量子密钥分发中波长相关攻击安全性研究

周飞^{①②}, 赵梅生^③, 王向斌^{①②*}

① 清华大学物理系低维量子物理国家重点实验室, 北京 100084

② 济南量子技术研究院, 济南 250101

③ 山东量子科学技术研究院有限公司, 济南 250101

* 通信作者. E-mail: xbwang@mail.tsinghua.edu.cn

收稿日期: 2013-09-10; 接受日期: 2014-01-15

国家自然科学基金 (批准号: 61073174, 61033001, 61061130540) 资助项目

摘要 本文主要解决在现实条件下, 量子密钥分发系统中光纤分束器的波长相关特性引起的测量基矢选择不随机的安全性问题, 通过分析分束器波长相关性引起的误码粒子分布偏差的大小, 理论推算实际系统中可提炼的最终安全码的下限, 从而较好地解决了存在被动基矢选择的波长相关性漏洞的安全性问题, 给出了类似安全性攻击方案的一个解决方法.

关键词 量子密钥分发 非理想性 基矢随机选择 波长相关攻击 系统安全性

1 引言

现代密码系统是军事部门、国家安全部门、重要基础设施 (机场、核电站等)、重要商业活动以及互联网通信中至关重要的组成部分. 密码术的一般原理是: 信息发送方将明文和密钥通过一种加密算法变成密文, 传送给接收方, 接收方再利用同样的密钥和一种解密算法将密文转换回明文, 从而读到发送方要传送的信息. 传统的信息加密技术, 比如当今应用最广的 RSA 公钥密码加密算法^[1,2] 和 AES 高级数据加密算法^[3,4], 都是依赖于计算的复杂度, 计算的高度复杂性确保窃听者在没有密钥的情况下, 在有限的时间内无法完成破解所需的大量计算, 来保证信息安全. 不同于经典信息, 量子信息的基本信息单元是量子比特, 对量子比特的处理过程遵从量子力学规律. 量子信息处理技术能够用一种革命性的方式对信息进行编码、存储、传输和操纵, 可以实现利用任何经典手段都无法完成的信息功能, 在提高运算速度、确保信息安全、增大信息传输容量等方面能突破经典信息的极限.

随着量子计算技术的飞速发展, 原有的传统密码体系受到了极大的威胁, 比如美国数学家 Peter Shor 于 1994 年提出的大数分解的量子算法^[5] 使得传统的 RSA 公钥密码体系的安全性基础遭遇到严峻的挑战, 随着新技术和新方案的涌现, 量子计算机的强大计算能力可以用来轻松破解 RSA 公钥密码体系. 而基于量子密钥分发的密码系统才被严格证明是绝对安全的^[6~9], 因为它不依赖于计算的复杂性来保证通信安全, 而是基于量子力学中单光子不可分割、海森堡测不准原理以及量子不可克隆原理来保证了通信双方共享绝对安全随机的密钥, 再结合“一次一密”的密码体制^[10], 从而实现无条件安全的保密通信方式. 量子密码技术在保障通信安全上的绝对优势, 使得西方各国投入了大量人力物

引用格式: 周飞, 赵梅生, 王向斌. 量子密钥分发中波长相关攻击安全性研究. 中国科学: 信息科学, 2014, 44: 322-328, doi: 10.1360/N112013-00165

图 1 光束分束器进行基矢随机选择

Figure 1 Random selection of basis vectors with beam splitter

力进行实用化研究,大量的商用量子密码产品出现¹⁾,而现实条件下实际量子密码系统的安全性^[11]也成为了国内外量子密码专家研究的重点,如有针对现实光源系统的安全性研究^[12~23]、接收探测系统的研究^[24~33],或者是有源编码调制器件的安全性研究^[34~39]以及有关无源光学器件的安全性问题^[40].

本文主要讨论了在现实量子密码系统中使用波长相关光纤分束器件作为基矢选择器件^[41]时的安全性问题,通过我们的分析可以得到,即使光纤分束器件存在一定的波长相关性,只要我们知道相关性的偏差范围,就可以通过测量不同基矢下实际误码率值,推算出最终安全的密钥率下限值,从而从理论上解决此类实际系统中的安全传输问题.

2 理论模型

在现实条件下,由于关键器件的非理想性,会遇到各种各样的安全性问题,其中在使用熔融拉锥光纤分束器的量子密钥分发系统中,就会遇到测量基矢选择不完全随机的安全性问题^[41].因为在实际量子密钥分发系统中,利用被动偏振编码方案的 BB84 协议系统,当 Bob 接收端对测量基的选择依赖于输入光波长时^[42~43],输入光波长一旦被控制发生偏离,基矢选择比例也随之发生对应变化,这将成为实际 QKD 系统的一个安全性漏洞,如图 1.

输入信号光 a , 经过光束分束器 BS 进行基矢随机选择, 输出端口 1 代表水平垂直基 (Z 基), 端口 2 代表对角基 (X 基), 当窃听者截获信号光, 发送不同波长的伪态至波长相关的光束分束器 BS 时, 窃听者可以有效地控制 Bob 端测量基的选择, 从而在引入小量额外噪声的情况下, 获取足够的测量基和测量结果信息. 对于一般的 BB84 协议的 QKD 系统, 其安全成码率可写成

$$R = 1 - H(t_b) - H(t_p), \quad (1)$$

其中最终安全码 R 的提炼是在同一测量基下进行的, t_b , t_p 分别对应同一测量基下的比特误码率和相位误码率, 在随机基矢测量下, 通常假定有 $t_p(\text{Z 基}) = t_p(\text{X 基})$ 或者 $t_b(\text{Z 基}) = t_b(\text{X 基})$, 而 $t_b(\text{Z 基})$, $t_p(\text{X 基})$ 一般可直接由测量结果得到, 即可根据 (1) 式提炼不同测量基下的最终安全码; 而非随机基矢测量时, 一般 $t_p(\text{Z 基}) \neq t_p(\text{X 基})$ 或 $t_b(\text{Z 基}) \neq t_b(\text{X 基})$, 从而无法直接从测量结果得到最终安全码. 如当使用波长相关光束分束器时, 测量基矢选择的概率会被窃听者掌握, 不同基矢下的误码率也相应会发生变化, 从而无法得到最终码, 但是如果我们知道分束器的波长相关特性和信号光的实际波

1) <http://www.idquantique.com/>, <http://www.magiqtech.com/>, <http://quintessencelabs.com/>, <http://www.quantum-info.com/>.

长, 给出基矢选择不随机概率偏差的范围, 可以通过测量 $X(Z)$ 基矢探测下的相位 (比特) 误码率大小估算出 $Z(X)$ 基矢探测下的相位 (比特) 误码率的上下限, 从而估算出最终安全码的下限, 从而提炼最终安全码信息, 达到安全通信的目的.

我们将具体给出我们的分析方法和结果, 这里我们以 Z 基下提炼最终密钥率为例. 假设在实际量子密钥分发过程中, 传输 n 个粒子, 相位误码粒子总数为 n_p , 对应误码粒子集合为 F ; Z 基下探测粒子总数 n_{z0} , X 基下探测粒子总数 n_{x0} , 有: $n = n_{z0} + n_{x0}$; 假设第 i 个粒子被选择在 X 基下测量的概率为 P_{X_i} , 同样第 i 个粒子被选择在 Z 基下测量的概率为 P_{Z_i} , 有 $P_{X_i} + P_{Z_i} = 1$; 如果在随机基矢测量条件下, 有 $P_{X_i} = P_{Z_i} = 1/2$.

当存在 BS 波长攻击时, 接收端测量基矢选择会以一定概率被窃听者操控, 从而有 $P_{X_i} \neq P_{Z_i}$, 即在 Z 基下, 由测量结果无法获得相应的相位误码率, 从而无法提炼最终安全码, 但我们可以假定有, 非随机基矢测量下

$$P_{X_i} = 1/2(1 + \varepsilon_i), \quad (2)$$

$$P_{Z_i} = 1/2(1 - \varepsilon_i), \quad (3)$$

ε_i 表示非随机基矢测量时, 第 i 个粒子被选择在 X 基或 Z 基下测量概率变化小量, 有 $-1 \leq \varepsilon_i \leq 1$, 可计算得被选择在 X 基和 Z 基下测量的相位误码的总粒子数 n_{p_x} , n_{p_z} 分别为

$$n_{p_x} = \sum_{i \in F} P_{X_i}, \quad (4)$$

$$n_{p_z} = \sum_{i \in F} P_{Z_i}. \quad (5)$$

对应 F 集合中相位误码粒子总数为 n_p , 有 $n_p = n_{p_x} + n_{p_z}$, 联合 (2)~(5) 式

$$n_{p_x} = 1/2(n_p + \sum_{i \in F} \varepsilon_i), \quad (6)$$

$$n_{p_z} = 1/2(n_p - \sum_{i \in F} \varepsilon_i). \quad (7)$$

设有

$$|\varepsilon_i| \leq \varepsilon, \quad (8)$$

分别联立 (6), (7) 和 (8) 式, 有

$$1/2n_p(1 - \varepsilon) \leq n_{p_x} \leq 1/2n_p(1 + \varepsilon), \quad (9)$$

$$1/2n_p(1 - \varepsilon) \leq n_{p_z} \leq 1/2n_p(1 + \varepsilon), \quad (10)$$

n_{p_x} 可在 X 基下实际测量得到, n_p 为未知, 由 (9) 和 (10) 式, 可得到 Z 基下测量的相位误码的粒子总数 n_{p_z} 有

$$\frac{n_{p_x}(1 - \varepsilon)}{(1 + \varepsilon)} \leq n_{p_z} \leq \frac{n_{p_x}(1 + \varepsilon)}{(1 - \varepsilon)}, \quad (11)$$

即在 Z 基下, 有

$$t_p = \frac{n_{p_z}}{n_{z0}}. \quad (12)$$

在 Z 基下, 可以直接由测量结果得到比特误码率 t_b , 所以我们只要得到 ε_i 的范围, 根据 X 基下误码粒子的个数, 就可以由 (1), (11) 和 (12) 式计算得 Z 基下的最终密钥率 R 的下限值.

图 2 最终安全码数值模拟

Figure 2 Numerical simulation of the final security key

3 数值模拟

在以前的研究中, 我们知道某些特定分束器不同端口透过率与信号光波长是存在严格关联的, 通过测量输入信号光波长, 根据相应透过率比率可估算出误码粒子被 X 基或者 Z 基测量的概率偏差最大值 ε , 从而推算出 Z 基或 X 基下提取最终安全密钥率的下限.

根据我们分析结果, 我们模拟 Z 基下可提取最终安全密钥率 R 的值, t_b, n_{z_0}, n_{p_x} 可以直接通过实际量子密钥分发过程测量得到, 假定有 $t_b = 0.03, n_{z_0} = 10^7, n_{p_x} = 10^5$, 由 $0 \leq \varepsilon < 1$, 由 (1) 式可得到最终安全码 R 如图 2 所示.

4 结论与展望

在这里, 我们研究了基矢选择中分束器的不完美性问题, 通过估算最终安全码的下限进行安全性研究, 使实际量子通信系统更加鲁棒, 抗噪能力更强. 量子密码技术是量子信息领域最接近实用化的技术, 量子通信的研究将对国家安全与信息科学技术产生不可估量的影响, 而实际系统下的量子密码技术安全性也越来越引起国内外学者的重点关注, 通过不断探索器件的非理想性可能引入的攻击漏洞和安全性问题, 从而进一步完善实用量子通信技术方案.

现实条件下的实用量子密码技术能有效地解决“一次一密”密码体制中的密钥分发信道问题, 极有希望成为新一代的标准密码技术, 根据安全性的级别, 未来可以将经典密码技术与量子密码技术有效的结合起来, 如 AES 加密算法取代一次一密加密算法, 从而在确保通信的安全性的基础上最大限度提高系统传输效率, 势必将会推动整个信息产业的技术革命.

参考文献

- 1 Diffie W, Hellman M E. New directions in cryptography. IEEE Trans Inform Theory, 1976, 22: 644-654
- 2 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. ACM Commun, 1978, 21: 120-126

- 3 Gaithersburg M D. National institute for standards and technology (NIST). Handbook Board Examiners, MBNQA, 1993
- 4 Stinson D R. Cryptography: Theory and Practice. 3rd ed. Boca Raton: CRC Press, Inc, 2006
- 5 Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, New York, 1994. 124–134
- 6 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 1999, 283: 2050–2056
- 7 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett*, 2000, 85: 441–444
- 8 Zhao Y B, Fung C H F, Han Z F, et al. Security proof of differential phase shift quantum key distribution in the noiseless case. *Phys Rev A*, 2008, 78: 042330
- 9 Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys Rev Lett*, 2009, 102: 180504
- 10 Shannon C E. Communication theory of secrecy systems. *Bell Syst Tech J*, 1949, 28: 656–715
- 11 Gottesman D, Lo H K, Lukenhaus N, et al. Security of quantum key distribution with imperfect devices. *Quantum Inf Comput*, 2004, 4: 325–360
- 12 Hwang W Y. Quantum key distribution with high loss: toward global secure communication. *Phys Rev Lett*, 2003, 91: 057901
- 13 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys Rev Lett*, 2005, 94: 230503
- 14 Lo H K, Ma X, Chen K. Decoy state quantum key distribution. *Phys Rev Lett*, 2005, 94: 230504
- 15 Wang X B, Peng C Z, Pan J W. Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source. *Appl Phys Lett*, 2007, 90: 031110
- 16 Wang X B. Decoy-state quantum key distribution with large random errors of light intensity. *Phys Rev A*, 2007, 75: 052301
- 17 Wang X B, Peng C Z, Zhang J, et al. General theory of decoy-state quantum cryptography with source errors. *Phys Rev A*, 2008, 77: 042311
- 18 Wang X B, Yang L, Peng C Z, et al. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J Phys*, 2009, 11: 075006
- 19 Muller A, Herzog T, Huttner B, et al. Plug and play systems for quantum cryptography. *Appl Phys Lett*, 1997, 70: 793–795
- 20 Zhao Y, Qi B, Lo H K. Quantum key distribution with an unknown and untrusted source. *Phys Rev A*, 2008, 77: 052327
- 21 Peng X, Jiang H, Xu B J, et al. Experimental quantum-key distribution with an untrusted source. *Opt Lett*, 2008, 33: 2077–2079
- 22 Zhao Y, Qi B, Lo H K, et al. Security analysis of an untrusted source for quantum key distribution: passive approach. *New J Phys*, 2010, 12: 023024
- 23 Nauerth S, Fürst M, Schmitt-Manderbach T, et al. Information leakage via side channels in freespace BB84 quantum cryptography. *New J Phys*, 2009, 11: 065001
- 24 Makarov V, Anisimov A, Skaar J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys Rev A*, 2006, 74: 022313
- 25 Makarov V, Hjelme D R. Faked states attack on quantum cryptosystems. *J Mod Opt*, 2005, 52: 691–705
- 26 Qi B, Fung C H F, Lo H K, et al. Time-shift attack in practical quantum cryptosystems. *Quantum Inf Comput*, 2007, 7: 73–82
- 27 Zhao Y, Fung C H F, Qi B, et al. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys Rev A*, 2008, 78: 042333
- 28 Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photonics*, 2010, 4: 686–689
- 29 Yuan Z L, Dynes J F, Shields A J. Avoiding the blinding attack in QKD. *Nat Photonics*, 2010, 4: 800–801
- 30 Lydersen L, Wiechers C, Wittmann C, et al. Avoiding the blinding attack in QKD. *Nat Photonics*, 2010, 4: 801

- 31 Wiechers C, Lydersen L, Wittmann C, et al. After-gate attack on a quantum cryptosystem. *New J Phys*, 2011, 13: 013043
- 32 Henning W, Harald K, Markus R, et al. Quantum eavesdropping without interception an attack exploiting the dead time of single photon detectors. *New J Phys*, 2011, 13: 073024
- 33 Liu D, Yin Z Q, Wang S, et al. Estimation of key rate after setting dead time. *Chin Phys B*, 2012, 21: 6060202
- 34 Fung C H F, Qi B, Kiyoshi T, et al. Phase-remapping attack in practical quantum-key-distribution systems. *Phys Rev A*, 2007, 75: 032314
- 35 Xu F, Qi B, Lo H K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J Phys*, 2010, 12: 113026
- 36 Sun S H, Gao M, Jiang M S, et al. Partially random phase attack to the practical two-way quantum-key-distribution system. *Phys Rev A*, 2012, 85: 032304
- 37 Li H W, Yin Z Q, Han Z F, et al. Security of practical phase-coding quantum key distribution. *Quantum Inf Comput*, 2010, 10: 0771–0779
- 38 Li H W, Yin Z Q, Wang S, et al. Security of quantum key distribution with state-dependent imperfections. *Quantum Inf Comput*, 2011, 11: 0937–0947
- 39 Huang J Z, Yin Z Q, Han Z F, et al. Effect of intensity modulator extinction on practical quantum key distribution system. *Eur Phys J D*, 2012, 66: 159
- 40 Sun S H, Jiang M S, Liang L M. Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system. *Phys Rev A*, 2011, 83: 062331
- 41 Li H W, Wang S, Huang J Z, et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multi-wavelength sources. *Phys Rev A*, 2011, 84: 062308
- 42 Ankiewicz A, Snyder A, Zheng X H. Coupling between parallel optical fiber cores—critical examination. *Lightw Technol J*, 1986, 4: 1317–1323
- 43 Tekippe V. Passive fiber-optic components made by the fused biconical taper process. *Fiber Int Opt*, 1990, 9: 97–123

Security of quantum key distribution under the wavelength-dependent quantum hack

ZHOU Fei^{1,2}, ZHAO MeiSheng³ & WANG XiangBin^{1,2*}

1 Department of Physics and State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China;

2 Jinan Institute of Quantum Technology, Shandong Academy of Information Technology, Jinan 250101, China;

3 Shandong Institute of Quantum Science and Technology Co., Ltd., Jinan 250101, China

*E-mail: xbwang@mail.tsinghua.edu.cn

Abstract The manuscript intend to offer a solution to the security loophole induced by the wave-length dependence of the fibre beam splitter loss. The lower bound of the final secure key rate generated by a practical QKD system is theoretically deduced via analysis on the quantum key error rate influenced by wave-length dependence of the fibre beam splitter. Thus, we made up the security loophole pretty well, and provide a solution to similar quantum hack scheme.

Keywords quantum key distribution, imperfection, randomness of basis election, wavelength-dependent quantum hack, system security

ZHOU Fei was born in 1983. He received his Ph.D. degree in 2012 from Department of Physics, Tsinghua University. Currently, he is a Senior Researcher at Jinan Institute of Quantum Technology. His research interests include the free space quantum communication and the passive decoy state quantum key distribution.

WANG XiangBin was born in 1967. He received the Ph.D. degree in philosophy from the National University of Singapore in 2001. Currently, he is professor and doctoral tutor at Tsinghua University. His research interests include the decoy-state method for quantum key distribution, the measurement-device-independent quantum key distribution(MDIQKD), and quantum process tomography(QPT). Professor Wang is a member of Quantum Cryptography Professional Committee of Chinese Association for Cryptologic Research, as well as the president of Jinan Institute of Quantum Technology.