УДК 621. 396. 67

М.А. ОМАРОВ, д-р. техн. наук, Р. И. ЦЕХМИСТРО, канд. физ.-мат. наук

ДИСПЕРСИОННОЕ ОГРАНИЧЕНИЕ ДЛИНЫ ЛИНИИ ПЕРЕДАЧИ В КВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ СВЯЗИ С ПОЛЯРИЗАЦИОННЫМ КОДИРОВАНИЕМ

Введение

Со времени появления первых сообщений о реализации передачи квантового ключа связи, фундаментально защищенного от декодирования, на расстояние 30 *см* в воздухе в лабораторных условиях до первой коммерческой криптографической оптической линии передачи (более 100 *км*) прошло менее 20 лет [1-10]. Однако, несмотря на использование протокола передачи ключа B92 и интенсивные работы по созданию источников и приемников однофотонных импульсов света и криогенных фотодетекторов, уменьшающих возможные помехи в приеме сообщений, существуют проблемы промышленного внедрения данных линий связи.

В первой практической квантовой линии связи использовалось стандартное многомодовое оптическое волокно, главное требование, которое предъявлялось к ней, состояло в сохранении поляризации фотонов (квантов) на всем пути следования от приемника к передатчику [2]. Повышение стабильности передачи квантового ключа сопровождалось усложнением схемы квантовой криптосистемы, например схема, представленная на рис. 1, имеет четыре лазерных излучателя (LD1-LD4) и три расчепителя поляризации (BS) в отличие от одного излучателя и разделителя поляризации в первой экспериментальной схеме Беннета и Брассарда [2]. В передатчике присутствует также ослабляющий фильтр – F, который в отличие от первой лабораторной схемы используется для уменьшения количества фотонов, приходящихся на один импульс. Приемник фотонов в данной схеме позволяет восстанавливать исходную поляризацию фотонов путем использования полуволновых пластин, поляризационных расщепителей (PBS) и четырьмя счетчиками фотонов (APD).

Схема, представленная на рис. 1, позволила обеспечить связь на 23 *км* при использовании фотонов с длиной волны 1300 *нм* [3].

Применение фазового кодирования бит позволяет снять ограничения, связанные с изменением поляризации в оптическом волокне, увеличивая тем самым дальность линии передачи [8-10]. Однако данные системы криптографической связи требуют наличия интерферометра Маха-Цендера и WDM-мультиплексоров, синхронизирующих работу диодов, регистрирующих фотоны, что неизбежно приводит к удорожанию данных систем.

Трудность в реализации данной схемы состоит в том, что несбалансированность интерферометров приемника и передатчика должна быть стабильной в пределах долей длин волн во время передачи ключа. Данное обстоятельство требует использования термостабилизированных контейнеров, необходимо также обеспечивать компенсацию дрейфа фазы и контроль поляризации в интерферометрах [11]. Все это приводит к существенному усложнению установки, хотя позволяет обеспечить дальность передачи ключа до 120 *км*, что осуществила компания MagiQ в первой коммерческой квантовой линии связи [10].

В данной работе проведена оценка задержки распространения сигнала вносимой внутримодовой и нулевой дисперсией современных оптических волокон, используемых в системах передачи на малые расстояния, в сравнении с интервалом когерентности полупроводниковых излучателей. Даны рекомендации по оптимальному использованию оптических волокон и лазеров в практических квантовых криптографических системах передачи с поляризационным кодированием.

Постановка задачи

Существуют две основные технологические проблемы, связанные с ростом:

– длины линии передачи;

– скорости передачи ключа.

Существуют также практические трудности создания надежных источников и приемников одиночных фотонов. Данные обстоятельства дают основание полагать, что системы (рис. 1) с реализованным протоколом передачи B92 могут представлять практическую значимость для организации относительно недорогой фундаментально защищенной линии связи [2-3].

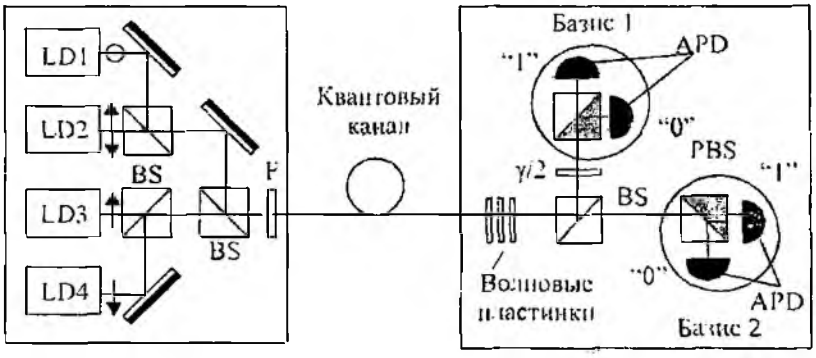

Рис.1

Использование вместо стандартного оптического волокна волокна с сохранением поляризации позволяет увеличить длину участка с контролируемой поляризацией.

Цель данной работы – оценка допустимой длины систем передачи с поляризационным кодированием путем анализа ограничений, вызванных дисперсией современных оптических волокон в сравнении с интервалом когерентности полупроводниковых лазеров на GaAs и светодиодов на основе InGaAsP, которые выпускаются промышленностью. Использование более дешевых промышленно выпускаемых оптических волокон возможно, однако коммерческое применение таких устройств будет затруднено из-за ограниченности длины передачи.

Поляризационная модовая дисперсия может изменить поляризацию фотонов, если вносимая ею задержка больше времени когерентности, что ограничивает используемые типы лазеров. Известно, что в одномодовом оптическом волокне распространяется одна мода HE_{11} (LP_{01}) и $\sigma = \sigma_{вн}$, т.е. уширение импульса определяется дисперсией материала и волноводной дисперсией:

$$\sigma_{вн} = 2\pi \frac{\sigma_\lambda L}{\lambda^2 c}\left|\frac{d^2\beta}{d\kappa^2}\right|, \qquad (1)$$

где $\sigma_\lambda = 0{,}1{-}4$ *нм* – среднеквадратичная длина спектральной линии источника; β – продольная постоянная распространения моды HE_{11}; $\kappa = 2\pi/\lambda$ – волновой вектор; L – длина участка передачи; c – скорость света [4] . Данное соотношение описывает дисперсию материала, волноводную дисперсию и дисперсию профиля показателя преломления.

В одномодовом режиме, при взаимной компенсации дисперсии материала и волноводной дисперсии, необходимо учитывать поляризационную дисперсию, вызванную различием групповых скоростей взаимоортогональных квазивырожденных поляризаций (HE^x_{11}, HE^y_{11}) основной моды. Если групповая скорость моды

$$V_{гр} = \frac{c}{\left|\frac{d^2\beta_{lm}}{d\kappa^2}\right|}, \qquad (2)$$

(β_{lm} – продольная постоянная распространения мод), то отрезок длиной L *км* мода проходит за время $L/V_{гр}$. Для получения численных значений задержки, вызванной поляризационной дисперсией, необходимо знать характеристики материала, профиль показателя преломления сердцевины и оболочки для построения дисперсионных кривых мод HE^x_{11}, HE^y_{11}. Для оценки диапазона значений дисперсии одномодового волокна можем воспользоваться имеющимися зависимостями уширения импульса в одномодовом оптическом волокне от длины волны для ступенчатого профиля показателя преломления.

Для когерентных ВОЛС требуются однополяризационные одномодовые световоды (ОС) В круглом одномодовом ВС основная мода может существовать в двух ортогональных поляризациях HE^{x}_{11}, HE^{y}_{11}. Абсолютно однополяризационным является ВС с аксиально-несимметричным распределением ПП (показателя преломления) в сердцевине. По обе стороны от области с ПП n_1 располагаются области с профилем показателя преломления n_p, причем $n_1 > n_2 > n_p$, где n_2 – профиль показателя преломления оболочки. На практике данные световоды получили название ВС с боковыми впадинами и с боковыми туннелями, однако частотный диапазон данных волокон ограничен.

В оптических световодах с линейным двулучепреломлением разность постоянных распространения двух поляризаций моды HE_{11} можно увеличить либо изменением формы поперечного сечения сердцевины или оболочки, например с эллиптической. Главный и вспомогательный диапазоны эллиптического поперечного сечения световода равны 0,85 и 2,14 *мкм*.

В строгих расчетах на длине волны нулевой дисперсии необходимо учитывать дисперсионные эффекты второго порядка.

Длина когерентности оптических излучателей соответствует расстоянию, в пределах которого сохраняется постоянной разность фаз излученных волн, т.е. она является длиной цуга и имеет связь с шириной спектра источника.

Современные одномодовые оптические волокна имеют следующие интересующие нас параметры:

– затухание на длине волны 1310 *нм* – 0,35 *dB/км* (при 1550 *нм* – 0,21 *dB/км*);

– коэффициент хроматической дисперсии при длине волны 1310 *нм* $\leq$ 3 *пс/нм км* (при 1550 *нм.* $\leq$ 22 *пс/нм км.*);.

– длину волны нулевой дисперсии 1302-1322 *нм* [11].

Сравнивая время, при котором разность фаз излученных лазером волн постоянна (время когерентности), с задержкой вносимой дисперсией одномодовых оптических волокон на конкретном расстоянии, можно вычислить дистанцию оптического канала связи, т.е. подобрать такое расстояние при котором оба времени будут равны друг другу.

Интервал когерентности связан с временем когерентности следующим соотношением:

$$\ell_K = c\tau_K, \tag{3}$$

здесь c – скорость света в свободном пространстве.

Ширина спектра излучателя (лазера или светодиода) и время когерентности связаны соотношением

$$\Delta\omega \cdot \tau_K = 1, \tag{4}$$

т.е. зная спектральные характеристики современных лазеров с волноводным каналом и волноводным усилением, можно вычислить интервал когерентности и время, в течение которого сохраняется постоянной разность фаз излученных волн.

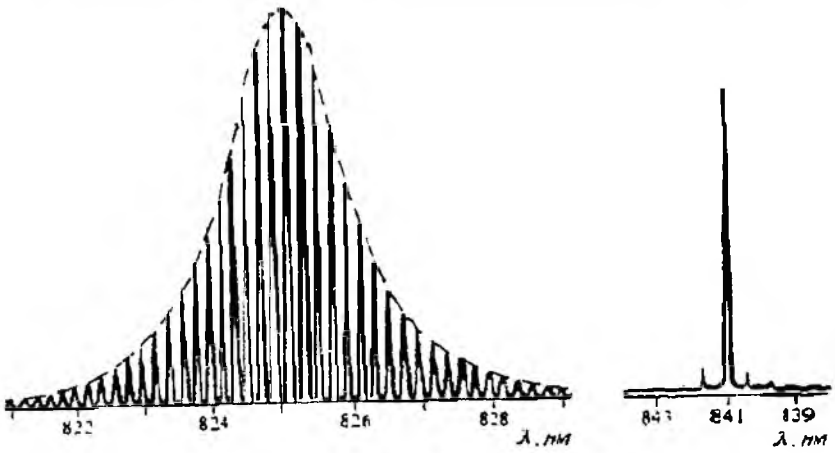

Рис. 2

На рис. 2 представлены спектральные характеристики GaAs/GaAlAs лазера (слева с волноводным усилением, справа с волноводным каналом) [5, 11]. Используя график, изображающий спектральную характеристику для лазера с волноводным усилением, и соотношения (3)-(4) можно установить, что интервал когерентности $l_к$ составил 54 *мкм*, т.е. $\tau_к = 0{,}18 * 10^{-12}$ *с*.

Для лазера с волноводным каналом интервал когерентности равен 1,1 *мкм* при $\Delta\lambda$= 0,1 *нм*, т.е. $\tau_к$= 3,6 *10^{-12} *с*. Хотя на практике ширину спектральной линии оценивают по измерению длины когерентности , известно, что ширина спектра отдельной моды лазеров данного типа не превышает 0,01 нм [5]. Интервал когерентности некоторых типов полупроводниковых лазеров может составить несколько метров. Зная дисперсионные характеристики, т.е. зависимости материальной дисперсии от длины волны при фиксированном значении радиуса сердцевины оптического волокна, легко определить расстояние, при котором временное уширение импульсов в световодах становится соизмеримым со временем когерентности указанных на рис. 2 лазеров.

На рис. 3 представлены спектральные характеристики светоизлучающих диодов:

– спектр диода на GaAs, легированного Si, представлен на графике слева ;

– спектры излучения диодов на основе InGaAsP трех различных составов, представлен на графике справа [12]. Воспользовавшись соотношениями (3-4) и данными, представленнями на графиках рис. 3, находим что $l_к$ диодов на основе InGaAsPсоставил 2,3 *мкм*, т.е. $\tau_к$= 76 *10^{-16} *с*. Данные диоды представляют большой практический интерес, поскольку работают в диапазоне длинн волн λ= 1300-1500 *нм*. Если использовать одномодовый световод с хроматической дисперсией $\sigma_{хр} \leq 3$ *нс/нм км*, то при использовании светодиодных излучателей на основе InGaAsP максимальная длина участка с неизменной поляризацией составит всего 2,5 *м*, при использовании волокна с нулевой (поляризационной дисперсией порядка σ = 1 *пс*) это расстояние равно уже 760 *м*.

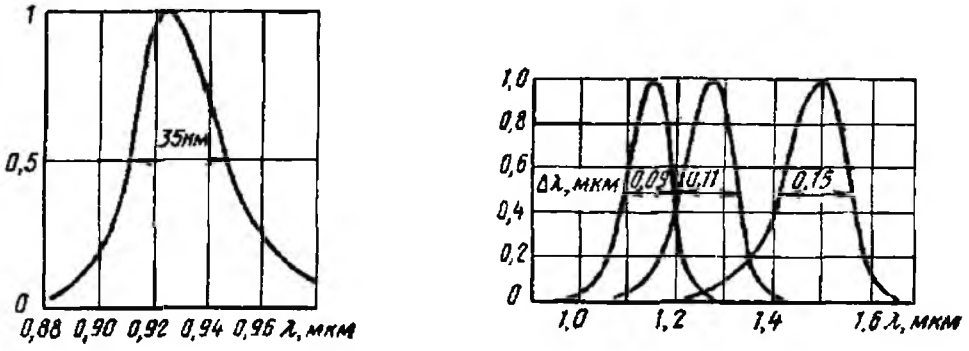

Рис. 3

Это обстоятельство наглядно демонстрирует возможность использования данных излучателей для организации локальных квантовых сетей при использовании одномодовых волокон с поляризационной дисперсией не более 10 *пс*. Если применять волокна с хроматической дисперсией, то для обеспечения приемлемых дистанций для локальной сети необходимо использовать лазер с волноводным усилением, например для лазера с волноводным усилением представленного на рис. 2 $L_{трассы}$= 1,8 *км*.

Для световодов из SiO_2 при длине волны 1300 *нм* значение материальной дисперсии D_m= 5 *нс/км*, для волокон на основе SiO_2 с добавлением 13% Be_2O_3 D_m= 17 *нс/км* [5]. В случае нулевой дисперсии, когда показатель степени параболического профиля показателя преломления волоконного световода близок к 2. среднеквадратичное уширение импульса составило σ = 0,01 *нс/км*. Расстояние, при котором временное запаздывание, вызванное дисперсионной задержкой (σ = 0,01 *нс/км*), сравняется с временем когерентности лазера с волноводным каналом, соответственно составило:

– $L_{трассы}$= 300 *м*. при $\tau_к$=3 *пс*;

– при $\tau_к$=3 *нс* $L_{трассы}$= 300 *км*.

Результат дает возможность использовать данную пару (лазер - оптоволокно) для организации связи на 20 *км* без использования оптических усилителей согласно стандарту IEEE

802.3ah (EPON), который создан на основе стандарта Ethernet и стандарта пассивных оптических сетей – PON (passive optical network) [13].

Выводы

Проведенный анализ позволил определить расстояние, в пределах которого возможна устойчивая передача квантового ключа методом поляризационного кодирования при использовании недорогих одномодовых и многомодовых градиентных оптических волокон. Использование лазеров с длиной когерентности излучения не менее 10^{-5} *мм* и многомодовых световодов с общей дисперсией порядка 3 *нс* позволяет создавать фундаментально защищенные от прослушивания локальные линии передачи.

Список литературы: 1. *Bennett C H., Brassard G.* Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conferenceon Computers, Systems and Signal Processing. 1984, P. 175-179. *2. Bennett C.H.* Quantum Cryptography Using Any Two Nonorthogonal States // Phys. Rev. Letters, Vol.68, 3121 (1992), p. 134-155. *3. Muler A.* Quantum cryptography over 23 km in installed under-lake telecom fibre // Europhysics Letters, 1996 vol. 33. p 234-246. 4. *С.В. Свечникова. Л.М. Андрушко* Справочник по волоконно-оптическим линиям связи. К.: Техника, 1988. 239с. 5. *Дж. Гауер.* Оптические системы связи. М: Радио и связь, 1989. 308с. 6. *Muler A.* Quantum cryptography over 23 km in installed under-lake telecom fibre // Europhysics Letters, 1996, vol. 33, p. 234-246. 7. *Gisin N.* Quantum Cryptography. Reviews of Modern Physics, 74, p. 145-195 (2002). 8. *Eliot Ch.* Quantum cryptography in practice // BBN Technology Preprint. 1, 2003. 9. *Hughes R.* Practical free-space quantum key distribution over 10 km. in daylight and at night. New J. Phys 4,43, 2002. p. 1012-1019. 10. *First* Commercial Quantum Cryptography System // www.magiqtech.com. 11. *K. Peterman, G. Arnold.* Noise and distortion of semiconductor lasers in optical fiber systems // IEEE Jnl. of Quantum Ets. QE -18, 1982. p.543-55. 12. *Wada O.* Perfomance and reliability of high radiance InGaAsP/ InP LEDs operating in 1,15-1,5 μm wavelength region // IEEE Jnl. of Quantum Ets. QE -18, 1982, p. 368-74. 13. *Р. Мищук* Пассивные оптические сети: знакомство с технологией // Сети и бизнес. Телекоммуникации и сети – технологии и рынок. 2006. 2 (27) С. 102-105.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 25.01.2008