Сама процедура аутентификации осуществляется через внутренний инструмент аутентификации, с момента запуска которого прецедентов взлома зафиксировано не было, что говорит о его надежности в контексте обеспечения безопасности. До настоящего времени персональные данные пользователя передавались на сервер в открытом виде, поэтому оставалась вероятность перехвата данных в момент аутентификации, например, если пользователь находился в одной беспроводной сети со злоумышленником.

Для решения задач безопасности системы «3Ducation» было решено использовать протокол шифрования SSL (англ. secure sockets layer), который позволяет шифровать данные на стороне сервера и клиента и в момент передачи обеспечивать их сохранность. Это является наиболее эффективным с точки зрения уровня обеспечения безопасности и затрат: в случае перехвата зашифрованных данных они уже не будут представлять для злоумышленника никакой ценности, так как расшифровка информации займет большое количество времени и средств.

С учетом того, что система «3Ducation» размещена на сервере СГАУ (virtual.itschool.ssau.ru), для ее защиты был использован сертификат класса 3, которым обладает СГАУ как юридическое лицо и который используется на всех поддоменах ssau.ru, это позволило избежать дополнительных издержек при обслуживании (оплата, предоставление необходимый данных и т.д.).

Для создания сертификата безопасности использовался инструмент OpenSSL, позволяющий создавать сертификат в формате *.pfx – представляющий из себя пару файлов из файла сертификата *.crt и файла закрытого ключа *.key. Установка сертификата безопасности производилась на веб-сервере IIS (англ. internet information services), работающем под управлением операционной системы Windows Server R2 2008.

После установки сертификата безопасности была проведена проверка корректности работы сервера: с помощью программы Wireshark был произведён перехват трафика во время аутентификации и работы клиента с игровой обучающей системой «3Ducation». Экспериментально было подтверждено, что информация, которой обменивается клиент и сервер, не представляет никакой ценности: без наличия закрытого ключа сертификата, хранящегося на сервере, расшифровка информации, в которой могут содержаться помимо технической информации: логин, пароль и другие личные данные, невозможна.

Таким образом, была реализована защита персональных данных пользователей системы «3Ducation» во время их передачи. В дальнейшем будут рассмотрены другие виды неявных угроз и целенаправленные виды атак с целью взлома и получения данных на стороне сервера. По результатам комплексного аудита безопасности системы планируется установка необходимых инструментов защиты, а также составление плана автоматического и запланированного аудита безопасности обучающей системы «3Ducation».

Литература

1. Как обеспечить безопасность веб-приложений? [Электронный ресурс]. – URL: http://internetno.net/category/obzoryi/mnenie/kak-obespechit-bezopasnost-veb-prilozhenijj/ (дата обращения 20.03.2016 г.).

2. Григорьев, А.О. Разработка пользовательского интерфейса виртуальной обучающей системы «3Ducation» [Текст]//Труды Всероссийской научно-технической конференции «Актуальные проблемы радиоэлектроники и телекоммуникаций». – Самара: изд-во СГАУ, 2014. – С. 145-148.

С.А. Бурлов

КОДИРОВАНИЕ С ПРОВЕРКОЙ НА ЧЕТНОСТЬ СВЕТОВОГО ПУЧКА ЛАГЕРРА-ГАУССА, НЕСУЩЕГО ОРБИТАЛЬНЫЙ УГЛОВОЙ МОМЕНТ

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

Введение. С конца XX века активно ведутся разработки квантового канала связи, использующего орбитальный угловой момент пучка фотонов для существенного повышения емкости канала связи. За разработками канала связи активно следуют разработки криптографических протоколов [2], [3]. По большей части они представляют собой модифицированную версию криптографического протокола *BB-84* с применением двух различных базисов: орбитально-углового, сформированного на состояниях мод с «чистым» показателем, и углового, описанного как суперпозиция определенного числа базовых состояний.

Работа [4] описывает Венский эксперимент по передаче сквозь сильно турбулентную атмосферу информации посредством суперпозиции световых пучков, противоположных по показателю орбитального углового момента. В эксперименте участвовала нейронная сеть, обеспечивающая детектирование сигнала, принимаемого на специальный экран. В процессе передачи информации неизбежно возникают искажения, которые приводят к ошибкам распознавания переданного значения.

Основной целью данной работы ставится рассмотрение возможности осуществления специального кодирования с проверкой на четность передаваемого сигнала для обеспечения информирования приемника о возможном искажении, полученном в процессе передачи.

Известно [1, 6], что пучки Лагерра-Гаусса можно получить из пучков Эрмита-Гаусса путем применения схемы, отраженной на рисунке 1. Пара цилиндрических линз переводит моду Эрмита-Гаусса с показателями (m, p) в моду Лагерра-Гаусса с показателями (m, p). На рисунке 2 отражены примеры профилей интенсивностей пучков Лагерра-Гаусса [5].

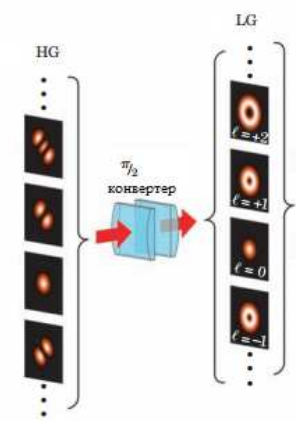

Рис. 1. Схема преобразования пучка Эрмита-Гаусса в пучок Лагерра-Гаусса.

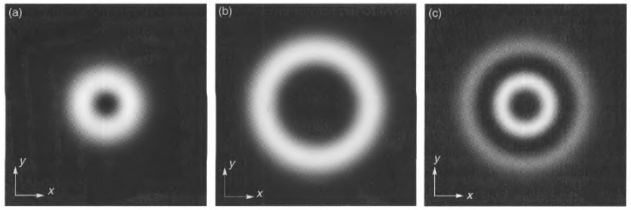

Рис. 2. Профили интенсивности пучков Лагерра-Гаусса. (a) $m = 1$, $p = 0$. (b) $m = 5$, $p = 0$. (c) $m = 2$, $p = 1$.

Первичная идея распознавания ошибок, возникающих в процессе передачи информации по каналу связи, была определена достаточно давно – это алгоритмы проверки на четность, так называемые *контрольные суммы*. В связи с тем, что компьютеры работают с двоичным представлением данных, схема проверки на четность передаваемого пакета, стала самым простым, быстрым и распространенным механизмом обеспечения проверки на возникновение ошибки. В пакет из k бит встраивается дополнительный бит, который является двоичной суммой всех бит в пакете и весь расширенный пакет передается после кодера получателю. Получатель, принимая пакет, извлекает информационные разряды, проверочный бит и проводит манипуляции по декодированию.

Результаты. В данной работе предложены несколько потенциальных схем применения методов контрольных сумм (проверки на четность).

Первая схема кодирования заключается в использовании служебных сигналов с показателем орбитального углового момента 0 или 1 после передачи информационного пакета, содержащего один показатель. Этот способ эффективно реализуем на практике, однако за счет передачи отдельного пакета – моды, теряется скорость передачи информации и, соответственно, информационная емкость установленного канала связи.

Несколько схем можно объединить в отдельный подтип: они подразумевают в каждый передаваемый пучок встраивать дополнительную информацию. Если вспомнить, что при формировании моды Лагерра-Гаусса из моды Эрмита-Гаусса, применяя пучок с дополнительны показателем $p = 1$ (рис. 2), новая мода получит дополнительное световое кольцо. При передачи нечетного показателя орбитального углового момента подразумевается использование моды HG_m^1 для генерации носителя, а при передачи четного показателя – HG_m^0.

Еще один способ встроить служебную информацию можно условившись передавать информацию только в положительных показателях орбитального углового момента. Таким образом, можно использовать для контрольной битовой суммы четного показателя – положительный знак, а для нечетного - отрицательный.

Формирование новой моды происходит с помощью численно рассчитанных голограмм, что в свою очередь позволяет использовать быстрый способ смены значения. Для генерации пучка с отрицательным значением можно воспользоваться призмой Дове.

Нужно отдать должное, что данный способ кодирования имеет свои сложности при детектировании: кроме увеличения времени, есть еще и технические ограничения, накладываемые на распознавание *двухколечного* пучка Лагерра-Гаусса.

Литература

1. Методы анализа и синтеза когерентных световых полей / В. Г. Волостников . – М. : Физматлит, 2014 . – 256 с.

2. R. W. Boyd, A. K. Jha, M. Malik, C. O’Sullivan, B. Rodenburg, and D. J. Gauthier, “Quantum key distribution in a high-dimensional state space: exploiting the transverse degree of freedom of the photon,” Proc of SPIE p. 79480L (2011).

3. M. Mirhosseini et al., “High-dimensional quantum cryptography with twisted light,” New J. Phys., vol. 17, no. 3, 2015, Art. ID. 033033.

4. M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, A. Zeilinger, “Communication with spatially modulated light through turbulent air across Vienna”, New Journal of Physics, vol. 16, 2014.

5. Götte, J. B. and S. M. Barnett. "Light beams carrying orbital angular momentum", *The Angular Momentum of Light*. Ed. David L. Andrews and Mohamed Babiker. 1st ed. Cambridge: Cambridge University Press, 2012. pp. 1-30.

6. Padgett M., Courtial J., Allen L., Light’s Orbital Angular Momentum. – Physics Today Online 57, 5, 35 (2004).