УДК 621.383.92

ПОТЕРИ ИНФОРМАЦИИ В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

Тимофеев А.М., Злобина Ю.В., Чупина А.Л.

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Аннотация. Применительно к квантово-криптографическому каналу связи, содержащему в качестве приемного модуля счетчик фотонов с мертвым временем, получено выражение для оценки энтропии потерь информации. По результатам математического моделирования установлена зависимость условной энтропии на выходе канала связи от средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0», что позволило обосновать выбор скоростей счета, обеспечивающих наименьшие потери передаваемой информации.

Ключевые слова: канал связи, счетчик фотонов, мертвое время.

LOSS OF INFORMATION IN THE QUANTUM CRYPTOGRAPHIC COMMUNICATION CHANNEL

Timofeev A., Zlobina Yu., Chupina A.

Belarusian State University of Informatics and Radioelectronics,
Minsk, Belarus

Abstract. A quantum cryptographic communication channel with a receiving module based on a dead time photon counter was investigated. For this communication channel, an expression is obtained to estimate the entropy of information loss. The dependence of the conditional entropy at the output of the communication channel on the average count rate of signal pulses at the output of the photon counter during the transmission of symbols «0» was obtained using mathematical modeling of the communication channel. This made it possible to substantiate the choice of pulse count rates that ensure the least loss of transmitted information.

Key words: communication channel, photon counter, dead time.

Адрес для переписки: Тимофеев А.М., ул. П. Бровки, 6, г. Минск 220013, Республика Беларусь
e-mail: tamvks@mail.ru

Существующие системы квантово-криптографической связи характеризуются достаточно высоким уровнем информационной безопасности [1]. Это становится возможным благодаря использованию квантово-механического ресурса при кодировании передаваемых данных (поляризации, частоты и фазы передаваемых фотонов). Регистрация таких данных требует наличия высокочувствительных приемных модулей – счетчиков фотонов [1, 2]. Однако счетчики фотонов ввиду неидеальности своих технико-эксплуатационных характеристик могут приводить к ошибкам при приеме информации, что снижает уровень информационной безопасности указанных систем связи. Одной из причин таких ошибок может являться ненулевое мертвое время счетчика фотонов, определяемое как длительность времени, в течение которого счетчик фотонов не чувствителен к падающему на него оптическому излучению [1–4]. В этой связи **целью данной работы** являлось определить влияние мертвого времени счетчика фотонов на потери передаваемой информации в квантово-криптографическом канале связи. **Объект исследования** – асинхронный двоичный несимметричный однородный однофотонный квантово-криптографический канал связи без памяти и со стиранием, содержащий в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. Выбор в качестве объекта исследования такого канала связи обусловлен тем, что его использование не требует наличия дополнительных линий связи для передачи и приема синхроимпульсов [3, 4]. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины [2].

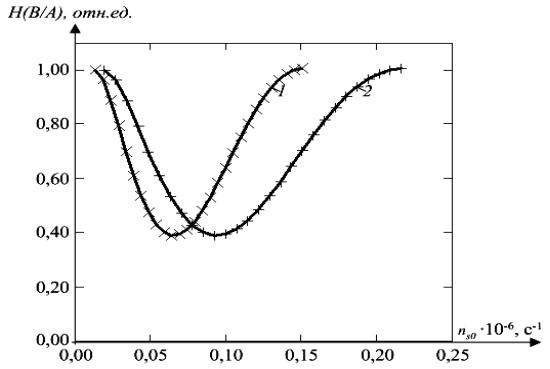
Выражение для оценки потерь информации. Для оценки потерь информации воспользуемся формулой условной энтропии, которая применительно к квантово-криптографическому каналу связи, содержащему в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа, будет выглядеть следующим образом [4]:

$$
\begin{aligned}
H(B/A) = -0{,}5\Bigg\{ & \left[\sum_{N=N_1}^{N_2} \frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N \exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}\right]\times \\
& \times \log_2\left[\sum_{N=N_1}^{N_2} \frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N \exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}\right]+ \\
& +\left[1-\sum_{N=0}^{N_2} \frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N \exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}\right]\times \\
& \times \log_2\left[1-\sum_{N=0}^{N_2} \frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N \exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}\right]+ \\
& +\left[\sum_{N=0}^{N_1-1} \frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N \exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}\right]\times \\
& \times \log_2\left[\sum_{N=0}^{N_1-1} \frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N \exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}\right]\Bigg\}-
\end{aligned}
\qquad (1)
$$

$$-0{,}5\left\{\left[\sum_{N=N_1}^{N_2}\frac{\left[(n_t+n_{s1})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s1})(\Delta t-\tau_d)\right]}{N!}\right]\times\right.$$
$$\times\log_2\left[\sum_{N=N_1}^{N_2}\frac{\left[(n_t+n_{s1})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s1})(\Delta t-\tau_d)\right]}{N!}\right]+$$
$$+\left[1-\sum_{N=0}^{N_2}\frac{\left[(n_t+n_{s1})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s1})(\Delta t-\tau_d)\right]}{N!}\right]\times$$
$$\times\log_2\left[1-\sum_{N=0}^{N_2}\frac{\left[(n_t+n_{s1})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s1})(\Delta t-\tau_d)\right]}{N!}\right]+$$
$$+\left[\sum_{N=0}^{N_1-1}\frac{\left[(n_t+n_{s1})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s1})(\Delta t-\tau_d)\right]}{N!}\right]\times$$
$$\left.\times\log_2\left[\sum_{N=0}^{N_1-1}\frac{\left[(n_t+n_{s1})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s1})(\Delta t-\tau_d)\right]}{N!}\right]\right\}.$$

В выражении (1) N_1 и N_2 – нижний и верхний пороговые уровни регистрации соответственно, n_t – средняя скорость счета темновых импульсов на выходе счетчика фотонов, n_{s0} и n_{s1} – средние скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» и «1» соответственно, Δt – среднее время однофотонной передачи, τ_d – средняя длительность мертвого времени продлевающегося типа.

Результаты исследования и их обсуждение. На рис. 1 представлены зависимости энтропии потерь от средней скорости счета сигнальных импульсов при передаче символов «0» как при наличии мертвого времени продлевающегося типа, так и при его отсутствии.



$N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\Delta t = 50$ мкс;
средняя длительность мертвого времени:
1 – × $\tau_d = 0$; 2 – + $\tau_d = 15$ мкс

Рисунок 1 – Зависимость энтропии потерь от средней скорости счета сигнальных импульсов при передаче символов «0»

Расчет проводился для одинаковых значений нижнего и верхнего пороговых уровней регистрации $N_1 = 1$ и $N_2 = 7$, средней скорости счета темновых импульсов $n_t = 10^3$ с$^{-1}$ и среднего времени однофотонной передачи $\Delta t = 50$ мкс. Все графики нормированы на максимальное значение условной энтропии, полученное для соответствующей средней длительности мертвого времени продлевающегося типа. При построении зависимостей $H(B/A)$ от n_{s0} диапазоны изменений n_{s0} и значения n_{s1} выбирались по методике [3].

Из рис. 1 видно, что рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средней скорости счета сигнальных импульсов, при которой достигаются наименьшие значения условной энтропии. Так, например, наименьшие значения $H(B/A)$ достигаются при $n_{s0} = 66{,}6 \times 10^3$ с$^{-1}$ и $n_{s0} = 95{,}6 \times 10^3$ с$^{-1}$ соответственно для $\tau_d = 0$ и $\tau_d = 15$ мкс. Причем с ростом n_{s0} вначале наблюдается спад зависимости $H(B/A)$ от n_{s0} вплоть до наименьшего значения, после чего эта зависимость растет. Такое поведение зависимости $H(B/A)$ от n_{s0} проявляется как при наличии мертвого времени продлевающегося типа, так и при его отсутствии, и объясняется следующим. При прочих равных параметрах приема с ростом скорости счета n_{s0} вероятность ошибочной регистрации символов «0» уменьшается вплоть до своего наименьшего значения, что соответственно снижает $H(B/A)$. Это обусловлено смещением статистических распределений смеси числа темновых и сигнальных импульсов при передаче символов «0», достаточно подробно исследованное в работах [3, 4]. Однако дальнейшее смещение указанных статистических распределений при увеличении n_{s0} приводит к росту вероятности ошибочной регистрации символов «0». В результате этого зависимость $H(B/A)$ от n_{s0} после достижения своего наименьшего значения растет.

Заключение. Таким образом, в данной работе проведено математическое моделирование квантово-криптографического канала связи, содержащего в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. Выполненные исследования показали, что рост средней длительности мертвого времени продлевающегося типа приводит к увеличению средней скорости счета сигнальных импульсов при передаче символов «0», при которой достигаются минимальные потери информации.

Литература

1. Килин, С. Я. Квантовая криптография: идеи и практика / С. Я. Килин ; под ред. С. Я. Килин и др. – Минск : Белорус. наука, 2007. – 391 с.

2. Гулаков, И. Р. Фотоприемники квантовых систем: монография / И. Р. Гулаков, А. О. Зеневич. – Минск : УО ВГКС, 2012. – 276 с.

3. Тимофеев, А. М. Оценка влияния интенсивности оптического сигнала на вероятность ошибочной регистрации данных в однофотонном канале связи / А. М. Тимофеев // Информатика, 2021. – Т. 18, № 2. – С. 72–82.

4. Тимофеев, А. М. Оценка влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных квантово-криптографических каналов связи / А.М. Тимофеев // Вестник связи, 2018. – Т. 147, № 1. – С. 56–62.