

基于BB84的量子密钥分发和身份认证

在现实世界中，一个完整的量子加密通常包括量子密钥分发和量子身份认证两个部分。然而，很少有协议一起完成这样的工作。为了解决这个问题，提出了一种基于BB84新的密钥分发方案。通过多次经典一次hash函数计算，可以确保身份认证，并能确定错误粒子的具体位置。除此之外，这个协议可以抵抗多种常见攻击。

王映康¹ 朱鹂²/1. 国网重庆市电力公司信息通信公司 2. 国网重庆市电力公司江北供电分公司

0 引言

量子机制的独特性是量子信息和量子计算的基石。由于经典加密系统是基于计算复杂性，可能遭受量子计算的严重威胁^[1]。幸运的是，基于量子机制物理特性的量子加密系统可以解决这个问题。量子密钥分发可以在两个通信者之间生成一个随机密钥，这在量子通信中非常重要。量子密钥分发协议最早是由Bennett 和 Brassard 在1984(BB84) 提出的^[3]。自从那以后，许多其他的密钥分发协议^[4-5]已经被提出。为了确保合法的用户可以共享一串测量基作为量子密钥，本文提出了一种新的量子密钥分发协议。

在量子加密系统中，量子身份认证是另一个重要的问题。量子身份认证的原理是接收者可以认证发送者的身份和消息的完整性。

为了实现量子身份认证，一些协议的提出是基于量子信道的理想性^[6-8]。而在现实的世界中，这样的情况是不切实际的。即使一些协议^[9-11]考虑了量子信道受到噪声的影响，它们只能通过错误率来检测到窃听是否存在，而不能直接通过身份认证来确定错误粒子的位置。而

且，量子纠缠和量子远程传态在量子身份认证中扮演着重要的角色。在实际应用中，有各种各样的传输粒子，例如贝尔态^[12-14]，GHZ态^[15-16]，cluster 态^[17-18]，W态^[19-20]和 χ 态^[20-22]等。由于量子纠缠态和量子远程传态的复杂性，这篇文章基于单光子提出的身份认证更为简单，更具有实用性。

在2011年，张提出了一个完整的量子加密系统的协议^[23]，这个协议用了压缩态。这个协议有几个优势，其中之一就是效率很高，然而，遗憾的是产生的会话密钥不能被重用，而且这个协议引进了额外的粒子。

本文旨在不需要可信第三方的帮助下，提出一个结合量子密钥分发和量子身份认证的协议。在密钥分发阶段，合法的用户可以直接共享一串测量基作为会话的密钥。然后，一个新的量子身份认证协议结合一次或多次经典一次hash函数计算来确保消息的完整性并认证身份。更为重要的是，在非理想的量子信道中，一个合法的用户可以定位错误块的位置。除此之外，他们可以通过海明码来快速纠错。

2 协议环境

设想这个协议包含两个通信方，Alice 和 Bob。其分别共享了量子信道和可认证的经典信道。如果Alice 想发送一个经典比特 p ，生成一个量子比特并基于以后规则发送给Bob：

- 1) R。垂直基表示为两个方向($\uparrow$, $\rightarrow$)。
- 2) D。对角基表示为两个直角方向($\nearrow$, $\searrow$)。
- 3) 如果 $p=0$ (1)，量子密钥是R基，量子比特是 $\uparrow$ ($\rightarrow$)。



王映康/高级工程师

关键词/Keywords

量子密钥分发 ·
量子身份认证 ·
经典hash函数 ·

4) 如果 $p=0$ (1), 量子密钥是D基, 量子比特是 $\nearrow(\searrow)$ 。

5) Alice和Bob默认一个一次hash函数为 $H=\{0, 1\}^n \rightarrow \{0, 1\}^m$ 。

3 提出的量子对话协议

3.1 量子密钥分发

(1) 步骤1

Alice 从 $\{0,1\}$ 随机选择 n 比特最为串 S 并从 $\{\times, +\}$ 随进选择 n 个基作为串 P_A 。然后Alice把 S 编码在 P_A 上, 并发送给Bob。

(2) 步骤2

Bob收到量子串 S_1 后, 从 $\{\times, +\}$ 随进选择 n 个基作为串 P_B , 去测量串 S_1 获得 S_2 。通过可认证的经典信道, Alice 和Bob公开讨论 S_1 和 S_2 。

(3) 步骤3

比较 S_1 和 S_2 每一个粒子, 如果相等, Alice和Bob丢弃对应的 P_A 和 P_B 基。否则, 保留下来。然后Bob反转所有基, 例如, 把 $+$ 变成 $\times$ 和把 $\times$ 变成 $+$ 。

(4) 步骤4

如果量子信道是不理想的, 通过可认证经典信道Alice 和Bob 随机选择足够多的保留测量基去检测是否有窃听。如果错误率低于门限值 $0.89\% \sim 1.89\%$ ^[24-25], Alice和Bob移除选择的基, 否则Alice终止协议。

(5) 步骤5

通过保密放大和可认证的经典信道, Alice 和Bob纠正保留的测量基^[26-27]。然后, 他们共享了一串基作为量子密钥。

表1 一个例子展示上面的协议

Alice的随机比特	0	1	1	0	1	0	0	1	1	0
Alice的随机选择基	+	+	+	×	×	×	×	+	+	×
Alice发送的光子	$\uparrow$	$\rightarrow$	$\searrow$	$\uparrow$	$\searrow$	$\nearrow$	$\nearrow$	$\rightarrow$	$\rightarrow$	$\nearrow$
Bob 随机选择的基	+	×	×	×	+	×	+	+	×	×
Bob 测量光子	$\uparrow$	$\nearrow$	$\searrow$	$\searrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\rightarrow$	$\uparrow$	$\nearrow$
Bob获得的比特	0	0	1	1	1	0	1	1	0	0
公开讨论										
Bob公开收到的比特	0	0	1	1	1	0	1	1	0	0
Alice公开哪个是错误的	NO	NO			NO		NO			
Bob反转对应的测量基	+	+			×		+			
若没有窃听	+								+	
可能收到的信息										
Bob随机选择测量基										
Alice证实正确性	OK						OK			
结果										
保留的密钥	+						×			

3.2 量子身份和消息完整性认证

量子信道可以分为理想的和非理想的。

3.2.1理想的量子信道

(1) 步骤1

Alice 想发送一个经典比特串 M 给Bob。Alice 计算 $H(M)=m$ 并从 $\{0,1\}$ 选择足够的诱骗粒子随机插入 M , 形成串 M_1 。然后, Alice 基于环境里的规则用 K 编码 M_1 形成串 M_1' , 并通过量子信道发送量子串 M_1' 给Bob。

(2) 步骤2

当Bob收到量子串后, 他给Alice发送确认。Alice 和Bob 然后公开讨论窃听检测。Alice通知Bob诱骗粒子和 m 的位置。Bob测量诱骗光子并发送测量结果给Alice。如果测量结果和初始态相同, Alice可以确认接收者是Bob, 而且量子信道是安全的。否则, Alice 放弃协议。

(3) 步骤3

Bob移除诱骗比特, 通过解码得到 M' 。Bob计算 $H(M')=m'$, 如果 $m=m'$, Bob可以确认发送者是Alice, 而且消息是完整的。

3.2.2量子信道是非理想的

(1) 步骤1

Alice 想发送消息 M 给Bob。她把 M 分成 $M_1, M_2 \cdots M_N$, 并且计算 $H(M_1)=m_1, H(M_2)=m_2 \cdots H(M_N)=m_N$ 。然后在 M 随机的插入足够的诱骗粒子, 形成串 M_2 。Alice通过密钥 K 编码 M_2 形成串 M_2' , 并通过量子信道发送给Bob。

(2) 步骤2

当收到量子串后, Bob给Alice发送确认。Alice和Bob公开讨论窃听检测。Alice公开诱骗比特和 $m_1, m_2 \cdots m_N$ 位置。Bob取出这些粒子并测量, 然后把测量结果发送给Alice。通过比较初始态和结果态, 如果错误率低于门限值, Alice可以确认接收者是Bob和量子信道的安全性。否则, Alice终止协议。

(3) 步骤3

Bob移除诱骗粒子。通过密钥 K , 他得到 M' 。Bob把 M' 分成 $M_1', M_2' \cdots M_N'$ 并计算 $H(M_1')=m_1', H(M_2')=m_2' \cdots H(M_N')=m_N'$ 。通过比较 m_1 和 m_1' , m_2 和 $m_2' \cdots m_N$ 和 m_N' , 若果错误率低于门限值, Bob可以确认发送者是Alice, 并且消息是完整的。

(4) 步骤4

基于海明码, Alice和Bob 通过可认证的经典信道纠正错误块。然后, Bob可以获得正确的粒子。

4 安全性分析

在这个部分, 讨论所提出协议的必须能够抵抗一些常见的攻击。由于这个新的量子密钥分发协议是基于BB84, 并且BB84已经被证明是无条件安全的^[28]。所以, 量子认证的安全性讨论如下。

4.1 截获重发

这个攻击^[29]意味着窃听者(Eve)截获传送的粒子并测量它们。按照测量的结果, 重新发送一个伪造的粒子串给目标用户。Eve的目标是从发送者获得编码信息。这个协议的安全性依靠BB84的基本原理: Eve仅可以控制量子信道, 但她不能控制可认证的经典信道。

设想Alice发送消息M给Bob, Eve截获M。因为Eve不知道密钥K, 她只能随机选择测量基 $\{\times, +\}$ 测量每一个粒子。在这种情况下, 对每一个粒子, Eve能够得到正确的结果是3/4。例如, 如果测量结果是 $\searrow$, Eve可以确定Alice的操作是基D。因此, 对于每一粒子, 这种攻击可能被检测出的概率是1/4。如果诱骗粒子数是 q , Eve可能被检测出的概率是 $(1-(3/4)q)$ 。如果 $q=1000$, 被检测出的概率是1。即使Eve通过了Alice的检测, Bob也能通过一次hash函数检测窃听。因为, 即使传送信息一位错误, hash值也会发生很大的变化。

4.2 扮演者攻击

在这个攻击里, Eve可能会扮演Alice发送一个伪造的消息给Bob, 也有可能扮演Bob获得Alice上的编码操作。在量子认证阶段, 设想Bob不在。Eve接收Alice发送来的消息。既然Eve不知道密钥K, 只能随机选择测量基 $\{\times, +\}$ 测量它们。例如, 密钥K的第 i 个基 $K_i = \times$ 。如果Eve选择 $\times$ 作为基去测量, 他可以得到正确的结果。否则, 它可能被Alice检测出的概率是1/2。因此, Alice能够检测出Eve的概率是 $(1-(3/4)q)$ 。如果 q 是足够大, 被检测出的可能性将为1。相反, Eve扮演Alice发送一个伪造的消息给Bob。通过经典一次hash函数, 可以检测出Eve的存在。因此, 这个协议可以抵抗扮演者攻击。

4.3 拒绝服务攻击

文献^[30]中提出了拒绝服务攻击。通过阻断量子信道, 攻击者Eve可以阻止Alice和Bob的通信。例如, Eve故意一次次引起错误的身份认证, 使得合法的用户丢弃所有的秘密信息, 因为这种攻击在非冗余的系统中是与生俱来的。如果这个协议能够适合网络, 那么信道通常设想为不可阻断或者阻塞。

5 结束语

本文提出了一个新的包含量子密钥分发的量子认证协议。提出的协议可以抵抗一些如上的经典攻击。通过利用单光子和一次hash函数, 两个合法用户可以共享一串密钥, 并实现身份和消息的完整性检验。更重要的是, 在非理想的量子信道中, 通过多次hash值得计算, 这个协议可以定位错误块的位置。因此, 这个方案也更具有实用性。

参考文献

- [1] Gisin, N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev. Mod. Physics. 1-44 (2002).
- [2] Cleve, R, Gottesman, D, Lo, H-K. How to share a quantum secret. Phys. Rev. Lett. 83, 648-651 (1999)
- [3] Bennett, C. H. Brassard, G. Quantum cryptography: public key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India. 175-179 (1984).
- [4] Ljunggren, D. Bourennane, M. Karlsson, A. Authority-based user authentication in quantum key distribution. Phys. Rev. A. 62, 022305 (2000).
- [5] Chen, T.-Y. Zhang, J. Boileau, J.-C. Jin, X.-M. Yang, B. Zhang Q Yang, T Laflamme, R Pan, J.-W.: Experimental Quantum Communication without a Shared Reference Frame. Phys. Rev. Lett. 96, 150504 (2006).
- [6] Sarath, R., .Shajin Nargunam, A., Sumithra, Dual, RP.: Dual Channel Authentication in Cryptography Using Quantum Stratagem, ICCEET. 1044-1048(2012)
- [7] Wang, T.-Y., Wen, Q.-Y., Zhu, F.-C.: Quantum communications with an anonymous receiver. Sci.

- China. Phys. Mech. Astron.53, 2227-2231(2010)
- [8] Curty, M., Santos, D.-J.: Quantum authentication of classical messages. Phys. Rev. A. 64, 062309 (2001)
- [9] Liu, D., Pei, C.-X., Quan, D.-X., Zhao, N.: A New Quantum Secure Direct Communication Scheme with Authentication. Chin.Phys.Lett. 27, 050506 (2010)
- [10] Liu, B., Gao, F., Wen, Q.-Y.: Single-Photon Multiparty Quantum Cryptographic Protocols with Collective Detection. IEEE Journal of Quantum Electronics.47,1 383-1390(2011)
- [11] Yang, C.-W., Hwang, T., Lin, T.-H.: Modification Attack on QSDC with Authentication and the Improvement. Int. J. Theor. Phys. 10, 2230-2234 (2013)
- [12] Yu, K.-F., Yang, C.-W., Liao, C.-H.: Authenticated semi-quantum key distribution protocol using Bell states, Quantum Inf. Process.13, 1457-1465 (2014)
- [13] Gao, F., Qin S.-J., Guo, F.-Z., Wen, Q.-Y.: Cryptanalysis of Quantum Secure Direct Communication and Authentication Scheme via Bell States. Chin. Phys. Lett. 28, 020303 (2011)
- [14] Pavii, M.: In quantum direct communication an undetectable eavesdropper can always tell ϕ from ϕ Bell states in the message mode.Phys. Rev. A. 87,042326 (2013)
- [15] Chang, Y., Xu, C.-X., Zhang, S.-B., Yan, L.-L.: Quantum broadcast communication and authentication protocol with a quantum one-time pad. Chin. Phys. B. 23, 010305 (2013)
- [16] Shi, W.-M., Zhou, Y.-H., Yang, Y.-G.: Quantum deniable authentication protocol. Quantum Inf. Process 13, 1501-1510 (2014)
- [17] Cao, W., Yang, Y., Wen, Q.-Y.: Quantum secure direct communication with cluster states. Chin. Phys. Mech. Astron.53, 1271-1275(2010)
- [18] Chang, Y., Zhang, S.-B., Yan, L.-L.: A Bidirectional Quantum Secure Direct Communication Protocol Based on Five-Particle Cluster State. Chin. Phys. Lett. 30, 090301 (2013)
- [19] Joo, J., Park, Y.-J., Oh, S.-C., Kim, J.: Quantum teleportation via a W state. New. J. Phys. 5, 136 (2003)
- [20] Eibl, M., Kiesel, N., Bourennane, M., Kurtsiefer, C., Weinfurter, H.: Experimental Realization of a Three-Qubit Entangled W State. Phys. Rev. Lett. 92, 077901 (2004)
- [21] Lin, S., Wen, Q.-Y., Gao, F., Zhu, F.-C.: Quantum secure direct communication with $\times$ -type entangled states. Phys. Rev. Lett. 78, 064304 (2008)
- [22] Yang, Y.-G., Cao, W.-F., Wen, Q.-Y.: Three-party quantum secret sharing of secure direct communication based on $\times$ -type entangled states. Chin .Phy. B. 19, 050306 (2010)
- [23] Zhang, S., Wang, J., Tang, C.-J., Zhang, Q.: A Composed Protocol of Quantum Identity Authentication Plus Quantum Key Distribution Based on Squeezed States. Commun. Ther. Phys. 56, 268-272 (2011)
- [24] Stucki, D., Walenta, N., Vannel, F., Then, R.-T., Gisin, N., Zbinden, H., Gray, S., Tower, C.-R., Ten, S.: High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. New. J. Phys.11,075003(2009)
- [25] Wang, S., Chen, W., Guo, J.-F., Yin, Z.-Q., Li, H.-W., Zhou, Z., Guo, G.-C., Han, Z.-F.: 2 GHz clock quantum key distribution over 260 km of standard telecom fiber . Optics. Lett. 37, 1008-1010 (2012)
- [26] Bennett, C.H., Brassard, G., Crkpeau, C., Maure, U.-M.: Generalized privacy amplification. IEEE Transactions on Information Theory.41,1915-1923(1995)
- [27] Bennett, C.-H., Brassard, G., Robert, J.-M.: Privacy amplification by public discussion. Siam. J.Comput. 17, 210-228 (1998)
- [28] W.Shor, P., Preskill, J.: Simple proof of security of BB84 quantum key distribution. Phys.Lett.A.85, 1-5 (2000)
- [29] Lin, T.-H, Hwang, T.: Man-in-the-middle attack on quantum secure communications with authentication. Quantum Inf. Process.13, 917-923 (2014)
- [30] Nguyen, B.-A.:Quantum dialogue. Phys. Lett. A.328,6-10(2004)

(收稿日期: 2015-05-26) EA

作者简介

王映康 (1965-) , 男, 高级工程师, 国网重庆市电力公司信息通信分公司副总工程师。