

# КОММЕНТАРИЙ К СТАТЬЕ «ДОСТАТОЧНО ЛИ СОСТОЯНИЙ ЛОВУШЕК (DECOY STATE-МЕТОДА) ДЛЯ ГАРАНТИИ СЕКРЕТНОСТИ КЛЮЧЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ?»

## С. Н. МОЛОТКОВА, К. С. КРАВЦОВА, М. И. РЫЖКИНА И К ПОПРАВКЕ К ЭТОЙ СТАТЬЕ

*Д. А. Кронберг<sup>a,b,c\*</sup>, Е. О. Киктенко<sup>a,b,d</sup>, А. С. Трушечкин<sup>a,b,d</sup>, А. К. Федоров<sup>d</sup>*

<sup>a</sup> *Математический институт им. В. А. Стеклова Российской академии наук  
119991, Москва, Россия*

<sup>b</sup> *Российский квантовый центр  
143025, д. Сколково, Москва, Россия*

<sup>c</sup> *Московский физико-технический институт (Национальный исследовательский университет)  
141701, Долгопрудный, Московская обл., Россия*

<sup>d</sup> *Кафедра математики и Центр квантовых коммуникаций НТИ,  
Национальный исследовательский технологический университет «МИСиС»  
119049, Москва, Россия*

Поступила в редакцию 25 мая 2021 г.,  
после переработки 20 ноября 2021 г.  
Принята к публикации 21 ноября 2021 г.

В статье [1] утверждается, что метод обманных состояний (“decoy state method”, другой перевод на русский язык — «метод состояний-ловушек») в протоколе квантовой криптографии BB84 завышает достижимую скорость генерации секретного ключа и потому генерируемый ключ фактически не является секретным. Это утверждение является результатом ошибки, которую авторы статьи признали в поправке [2], однако там также были допущены неверные утверждения. Таким образом, неправильные утверждения в работах [1, 2] привели к неверным выводам.

DOI: 10.31857/S0044451022050017

### 1. ВВЕДЕНИЕ

Основной результат статьи [1] выражается в неравенстве (30) и графиках на рис. 2, в которых сравниваются достижимые длины (эквивалентно — достижимые скорости генерации) секретного ключа, рассчитанные для атаки расщеплением по числу фотонов (обычно рассматриваемой в методе обманных состояний) и для альтернативной атаки светоделителем. На основании этого неравенства и этих графиков утверждается, что первая величина больше второй, т. е. метод обманных состояний в настоящем виде завышает достижимую скорость генерации секретного ключа. Однако в неравенстве (30)

скорость генерации секретного ключа, рассчитанная для атаки расщеплением по числу фотонов, вычислена неверно: перед  $1 - h(e_1)$  должен присутствовать множитель  $Q_1(\mu)/Q(\mu)$  — ср. с формулой (9), которая записана правильно. Авторы признали это в поправке к статье [2], но допустили ряд новых неверных утверждений, итогом чего явился вывод о неполноте доказательства стойкости для метода обманных состояний.

### 2. ВОПРОС ЗАВИСИМОСТИ МЕТОДА ОБМАННЫХ СОСТОЯНИЙ ОТ МОДЕЛЬНЫХ ПРЕДПОЛОЖЕНИЙ

Как в работе [1], так и в поправке [2] утверждается, что в методе обманных состояний используются модельные предположения о параметрах канала и

\* E-mail: dmitry.kronberg@gmail.com

детекторов. Так, в частности, в статье-поправке [2] говорится: «... Оценка информации подслушивателя, в отличие от Decoy state-оценок, не содержит никаких модельных предположений о параметрах канала и детекторов (квантовой эффективности  $\eta$ , вероятности  $p_d$  темновых шумов)». В статье [3] говорится о том же: «Протокол Decoy State явно использует предположения о свойствах лавинных однофотонных детекторов, так как в протоколе требуется отличать состояния ослабленного лазерного излучения с разным средним числом фотонов, что неприемлемо, поскольку свойства детектора, например, квантовая эффективность, могут флуктуировать в процессе регистрации квантовых состояний, т. е. в формулу для длины секретного ключа напрямую входят квантовая эффективность однофотонных детекторов, что неприемлемо, поскольку квантовая эффективность флуктурует со временем». Однако на самом деле в методе обманных состояний легитимные пользователи не опираются на знание этих характеристик, а оценивают их исходя из наблюдаемых параметров.

Метод обманных состояний используется для оценки величин  $Y_k$ . В статье [4] (в которой излагается метод обманных состояний и на которую ссылаются и авторы статьи [1])  $Y_k$  определяется как условная вероятность того, что на приемной стороне сработает один из детекторов, при условии, что на стороне отправителя посылка содержала  $k$  фотонов. В разд. 4 статьи [1] дается вместо этого другое определение: «Пусть  $Y_k$  — условная вероятность того, что подслушиватель оставит данное среднее число фотонов  $k$  в посылке, которое будет доставлено на приемную сторону для детектирования, возможно через идеальный без потерь канал связи». Но, как видно из определения работы [4], величина  $Y_k$  на самом деле учитывает не только действия перехватчика, но и характеристики оборудования легитимных пользователей: показатель затухания в оптоволоконной линии связи, неполную эффективность детекторов, показатель темновых шумов и т. д. — все эти эффекты учитываются в оценке  $Y_k$ . Никакие модельные предположения при этом не используются ввиду общности определения  $Y_k$ .

Также заметим, что в статье [1] индекс  $k$  в величине  $Y_k$  интерпретируется как количество фотонов, оставляемое подслушивателем, а не как количество фотонов в посылке отправителя. Помимо этого, при определении величин  $Q_k(\mu)$ , характеризующих совместную вероятность отправки  $k$  фотонов и срабатывания детектора на приемной стороне, в правой части формулы (7), в которой введены эти вели-

чины, не должно быть экспонент, стоящих перед знаком суммы, так как они должны входить в величины  $Q_k(\mu)$  и  $Q_k(\nu_i)$ , соответственно. В принципе, определения могут отличаться от соответствующих определений в основных работах по методу обманных состояний, однако это должно приводить к другому выражению для длины секретного ключа (9) в [1].

После формулы (13) статьи [1] авторы пишут: «Если лавинный детектор на приемной стороне имеет не единичную квантовую эффективность, то в этом случае в формулах (7), (8), (10)–(13) нужно провести замену  $\mu \rightarrow \eta\mu$ ». Аналогично далее в разд. 6 говорится, что эти интенсивности надо умножить на коэффициент прохождения канала связи  $T(L)$ . Однако в величине

$$Q_k(\mu) = e^{-\mu} \frac{\mu^k}{k!} Y_k \quad (1)$$

интенсивность  $\mu$  участвует только в качестве вероятности испускания  $k$  фотонов на передающей стороне, и она не зависит от затухания в линии связи, поэтому в этом выражении никакие члены не следует умножать на  $\eta T(L)$ . Все потери в канале связи и детекторах, а также действия перехватчика, включены в параметр  $Y_k$ , который зависит от числа фотонов  $k$ , но не зависит от интенсивности  $\mu$ . Выражения для  $Y_k$  в условиях отсутствия перехвата действительно будут содержать показатель затухания канала:

$$Y_k \approx p_d + \eta_k = p_d + 1 - (1 - \eta T(L))^k. \quad (2)$$

Здесь мы сначала следуем обозначениям [4] (формулы (5)–(7)), где  $\eta_k$  — вероятность доставки и детектирования состояния с  $k$  фотонами, а затем переходим к обозначениям [1] и выражаем  $\eta_k$  через показатель затухания  $T(L)$  и эффективность детекторов  $\eta$ . Как видно, только  $Y_k$  зависят от затухания в линии связи и показателей оборудования. Скорость генерации секретного ключа (выражение (9) в работе [1]) включает величины  $Y_1$  и  $e_1$ , которые и оцениваются в методе обманных состояний.

Формулы (29) в статье [1] должны записываться следующим образом:

$$Y_1 \approx p_d + \eta T(L), \quad (3)$$

$$e_1 = \frac{p_d}{2Y_1}. \quad (4)$$

Смысл формулы (3) состоит в том, что один из детекторов приемной стороны срабатывает, либо если произошло темновое срабатывание, либо фотон

не поглотился в канале связи или детекторе и привел к срабатыванию детектора. Вероятность темнового срабатывания —  $p_d$ , вероятность непоглощения фотона —  $\eta T(L)$ ,  $T(L) = 10^{-\delta L/10}$  — коэффициент прохождения в линии связи длины  $L$ ,  $\delta$  — удельный коэффициент потерь. Совместная вероятность этих двух событий пренебрежимо мала. Как и в [1], мы предполагаем, что ошибки возникают только из-за темнового шума, а оптическая схема приемной стороны настроена идеально.

Доля ошибок в позициях, полученных из однофотонных посылок, равна отношению вероятности ошибочного приема однофотонной посылки  $p_d/2$  к общей вероятности приема однофотонной посылки  $Y_1$ . То, что вторая формула в (29) неверна, можно понять и по тому, что если  $p_d > 2\eta$ , то доля ошибок получается больше единицы, а величина  $h(e_1)$  не определена вовсе, поскольку содержит член  $\log(1 - e_1)$ . Напротив, правая часть (4) не может быть больше  $1/2$ , как видно из (3). Отметим, что условие  $p_d > 2\eta$  вряд ли может выполняться на практике, но формально ничему не противоречит. К тому же, перед формулой (29) авторы пишут: «При малых  $\eta_{1,2} \rightarrow 0$  получаем».

Отметим, что первая формула в (29) дублирует формулу (7) из работы [4], однако в статье [1] под  $\eta$  подразумевается эффективность детектора на приемной стороне, а потери в линии связи и детекторах равны  $\eta T(L)$ , тогда как в [4] через  $\eta$  описываются общие потери в детекторах и линии связи, что можно видеть в формулах (5) и (6) в [4].

### 3. НЕКОРРЕКТНОЕ ИСПОЛЬЗОВАНИЕ ВЕЛИЧИНЫ ХОЛЕВО

Во Введении к основной статье [1] говорится: «В данной работе построен явный пример простой атаки со светоделителем, при которой длина секретного ключа получается принципиально меньше, чем по Decoy state-методу», при этом в статье-поправке [2] уже не предлагается конструктивных примеров атаки, однако повторяются утверждения о недоказанной стойкости метода обманных состояний.

В статье-поправке [2] было отмечено, что в основной формуле (30) исходной статьи [1] пропущен ключевой множитель. Однако этот множитель ошибочно указан как  $e^{-\mu}$  (где  $\mu$  — среднее число фотонов в информационных посылках). На самом деле это множитель  $Q_1(\mu)/Q(\mu)$ , который соответствует доле испущенных однофотонных посылок среди зарегистрированных на приемной стороне, в то время как множитель  $e^{-\mu}$  есть доля вакуумных посылок среди информационных посылок.

Далее в статье-поправке в качестве оценки информации противника используется величина Холево исходного ансамбля состояний. Эта оценка названа консервативной. Однако в общем случае эта величина не является ни консервативной, ни достижимой оценкой информации противника о ключе. Разберем оба этих утверждения.

В статье-поправке [2] справедливо утверждает про величину Холево: «Данная граница включает в себя информацию от всех компонент состояния: однофотонных, двухфотонных и т. д.». Таким образом, авторы признают, что эта оценка для противника достижима, только когда он забирает себе, в частности, все однофотонные посылки. Но в этом случае однофотонные посылки уже не дойдут до приемной стороны, и метод обманных состояний даст строго нулевую длину ключа, поэтому в статье-поправке авторы некорректно сравнивают длины ключей. Применение оценки на основе величины Холево игнорирует основной результат квантовой криптографии: доказательство стойкости протокола BB84 в однофотонном случае, так как в этой оценке полагается, что противник получает всю информацию о ключе из однофотонных посылок, но при этом эти посылки доходят до приемной стороны без превышения критической доли ошибок. В частности, величина Холево выходного ансамбля состояний в протоколе BB84 со строго однофотонным источником равна единице (т. е. максимально возможному значению), но, тем не менее, протокол, как хорошо известно, является стойким. Таким образом, величина Холево в общем случае не является достижимой для противника.

Также эта величина не является в общем случае и консервативной оценкой, т. е. оценкой сверху информации противника о ключе. А именно, информация противника об одном бите сырого ключа может быть и больше величины Холево исходного ансамбля вследствие постселекции, что не учитывается авторами. В качестве примера допустим, что легитимные стороны используют источник с пуассоновской статистикой числа фотонов и не применяют метод обманных состояний. Тогда, если противник проводит атаку расщеплением по числу фотонов с блокировкой однофотонных посылок, он получает полную информацию о ключе. Таким образом, его информация превосходит величину Холево исходного ансамбля состояний (которая с учетом вакуумных посылок равна  $1 - e^{-\mu}$ , т. е. меньше единицы). Постселекция заключается в данном случае в отбрасывании тех позиций, в которых приемная сторона не зарегистрировала фотон. Следовательно, ис-

пользование величины Холево исходного ансамбля для оценки информации противника относительно ансамбля после постселекции некорректно.

#### 4. ЗАКЛЮЧЕНИЕ

Подробное описание метода обманных состояний можно найти, например, в работах [4, 5]. Важно лишь в очередной раз отметить, что уязвимости в рамках стандартной используемой модели в методе обманных состояний отсутствуют.

Таким образом, в данном Комментарии показано, что результаты статьи [1] основаны на неверном понимании метода обманных состояний, а именно, утверждении, что метод зависит от модельных предположений о канале связи и детекторах, а также на неверном учете затухания.

В статье-поправке [2] некорректно используется величина Холево для оценки информации противника, что приводит к неверному выводу о недоказанной стойкости метода обманных состояний. Фак-

тически, эти рассуждения игнорируют основной результат квантовой криптографии о стойкости протокола BB84 со строго однофотонными посылками, поскольку применяемая оценка допускает, что информация об однофотонных посылках полностью известна противнику.

#### ЛИТЕРАТУРА

1. С. Н. Молотков, К. С. Кравцов, М. И. Рыжкин, ЖЭТФ **155**, 636 (2019).
2. С. Н. Молотков, К. С. Кравцов, М. И. Рыжкин, ЖЭТФ **156**, 379 (2019).
3. К. А. Балыгин, В. И. Зайцев, А. Н. Климов и др., Письма в ЖЭТФ **105**, 570 (2017).
4. X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
5. А. С. Трушечкин, Е. О. Киктенко, Д. А. Кронберг, А. К. Федоров, УФН **191**, 93 (2021).