Использование псевдослучайных последовательностей в системах квантовой связи

А.В. Горбунов, Р.С. Даюнов
Южный федеральный университет

Введение

Квантовая связь – вид связи, в которой для передачи информации используются квантовые состояния объектов (как правило, фотонов)[1]. С точки зрения информационной безопасности основной отличительной особенностьюквантовой связи является тот факт, что злоумышленник не может перехватить информацию, оставаясь незамеченным, так как измерение квантового состояния объекта означает разрушение этого состояния. Наибольшего развития технологии квантовой связи достигли в области систем квантовой криптографии [2, 3]. Однако принцип работы таких систем основан на формировании и распределении ключей между пользователями, но не на передаче информации от одного пользователя к другому, поэтому непосредственный перенос технологий квантовой криптографии на системы связи невозможен. В то же время задача построения систем квантовой связи является достаточно актуальной, что можно объяснить более высоким уровнем защищённости передачи информации по сравнению с классическими системами связи и более эффективным расходованием энергетической ёмкости канала связи [4-6].

Целью данной работы является обоснование возможности построения системы квантовой связи с использованием псевдослучайных последовательностей для кодирования передаваемой информации. Для достижения поставленной цели используются методы статистического моделирования, а также методы теории помехоустойчивой связи и обнаружения сигналов.

Проблема исследований

Основной проблемой, препятствующей использованию технологий квантовой криптографии для построения системы квантовой связи, является низкая эффективность коммерческих однофотонных детекторов, работающих на длине волны 1550 нм и построенных на основе лавинных фотодиодов[7, 8]. Например, модули однофотонного детектирования id201 и id210 швейцарской компании id Quantique (один из лидеров построения систем квантовой криптографии) обеспечивают эффективность детектирования в режиме стробирования до 25%, в режиме свободного счёта – до 10% [9, 10]. Также следует иметь ввиду, что увеличение вероятности детектирования приводит к увеличению уровня темновых шумов и вероятности появления остаточных импульсов (явление «afterpulsing»). В системах квантовой криптографии низкая вероятность детектирования не нарушает их функционирования, а только лишь ограничивает скорость формирования ключа, так как непринятые или ошибочно принятые фотоны просто отбрасываются на этапе «просеивания».

Задача обеспечения возможности передачи информации при низкой вероятности правильного приёма отдельных фотонов может быть решена путём внесения значительной избыточности в передаваемый сигнал. В технике связи такой подход находит широкое распространение и связан с использованием шумоподобных сигналов, помехоустойчивых икорреляционных кодов[11, 12].

Применение М-последовательностей для кодирования информации в системах квантовой связи

В качестве одного из возможных решений для систем квантовой связи, учитывая дискретную природу переносчиков информации, предлагается использовать псевдослучайные двоичные последовательности с ярко выраженными корреляционными свойствами. Например, при кодировании в передаваемом сообщении символа «1» псевдослучайной последовательностью длиной $M >> 1$ бит задачу приёма сигнала можно

рассматривать как задачу обнаружения сигнала (в качестве помех в канале связи здесь можно рассматривать низкую вероятность правильного детектирования отдельных одиночных фотонов и наличие темновых шумов детектора). Причём, чем в более сложных условиях будет осуществляться передача сигнала, тем большую длину последовательности M необходимо будет использовать.

В качестве псевдослучайных последовательностей для кодирования символа «1» предлагается использовать последовательности максимальной длины (М-последовательности), а в качестве критерия обнаружения передаваемого сигнала – автокорреляционные свойства таких последовательностей.

Символ «0» в передаваемом сообщении при этом может кодироваться различными способами: M нулевыми битами, последовательностью случайных бит длиной M, другой М-последовательностью из M бит (в этом случае задача обнаружения символа «1» трансформируется в задачу различения символов «1» и «0») и др.

Известно, что М-последовательности обладают следующими важными свойствами:

- период М-последовательности равен $M = 2^N - 1$;

- на длине одного периода М-последовательности количество символов, принимающих единичное значение, на единицу больше, чем количество символов, принимающих нулевое значение;

- нормированная автокорреляционная функция усечённой М-последовательности (непериодическая последовательность длиной в период M) имеет значение уровня боковых лепестков, близкое к $1/\sqrt{M}$.

Псевдослучайные последовательности уже нашли широкое применение в системах связи и криптографии [13, 14], их легко получить как алгоритмически, так и аппаратно.

Результаты моделирования

На рис. 1показана одна из возможных М-последовательностей при $N = 8$ (длина М-последовательности равна $M = 2^8 - 1 = 255$) и её автокорреляционная функция, полученные в математическом пакете Maple.

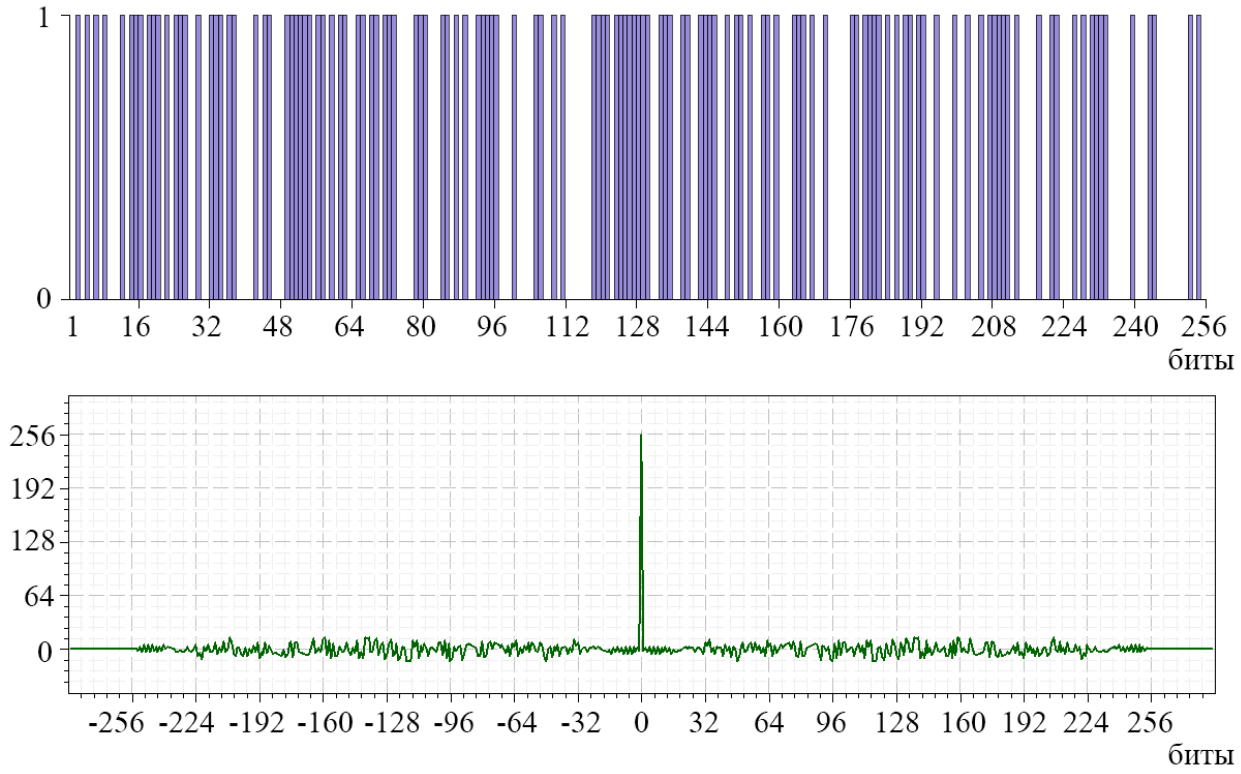

Рис. 1. М-последовательность из 255 бит (вверху) и её автокорреляционная функция (внизу)

При пиковом значении автокорреляционной функции $R_0 = 255$ максимальный уровень боковых лепестков для приведённой на рис. 1 М-последовательности составляет $R_{side.max} = 15$.

Следует отметить, что здесь и далее при расчёте корреляционных функций в двоичных последовательностях логический «0» заменялся на значение минус 1, а логическая «1» – на значение +1.

Для моделирования работы однофотонного детектора принято, что каждый единичный бит исходной М-последовательности верно детектируется с вероятностью $p_{дет}$. На рис. 2 показаны один из результатов моделирования продетектированной М-последовательности при $p_{дет} = 20\%$

(для показанной реализации моделирования из 127 единиц в исходной М-последовательности в продетектированной осталось только 24) и взаимнокорреляционная функция между такой продетектированной М-последовательностью и исходной М-последовательностью. При этом темновые шумы фотодетектора и вероятность возникновения остаточных импульсов не учитывались.

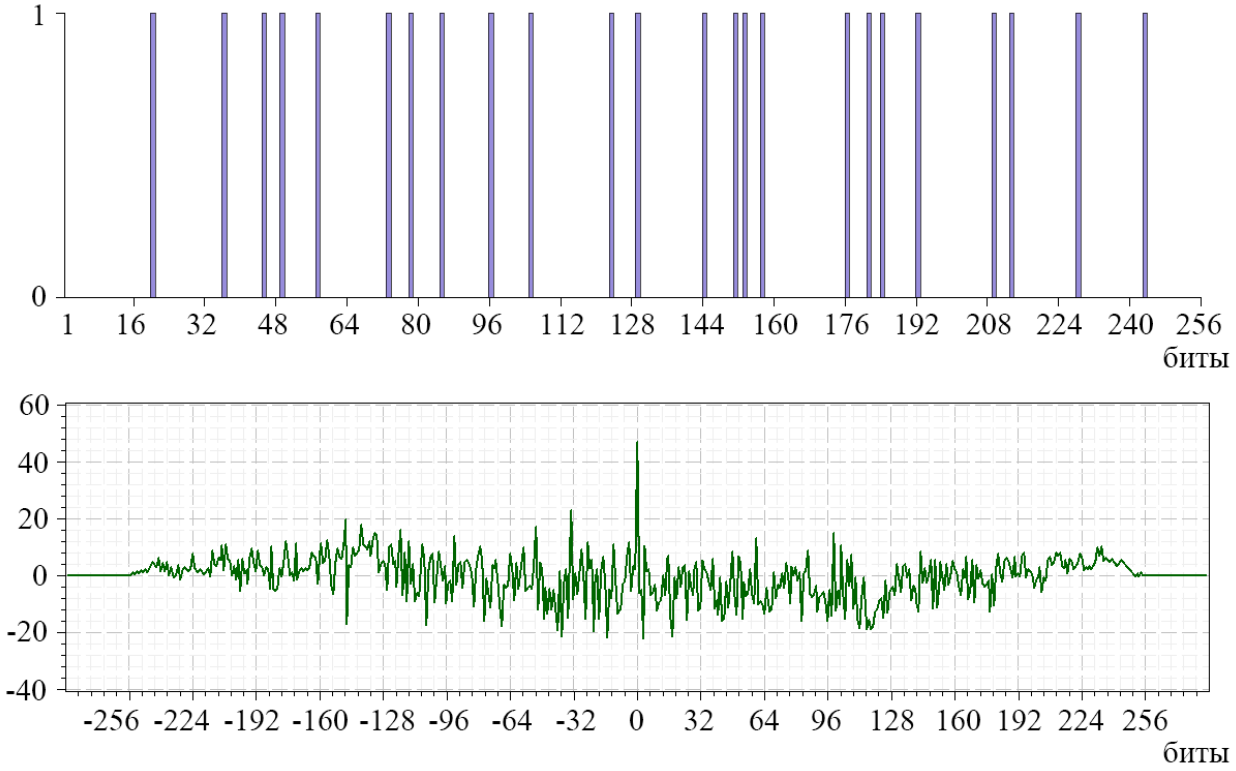

Рис. 2. Результаты моделирования продетектированной М-последовательности при вероятности детектирования отдельных бит $p_{дет} = 20\%$(вверху), и взаимнокорреляционная функция между ней и исходной М-последовательностью(внизу)

Для показанных на рис. 2 результатов моделирования пиковое значение взаимнокорреляционной функции составляет $R_0 = 47$, максимальный уровень боковых лепестков примерно в два раза ниже и равен $R_{side.max} = 23$. Наличие ярко выраженного пика на взаимнокорреляционной функции может являться критерием принятия решения о наличии логической «1» в исходном передаваемом сообщении.

В качестве количественного показателя возможности различения сигнала предлагается использовать понятие контраста γ корреляционной картины, определяемого как отношение разности значений пикового и максимального из боковых уровней взаимнокорреляционной функции к их сумме:

$$\gamma = \frac{R_0 - R_{side.max}}{R_0 + R_{side.max}}, \qquad (1)$$

где R_0 – пиковое значение взаимнокорреляционной функции, соответствующее нулевому сдвигу между анализируемыми функциями, $R_{side.max}$ – максимальный из боковых уровней взаимнокорреляционной функции.

При нулевом уровне боковых лепестков значение контраста будет равно $\gamma = 1$, в случае двукратного превышения пикового значения над боковыми $\gamma = 1/3$, при равенстве пикового уровня и уровня боковых лепестков (предельно допустимый случай с точки зрения правильного различения передаваемого информационного символа) значение контраста будет равно $\gamma = 0$ (в случае превышения боковых лепестков над значением R_0 значение контраста становится отрицательным). При этом в качестве критерия уверенного выделения обнаружения пика взаимнокорреляционной функции можно предложить использовать значения $\gamma \geq 0{,}2$ (например, для показанной на рис. 2реализации моделирования значение контрастаравно $\gamma = (47 - 23)/(47 + 23) = 0{,}343$).

Для получения статистически значимых результатов проведено моделирование процесса детектирования М-последовательности ирасчёта контраста корреляционной картины $\gamma(1)$ между такой продетектированной М-последовательностью и исходной М-последовательностьюпри вероятности правильного приёма отдельных бит $p_{дет} = 15; 20$ и 25% (для каждой вероятности детектирования проведено по 10000 реализаций

моделирования). Результаты статистического моделирования в виде гистограмм плотности распределения контраста корреляционной картины при приёме М-последовательности с различной вероятностью детектирования отдельных бит показаны на рис. 3.

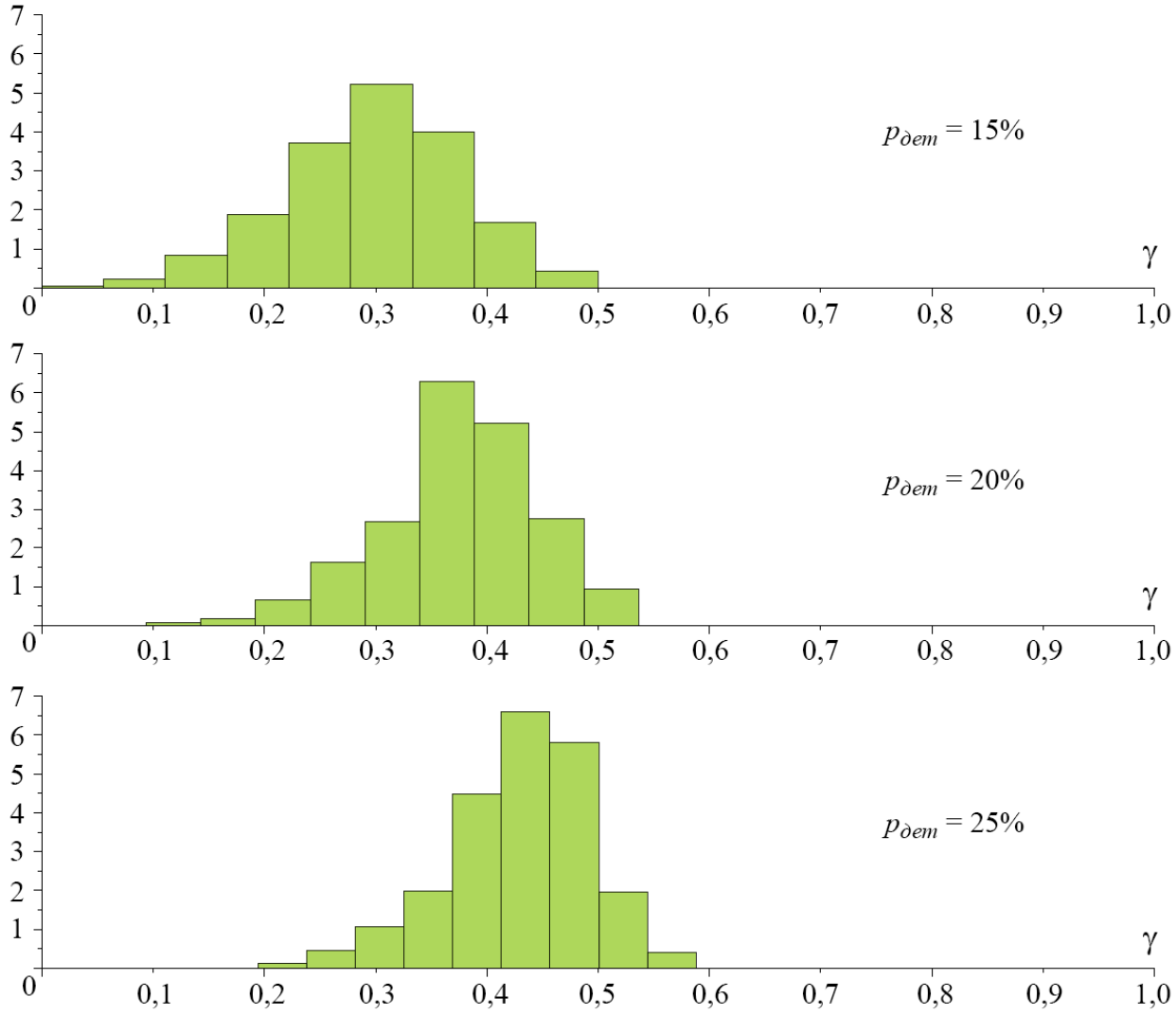

Рис. 3. Гистограммы плотности распределения контраста корреляционной картины при приёме М-последовательности с вероятностью детектирования отдельных бит $p_{дет} = 15; 20$ и 25%

В результате моделирования оценка математического ожидания контраста корреляционной картины при $p_{дет} = 15\%$ составила $\gamma_0 = 0{,}299$ (минимальное значение – $\gamma_{мин} = 0$, максимальное значение – $\gamma_{макс} = 0{,}500$, среднеквадратическое отклонение – $\gamma_{ско} = 0{,}0793$), при $p_{дет} = 20\%$ оценка

математического ожидания составила $\gamma_0 = 0{,}374$ ($\gamma_{мин} = 0{,}094$; $\gamma_{макс} = 0{,}537$; $\gamma_{ско} = 0{,}0706$), при $p_{дет} = 25\%$ – $\gamma_0 = 0{,}430$ ($\gamma_{мин} = 0{,}194$; $\gamma_{макс} = 0{,}588$; $\gamma_{ско} = 0{,}0638$).

Предложенному ранее критерию уверенного обнаружения пика взаимнокорреляционной функции $\gamma \geq 0{,}2$ при $p_{дет} = 15\%$ соответствуют около 88,6% реализаций моделирования, при $p_{дет} = 20\%$ – около 98,7% реализаций, при $p_{дет} = 25\%$ – около 99,9%.

Для снижения уровня ошибок в принимаемом сигнале возможно использовать М-последовательности большей длины либо применять предварительное кодирование информационного сообщения с использованием корректирующих кодов, позволяющих обнаруживать и исправлять ошибки в принятом сигнале.

Заключение

Результаты проведённого статистического моделирования подтвердили возможность использования в системах квантовой связи псевдослучайных последовательностей для кодирования символов передаваемой информации. Показано, что путём вычисления на приёмной стороне взаимнокорреляционной функции между продетектированным с заданной вероятностью потоком бит и исходной М-последовательностью, которой кодируются символы логической «1», возможно выделение информационной составляющей сигнала. Например, при вероятности детектирования одиночных фотонов $p_{дет} = 20\%$ пиковое значение взаимнокорреляционной функции для М-последовательности из 255 бит в среднем более чем в 2 раза превышало уровень боковых лепестков (оценка математического ожидания контраста корреляционной картины (1) на 10000 реализациях моделирования равна $\gamma_0 = 0{,}374$). Для обеспечения возможности работы в более сложных условиях (меньшая вероятность детектирования фотонов, наличие темновых шумов фотодетектора и остаточных импульсов) необходимо переходить к

использованию М–последовательностей большей длины и, при необходимости, применять дополнительные корректирующие коды.

Литература

1. Shapiro J.H. The Quantum Theory of Optical Communications// IEEE Journal of Selected Topics in Quantum Electronics. – 2009. – №6. – vol.15. – pp.1547-1569.
2. Кулик С.П. Квантовая криптография [Текст]// Фотоника.– 2010. – № 2. – С.36-41; Фотоника. – 2010. – №3. – С.56-59; Фотоника. – 2010. – №4. – С.28-35.
3. Румянцев К.Е., Розова Я.С.Патентно-лицензионная ситуация в области квантовой криптографии [Текст] // Электротехнические и информационные комплексы и системы. – 2011. – №1. – Т.7. – С.58-64.
4. Pinto A.N., Silva N.A., Almeida A.J., Muga, N.J. Using quantum technologies to improve fiber optic communication systems // IEEE Communications Magazine. – 2013. – №8. – vol.51. – pp.42-48.
5. LongG.L., Wang C.,DengF.-G., Wang W.-Y. From Quantum Key Distribution to Quantum Secure Direct Communication// CLEO/Pacific Rim 2007. Conference on Lasers and Electro-Optics, Pacific Rim, 26-31 Aug. 2007. – 2007. – vol. – pp.1-2.
6. Маро Е.А. Алгебраический анализ стойкости криптографических систем защиты информации [Электронный ресурс] // Инженерный вестник Дона,2013, №4. – Режим доступа: http://ivdon.ru/magazine/archive/n4y2013/1996 (доступ свободный). – Загл. с экрана. – Яз. рус.
7. Farr W.H. Overview of single photon detection technologies// 2012 IEEE Photonics Conference (IPC), 23-27 Sept. 2012. – 2012. – pp.20-21.
8. Соколова Т.В., Горбунов А.В. Регистрация слабых оптических сигналов в защищённых волоконно-оптических системах передачи информации [Текст]// Международная научно-техническая и научно-

методическая интернет-конференции в режиме off-line «Проблемы современной системотехники», 1-30 октября 2009 г. – Таганрог: Изд-во ТТИ ЮФУ, 2009. – С.153-159.

9. Id201 seriessingle-photondetectorforthenearinfrared. – URL: http://www.idquantique.com/images/stories/PDF/id201-single-photon-counter/id201-specs.pdf.

10. Id210 advancedsystemforsinglephotondetection. – URL: http://www.idquantique.com/images/stories/PDF/id210-single-photon-counter/id210-specs.pdf.

11. Варакин Л.Е. Системы связи с шумоподобными сигналами [Текст]. – М.: Радио и связь, 1985. − 384 с.

12. Никонов В.И., Никонова Г.С. Применение корреляционных кодов для систем синхронизации и связи [Текст] // Техника радиосвязи. – 2008. – №13. – С.87-90.

13. Петелин Ю.В., Ковалев М.А., Макаров А.А. Перспективы использования сигнально-кодовых конструкций типа троичных М-последовательностей в спутниковых каналах связи [Текст] // Информационно-управляющие системы. – 2006. – №5. – С.32-35.

14. Бабенко М.Г., Вершкова Н.Н., Кучеров Н.Н., Кучуков В.А. Разработка генератора псевдослучайных чисел на точках эллиптической кривой [Электронный ресурс] // Инженерный вестник Дона, 2012, №4. – Режим доступа: http://ivdon.ru/magazine/archive/n4p2y2012/1408 (доступ свободный). – Загл. с экрана. – Яз. рус.