Письма в ЖЭТФ, том 104, вып. 5, с. 349 – 355 © 2016 г. 10 сентября

О коррекции ошибок в системах квантовой криптографии

К. А. Балыгин[×], *А. Н. Климов*[×∇], *С. П. Кулик*[×], *С. Н. Молотков*[+*∘1)]

[+]*Институт физики твердого тела РАН, 142432 Черноголовка, Россия*

[*]*Академия Криптографии Российской Федерации, 121552 Москва, Россия*

[×]*Физический факультет МГУ им. Ломоносова, Москва, Россия*

[∘]*Факультет вычислительной математики и кибернетики МГУ им. Ломоносова, 119991 Москва, Россия*

[∇]*Институт общей физики РАН им. Прохорова, 119991 Москва, Россия*

Поступила в редакцию 23 июня 2016 г.
После переработки 27 июля 2016 г.

Приведены результаты по генерации ключей в двухпроходной системе квантовой криптографии, использующей протоколы на геометрически однородных когерентных состояниях. Представлены результаты по коррекции ошибок в данной системе, которые не используют раскрытия части последовательности сырого ключа для оценки вероятности ошибки, а используют мониторинг набора параметров системы и квантового канала связи, достаточных для априорной оценки вероятности ошибки, которая используется для выбора корректирующего кода.

DOI: 10.7868/S0370274X16170112

Введение. Квантовая криптография позволяет получить общий секретный ключ между двумя удаленными пользователями, соединенными открытыми квантовым и классическим каналами [1]. Принципиальным моментом для гарантии секретности передаваемых ключей является оценка утечки информации в зависимости от наблюдаемой ошибки в передаваемой последовательности на приемной стороне. Квантовая теория информации в однофотонном случае позволяет через фундаментальные энтропийные соотношения неопределенностей связать наблюдаемую ошибку на приемной стороне с утечкой информации через квантовый канал связи и длиной секретного ключа [2]. При этом энтропийные соотношения неявно учитывают всевозможные атаки подслушивателя (Евы) на канал связи. Если состояния не строго однофотонные, то воспользоваться энтропийными соотношениями неопределенностей для вычисления зависимости утечки информации и длины ключа от наблюдаемой ошибки уже не удается. При наличии потерь в канале возможны атаки, которые не приводят к ошибкам, но дают утечку информации [3]. Знание вероятности ошибки нужно как для оценки величины утечки информации, так и для выбора кода коррекции ошибок. Как показывает подход, принятый нами, возможно вообще не раскрывать часть последовательности для оценки вероятности ошибки и утечки информации.

1) *Консервативная оценка утечки информации к Еве может быть получена и без оценки вероятности ошибки.* Теория квантовых каналов связи позволяет получить фундаментальную верхнюю границу на величину классической информации, которую можно извлечь из квантового ансамбля, так называемая граница Холево [4], что позволяет “развязать” максимальную утечку к Еве с наблюдаемой ошибкой.

2) *Оценка вероятности ошибки может быть получена и без раскрытия части последовательности.* Поскольку в отсутствии Евы все параметры системы, влияющие на величину ошибки (темновые шумы однофотонного детектора, засветки, видность интерферометра и т.д.) перед посылкой каждой серии контролируются, то при данной длине линии можно получить априорную оценку ошибки и выбрать соответствующий корректирующий код.

Возможны две ситуации. 1) Если реальная ошибка окажется больше априорной оценки, но будет еще меньше критической (и в принципе можно было бы еще получить ключ), но корректирующей способности кода не хватает, чтобы исправить ошибки, то ключ не будет сгенерирован. Превышение ошибки над априорной оценкой уже будет указывать на наличие вторжения в канал. 2) Если реальная ошибка окажется больше априорной и больше критической, то ключ не будет сгенерирован. Превышение ошибки

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

над критической опять будет указывать на вторжение в канал связи. *Важно, что никогда не будет ситуации, когда ключ сгенерирован, и считается, что он секретен, а на самом деле таковым не является.*

Протокол квантового распределения ключей (КРК). Протоколы BB84, SARG [3] при использовании ослабленного лазерного излучения не могут гарантировать секретность ключей в реальных системах при больших потерях, поэтому необходимо использовать протоколы с большим числом информационных состояний и базисов. Для протокола DPS (Differential Phase Shift) [5] и COW (Coherent One Way) [6] из-за распределенного кодирования до сих пор нет внятного доказательства их секретности. Кроме того, доказательства секретности в строго однофотонном случае дают оценку критической ошибки $\approx 4.12\,\%$ [7], поэтому критическая ошибка при использовании ослабленного лазерного излучения вряд ли будет больше. Протокол Decoy State [8] явно использует предположения о свойствах лавинных однофотонных детекторов, т.к. 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.

Информационные состояния ослабленного лазерного излучения (когерентные состояния) являются линейно независимыми, что приводит к атаке с UM (Unambiguous Measurements) измерениями [9] (PNS (Photon Number Splitting) атака [3] – частный случай UM измерений). Поэтому протокол должен учитывать такую атаку. Для ряда состояний имеются точные решения [9], которые позволяют получить величину утечки информации в зависимости от потерь в квантовом канале связи. Одним из таких протоколов является протокол на геометрически однородных состояниях. Число базисов $N_{\text{basis}}/2 = 4$ ($N_{\text{basis}} = 8$ – число информационных состояний) уже достаточно для гарантии секретности ключей при полных потерях 0.999. Информационными состояниями являются геометрически однородные когерентные состояния $|\alpha_j\rangle$, которые получаются унитарным поворотом U^j, $U^N = I - |\alpha_j\rangle = U^j|\alpha\rangle$, где $\alpha_j = e^{i\frac{2\pi j}{N_{\text{basis}}b}}\alpha$ ($j = 0, 1, ...N_{\text{basis}} - 1$). В протоколе используется $\frac{N_{\text{basis}}}{2} = 4$ базиса, в каждом базисе имеется пара неортогональных состояний с $|\alpha_j\rangle$ и $|\alpha_{j+1}\rangle$, отвечающих 0 и 1.

Критерий секретности. Мерой секретности ключей является следовое расстояние между реальной матрицей плотности Алиса–Ева (ρ^n_{XE}) и некоррелированными матрицами плотности Алиса–Ева ($\rho^n_U \otimes \rho^n_E$) – *идеальная ситуация.* Протокол должен гарантировать, что следовое расстояние Δ между данными матрицами плотности может быть сделано меньше наперед заданной величины ε. В этом случае протокол называется ε-секретным,

$$\Delta = ||\rho_{XE} - \rho_U \otimes \rho_E||_1, \tag{1}$$

где следовое расстояние между операторами $||\rho_1 - \rho_2||_1 = \text{Tr}\{|\rho_1 - \rho_2|\}$. Согласно лемме об остатке хэширования [10, 11], после коррекции ошибок и сжатия очищенного ключа универсальными хэш-функциями второго порядка следовое расстояние становится равным

$$\Delta = \sqrt{2^{-(H^{\varepsilon}_{\min}(X|CE)-R)}} < \varepsilon, \tag{2}$$

здесь $H^{\varepsilon}_{\min}(X|CE)$ – условная min энтропия, C – включает в себя корректирующую информацию, переданную Алисой через открытый канал к Бобу. Протокол является ε-секретным [10], если длина финального секретного ключа R не превышает

$$R = H^{\varepsilon}_{\min}(X|CE) - 2\log\left(\frac{1}{\varepsilon}\right), \tag{3}$$

естественно в (3) берется целая часть. Для $H^{\varepsilon}_{\min}(X|CE)$ может быть получена оценка [10],

$$H^{\varepsilon}_{\min}(X|CE) \geq H(X|E) - \text{leak}, \tag{4}$$

leak – классическая, переданная через открытый канал при коррекции ошибок. В итоге

$$R = H^{\varepsilon}(X|E) - \text{leak} - 2\log\left(\frac{1}{\varepsilon}\right), \tag{5}$$

$H^{\varepsilon}(X|E)$ – ограничена сверху информацией Холево (см. детали в [12]). Данное слагаемое при наличии потерь в линии учитывает также UM измерения.

Длина секретного ключа *должна зависеть только от: 1) наблюдаемой ошибки на приемной стороне – числа раскрытых бит при коррекции ошибок leak; 2) числа посланных и зарегистрированных состояний при совпадающих базисах; 3) структуры квантового состояния, посланного в канал связи. Внутренние параметры: квантовая эффективность детекторов, вероятность темновых шумов, потери во внутренней оптической части и канале не должны входить в длину секретного ключа, т.к. они могут меняться в каждой посылке.*

Для геометрически однородных состояний имеется точное решение для вероятности неопределенного исхода [9]

$$\Pr(?) = 1 - \min_r \left| \sum_{j=0}^{N_{\text{basis}}-1} e^{\mu(e^{i\frac{2\pi j}{N_{\text{basis}}}}-1)} e^{-i\frac{2\pi jr}{N_{\text{basis}}}} \right|, \quad 0 \le r \le N_{\text{basis}} - 1. \tag{6}$$

Принципиально важно учитывать не только потери в канале связи, но и потери в приемной части системы. Ниже под потерями будем понимать полные потери как отношение числа посланных и зарегистрированных посылок – $\Pr(Loss) = \frac{N_{\text{registr}}}{N_{\text{send}}}$. Даже при $\Pr(Loss(ch)) < \Pr(?)$ Ева может проводить UM измерения, используя потери внутри приемной части. Полные потери определяются квантовой эффективностью детектора ($\eta \approx 0.1 \div 0.5$), средним числом фотонов ($\mu \approx 0.1 \div 0.5$) в когерентном состоянии, потерями в приемной оптической части и потерями в канале. Заметим, что внутренние потери $1 - \eta \cdot \mu \approx 1 - 10^{-2}$ что эквивалентно потерям при длине линии на стандартном одномодовом волокне в 100 км. Для $H(X|E)$ используется верхняя консервативная оценка – $H(X|E) \ge 1 - C_1(N_{\text{basis}} b) = 1 - (\xi^- \log \xi^- + \xi^+ \log \xi^+)/2$, где $\xi^\pm = (1 \pm \sqrt{1 - \varepsilon_b^2})$, и $\varepsilon_{\text{basis}} = |\langle \alpha_i | \alpha_{i+1} \rangle|$ – скалярное произведение состояний внутри одного базиса. В итоге для длины секретного ключа находим [12]

$$\begin{aligned} R = n((1 - \Pr(Loss))(1 - \text{leak}) - \\ - (1 - \Pr(Loss, ?))C_1(N_{\text{basis}}) - \\ - \Pr(Loss, ?)(1 - \Pr(?))), \end{aligned} \tag{7}$$

где $\Pr(Loss, ?) = \Pr(Loss)/\Pr(?)$, и n – число зарегистрированных отсчетов при *совпадающих базисах*. В (7) опущено слагаемое, связанное с ε. Величина ε определяет сложность перебора ключей (см. [13]) при их использовании в алгоритмах шифрования и устанавливается конкретными требованиями потребителей ключей и используемыми алгоритмами шифрования, что выходит за рамки данной работы. Это слагаемое подразумевает дополнительное сжатие ключа. Кроме того, если после коррекции ошибок производится M раз проверка идентичности очищенного ключа, то длина ключа в (7) заменяется на $R \to R - M$.

Выбор корректирующего кода. В качестве корректирующего кода было выбрано семейство кодов Хэмминга [14] с дополнительной проверкой на четность в блоках. Коды Хэмминга, в отличие от процедуры Cascade [15], используемой в квантовой криптографии, требуют меньшего числа обменов по открытому каналу *и эффективно и просто переносятся на нижний аппаратный уровень*. По сранению с кодами с низкой плотностью проверок на четность (LDPC – Low Density Parity Check Codes [16, 17]) коды Хэмминга требуют меньшего числа итераций при коррекциии ошибок, хотя и уступают в корректирующих свойствах. Кроме того, LDPC коды более чувствительны к оценке вероятности ошибки, поэтому неизбежно приходтся прибегать к раскрытию части последовательности.

Коды Хэмминга исправляют одну ошибку в блоке. При наличии двух ошибок применение кода приводит к увеличению ошибок. Поэтому, если известна априорная ошибка, то можно выбрать такой код, чтобы в каждом блоке была в среднем одна ошибка. В квантовой криптографии используются длины блоков 7, 15, 31, что подходит для ошибок до 14 %. Алиса и Боб разбивают свои последовательности на блоки одинаковой длины и сравнивают их биты четности. Если бит четности не совпадает, то блок содержит нечетное число ошибок (одну, три или более, что мало вероятно). Для блоков с несовпадающей четностью Алиса вычисляет набор контрольных символов (синдром) и отправляет Бобу. Для этих блоков Боб вычисляет свой синдром и складывает с синдромом Алисы. Возникает бинарное представление числа – номер, который сразу дает позицию ошибки в блоке.

Перемешивание. Исходная битовая строка длиной n предварительно перемешивается, чтобы избежать скопления ошибок в одном месте. Такая процедура необходима, поскольку ошибки могут группироваться. При перемешивании происходит перенумерация номеров старых позиций i в новые номера $index[i]$, $index[i] = Round((n - 1 - i) \cdot r_i)$, $r_i \in (0, 1)$, r_i, после этого биты в позициях $(n - 1 - i)$ и $index[i]$ переставляются.

Выбор длины блоков. В зависимости от априорной оценки ошибки Q выбирается длина блока кода $x_{A,B} \approx \frac{1}{Q}$ – в среднем в блоке одна ошибка. Длина последовательности должна быть кратной выбранной длине блока. Лишние биты отбрасываются. Далее происходит последовательное заполнение блоков из перемешанной на предыдущем шаге последовательности.

Заполнение блоков. Для каждого бита перемешанной последовательности происходит вычисление номера блока, в который данный бит попадет. Номер блока b_n равен $b_n = (j \cdot i + k)\text{mod } p)\text{mod } BlockNumber$, $i \in [1, n]$, где $BlockNumber$ – число блоков, новая длина (обозначения сохраняем прежними) n – теперь кратно числу блоков, j и k – случайные числа из $[1, n]$, которые выбираются раз и навсегда, p – первое простое число, превышающее n.

Исправление ошибок. Для каждого блока с несовпадающей четностью Алиса вычисляет синдром (все операции по mod 2) и посылает Бобу, Боб вычисляет свой синдром

$$S_A = H \cdot x_A, \quad S_B = H \cdot x_B,$$

$$H = \begin{pmatrix} \alpha_1, & \alpha_2, & \alpha_3, & \ldots, & \alpha_{2^m-1} \end{pmatrix}, \quad m = 3, 4, 5,$$

где x_A, x_B – блоки Алисы и Боба (у Боба, возможно, с ошибкой), α_i – бинарное (в виде столбца) представление числа. Вычисляется и сравнивается общий синдром $S = S_A \oplus S_B$. Битовый вектор S длины 3, 4, 5 в зависимости от выбора длины блока дает прямо номер позиции в блоке, где произошла ошибка. Процедура выполняется итерационно до тех пор, пока в последовательности присутствуют блоки с несовпадающей четностью. *Важно, что при чистке никакие биты не выбрасываются. Запоминается полное число раскрытых битов за все проходы. Полное число раскрытых бит есть утечка классической информации к Еве (см. выше, формула (7)).*

Проверка идентичности очищенных ключей. Генерируется случайная последовательность с длиной, равной длине очищенного ключа. Алиса и Боб независимо складывают по mod 2 свои (x_A и x_B) последовательности со случайной, затем вычисляют и сравнивают бит четности результирующей последовательности. Процедура повторяется M раз, каждый раз с новой случайной последовательностью. Если все биты четности совпали, то вероятность того, что последовательности тем не менее не совпадают, не более $\Pr(x_A \neq x_B) \leq \frac{1}{2^M}$. Например, при $M = 32$, в среднем на 10^9 очищенных ключей, прошедших тест, возможно, один не будет совпадать. При такой процедуре раскрывается дополнительно M бит информации (формула (7)), которая "изымается" у Евы на стадии усиления секретности.

Реализация усиления секретности очищенных ключей. Генерируется случайная битовая строка R длиной n, равной очищенному ключу K. Битовые строки R и K рассматриваются как коэффициенты полиномов степени $n-1$ с коэффициентами в поле $GF(2)$. Берется неприводимый полином $Prime_n(x)$ степени $n-1$ с коэффициентами в $GF(2)$, набор данных полиномов вычисляется заранее. Вычисляется полином $RK(x) = (R(x) \cdot K(x)) \bmod Prime_n(x)$, который имеет степень $n-1$, коэффициенты которого представляют собой битовую строку длины n. Из этой строки оставляются только (см. (7)) младших бит, которые и являются финальным секретным ключом – R. Приведем пример нескольких неприводимых полиномов разной степени (полная таблица полиномов до степени 10^4 была сгенерирована заранее):

$$\begin{aligned}
&Prime_{7000}(x) = x^{7000} + x^{27} + x^{26} + x^{11} + 1 \\
&Prime_{8000}(x) = x^{8000} + x^{16} + x^{3} + x + 1 \\
&Prime_{9000}(x) = x^{9000} + x^{28} + x^{19} + x^{17} + 1 \\
&Prime_{10000}(x) = x^{10000} + x^{19} + x^{13} + x^{9} + 1.
\end{aligned}$$

Оценка вероятности ошибки без раскрытия части последовательности. Пусть вероятность темновых шумов за время строба есть p_{dark}, тогда ошибка, с точностью до линейных по вероятностям членов (см. детали для общего случая в [18]), равна

$$Q = \frac{1}{2}\frac{p_{\text{dark}}}{p_{\text{dark}} + p_{\text{reg}}(\mu, V, Loss_{\text{Alice}}, L, \delta, \eta, \{prot\})}, \quad (8)$$

здесь $p_{\text{reg}}(\mu, V, L, \delta, \eta, \{prot\})$ – вероятность регистрации квантового состояния, которая зависит от среднего числа фотонов μ, потерь в приемной части $Loss_{\text{Alice}}$, длины линии L, потерь в линии δ, видности интерферометра V, квантовой эффективности APD и от протокола $\{prot\}$ квантового распределения ключей. Пропускание оптической части

$$\begin{gathered}
T_{\text{opt}}(L, \delta, Loss_{\text{Alice}}) = T_{Ch}(L, \delta) \cdot T_{\text{Alice}}, \\
T_{Ch}(L, \delta) = 10^{-\dfrac{\delta L}{10}}, \quad T_{\text{Alice}} = \tfrac{1}{5.1},
\end{gathered} \quad (9)$$

для стандартного одномодового волокна $\delta = 0.2$ ДБ/км. Потери за счет протокола включают потери из-за неидеальной видности интерферометра. Эффективность протокола по отсчетам APD

$$\begin{gathered}
T(\eta) = \eta \frac{2}{N_{\text{state}}^2} \sum_{i=1}^{N_{\text{state}}} \sum_{j=1}^{N_{\text{state}}} \sin^2\left(\frac{\Delta\varphi_{ij} - \varphi_V}{2}\right), \\
\varphi_{ij} = \varphi_i - \varphi_j,
\end{gathered} \quad (10)$$

разница фаз двух когерентных состояний, N_{state} – число информационных состояний. В (10), (11) величина φ_V отвечает за неидеальность балансировки интерферометра. Поскольку система автоматической балансировки держит видность интерферометра не хуже $V > 0.99$ (см. детали в [12]), то как показывает опыт, данное слагаемое может быть положено равным нулю. Эффективность протокола по отсчетам APD при совпадающих базисах

$$T(\eta) = \eta \frac{2N_{\text{basis}}}{N_{\text{state}}^2} \sum_{i=1}^{2} \sum_{j=1}^{2} \sin^2\left(\frac{\Delta\varphi_{ij} - \varphi_V}{2}\right), \quad (11)$$

где N_{basis} – число базисов. С учетом того, что детектор не реагирует на вакуумную компоненту когерентного состояния, то эффективность по отсчетам APD при совпадающих базисах равна

$$p_{\text{reg}}(\mu, V, Loss_{\text{Alice}}, L, \delta, \eta, \{prot\}) = \\ = 1 - \exp\left(-\mu \cdot T(\eta) \cdot T_{\text{opt}}(L, \delta, Loss_{\text{Alice}})\right). \quad (12)$$

Таким образом, формулы (8)–(12) позволяют оценить текущую ошибку без раскрытия части последовательности. Практически это выполняется следующим образом. Перед посылкой серии N_{pulses} система определяет текущую вероятность темновых шумов p_{dark} и квантовую эффективность однофотонного детектора η. Далее измеряется видность интерферометра. Учитывая теоретическую оценку потерь в линии, система определяет ожидаемое число регистрируемых состояний, как полного числа (10), так и в совпадающих базисах (11). Оценивается вероятность априорной ошибки по формуле (8). После передачи серии из N_{pulses} определяется как полное число реально зарегистрированных отсчетов, так и число отсчетов в совпадающих базисах. Сравнивается оценочное число с реальным числом отсчетов. Уточняется оценка вероятности ошибки. При ошибке выше критической ($\approx 11\,\%$, см. рис. 2b), и невозможности получить секретный ключ, система информирует пользователя и повторяет попытку получить ключ с самого начала. Если ошибка меньше критической, то система выбирает начальную длину блока для корректирующего кода, и автоматически запускает процедуру очистки, проверки очищенных ключей, процедуру усиления секретности и проверки статистических свойств финального секретного ключа.

Экспериментальные результаты. Было проведено тестирование процедуры коррекции ошибок самой по себе. Для этого генерировалась случайная битовая строка, в которую случайным образом вносились ошибки. Затем производилась коррекция ошибок при помощи описанной выше процедуры. Были исследованы два варианта: 1) длина блока была постоянной; 2) длина блока изменялась в процессе итераций. Число ошибок изменяется по ходу итераций процедуры. В первом случае длина блока оставалась постоянной, несмотря на изменение числа ошибок в последовательности. Во втором случае по мере уменьшения ошибок длина кодового слова увеличивалась так, чтобы в новом более длинном кодовом слове была примерно одна ошибка. Результаты тестирования приведены на рис. 1. При некоторой ошибке вся последовательность расходуется на исправление ошибок. Из рис. 1 видно, что коррекция

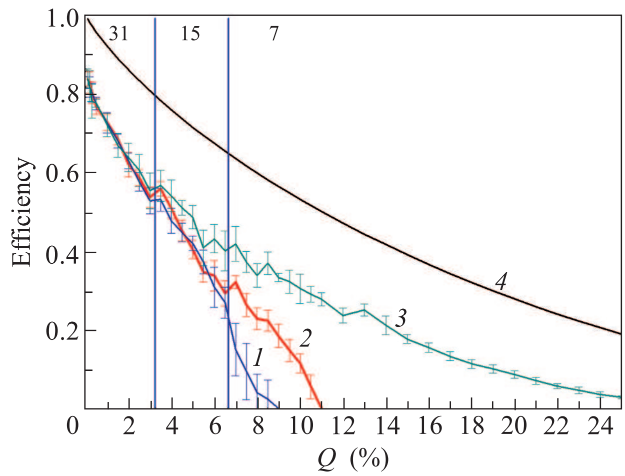

Рис. 1. (Цветной онлайн) Зависимости эффективности процедуры коррекции ошибок от процента ошибок в исходной последовательности с использованием постоянной и переменной длины блока. *1* – При постоянной длине блока, выбираемой по начальной ошибке. *2* – При длине блока, изменяемой в процессе очистки в зависимости от текущей ошибки. Величина текущей ошибки может быть оценена исходя из начальной и числа битов, исправленных в текущей итерации. *3* – При постоянной длине блока, но с выбрасыванием числа раскрытых битов (битов четности, контрольных бит) на каждой итерации. *4* – Зависимость эффективности коррекции ошибок в шенноновском теоретическом пределе. Переключение на другую длину блока обозначено вертикальными линиями. Длина исходной последовательности была равна $N_{\text{raw}} = 10^4$. Эффективность процедуры определялась как Efficiency $= \frac{N_{\text{raw}} - N_{\text{leak}}}{N_{\text{raw}}}$, где N_{leak} – число раскрытых бит через классический канал при коррекции ошибок

ошибок с увеличением длины кодового слова обеспечивает коррекцию ошибок до большего процента исходных ошибок. Поэтому в дальнейшем при генерации секретных ключей в системе использовалась процедура с переменной длиной кодового слова.

В литературе можно встретить утверждения, что можно изымать контрольные биты четности в процессе самой процедуры исправления ошибок [20]. Изъятие битов четности и контрольных проверочных битов четности в кодовых словах изменяет переходные вероятности. Изъятие контрольных битов на ходу при чистке позволяет получить финальный ключ большей длины, что не верно. Для иллюстрации этого факта на рис. 1 приведена эффективность очистки при изъятии битов четности и синдромов на ходу (кривая *3*). Кривая *4* (рис. 1) отвечает шенноновскому пределу. При этом, как видно из рис. 1, при изъятии битов четности на ходу может быть получена бо́льшая длина ключа и длина линии связи.

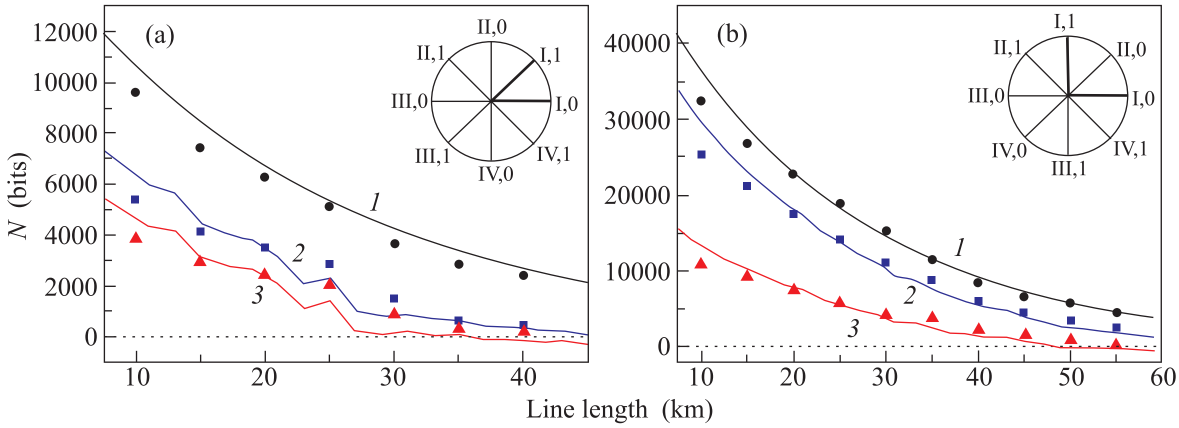

Рис. 2. (Цветной онлайн) Число секретных бит в зависимости от длины квантового канала связи для протокола с 8 состояниями и 4 базисами. (a) – Для протокола с углом 45° между информационными состояниями внутри базиса. Эффективность такого протокола по базисам (см. пояснения в разделе с оценкой ошибки) равна $3.66 \cdot 10^{-2}$. (b) – Для протокола с углом 90° между информационными состояниями внутри базиса. Его эффективность по базисам равна $1.25 \cdot 10^{-1}$. Расположение состояний 0 и 1 в базисах I, II, III, IV показано на вставках. Кривые (*1*) отвечают теоретической зависимости числа зарегистрированных отсчетов в совпадающих базисах, соответственно, круглыми маркерами обозначено число экспериментальных отсчетов. Кривые (*2*) – вычисленное число бит, оставшихся после исправления ошибок. Для этого использовалась теоретическая зависимость 1, из которой вычиталось число бит после коррекции ошибок. Квадратными маркерами обозначено число бит, оставшихся после коррекции ошибок в экспериментальной последовательности. Кривые (*3*) – зависимость ожидаемого числа секретных бит, рассчитанная по формулам (7), (8)–(11), с использованием экспериментального числа раскрытых бит при коррекции ошибок. Соответственно, треугольными маркерами показана экспериментальная зависимость числа секретных бит от длины линии связи

Описанная выше процедура коррекции ошибок была применена при распределении секретного ключа на полностью автоматической двухпроходной системе, описанной в [17]. Распределение ключей проводилось по протоколу на геометрически однородных когерентных состояниях (см. детали в [12]). Экспериментально полученное число секретных бит в зависимости от длины квантового канала связи представлено на рис. 2. Длина передаваемой последовательности в каждой серии составляла $N_{\text{pulses}} = 27962016$, среднее число фотонов на одно состояние $\mu = 0.4$, потери в линии связи $\delta = 0.2$ ДБ/км, потери в сервере составляли 5.1 раза, вероятность темновых шумов однофотонного лавинного детектора $p_{\text{dark}} = 3 \cdot 10^{-6}$ на строб (длительность строба $\tau = 670$ пс).

Таким образом, продемонстрирована достаточность мониторинга набора параметров системы и квантового канала связи для априорной оценки вероятности ошибки без использования раскрытия части последовательности сырого ключа. Экспериментально подтверждена возможность распределения секретных ключей для протоколов на геометрически однородных когерентных состояниях и использованием кодов Хэмминга для длин линии вплоть до 50 км.

Выражаем благодарность Д.А. Кронбергу за обсуждения, а также коллегам по Академии Криптографии Российской Федерации за постоянную поддержку и обсуждения. Работа выполнена при поддержке гранта РНФ # 16-12-00015.

1. C. H. Bennett and G. Brassard, *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India (1984), p. 175.
2. M. Tomamichel, C. Ci Wen Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 634 (2011).
3. V. Scarani, V.H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
4. A.S. Holevo, Russian Math. Surveys **53**, 1295 (1998).
5. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); Phys. Rev. A **68**, 022317 (2003); H. Takesue, S.W. Nam, Q. Zhang, R.H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nature Photonics **1** 343 (2007).
6. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
7. K. Wen, K. Tamaki, and Y. Yamamoto, arXiv:0806.2684.
8. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901-1 (2003).
9. A. Chefles, Phys. Lett. A **239**, 339 (1998); A. Chefles and S.M. Barnett, Phys. Lett. A **250**, 223 (1998).
10. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. (2005); arXiv:0512258.

11. H. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57** (2011); arXiv:10022436.
12. С. Н. Молотков, Письма в ЖЭТФ **101**, 579 (2015).
13. С. Н. Молотков, ЖЭТФ (в печати).
14. R. W. Hamming, *Coding and Information Theory*, Prentice Hall, New Jersey (1980).
15. G. Brassard and L. Salvail, Lect. Notes Comput. Sci. **765**, 410 (1994).
16. R. G. Gallager, *Low-Density Parity-Check Codes*, MIT Press, Cambridge, MA (1963).
17. D. J. C. MacKay and R. M. Neal, Electron. Lett. **32**, 1645 (1996).
18. С. Н. Молотков, ЖЭТФ **134**, 39 (2008).
19. К. А. Балыгин, А. Н. Климов, С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **103**, 496 (2016).
20. W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, Phys. Rev. A **67**, 052303 (2003).