第 59 卷 第 4 期 2010 年 4 月
1000-3290/2010/59(04)/2493-05

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 4, April, 2010

基于单光子的单向量子安全通信协议*

权东晓† 裴昌幸 刘 丹 赵 楠

(西安电子科技大学综合业务网理论及关键技术国家重点实验室,西安 710071)

(2009 年 7 月 11 日收到;2009 年 7 月 30 日收到修改稿)

提出了基于单光子的单向量子安全通信方案. 发送方在对信息序列进行编码操作之前首先将其和随机序列进行异或操作并插入校验序列. 接收方收到光子后对其进行延迟,此后发送方公布编码基从而使接收方在正确的基下进行测量. 接着双方通过校验序列判断信道的安全性,如果信道安全,则发送方公布接收方有测量结果的位置所对应的随机序列,接收方由此恢复出信息序列;如果信道不安全,窃听者所获得的只是随机的发送序列,信息序列仍然是安全的. 此协议与双向通信协议相比具有传输效率高、易于实现等优点.

关键词: 量子密码, 量子安全通信, 单光子, 单向通信

PACC: 4250, 4230Q, 0365

1. 引 言

自从 Bennett 和 Brassard 在 1984 年提出第一个量子密钥分发协议[1](BB84)以来,量子通信得到了快速的发展. 量子通信主要包括量子密钥分发[1—8](quantum key distribution, QKD),量子秘密共享[9—11](quantum secret sharing, QSS)和量子安全直接通信[12—21](quantum secure direct communication, QSDC). 通过 QKD 可以在发送端和接收端协商出无条件安全的量子密钥,从而利用此密钥对信息进行一次一密加密,就可以通过经典信道进行安全的通信. 通过 QSS 可以在量子场景下实现经典的秘密共享,可以在共享者之间共享经典信息和量子信息.

QSDC 是量子通信的一个新的分支,它可以直接安全地传输信息,而不需要先产生密钥,然后再对信息进行加密[22]. 2002 年, Bostrom 和 Felbinger 借鉴量子密集编码[23]的思想提出了"ping-pong"协议[12],利用纠缠对作为信息载体,但是这只是一个准安全的量子安全直接通信方案[24,25]. 2003 年,邓富国等利用块传输的思想,提出了基于纠缠对的两步 QSDC 方案[13]和基于单光子的 QSDC 方案[14]. 王川等利用量子密集编码的思想提出了高维度 QSDC 方案[15]. 朱爱东等提出了基于顺序重排的 QSDC 协议[16],李熙涵等指出此协议对木马攻击是不安全的,并进行了改进[17]. 王剑等提出了基于单光子顺序重排的 QSDC 协议[18]和多方控制的 QSDC 协议[19]. 最近利用 χ 型纠缠态的 QSDC 协议[20]、利用身份认证来提高 QSDC 安全性的协议[21]等分别被提出.

量子安全通信的另一个分支是 DSQC[26—29](deterministic secure quantum communication),接收者不能直接从测量结果中读出秘密信息,而是必须收到发送者传来的经典信息后才能够读出秘密信息. Beige 等[26]提出了基于单光子的 DSQC 方案,高亭等[27]、满钟晓等[28]分别提出了基于纠缠交换的 DSQC 方案. 李熙涵等提出了基于纯纠缠态的 DSQC 和基于任意 d 维单光子的单向 DSQC[29]. 虽然 DSQC 要交换大量的经典信息,但是在确定信道安全以后就不需要传递携带信息的量子比特了,在有噪声的情况下适应性更好.

本文提出了基于单光子的单向量子安全通信方案,在对信息序列进行编码操作之前首先将其和随机序列进行异或操作并插入校验序列,接收方对光子进行延迟后可以顺序对光子进行测量. 分析表明此协议能够保证信息序列的安全性,并且具有传输效率高、易于实现等优点.

* 国家自然科学基金(批准号:60572147, 60672119)、高等学校学科创新引智计划(批准号:B08038)和国家重点实验室专项基金(批准号:ISN02080002, ISN090307)资助的课题.

† E-mail: dxquan@xidian.edu.cn

2. 基于单光子的单向量子安全通信协议

假设 Alice 要和 Bob 通信,其通信过程描述如下:

1)Alice 利用随机数产生器产生随机序列,并将随机序列与信息序列进行按位异或操作,构成准发送序列.

2)Alice 在准发送序列中插入部分随机比特,这些随机比特称为校验序列,准发送序列和校验序列构成发送序列.

3)Alice 根据发送序列,随机地选择 Z 基和 X 基按下述规则进行编码. Z 基:$|H\rangle = 0$,$|V\rangle = 1$,X 基:$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = 0$,$|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) = 1$,并将这些光子序列发送给 Bob.

4)Bob 收到光子后对其进行简单延时. Alice 在确定 Bob 收到光子序列后,公布发送序列的编码基,Bob 在相应的测量基下进行测量,得到结果序列.

5)Alice 公布校验序列的位置,Bob 公布这些位置的测量结果,Alice 通过错误率判断是否存在攻击. 如果错误率高于门限值,则终止通信,此时 Eve 得到的只是没有任何意义的发送序列;如果信道安全,则进入下一步.

6)Bob 公布他在哪些位置收到了光子,Alice 公布这些位置对应的随机序列的数值,Bob 通过异或操作恢复出信息序列. 注意在此过程中,仅公布 Bob 有测量结果的位置的随机数值. 这样即使 Eve 截取了部分光子,并在步骤 4 公布的测量基下进行了正确地测量,但是由于她不知道对应位置的随机数值,仍然不能够得到有用信息.

此协议信息序列和检验序列的编码基可以同时公布,这是因为在此之前对信息序列进行了加密,即使信道不安全,窃听者得到的也只是密文. 因此只需要对光子进行简单的延迟,确保公布编码基后窃听者不能再对光子进行操作就可以了,并不需要先测量某些位置的光子判断信道的安全性. 所以对接收端的存储能力要求低,易于实现. 本协议虽然编码基序列是即时公布的,但需要在通过校验序列确定一块信息传输期间信道的安全性后再公布之前采用的随机序列,仍然体现了邓富国等提出的块传输的思想.

由于随机序列、编码基和校验序列的位置在通信过程中是公布的,因此每次通信都要选用新的随机序列和编码基序列并改变校验序列的位置,在安全性分析中进行具体说明. 虽然协议中传输的是 4 个不同状态的光子,但每个光子只能代表 1 bit 的信息,因为在通信过程中需要公布编码基,否则会带来信息泄漏.

可以看出,本文所提协议与邓富国等[5]提出的基于延迟的 BB84 协议,李熙涵等[29]提出的基于任意 d 维单光子的量子安全通信协议和经典密码通信都具有相似之处. 与延迟的 BB84 协议的区别在于 BB84 协议传输的不是有用信息,对安全性要求低,所要做到的是如果有窃听存在,通过后续的分析能够发现,放弃本次通信就可以了. 如果直接把文献[5]的方案应用到量子安全通信中,则窃听者只要在 Z 基下窃听就可以获得大部分信息. 虽然通过后续检测能够发现窃听者的存在,但此时已经造成了信息的泄露. 因此本文方案在编码操作之前的异或操作是必不可少的,是保证协议安全性的必要步骤. 文献[5]中的方法由于大部分量子态在 Z 基下制备,因此在公布测量基时公布的经典信息较少,这是此方案的优点. 在本文所提的方案中,可以在步骤 3 中,对信息序列均在 Z 基编码,对校验序列随机的选择在 Z 基或 X 基编码,这样在步骤 4 中就可以只公布在 X 基编码的光子位置,减少公布的经典信息.

本文所提协议与李熙涵等提出的基于任意 d 维单光子的量子安全通信协议[29]相比,在 2 维情况下此协议的随机序列相当于 Li 中随机准备的初始状态,此协议的异或操作相当于 Li 的 U 操作;在多维($d>2$)情况下文献[29]的效率较高. 不同之处在于公布编码基的顺序,文献[29]是在确定信道安全之后才公布信息序列的初始状态的,因此需要先挑选出某些位置的光子进行测量. 本协议的测量基是顺序公布的,不需要先挑选出某些位置的光子进行测量,更易于实现. 另外,在步骤 6 中 Alice 只公布 Bob 有探测结果的位置对应的随机序列,这样能够保证如果 Eve 截取了部分光子并在正确的测量基下进行了测量,但是由于她不知道随机数值仍然不能得到有用信息.

本文所提协议与经典通信的不同在于经典通信需要通信双方在通信之前已经具备密钥,但此协

议的加密信息在确定信道安全之后是完全公布的，信息的安全性是由量子测不准原理和不可克隆原理来保证的.

3. 安全性分析

在本协议的步骤 3 光子从 Alice 到 Bob 的传输过程中，通常存在的攻击包括：测量重发攻击、辅助粒子攻击、拒绝服务攻击和木马攻击等.

简单的测量重发攻击是指窃听者 Eve 随机地选择测量基对光子进行测量，然后根据测量结果再制备光子发送给接收方. 如果她选择的测量基正确，则完全可以得到信息；如果选择的测量基不正确，则以 50% 的概率得到正确的结果. 也就是说如果测量者随机地选择两种测量基，则这种攻击将会带来 25% 的错误率，必然会被检测过程发现.

假定 $|\phi\rangle$ 和 $|\varphi\rangle$ 是非正交的量子状态，辅助粒子攻击是指 Eve 将会使用一个辅助粒子结合一个幺正演化，对 $|\phi\rangle$ 和 $|\varphi\rangle$ 进行识别. 假设演化过程没有扰动量子态 $|\phi\rangle$ 和 $|\varphi\rangle$，即

$$U|\phi\rangle|e\rangle = |\phi\rangle|e_0\rangle, \tag{1}$$

$$U|\varphi\rangle|e\rangle = |\varphi\rangle|e_1\rangle, \tag{2}$$

其中，U 是幺正算子，$|e\rangle$ 是辅助粒子的初始状态，$|e_0\rangle$ 和 $|e_1\rangle$ 是演化后辅助粒子的状态. 因为幺正变化保持内积不变，因此得到

$$\langle\phi|\varphi\rangle\langle e_0|e_1\rangle = \langle\phi|\varphi\rangle\langle e|e\rangle, \tag{3}$$

由于 $|\phi\rangle$ 和 $|\varphi\rangle$ 非正交，于是必有

$$\langle e_0|e_1\rangle = \langle e|e\rangle = 1, \tag{4}$$

这说明 $|e_0\rangle$ 和 $|e_1\rangle$ 必然相同. 因此 Eve 为区分 $|\phi\rangle$ 和 $|\varphi\rangle$，必然不可避免地要干扰至少其中的一个状态，必然会在检测过程中发现错误，从而发现该攻击.

拒绝服务攻击是指 Eve 只是对光子进行随机的操作来破坏传输的信息，她自己并不试图获取任何信息. 这种攻击扰乱了光子的状态，通过检测过程也是可以发现该攻击的.

此协议虽然能够识别测量重发攻击、辅助粒子攻击和拒绝服务攻击，但是每次通信都要重新选择随机序列，改变检测序列的位置，并重新随机选择编码基进行编码. 每次都要选择新的随机序列，这样才能够保证如果窃听者窃取了密文，她不能用别的随机序列恢复出信息序列；而她的窃听会被检测过程发现，因而本次通信的随机序列不会公布，从而保证了安全性. 每次都要改变检测序列的位置，否则 Eve 可以转发检测序列，截取其余的光子并发送虚假光子给 Bob，从而能够顺利地通过检测，在公布随机序列后恢复出信息序列. 每次都要改变编码基，否则 Eve 能够在正确的测量基下进行测量并不带来错误，从而不被发现.

木马攻击存在于双向通信协议中，主要包括不可见光子木马攻击[30]和时间延迟木马攻击[17]. 不可见光子木马攻击是指 Eve 在光子到达发送者之前插入与光子同步但波长不同的光子；时间延迟木马攻击是指 Eve 在光子到达发送者之前插入与光子时间稍微不同（仍然在操作门限时间以内）但波长相同的光子. 如果发送者对接收到的光子没有进行检测，则发送者在编码的时候就会对木马光子进行相同的操作. Eve 在编码之后再分离出木马光子，通过对木马光子的测量就可以得知发送者的信息. U 操作通常是与波长相关的，所以通过不可见光子木马攻击会带来错误，当插入的光子的波长和通信采用的波长几乎一致时，也可以以概率 1 得到信息；由于延迟木马攻击插入的光子波长和通信采用的波长一致，因此通过延迟木马攻击可以正确地获得发送的所有信息. 文献[18]中的协议虽然采用了顺序重排，但是木马攻击并不影响信息光子序列，在检测阶段检测不到错误，Eve 可以在公布重排顺序后，进行顺序重排获得所有信息. 文献[14]，[16]，[18]，[19]提出的协议都存在这种安全性问题，文献[17]对这种不安全性进行了分析和改进. 在光子到达发送者之前用滤波片滤除不可见光子，然后以一定概率通过光子数目分割器和单光子探测器判断光脉冲是否含有多个光子，通过多光子的概率判断是否存在木马攻击，但增加了实现的复杂度. 本文所提出的协议采用单向通信过程，不存在木马攻击.

4. 结　　论

本文提出的基于单光子的单向量子安全通信协议具有以下优点：1）易于实现：不需要 Bell 态的产生和测量，不需要进行 U 操作编码. 通过将信息序列和随机序列进行异或操作后，信息序列和校验序列的编码基是同时公布的，接收方只需要进行简单的延迟就可以按顺序进行测量，并不需要先挑出某些位置的光子进行测量，对存储能力要求低. 2）和双向通信相比，传输效率高，通信距离加倍.

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* Bangalore, India, December,1984 p175

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Long G L, Liu X S 2002 *Phys. Rev.* A **65** 032302

[4] Deng F G, Long G L 2003 *Phys. Rev.* A **68** 042315

[5] Deng F G, Long G L, Wang Y, Xiao L 2004 *Chin. Phys. Lett.* **21** 2097

[6] Wang X B 2005 *Phys. Rev.* A **72** 012322

[7] He G Q, Yi Z, Zhu J, Zeng G H 2007 *Acta Phys. Sin.* **56** 6427 (in Chinese) [何广强、易 智、朱 骏、曾贵华 2007 物理学报 **56** 6427]

[8] Zhao Y B, Heid M, Rigas J, Lütkenhaus N 2009 *Phys. Rev.* A **79** 012307

[9] Hillery M, Buzek V, Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[10] Karlsson A, Koashi M, Imoto N 1999 *Phys. Rev.* A **59** 162

[11] Bogdanski J, Rafiei N, Bourennane M 2008 *Phys. Rev.* A **78** 062307

[12] Bostrom K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[13] Deng F G, Long G L, Liu X S 2003 *Phys. Rev.* A **68** 042317

[14] Deng F G, Long G L 2004 *Phys. Rev.* A **69** 052319

[15] Wang C, Deng F G, Li Y S 2005 *Phys. Rev.* A **71** 044305

[16] Zhu A D, Xia Y, Fan Q B, Zhang S 2006 *Phys. Rev.* A **73** 022338

[17] Li X H, Deng F G, Zhou H Y 2006 *Phys. Rev.* A **74** 054302

[18] Wang J, Zhang Q, Tang C J 2006 *Phys. Lett.* A **358** 256

[19] Wang J, Chen H Q, Zhang Q, Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese) [王 剑、陈皇卿、张 权、唐朝京 2007 物理学报 **56** 673]

[20] Lin S, Wen Q Y, Gao F, Zhu F C 2008 *Phys. Rev.* A **78** 064304

[21] Wang M J, Pan W 2008 *Chin. Phys. Lett.* **25** 3860

[22] Long G L, Deng F G, Wang C 2007 *Front. Phys. China* **2** 251

[23] Bennett C H, Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881

[24] Wojcik A 2003 *Phys. Rev. Lett.* **90** 157901

[25] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801

[26] Beige A, Englert B G, Kurtsiefer C, Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357

[27] Gao T, Yan F L, Wang Z X 2005 *J. Phys.* A **38** 5761

[28] Man Z X, Zhang Z J, Li Y 2005 *Chin. Phys. Lett.* **22** 18

[29] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P, Zhou H Y 2006 *J. Korean Phys. Soc.* **49** 1354

[30] Cai Q Y 2006 *Phys. Lett.* A **351** 23

One-way deterministic secure quantum communication protocol based on single photons*

Quan Dong-Xiao† Pei Chang-Xing Liu Dan Zhao Nan

(*State Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071, *China*)

(Received 11 July 2009; revised manuscript received 30 July 2009)

Abstract

One-way deterministic secure quantum communication protocol based on single photons is proposed in this paper, in which the XOR operation by bits of the information sequence and random sequence is performed and the checking sequence is inserted before the sender's coding operation. When the photons arrive at the receiver, they are delayed at the receiver, and the sender then publishes the coding basis, so the photons can be measured in the correct basis. Then the two parties estimate the security of the quantum channel by the checking bits. When the channel is secure the sender publishes the random bits where the receiver has results, and the information sequence can be recovered by the receiver. Even the channel is not secure, what the eavesdropper gets is the random sending sequence, the information sequence is still secure. This protocol has the advantages of higher transmission efficiency and easier implementation compared with the two-way communication.

Keywords: quantum cryptography, deterministic secure quantum communication, single photons, one-way communication

PACC: 4250, 4230Q, 0365

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60572147,60672119), the Program of Introducing Talents of Discipline to Universities (Grant No. B08038) and the State Key Laboratory of Integrated Services Networks (Grant Nos. ISN 02080002, ISN090307).

† Corresponding author. E-mail: dxquan@xidian.edu.cn