讲 座

量子信息讲座续讲

第二讲 量子信息安全系统*

曾 贵 华

(上海交通大学电子工程系 上海 200030)

摘 要 详细介绍了量子密码的相关内容,包括量子密码理论基础、量子保密系统、量子认证系统、量子密码与其他学科的关系以及量子密码的应用与展望,并追踪了量子信息安全系统的最新研究进展.

关键词 量子信息理论,检测敌手,量子保密系统,量子认证系统,量子密码应用

QUANTUM INFORMATION SECURITY SYSTEMS

ZENG Gui-Hua

(*Electrical engineering department, Shanghai Jiaotong University, Shanghai* 200030)

Abstract Quantum cryptography is reviewed in detail, including its theoretical basis, quantum cryptographic systems, quantum authentication systems, the relationship between quantum cryptography and other subjects, and its prospective applications. In addition, the latest developments of quantum cryptography are presented.

Key words quantum cryptographic information theory, detection of eavesdropping, quantum cryptographic system, quantum authentication system, application of quantum cryptography

1 量子密码学的起源与发展

利用量子现象(效应)对信息进行保密是1969年哥伦比亚大学的科学家 S. Wiesner 首先提出的[1].当时,Wiesner 写了一篇题为"共轭编码"(conjugate coding)的论文,在该文中,Wiesner 提出了两个概念:量子钞票(quantum bank notes)和复用信道(multiplexing channel). Wiesner 的这篇论文开创了量子信息安全研究的先河,在密码学史上具有重要的意义.遗憾的是这篇论文当时没能获准发表.

在一次偶然的谈话中,Wiesner 向 IBM 公司的科学家 C.H.Bennett 提及他10年前的思想,引起 Bennett 的注意.在1979年举行的第20次 IEEE 计算机科学基础大会上,Bennett 与加拿大 Montreal 大学的密码学家 G.Brassard 讨论了 Wiesner 的思想.但最初他们没能正确理解 Wiesner 的思想,在1983年发表的论文中他们利用量子态储存来实现量子密码并提出了量子公钥算法[1)][2]体制,而长时间储存量子态在目前的实验上不能实现,因此他们的论文没引起人们的共识,甚至有人认为他们的想法是天方夜谭.不久他们意识到在量子密码中量子态的传输可能比量子态的储存更重要[2)],于是在1984年重新考虑了量子密码,并开创性地提出了量子密钥分发的概念,并提出了国际上第一个量子密钥分发协议(BB84协议)[3].从此量子密码引起了国际密码学界和物理学界的高度重视.在以后的十多年的研究中,量子密码学获得了飞速发展.目前,量子密码也引起了非学术界的有关部门(如军方、政府)等的注意.

2 量子密码的基本理论

2.1 量子密码信息理论基础

* 国家自然科学基金(批准号:69803008)资助项目
2000-06-01 收到

1) 现在已经证明该算法不安全

2) 随着量子计算机和量子密码的发展,目前量子态的存储变得很重要,并引起人们的注意

密码学的发展经历了三千多年的历史,但直到1940年C.E.Shannon提出信息论[4]后,密码学才上升到科学的体系,成为一门真正的学科,因此,信息论是密码学的基础.事实上,在密码学中,信息理论是与安全性[1]联系在一起的,Shannon信息论包括信息安全和计算安全.量子密码的安全属于信息安全,因此量子密码应建立在信息论的基础上.值得指出的是,量子密码的实现是以量子物理学为基础的,而Shannon信息论对应经典物理学.众所周知,量子物理学和经典物理学依赖于不同的法则,因此量子信息论不能简单地套用Shannon信息论,必须在Shannon信息论的基础上建立新的理论体系.

文献[5]从信息的角度提出了适合非正交量子态信道的信息理论,但他们的理论只能解释BB84协议以及改进版.文献[6]研究了量子相干性与量子保密性的关系.文献[7]做了较系统的研究,提出了一个理论体系.但到目前为止,这方面的研究还相当匮乏,可以认为量子密码的信息基础理论体系目前极不完善,急需进一步研究.

2.2 对敌手的检测理论

与经典密码[2]相比,量子密码的优势在于它的无条件安全性和对敌手的检测性,而量子密码协议或算法是否安全与对敌手的检测情况紧密相关,因此量子密码表现出来的对敌手[3]的可检测性应该有一个很好的检测标准.事实上,在量子密码中,对敌手的检测标准对协议或算法的安全性是非常重要的,如果没有好的标准,协议和算法将可能不安全,因为通信中合法通信者可能把有窃听的情况视为安全!因此,如何检测敌手的存在与否是量子密码中的一个重要问题.例如在量子保密通信中,如果出错率大于检测标准,但仍然当作没有敌手存在处理,就必然导致敌手获得某些信息,甚至窃取全部信息.因此检测理论是必要的,遗憾的是,除了文献[8]对基于共轭基的协议中的检测问题做了研究外,目前仍没有一般性的检测理论.

2.3 保密加强理论与技术

保密加强是一种蒸馏技术,其基本思想如下:对于敌手知道部分比特消息的一个较长的比特串(量子比特串或经典比特串),例如长为 n 的比特串 $\{x\}=\{x_1,x_2,\cdots,x_n\}$,在一定的编码规则下浓缩为一个短于 $\{x\}$ 的比特串(例如长为 k 的比特串 $\{y\}=\{y_1,y_2,\cdots,y_k\}$, $k<n$),从而使敌手对 $\{y\}$ 中的比特信息知道得极少或不知道,最终在保密性方面提高强度.保密加强技术包括经典保密加强和量子保密加强,它是量子保密通信中的必要步骤,也是提高密钥安全强度的重要技术.经典保密加强得到了充分的研究[9],但目前只有一篇文献研究了量子密码中的保密加强技术[10].保密加强的目的是使敌手获得的信息量最小,从而提高所获得密钥(或信息)的安全性.作者认为,量子保密加强技术在其他方面如量子身份认证技术等方面有着潜在的应用,这方面有待进一步研究.

3 量子保密系统

所谓量子保密系统可定义为用量子的方法对信息进行保密的通信系统.虽然目前还没有加、解密算法,但量子保密系统中已经提出了秘密共享和信息分拆算法.

3.1 秘密共享和信息分拆算法

定义1:设 m,n 是正整数,且 $m\leqslant n$.将秘密S在一组参与者P中进行分配,如果 n 个参与者按如下方式共享秘密信息S:其中任意 m 个参与者可以协同恢复S,但任意少于 m 个参与者都不能恢复该信息,称为秘密共享体制,秘密共享体制亦称为 (m,n) 门限方案[11].

1998年6月,Hillery,Berthiaume和Buzek提出了量子秘密共享和量子信息分拆的概念[12].他们提出的秘密共享算法用Greenberger-Horne-Zeilinger(GHZ)量子纠缠态实现(简称为HBB量子秘密共享算法),同时他们基于GHZ量子纠缠态提出了一个量子信息分拆协议.同年,日本NTT的科学家A.Karlsson,M.Koashi和N.Imoto参照HBB方案,用Bell量子纠缠态亦实现了量子秘密共享[13],提出了两态量子秘密共享算法(简称为KII量子秘密共享算法),然后,他们对HBB量子信息分拆进行了延拓,并研究了量子 (m,n) 门限方案实现的可能性.这两个小组的方案都是基于量子纠缠态的量子秘密共享协议.最近,文献[14]基于量子纠错码的方法提出了国际上第一个量子 (m,n) 门限方案.

3.2 量子密钥管理

密钥管理包括密钥的产生、分发、储存、验证、删

1) 安全性在密码学中是非常重要的,一个方案如果不安全的话,即使在理论上再完善、实验上再完美也是毫无价值的

2) 本文中的"经典"相对于"量子"而言

3) 本文中的"敌手"可以包括主动攻击者或(和)被动攻击者(窃听者)

除等,它是经典密码学中最困难的问题[11].密钥管实现.为了解决密钥分发问题,人们试图利用物理学的方法解决这一难题,目前量子密钥管理提供了一种可证明安全的方法.从目前的研究来看,量子密钥管理包括量子密钥产生与分发、存储、验证等三个方面.

所谓量子密钥分发是指两个或多个合法通信者在公开量子信道上利用量子效应或原理获得秘密信息(量子密钥)的过程.量子密钥分发是目前量子信息安全系统中研究得最多的课题,部分技术正试图走向实用.已有的研究包括以下几个方面:(1)协议方面[15].目前典型的且受到重视的量子密钥分发协议有 BB84 协议、B92 协议、EPR 协议,在这些协议的基础上,各国的研究人员对以上的三种协议进行了改进,提出了各种改进型的 BB84 协议和 EPR 协议.虽然提出了许多协议,但这些方案均包括量子传输、检测敌手、数据纠错及保密加强四个过程.(2)安全性分析方面[16].人们利用物理方法、信息论分析方法、经典密码分析方法针对所提出的协议分析了其安全性,这些研究结果表明,目前所提出的量子密钥分发协议是无条件安全的.但作者认为,目前的安全性分析方面的论文都是在试图说明协议是安全的,而不是设法分析协议的不安全性,这种方式不符合密码学的思路1).(3)实验验证方面[17].1992 年,Bennett 等人首次开展了实验研究,不久人们利用光子在光纤中传输,亦成功地实现了量子密钥分发,传输距离目前可达 30km.最近,Los Alamos 实验室将自由空间中的传输距离延长到超过 1km.(4)网络中密钥分发研究[18].以上介绍的量子密钥分发都是两方通信,当涉及三方或更多方的通信时,人们提出了网络中量子密钥分发方法.目前有两种模型:多方通信模型和远距离双方通信模型.网络密钥分发方面主要是以色列的经典密码学家 E.Biham 等人的工作以及英国 BT 实验室的工作,其中前者提出的网络密钥分发协议是基于逻辑网络结构的,而后者提出的是基于物理结构的方案.

量子密钥存储是指保存所获得的量子密钥以备后用.目前可用 EPR 量子纠缠态和量子内存实现量子密钥的存储,利用量子内存的存储时间可达 10min 左右,理论上可以达到无穷大.量子比特的存储在量子信息学中是一个重要的基本问题,它在量子通信、量子计算等方面都有重要的作用.因此这方面应该得到重视.

量子密钥验证是指对所获得的密钥进行验证,理方面的困难使得无条件安全的一次一密算法难以以便确认密钥来自于真正的合法通信者而不是敌手.目前所提出的量子密钥分发协议都是假定通信者是合法的,但在实际的应用中必存在假冒的情况和中间人攻击[11].因此有必要对获得的量子密钥进行真实性验证.最近作者首次研究了这个问题,提出了一个量子密钥验证协议[19].

4 量子认证系统

4.1 量子身份认证

在网络通信中常常涉及用户身份识别的问题.经典网络系统中可用经典身份认证技术,如口令、密钥等实现.为了实现量子网络中的身份识别,文献[20]提出了一个量子身份认证协议;最近作者亦研究了量子身份认证有关问题,提出了量子身份认证协议,并研究了相应协议的安全性问题[20].

4.2 量子比特承诺、量子不经意传输、量子多方计算[21]

在量子摇币协议的基础上,人们试图将其延伸,于是提出了各种量子方案.在量子比特承诺方面,1990 年,Brassard 等人对量子摇币协议进行修改后实现了量子比特承诺;在此基础上,1993 年,Brassard 等提出了一个量子比特承诺方案(BCJL 方案),他们声称该方案是无条件安全的;对任意 NP 问题,由量子比特承诺可获得量子零知识协议(quantum zero-knowledge protocol),这是由 S.Goldwasser 等首先提出的.在量子不经意传输方面,1991 年,Bennett 等在 Wiesner 的基础上提出一个实用量子不经意传输协议(BBCS 协议),Yao 以量子比特承诺是安全的为基础证明了 BBCS 协议的安全性.量子不经意传输协议的应用导出两方量子计算,Crepeau 等在量子不经意传输协议基础上提出了量子两方计算协议并进行了研究.然而 Mayers 于 1995 年开始对已提出的量子比特承诺质疑,并在 1995 年发现了一个细微而关键的安全漏洞.1997 年,Mayers 以及 Lo 和 Chau 独立地证明量子比特承诺的不安全性,由此证明了 1997 年前的量子比特承诺及建立在此基础上的各种协议都是不安全的,这给量子比特承诺及其相关方面的研究者们以致命的打击.尽管如此,量子比特承诺仍然是人们关注的课题,人们企图发现并

1)在经典密码学中,一个协议一经提出,人们就试图论证该协议是不安全的,因为只有这样才能真正保证协议的安全性和实用性

构造安全量子比特承诺协议,最近人们又提出了几个方案[22],当然这些方案的安全性是在一定的条件下得到保证的.量子比特承诺及其相关方面引起人们的兴趣的原因在于安全的比特承诺及相关协议在量子认证系统中有重要的应用价值.

5 量子信息安全与其他学科的关系

量子信息安全是一门交叉学科,它是量子力学和经典密码学相结合的产物,同时与量子光学、光纤通信、激光通信、非线性光学等学科有着紧密联系.量子力学和经典密码学为量子密码学提供理论基础,可以认为它们是构成量子密码学的基石,例如量子密码离不开测不准原理,同时量子密码的基本思想来源于经典密码学.量子光学为量子密码提供实现各种方案的物理基础,同时提供寻找新方法的可能性,到目前为止,所有的量子密码学协议和算法都是以量子光学的某一物理现象为基础而实现的.例如,正是由于在80年代光子纠缠态的实验发现使得英国牛津大学的A.K.Ekert发现了利用光子纠缠态来实现量子密钥分发和存储.光纤通信、激光通信和非线性光学是实现量子密码学的物理保障,它们用来验证量子密码学,同时为量子密码学的实验和商用化提供基础.

6 量子密码学应用与展望

量子密码经过多年的研究取得了丰富的成果,其无条件安全性和潜在商机不但吸引了学术界的重视,也引起了一些国家的政府和军事部门(主要是美国和欧洲一些国家)的注意.人们预测,当量子计算机成为现实时,经典密码体制将无安全可言,量子信息安全系统可能成为保护数据安全的最佳的选择之一.目前,在量子密钥分发的实用化实验研究中,量子比特的传输距离可达30km左右,但传输速率仅有几百kb/s,虽然可以在小规模网络中应用,但离商用还有一段路程.因此量子信息安全系统的商用化还有一系列工作要做,例如,如何提高量子信道中的传输速度和传输距离,以及改善出错率将是今后量子信息安全系统的实用化进程中首先必须解决的几个技术问题.

参 考 文 献

[1] Wiesner S. Sigact News, 1983, 15: 78 (原稿写于1970)

[2] Bennett C H, Brassard G. IEEE International Symposium on Information Theory, September 1983, 91

[3] Bennett C H, Brassard G. Advances in Cryptology: Proceedings of Crypto 84, August 1984, Springer-Verlag, 475

[4] Shannon C E. Bell Syst. Tech. J., 1948, 27: 379, 623

[5] Barnett S M, Phoenix S J D. Phys. Rev. A, 1993, 48: R5

[6] Schumacher B, Phys. Rev. Lett., 1998, 80: 5695

[7] Bennett C H, Shor P W. IEEE Trans. on Inf. Theory, 1998, 44: 2724

[8] Fuchs C A, Peres A. Phys. Rev. A, 1996, 53: 2038

[9] Bennett C H, Brassard G, Crepeau C *et al*. IEEE Trans. Inform. Theory, 1995, 41: 1915

[10] Deutsch D, Ekert A, Jozsa R *et al*. Phys. Rev. Lett., 1996, 77: 2818

[11] Schneier B. Applied Cryptography. John Wiley & Sons, Inc., 1996

[12] Hillery M, Buzek V, Berthiaume A. Los Alamos e-print archieve, quant-ph/9806063 Phys. Rev. A, 1999, 59: 1829

[13] Karlsson A, Koashi M, Imoto N. Phys. Rev. A, 1999, 59: 162

[14] Cleve R, Cottesman D, Lo H K. Phys. Rev. Lett., 1999, 83: 648

[15] Bennett C H. Phys. Rev. Lett., 1992, 68: 3121; Ekert A K. Phys. Rev. Lett., 1991, 67: 661; Ekert A K, Rarity J G, Tapster P R *et al*. Phys. Rev. Lett., 1992, 69: 1293

[16] Slutsky B A, Rao R, Sun P C *et al*. Phys. Rev. A, 1998, 57: 2383; Lutkenhaus N. Phys. Rev. A, 1996, 54: 97

[17] Bennett C H, Bessette F, Brassard G *et al*. J. Cryptology, 1992, 5: 3; Breguet J, Muller A, Gisin N. J. Modern Optics, 1994, 41: 2405; Phoenix S, Barnett S, Townsend P *et al*. J. Modern Optics, 1995, 42: 1155

[18] Biham E, Huttner B, Mor T. Phys. Rev. A, 1996, 54: 2651; Townsend P D, Rarity J G, Tapster P R. Electronics Letters, 1993, 29: 634; Townsend P D, Rarity J G, Tapster P R. Electronics Letters, 1993, 29: 1291

[19] Zeng G, Zhang W. Phys. Rev. A, 2000, 61: 2303

[20] Dusek M, Haderka O, Hendrych M *et al*. Phys. Rev. A, 1999, 60: 149; Zeng G H, Guo G, e-print archieve, quant-ph/0001045

[21] Crepeau C. J. Modern Optics, 1994, 41: 2445; Lo H, Phys. Rev. A, 1997, 56: 1154

[22] Kent A. Phys. Rev. Lett., 1999, 83: 1447