Письма в ЖЭТФ, том 79, вып. 9, с. 554 – 559 © 2004 г. 10 мая

Мультиплексная квантовая криптографии с временным кодированием без интерферометров

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия

Факультет вычислительной математики и кибернетики Московского государственного университета им. М. В. Ломоносова 119899 Москва, Россия

Поступила в редакцию 3 марта 2004 г.

Описаны три принципиально новых экспериментальных прототипа оптоволоконных схем квантовой криптографии, которые существенно проще имеющихся, более устойчивы в работе, содержат меньшее число оптических оптоволоконных компонентов и не требуют подстройки во время генерации ключа. Данные криптосистемы естественно назвать квантовой криптографией на временных сдвигах. Данные схемы реализуют протокол B92 и используют в качестве информационных состояний пару неортогональных однофотонных квантовых состояний. Одна из схем не использует оптоволоконных интерферометров типа Маха–Цандера, что позволяет естественным образом реализовать мультиплексный режим передачи секретного ключа.

PACS: 03.67.Dt, 42.50.−p, 89.70.+c

Криптосистемы с одноразовыми ключами дают возможность создать абсолютно стойкие системы шифрования [1,2]. Квантовая криптография позволяет реализовать распространение секретного ключа между пространственно удаленными легитимными пользователями, которое гарантируется фундаментальными законами природы, а не ограниченными вычислительными или техническими возможностями подслушивателя [3,4]. Безусловная секретность квантовой криптографии в нерелятивистской области базируется, по сути, на принципе неопределенностей Гейзенберга. Более формально, на невозможности одновременного измерения наблюдаемых, которые описываются некоммутирующими операторами. В терминах пары векторов состояний квантовой системы, в которые кодируется классическая информация о ключе, это означает невозможность получения любой информации о передаваемых квантовых состояниях без их возмущения, если последние являются неортогональными [5]. Другим фундаментальным запретом квантовой механики, тесно связанным с предыдущим, является запрет на копирование заранее неизвестного квантового состояния [6]. На сегодняшний день уже создано несколько различных прототипов квантовых криптосистем на базе оптоволоконных линий связи [7]. Рекорд дальности передачи секретного ключа в квантовой криптосистеме с так называемой самокомпенсацией при помощи фарадеевских оптоволоконных отражателей на сегодняшний день принадлежит японской (100 км) [8] и швейцарской (67 км) [9] группам. Имеющиеся прототипы квантовых криптосистем используют, в основном, следующие принципы. 1) Информация о ключе кодируется в поляризационные степени свободы [10]. 2) Фазовое кодирование, когда используются интерферометр Маха–Цандера, и информация кодируется в разность фаз, которая набирается на приемном и передающем плечах интерферометра [11,12]. 3) Квантовые криптосистемы с частотной модуляцией несущей частоты [13]. 4) Квантовая криптография на когерентных состояниях с использованием гомодинного детектирования на приемном конце [14]. Наибольший прогресс достигнут в криптосистемах с фазовым кодированием и самокомпенсацией [8,9] с использованием фарадеевских отражетелей [15]. Апробирована первая локальная квантовая криптографическая сеть в Бостоне для распространения секретных ключей между пользователями на расстоянии в 10 км (проект выполняется по заказу DARPA – Defense Advanced Research Projects Agency) [16]. Существуют реализации прототипов квантовых криптосистем, осуществляющих передачу секретного ключа через открытое пространство [17,18]. Рекорд по дальности (из опубликованных данных [19]) составляет 23.4 км как в дневное, так и ночное время. Целью использования квантовых криптосистем (данное обстоятельство не скрывается в западных проектах) является генерация и передача секретных ключей через открытое пространство между наземными объектами и спутника-

[1)] e-mail: molotkov@issp.ac.ru

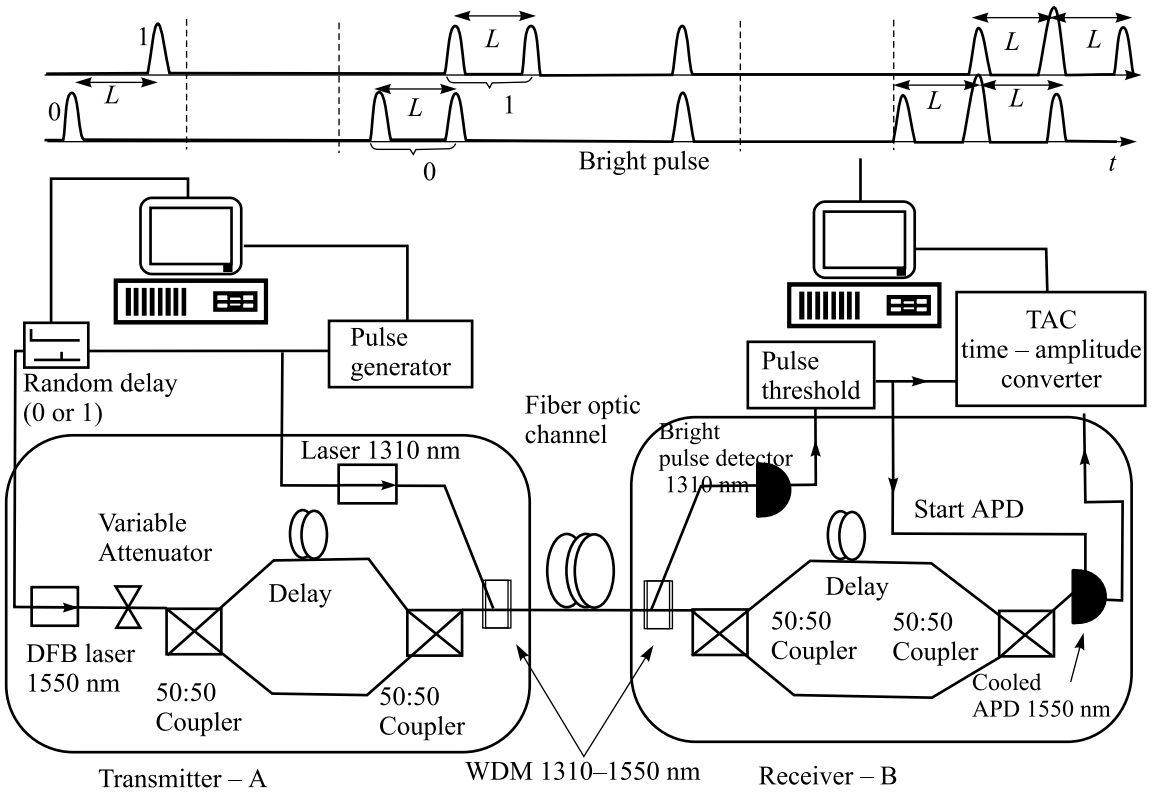

Рис.1. Блок-схема оптоволоконной квантовой криптосистемы на временных сдвигах: протокол B92

ми или между наземными объектами через спутники [17]. По оценкам разработчиков, это может быть осуществлено в ближайшие годы, поскольку существующий технологический уровень достаточен и планируемая цена является уже вполне приемлемой. Упомянутые криптосистемы, особенно схемы с фазовым кодированием и самокомпенсацией, достаточно сложны в реализации.

Опишем работу предлагаемой схемы (рис.1). Входные импульсы формируются схемой генератора импульсов, которая запускает одномодовый лазер с длиной волны 1310 нм. Данный лазер формирует синхронизирующий импульс в оптоволоконной линии, относительно которого происходит "привязка" по времени в каждой посылке однофотонных импульсов одномодового лазера с длиной волны 1550 нм (см. временну́ю диаграмму на рис.1). Данный лазер выдает в оптоволоконный канал связи, ослабленные до уровня $\sim$ 0.1 фотонов в среднем в импульсе информационного состояния. Схема задержки-выбора 0 или 1 запускается тактовым генератором и формирует импульсы для запуска лазера на 1550 нм, сдвинутые по времени относительно синхронизующего импульса с длиной волны 1310 нм. Величина сдвига по времени состояний 0 и 1 равна разности времен прохождения длинного и короткого путей в передающем плече интерферометра (см. рис.1). Затем состояние поступает на вход оптоволоконного 50/50 светоделителя. Разные длины оптических путей приводят к формированию "двухпичкового" состояния (суперпозиции двух "половинок" однофотонного состояния, сдвинутых за счет разности оптических путей в плече интерферометра). После второго светоделителя двухпичковое состояние направляется в канал связи вслед за синхронизирующим импульсом от лазера с длиной волны 1310 нм. Синхроимпульс в каждой посылке поступает первым в канал связи и от него отсчитывается время в каждой посылке. Данный импульс является классическим (многофотонным) и поступает на фотодетектор, который запускает пороговую схему. Пороговая схема требуется для того, чтобы не было ложных случайных срабатываний схемы запуска генератора в схеме TAC (конвертора время-амплитуда, Time-Amplitude-Converter). После прихода синхроимпульса и запуска пороговой схемы "запускается" однофотонный детектор (APD). Детектор работает в ждущем режиме (гейгеровской моде счета фотонов). Для уменьшения вероятности темновых отсчетов на детектор подается напря-

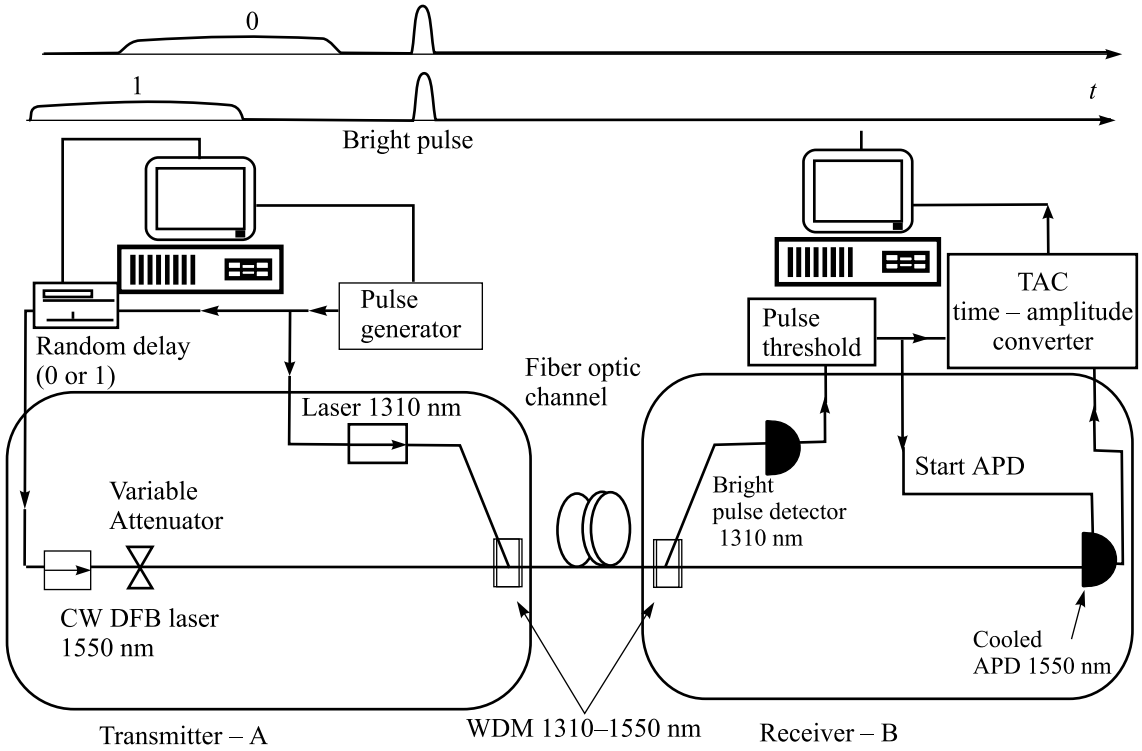

Рис.2. Блок-схема оптоволоконной квантовой криптосистемы на временных сдвигах без интерферометров: протокол B92

жение обратного смещения к моменту прихода информационных импульсов. После детектирования информационного импульса сигнал с APD поступает на конвертер время-амплитуда, который фиксирует время срабатывания APD. Соответственно, время срабатывания APD позволяет отличить состояние для 0 и 1 (см. выше). По времени регистрации существуют области однозначного различения состояний (conclusive result) для 0 и 1 (естественно, с вероятностью, меньшей единицы, из-за неортогональности состояний) и области неоднозначного различения (inconclusive result) (см. временную диаграмму на рис.1)

Приведем некоторые числовые оценки для параметров системы. В данной схеме не требуется очень точной балансировки плеч интерферометра на приемном и передающем концах. Поскольку исходно длительность импульса (l) $l \ll L$ (L – величина раздвижки – разность длинного и короткого путей (верхнего и нижнего) в плечах интерферометра), то не требуется идеально точной балансировки плеч между передающим и приемным концами интерферометра. Иначе говоря, “половинки” состояния на приемном конце не обязательно точно должны “собираться” в состояние, локализованное во временном окне l, лишь бы раздвижка за счет разной длины плеч на приемном и передающем концах не превышала L, чтобы еще можно было отличать 0 от 1 в соответствующих временных окнах. Например, если длительность входного импульса составляет $l \sim 1$ нс, то раздвижка “половинок” $T \sim 10$ нс. Данная раздвижка возникает за счет разности длин длинного и короткого путей в плече интерферометра на передающем конце, которая в пересчете на разницу путей в оптоволокне дает $L = T(c/n) = 200$ см ($n = 1.42$ – показатель преломления оптоволокна). На приемном конце для сведения двух половинок вместе требуется такая же разность длин плеч с точностью порядка длительности отдельной половинки, что составляет в пересчете на длину $l \sim 20$ см.

Поскольку в схеме на временных сдвигах фазовые соотношения не используются, а используется лишь факт их перекрытия, то для обеспечения перекрытия *можно даже вообще не использовать интерферометр, что является дальнейшим и радикальным упрощением.*

Схемы на рис.2,3 также используют идею временного кодирования. Разница по сравнению с предыдущей состоит только в выборе информационных состояний. Генератор тактовых импульсов запускает лазер с длиной волны 1310 нм и длительностью импульса l. Со случайной задержкой, выбираемой из

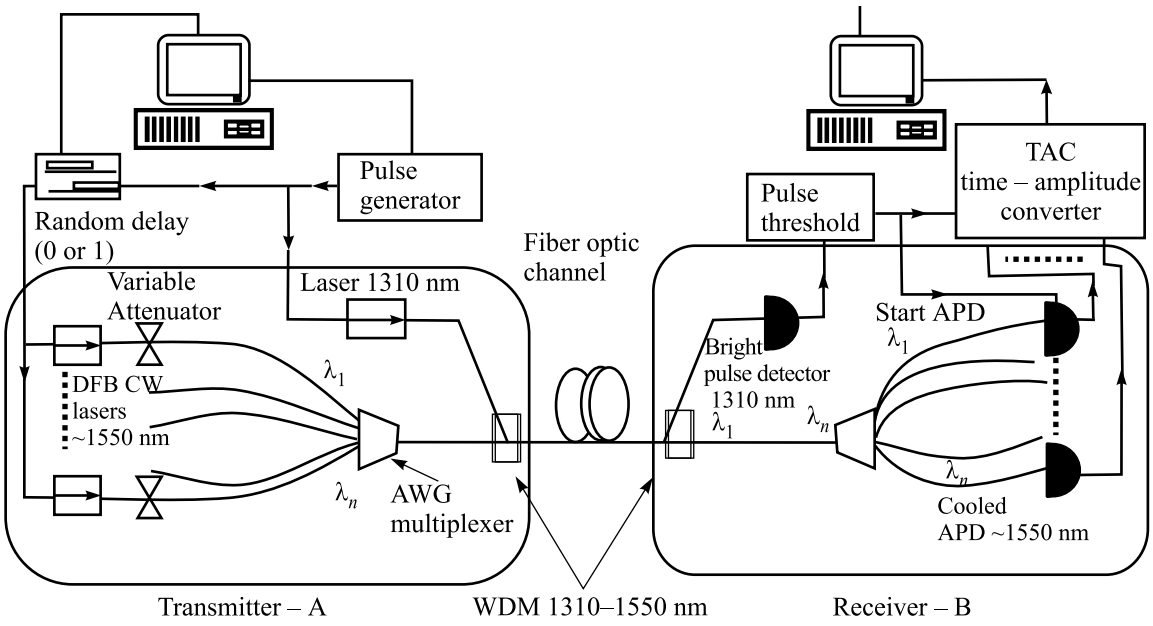

Рис.3. Блок-схема мультиплексной оптоволоконной квантовой криптосистемы на временных сдвигах: протокол B92

двух значений, запускается CW лазер с длиной волны 1550 нм. Грубо говоря, CW лазер – это источник, который либо постоянно включен и имеет на выходе заданное значение мощности, либо почти включен (находится чуть ниже порога генерации). При непосредственной модуляции приложение "ступеньки" дополнительного напряжения к CW лазеру длительностью $L \gg l$ приводит к появлению сигнала в оптоволоконной линии связи (см. временную диаграмму рис.2). Таким образом, приложение "ступеньки" напряжения к CW лазеру, сдвинутой в разных посылках относительно синхроимпульса, приводит к появлению в канале связи пары неортогональных (перекрывающихся) состояний (см. рис.2). В хороших CW лазерах с квантовыми ямами ширина линии может достигать сотен kHz. Для наших целей достаточно длительности информационного состояния, например, в 20 нс (соответственно, достаточно ширины линии излучения CW лазера в $\sim 10^7$ Hz). Не имеет смысла выбирать длительность информационных состояний слишком большой, поскольку требуется в течении этого времени держать APD обратно смещенным, что увеличивает вероятность паразитных темновых отсчетов.

Работа блок-схемы аналогична предыдущему. Тактовый генератор через схему формирования запускает лазер на 1310 nm, который выдает короткий синхроимпульс. Одновременно запускается схема выборки для информационных состояний, которая в зависимости от состояния генератора случайных чисел (0 или 1), формирует управляющий токовый импульс сдвинутый относительно синхроимпульса на разную задержку. На приемном конце с приходом синхроимпульса срабатывает пороговая схема, которая синхронизирует запуск конвертора время-амплитуда и прикладывает обратное смещение на APD детектор. Момент срабатывания APD через TAC-конвертер записывается в память.

Данная схема допускает естественное обобщение на мультиплексный случай с разделением каналов по длинам волн. На рис.3 приведена блок схема мультиплексной криптосистемы, принцип работы которой аналогичен предыдущей схеме. Единственное изменение связано с введением в схему маршрутизатора (дифракционной решетки на массиве волноводов), изготовленного по AWG технологии, которая позволяет "свести" на передающем конце в один оптоволоконный кабель, а на приемном "развести" по разным каналам состояния с различными длинами волн.

Проведем краткий сравнительный анализ на примере двух оптоволоконных схем квантовой криптографии, основанных на принципе фазового кодирования. Именно на таких схемах на сегодняшний день в мире достигнуты рекорды по дальности. Главное преимущество данной схемы по сравнению со схемой на фазовом кодировании, когда информация кодируется в разность фаз, по сути, *в разность разности длин плеч интерферометров на передающем и приемном концах*, состоит в том, что точность такой разности должна составлять доли длины волны, т.е. *раз-*

ность разности длин плеч интерферометра на расстоянии в несколько десятков километров должна быть доли микрона, иначе схема просто не будет работать. Из-за высоких требований к точности в разности хода неизбежно приходится использовать поляризационный контроль, что также усложняет схему и снижает быстродействие. Двояколучепреломление, ответственное за разную скорость распространения излучения с разными компонентами поляризации, приводит к паразитному фазовому набегу. Такой набег приводит к тому, что схема с фазовым кодированием становится неработоспособной на больших расстояниях, если не производить компенсацию данного набега. Для устранения этого паразитного эффекта используют дополнительные фарадеевские отражатели. Сравнение проводится со схемой с фазовым кодированием и самокомпенсацией при помощи фарадеевских отражателей. Рекорды по дальности в квантовых криптографических системах достигнуты в схемах с самокомпенсацией при помощи фарадеевских отражателей. Данные схемы, кроме упомянутых выше тонких моментов при реализации, содержат дополнительные оптоволоконные компоненты. При помощи фарадеевских отражателей решается проблема с двояколучепреломлением. Паразитный набег фазы для различных компонент поляризации при распространении от передающего к приемному концу компенсируется при обратном проходе. Упомянутые выше требования к точности юстировки плеч сохраняются и здесь. Схема может работать на больших расстояниях (вплоть до 100 км, как это было продемонстрировано японской группой) за счет устранения паразитных эффектов двояколучепреломления. Однако двухпроходность схемы приводит к большей чувствительности схемы к затуханию, поскольку вдвое удлиняет эффективную длину оптоволокна при том же физическом расстоянии, на которую осуществляется передача ключа. Поэтому данная схема является более сложной и дорогостоящей, чем предыдущая схема с фазовым кодированием без самокомпенсации. Еще один недостаток системы квантовой криптографии с самокомпенсацией при помощи фарадеевских зеркал состоит в ее более слабой криптостойкости относительно специфической атаки типа “троянский конь”.

Отметим, что схемы с фазовым кодированием не допускают простого обобщения на мультиплексный случай, поскольку набег разности фаз будет различным для разных длин волн. Таким образом, обсуждаемые выше схемы прототипов квантовой криптографии по сравнению с существующими обладают, на наш взгляд, рядом принципиальных преимуществ:

- Простота оптоволоконного интерферометра (рис.1), не требующего точной (до долей микрона) балансировки плеч и постоянной юстировки во время работы. Не требуется электроники для управления оптическими фазовыми модуляторами в плечах интерферометра.

- Схемы с временным кодированием могут быть сконструированы даже без использования оптоволоконных интерферометров типа Маха-Цандера (рис.2,3). Схемы без интерферометров допускают естественное расширение на мультиплексный режим, что позволяет увеличить скорость передачи ключа за счет увеличения частотных каналов и позволяет использовать криптосистему в локальных сетях, когда каждому получателю отвечает своя длина волны.

- Поскольку не требуется термостабилизация и юстировка плеч интерферометра во время работы, то скорость генерации ключа выше, чем в схемах с фазовым кодированием.

- Схема является однопроходной, что позволяет, из-за меньших потерь в оптоволокне, увеличить длину оптоволоконного квантового канала связи.

Выражаю благодарность М. И. Беловолову, А. В. Королькову, М. И. Лебедеву, А. Н. Пенину, М. В. Чеховой за полезные обсуждения. Работа поддержана Академией Криптографии Российской Федерации, а также проектом Российского фонда фундаментальных исследований (# 02-02-16289).

1. В. А. Котельников, Отчет (1941).
2. C. E. Shannon, Bell Syst. Tech. Jour. **28**, 658 (1949).
3. S. Wiesner, SIGACT News **15**, 78 (1983).
4. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December, 1984, p. 175.
5. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
6. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
7. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).
8. H. Kosaka, A. Tomita, Y. Nambu et al., quant-ph/0306066.
9. D. Stucki, N. Gisin, O. Guinnard et al., quant-ph/0203118.

10. A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993); A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995); A. Muller, H. Zbinden, andN. Gisin, Europhys. Lett. **33**, 335 (1996).
11. Ch. Marand and P. D. Tounsend, Optics Lett. **20**, 1695 (1995); P. D. Tounsend, Nature **385**, 47 (1997); IEEE Photonics Tech. Lett. **10**, 1048 (1998).
12. R. Hughes, G. G. Luther, G. L. Morgan, and C. Simmons, Lecture Notes in Computer Science **1109**, 329 (1996); R. Hughes, G. Morgan, and C. Peterson, J. Mod. Opt. **47**, 533 (2000).
13. P. C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. **20**, 1062 (1995); Y. Mazurenko, R. Giust, and J. P. Goedgebuer, Optics Commun. **133**, 87 (1997).
14. F. Grosshans, G. Van Assche, J. Wenger et al., Nature **421**, 238 (2003).
15. M. Martinelli, Opt. Commun. **72**, 341 (1989); J. Mod. Opt. **39**, 451 (1992).
16. C. Elliot, D. Pearson, and G. Troxel, *Quntum Cryptography in Practice*, quant-ph/0307049 (2003).
17. J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, *Ground to Satellite Secure Key Exchange using Quantum Cryptography*, New J. Phys. 4, 82.1 (2002).
18. R. J. Huges, J. E. Nordholt, D. Derkas, and C. G. Peterson, *Practical Free-Space Quantum Key Distribution over 10 km in Daylight and at Night*, quant-ph/0206092 (2002).
19. C. Kurtsiefera, P. Zarda, M. Halder et al., *Long Distance Free Space Quantum Cryptography*, preprint (2002).