной стороне. Данную фундаментальную границу позволяют получить энтропийные соотношения неопределенностей [11], которые также являются следствием некоммутируемости наблюдаемых.

Все сказанное касалось однофотонных состояний. В реальных системах, ввиду отсутствия на данный момент строго однофотонного источника информационных состояний, используются квазиоднофотонные состояния лазерного излучения – сильно ослабленное когерентное состояние, которое является суперпозицией состояний с разным фоковским числом фотонов. Секретный ключ формируется только из однофотонной компоненты состояний, достигающей приемной стороны. Вся информация, содержащаяся в многофотонных компонентах состояний, считается известной подслушивателю (“отдается” подслушивателю). Decoy State метод [21–23] позволяет оценить долю однофотонной компоненты, достигающей приемной стороны.

Таким образом, относительно атак на информационные состояния в квантовом канале связи на сегодняшний день достигнуто глубокое понимание. Однако системы квантовой криптографии являются открытыми системами, в том смысле, что подслушиватель имеет в своем распоряжении, кроме квантового канала, побочные каналы утечки информации, а также может активно зондировать оптические компоненты системы – фазовые модуляторы, модуляторы интенсивности, состояние которых несет на себе информацию о передаваемом ключе. Измерение подслушивателем зондирующих состояний не приводит к ошибкам на приемной стороне, поскольку не возмущает информационных состояний, и является дополнительным информационным "бонусом" для подслушивателя.

Без учета утечки информации по побочным каналам невозможно всерьез говорить о секретности ключей в квантовой криптографии.

В данной работе предложена новая атака на системы квантовой криптографии с использованием совместной атаки на информационные квантовые состояния (PNS атака) и атаки с измерениями с определенным исходом (UM измерения) отраженных состояний от модулятора интенсивности в побочном канале. Данная атака не детектируется известными методами, поскольку не изменяет относительной статистики фотоотсчетов в Decoy State методе, но приводит только к дополнительным потерям в квантовом канале связи, которые Decoy State метод не регистрирует. Более того, считалось до сегодняшнего дня, что за потерями в линии связи следить не нужно, поскольку напрямую они не влияют на секретность, если используется Decoy State метод.

Приведенное выше рассмотрение показывает, что учет утечки информации по побочным каналам требует учета потерь в квантовом канале связи при получении оценок для длины секретного ключа. Наши оценки дают уровень потерь при известной максимальной интенсивности отраженных зондирующих состояний, при которых подслушиватель знает весь ключ и не производит ошибок на приемной стороне, и не детектируется, если не следить за общими потерями в линии. При уровне потерь меньше критического, подслушиватель неизбежно будет производить либо ошибки, либо изменение относительной статистики фотоотсчетов на приемной стороне.

Еще раз подчеркнем, что критический уровень потерь зависит от конкретной физической реализации системы квантовой криптографии, которая определяет верхнюю границу интенсивности отраженных зондирующих состояний. Знание данной границы принципиально необходимо для обеспечения секретности ключей. Например, если система должна гарантировать секретность ключей при длине линии 100 км (коэффициент прохождения $T = 10^{-2}$), а ее физическая реализация такова, что интенсивность отраженных состояний приводит к критическим потерям при описанной выше атаке, того же порядка (коэффициент прохождения линии того порядка $T_{\mathrm{Eve}} = 10^{-2}$) или больше, то система будет неспособна гарантировать секретность распределяемых ключей – подслушиватель не будет детектироваться.

Детектирование атаки обеспечивается не средствами протокола квантового распределения ключей, а физической реализацией системы, которая должна "приводить" к тому, что подслушиватель при данной атаке будет производить уровень потерь, заметно превышающий уровень потерь при длине линии, при которой должна работать система.

В заключение, во избежание недоразумений отметим. Не нужно думать, что учет побочных каналов утечки информации переводит системы квантовой криптографии из разряда криптографических систем, где секретность ключей гарантируется фундаментальными законами квантовой механики, в разряд систем, где секретность гарантируется техническими ограничениями. Даже при наличии побочных каналов утечки информации секретность ключей по-прежнему гарантируется фундаментальными ограничениями квантовой механики на различимость состояний.

Интенсивность (среднее число фотонов) в информационных состояниях – квазиоднофотонных, в идеале однофотонных, выходящих из передающей станции, также достигается техническими средствами – ослаблением до нужного уровня исходного сигнала. При заданном уровне сигналов их максимально допустимая – наилучшая возможная различимость диктуется квантовой механикой. Точно также и для состояний в побочных каналах. Верхняя граница интенсивности состояний в побочных каналах достигается техническими средствами – реализацией системы, которая дает верхний предел различимости состояний, который также диктуется фундаментальными запретами квантовой механики.

Выражаю благодарность И. М. Арбекову, К. А. Балыгину, С. П. Кулику, А. Н. Климову за интересные и многочисленные обсуждения, а также коллегам по Академии криптографии Российской Федерации за обсуждения и поддержку.

Работа выполнена при поддержке проекта Российского научного фонда # 16-12-00015 (продолжение).

1. A.O. Bauer, *Some aspects of military line communications as deployed by the German armed forces prior to 1945. The History of Military Communications, Proceedings of the Fifth Annual Colloquium, Centre for the History of Defence Electronics*, Bournemouth University, 24 September (1999).
2. *Electromagnetic Pulse (EMP) and Tempest Protection for Facilities*, Engineer Pamphlet EP 1110-3-2, U.S. Army Corps of Engineers, Publications Depot, Hyattsville, December 31 (1990).
3. W. van Eck, Computers & Security **4**, 269 (1985).
4. P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*, in *Advances in Cryptology – CRYPTO'99, LNCS 1666*, ed. by M. Wiener, Springer, 388 (1999).
5. P. Wright, *Spycatcher – The Candid Autobiography of a Senior Intelligence Officer*, William Heinemann Australia (1987).
6. P. Smulders, Computers & Security **9**, 53 (1990).
7. M.G. Kuhn, Technical Report, Cambridge University, UCAM-CL-TR-577, **577** (2003).
8. C.H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Comp. Sys. and Sign. Process. (IEEE, 1984)*, p. 175.
9. R. Renner, *Security of Quantum Key Distribution*, PhD thesis, ETH Zürich, (2005); arXiv:0512258.
10. J.M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).
11. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
12. M. Lucamarini, I. Choi, M.B. Ward, J.F. Dynes, Z.L. Yuan, and A.J. Shields, Phys. Rev. X **5**, 031030 (2015); arXiv:1506.01989.
13. K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).
14. W. Wang, K. Tamaki, and M. Curty, New J. Phys. **20**, 083027 (2018).
15. S.N. Molotkov, Laser Phys. Lett. **17**, 015203 (2020).
16. S.N. Molotkov, K.A. Balygin, A.N. Klimov, and S.P. Kulik, Laser Phys. **29**, 124001 (2019).
17. S.N. Molotkov and K.A. Balygin, Laser Phys. **30**, 065201 (2020).
18. С.Н. Молотков, ЖЭТФ **157**, 963, (2020).
19. С.Н. Молотков, Письма в ЖЭТФ **111**, 778 (2020).
20. С.Н. Молотков, Письма в ЖЭТФ **111**, 608 (2020).
21. W.-Y. Hwang, arXiv[quant-ph]: 0211153.
22. X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
23. H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, arXiv[quant-ph]: 0503005.
24. С.Н. Молотков, ЖЭТФ **153** 895 (2018).
25. S.N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).
26. A. Chefles, Phys. Lett. A **239**, 339 (1998).
27. I.D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
28. D. Dieks, Phys. Lett. A **126**, 303 (1988).
29. G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
30. A. Peres and D.R. Terno, J. Phys. A **31**, 7105 (1998).
31. U. Herzog, Phys. Rev. A **75**, 052309 (2007).
32. T. Rudolph, R.W. Spekkens, and P.S. Turner, Phys. Rev. A **68**, 010301 (2003).
33. P. Raynal and N. Lütkenhaus, Phys. Rev. A **72**, 022342 (2005).
34. S.W. Allison, G.T. Gillies, D.W. Magnuson, and T.S. Pagano, Appl. Opt. **24**, 1 (1985).
35. L.W. Tutt and T.F. Boggess, Progress in Quantum Electronics **17**, 299 (1993).
36. R.M. Wood, *Laser-induced damage of optical materials*, Taylor & Francis (2003).
37. W.K. Wooters and W.H. Zurek, Nature **299**, 802 (1982).
38. W. Heisenberg, Z. Phys. **43**, 172 (1927).
39. H.P. Robertson, Phys. Rev. **34**, 163 (1929).