Инженерный вестник Дона, №5 (2020)
ivdon.ru/ru/magazine/archive/n5y2020/6438

Построение многоканальной системы квантового распределения ключей с частотным кодированием

И.М. Габдулхаков[1,2], О.Г. Морозов[2]

[1]ПАО "Таттелеком", Казань
[2]Казанский национальный исследовательский технический университет им. А. Н. Туполева - КАИ

Аннотация: В данной работе мы предлагаем вариант построения многоканальной системы квантового распределения ключей с частотным кодированием, основанной на электрооптической схеме системы квантового распределения ключей (далее КРК)с парами амплитудного модулятора и фазового модулятора на стороне Алисы, и парами фазового модулятора и амплитудного модулятора на стороне Боба (далее АМФМ-ФМАМ), с использованием Comb-генератора, мультиплексора и демультиплексора для образования множества параллельных квантовых подканалов.
Ключевые слова: квантовая криптография, квантовое распределение ключей; частотное кодирование, электрооптическая модуляция фотона, амплитудно-фазовая тандемная модуляция.

На сегодняшний день квантовые сети связи дают самую высокую гарантию криптографической защиты передаваемых данных [1-3]. Но скорость передачи квантовых ключей по оптическим линиям связи остается существенно низкой. Для решения данной проблемы, мы предлагаем создание многоканальной системы КРК с частотным кодированием [4-6].

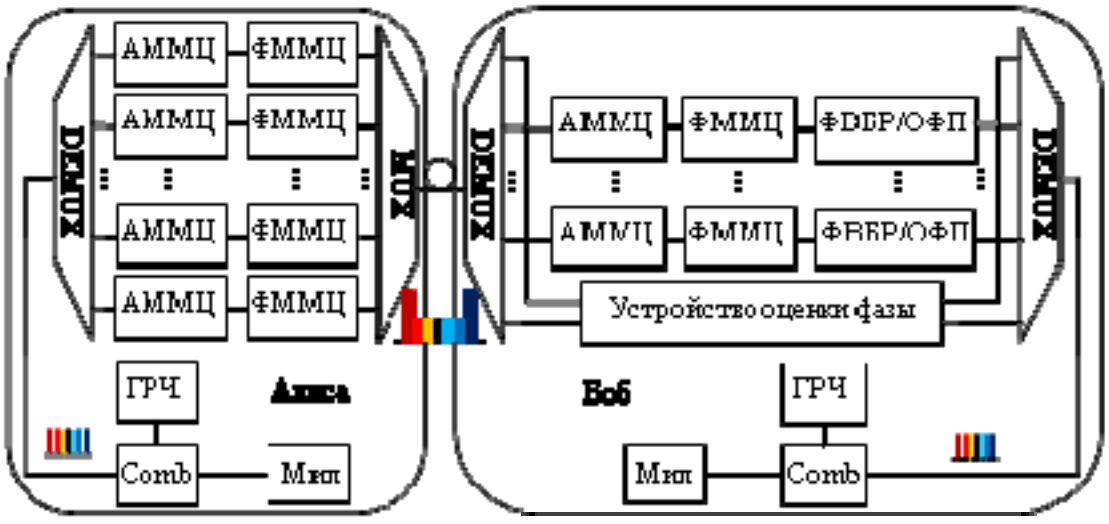


Рис. 1. Структурная схема многоканальной системы КРК

При многоканальной схеме общая скорость передачи секретного ключа может быть выражена как сумма скорости каждого подканала:

$$V_{общ} = \sum_{k} V_k, \quad (1)$$

где k – это количество квантовых подканалов.

Алиса генерирует оптические частотные гребенки с центральной частотой f_0 и частотой повторения f_s в качестве многоволнового источника, который может быть выражен как:

$$\Im(t) = \sum_{n=n_{min}}^{n_{max}} \hat{a}_n \exp\{j[\varphi(t) + 2\pi f_n t]\}, \quad (2)$$

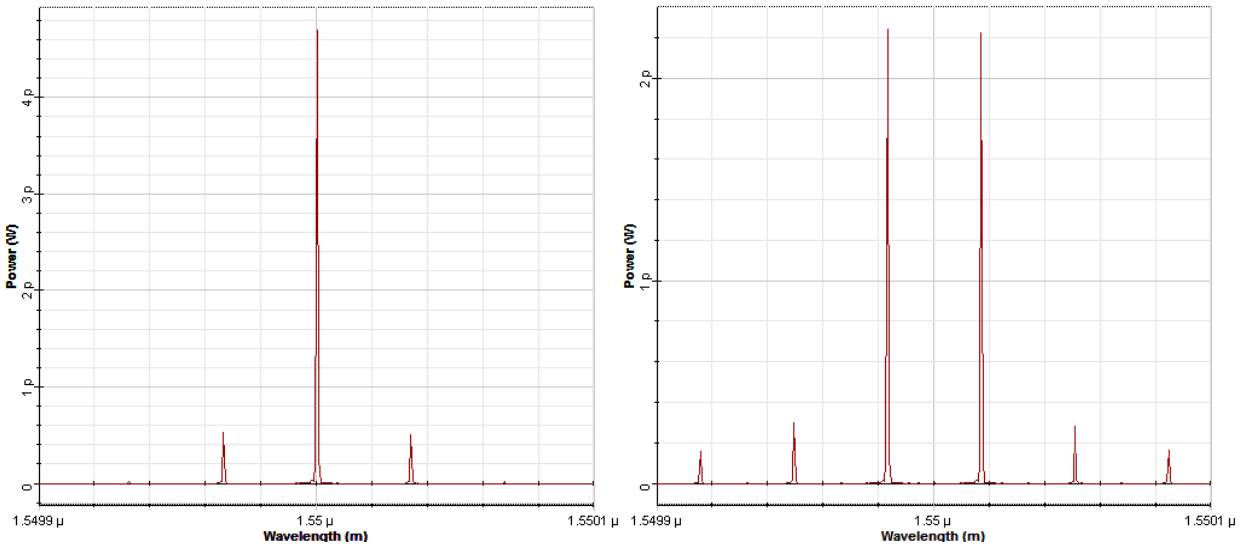
где - $\hat{a}_n$ безразмерный комплексный оператор амплитуды, соответствующий режиму, представляющий в n-ых гребенчатых линиях с частотой $f_n = f_0 + nf_r$. $\varphi(t)$ случайная функция представляет собой фазовый шум в гребне, n_{max} и n_{min} обозначает две крайние внешние линии оптические частотные гребенки [7].

Оптические частотные гребенки сначала проходят через демультиплексор для формирования N подканалов, где количество подканалов равно количеству гребенчатых линий [8]. Подканал k, который изменяется от n_{min}+ 1 до n_{max}-1, независимо модулируются амплитудным модулятором, помощью V_k, с последующей фазовой коммутацией с помощью Φ_k. После этого все подканалы объединяются частотным мультиплексором и передаются Бобу.

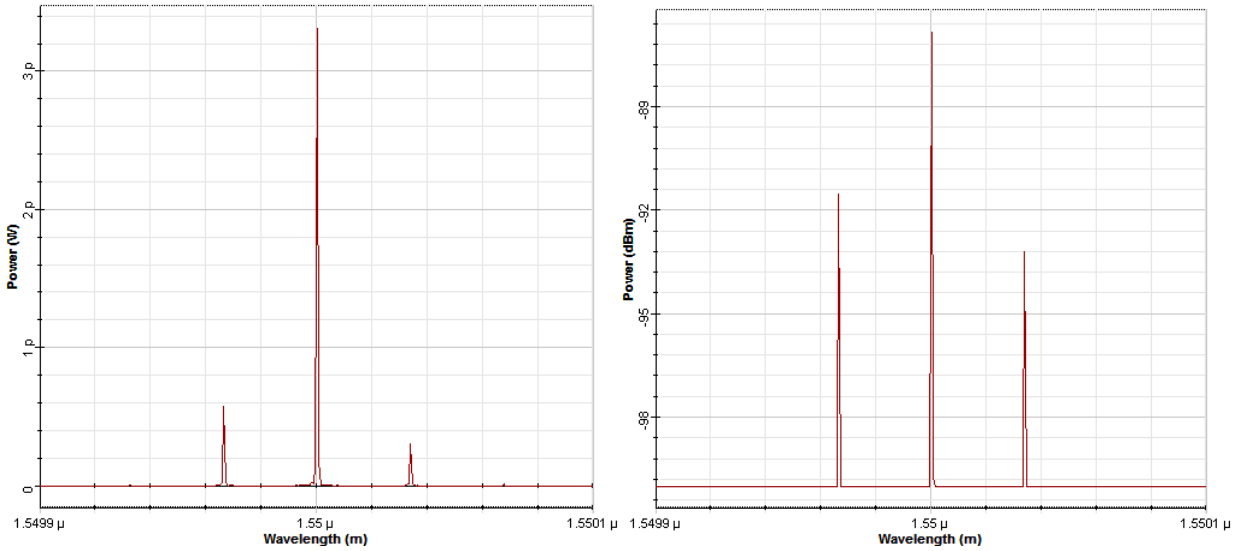
Неопределенное смещение фазы происходит во время передачи по квантовому каналу, вызывая фазовую декорреляцию между двумя сторонами.

После приема многочастотного сигнала, отправленного Алисой, Боб использует демультиплексор частоты, чтобы разделить полученный оптические частотные гребенки и локально генерирует гребни N на своем comb-генераторе с теми же параметрами что и Алиса [9]. Тогда крайние две пилотные линии сигнала гребенка и соответствующие линии гетеродина выбираются и отправляются на устройство оценки фазы. Оставшиеся пары сигнальных линий и локально генерированные линии направляются на детекторы для обнаружения факта получения фотонов. Фазовые модуляторы на стороне Боба используются, чтобы выбрать другую основу в разных подканалах, для восстановления несущей сигнала. Элементом фильтрации сигнала являются волоконные брэгговские решетки [10].

Варианты конструктивной АМ интерференции показаны на рис. 2 в случае конструктивной ФК.



а *б*



в *г*

Рис. 2. – Варианты конструктивной интерференции при совпадении параметров амплитудной модуляции (далее АМ) и фазовой коммутации (далее ФК) на стороне Алисы и Боба для каждого канала: результаты АМ (а) и ФК (б) на выходе модуляторов на стороне Алисы, результаты ФК (в) и АМ (г) на выходе модуляторов на стороне Боба.

В каждом цикле распределения ключей квантовый сигнал в k-й гребенчатой линии может быть выражен как когерентное состояние $|a_k\rangle = |X_k + iP_k\rangle$, где X_k и P_k оба распределены как $N(0, V_a)$. Опорный сигнал в контрольной линии r также находится в когерентном состоянии $|a_r\rangle = |X_r + iP_r\rangle$, чьи квадратурные значения раскрываются. Амплитуда $|a_r|$ пилотной линии фиксирована и может быть в несколько раз больше чем амплитуда $|a_k|$ квантового сигнала, но гораздо меньше, чем локально сгенерированный Бобом. Боб может оценить фазовый сдвиг θ между пилотной линии и соответствующей локально сгенерированной линией с

использованием общедоступных квадратур (X_{TA}, P_{TA}) и измеренных квадратур (X_{TB}, P_{TB}), что удовлетворяет ограничениям

$$\begin{pmatrix} X_{TB} \\ P_{TB} \end{pmatrix} = \begin{pmatrix} cos\hat{\theta}_T & -sin\hat{\theta}_T \\ sin\hat{\theta}_T & cos\hat{\theta}_T \end{pmatrix} \begin{pmatrix} X_{TA} \\ P_{TA} \end{pmatrix}, \quad (3)$$

сдвиг фазы θ_T может быть получен как:

$$\hat{\theta}_T = tan^{-1}\left(\frac{P_{TB}X_{TA} - X_{TB}P_{TA}}{X_{TB}X_{TA} + P_{TB}P_{TA}}\right), \quad (4)$$

Поскольку для передачи опорных сигналов выбраны два крайних подканала, мы можем получить $\theta_{n_{max}}$ и $\theta_{n_{min}}$ через формулу (3). Из-за фазовой согласованности оптических частотных гребенок, зная фазу смещение двух пилотных линий, мы можем получить сдвиг фазы в k-м квантовом подканале, как

$$\hat{\theta}_k = \hat{\theta}_{n_{min}} + \frac{k - n_{min}}{n_{max} + n_{min}}\left(\hat{\theta}_{n_{max}} - \hat{\theta}_{n_{min}}\right), \quad (5)$$

Наконец, Алиса может корректировать фазовый сдвиг в каждом подканале, корректируя свои значения (X_{kA}, P_{kA}) с θ_k, чтобы получить оценочные значения измерения Боба, заданные как:

$$\begin{pmatrix} X_{kB} \\ P_{kB} \end{pmatrix} = \begin{pmatrix} cos\hat{\theta}_k & -sin\hat{\theta}_k \\ sin\hat{\theta}_k & k \end{pmatrix} \begin{pmatrix} X_{kA} \\ P_{kA} \end{pmatrix}, \quad (6)$$

Большинство экспериментальных установок квантовой криптографии и коммерческих продуктов используют ослабленный лазерный источник как источник квантовых состояний со средней вероятностью однофотонного излучения за период («среднее число фотонов») около $\mu \approx 0.1$ [11]. В этом случае условие безопасности больше не является строгим из-за пуассоновского распределения фотонов когерентного света: некоторые

импульсы или несущая, или поднесущая могут содержать более одного фотона. Этот факт может быть легко использован Евой (нелегальный абонент). Она успешно может выполнять не обнаруживаемое разделение пучка PNS без изменения коэффициент квантовых ошибок (Quantum Bit Error Rate, далее QBER) и получать часть ключа, которая может быть значительной при более высоких значениях μ.

Данный метод увеличивает безопасность передачи за счет исключения несущей из структуры сигнала, передаваемого по квантовому каналу распределения ключей и разбиение информации о ключе на множество каналов. Таким образом, для получения положительного результата Еве необходимо получить информацию о передаваемом сигнале в каждом подканале одновременно, поскольку квадратурная информация каждого подканала не зависит друг от друга.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90057

Funding: The reported study was funded by RFBR, project number 19-37-90057

Литература

1. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Lütkenhaus N., Peev M. The security of practical quantum key distribution // Reviews of modern physics. 2009. Vol. 81. Pp. 1301-1310.

2. Muller A, Breguet J, Gisin N. Experimental demonstration of quantum cryptography using polarized photons in optical ibre over more than 1 km. Europhysics Leters. 1993. Pp. 383-388.

3. Zbinden H, Gautier JD, Gisin N, Hutner B, Muller A, Titel W. Interferometry with Faraday mirrors for quantum cryptography. Electronics Leters. 1997. Pp. 586-588.

4. Inoue K, Waks E, Yamamoto Y. Diferential phase shift quantum key distribution. Physical Review Leters. 2002. Pp. 037902-037904

5. Durafourg L, Merolla J-M, Goedgebuer J-P, Mazurenko Y, Rhodes WT. Compact transmission system using single-sideband modulation of light for quantum cryptography. Optics Leters. 2001. 26(18) Pp. 1427-1429.

6. Dixon AR, Yuan ZL, Dynes JF, Sharpe AW, Shields AJ. Gigaherz decoy quantum key distribution with 1 Mbit/s secure key rate. Optics Express. 2008. Pp. 18790-18799.

7. Габдулхаков И.М., Морозов О.Г., Исламов А.Р. Многоканальная система квантового распределения ключей с частотным кодированием // Материалы XVII Международной научно-технической конференции. «Оптические технологии в телекоммуникациях ОТТ-2019». Казань: Издательство КНИТУ-КАИ, 2019. С. 269-271.

8. Yijun Wang, Yiyu Mao, Wenti Huang, Duan Huang, and Ying Guo. Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution Optics Express. 2019. Vol. 27, No. 18 25314-25329

9. Морозов О.Г., Ильин Г.И., Морозов Г.А., Нуреев И.И., Фасхутдинов Л.М. Модуляционные методы формирования спектрально чистого

двухканального полигармонического излучения с одинаковой разностной частотой и поляризационным мультиплексированием. Постановка задачи // Инженерный вестник Дона, 2017, №4. URL: ivdon.ru/ru/magazine/archive/n4y2017/4587.

10. Морозов О.Г., Мисбахов Рус.Ш., Мисбахов Рин.Ш. и др. Волоконные брэгговские решетки с двумя фазовыми сдвигами как чувствительный элемент и инструмент мультиплексирования сенсорных сетей // Инженерный вестник Дона, 2017, №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4343

11. Lundberg L., Karlsson M., Lorences-Riesgo A., Mazur M., Schröder J., and Andrekson P. Appl. Sci. 8(5), 718. 2018.

References

1. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Lütkenhaus N., Peev M. Reviews of modern physics. 2009. Vol. 81. Pp. 1301-1310.

2. Muller A, Breguet J, Gisin N. Europhysics Leters. 1993. Pp. 383-388.

3. Zbinden H, Gautier JD, Gisin N, Hutner B, Muller A, Titel W. Electronics Leters. 1997. Pp. 586-588.

4. Inoue K, Waks E, Yamamoto Y. Physical Review Leters. 2002. Pp. 037902-037904

5. Durafourg L, Merolla J-M, Goedgebuer J-P, Mazurenko Y, Rhodes WT. Optics Leters. 2001. 26(18) Pp. 1427-1429.

6. Dixon AR, Yuan ZL, Dynes JF, Sharpe AW, Shields A.J. Optics Express. 2008. Pp. 18790-18799.

7. Gabdulhakov I.M., Morozov O.G., Islamov A.R. Materialy XVII Mezhdunarodnoj nauchno-tehnicheskoj konferencii. «Opticheskie tehnologii v telekommunikacijah OTT-2019». [Materials of the XVII International scientific and technical conference. "Optical technologies in telecommunications OTT-2019"]. Kazan: 2019. Pp. 269-271.

8. Yijun Wang, Yiyu Mao, Wenti Huang, Duan Huang, and Ying Guo. Optics Express. 2019. Vol. 27, No. 18 25314-25329

9. Morozov O.G., et al. Inzhenernyj vestnik Dona, 2017, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2017/4587.

10. Morozov O.G., et al. Inzhenernyj vestnik Dona, 2017, № 3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4343

11. Lundberg L., Karlsson M., Lorences-Riesgo A., Mazur M., Schröder J., and Andrekson P. Appl. Sci. 8(5), 718. 2018.