第 51 卷 第 4 期 2002 年 4 月
1000-3290/2002/51(04)/0727-04

物 理 学 报
ACTA PHYSICA SINICA

Vol.51,No.4,April,2002

基于非正交态的量子密钥验证方案*

曾贵华† 诸鸿文

(上海交通大学电子工程系,上海 200030)

(2000 年 9 月 30 日收到;2001 年 10 月 11 日收到修改稿)

研究了量子密钥分发的验证问题,并利用非正交量子态设计了一个协议,该协议既能分发量子密钥,又能验证所分发的量子密钥的真实性,从而防止了以往所提出协议中可能存在的假冒问题.

关键词:量子密钥验证,量子密码,量子物理,密码学

PACC:0367,0365

1. 引 言

自从 IBM 公司和 Montreal 大学联合提出第一个量子密钥分发协议——BB84 协议以来[1],量子密码经过多年的研究取得了丰富的成果,形成了一个系统的理论体系[2,3].目前量子密码的主要研究成果包括量子密码理论基础[4]、量子保密系统[5]、量子认证系统[6]等几个方面.量子密码的无条件安全性和潜在商机不但吸引了学术界的重视,也引起了非学术界有关部门如军方、政府与银行等部门的密切关注.

在现代保密系统中,由于算法的结构一般是公开的,密钥的管理变得特别重要.一般而言,密钥管理包括密钥分发、密钥存储、密钥验证等方面,其中密钥的验证是为了保证所获得密钥的可靠性,这是保证密钥安全的一个重要方面.在最近提出的量子密码术中,物理学家和密码学家对量子密钥分发进行了大量的研究和探讨,但所提出的量子密钥分发协议都是假定通信者是合法的,这种假设无法确保所获得密钥的可靠性,因为在实际应用中存在假冒的可能.因此,为了获得真正安全的密钥,有必要对所获得的量子密钥进行真实性验证.

最近文献[7]对量子密钥的验证问题首次做了研究,提出了一个基于纠缠态[8,9]的量子密钥验证协议.本文从另一个角度研究量子密钥的验证问题,并利用非正交量子态提出了一个新的量子密钥验证协议,该协议不但能分发量子密钥,而且能验证所获得的密钥的可靠性,同时该协议具有无条件安全性.

2. 预备知识

量子密码研究如何利用量子物理的有关原理、效应或现象来实现密码与保密通信中的协议与算法,这与经典[1)]密码的方式类似(经典密码利用有关的数学问题来实现密码与保密通信中的协议与算法).目前量子密码研究的内容仍然是密钥分发、秘密共享、签名等经典密码中出现过的问题,但量子密码采用的方法是量子物理的方法.如何采用相关的物理原理、效应或现象而不是用数学问题来实现保密通信是量子密码的关键所在.本文所提出的协议的实现基础是非正交量子态不可区分原理,下面首先介绍这个原理.

在量子物理中,任意两个非正交量子态($|\psi\rangle$,$|\phi\rangle$)是不可区分的.因此,对两个非正交量子态做量子测量后不可能获得精确结果,这是由著名的不确定原理所决定的.量子测量有很多种测量方式,不同的测量方式会得到不同的测量结果,这里介绍两种.

1) Bennett 的方法:这种方法中选取两个不兼容的投影算符

$$P_\psi = 1 - |\psi\rangle\langle\psi|, \tag{1}$$

$$P_\phi = 1 - |\phi\rangle\langle\phi|. \tag{2}$$

* 国家自然科学基金(批准号:69803008)资助的课题.

† E-mail address: guihuazeng@hotmail.com

1) 因为基于数学的密码学中亦有经典和现在之分,所以请读者注意,这里"经典"相对于"量子"而言.

在这种情况下,获得正确量子态概率为

$$p_c = \frac{1 - |\langle\psi | \phi\rangle|^2}{2}, \tag{3}$$

出现错误结果的概率为

$$p_e = \frac{1 + |\langle\psi | \phi\rangle|^2}{2}. \tag{4}$$

显然,最终测量结果中的错误率超过 50% .

2) Ekert 方法 构造如下算符:

$$A_\psi = \frac{1 - |\psi\rangle\langle\psi|}{1 + |\langle\psi|\phi\rangle|}, \tag{5}$$

$$A_\phi = \frac{1 - |\phi\rangle\langle\phi|}{1 + |\langle\psi|\phi\rangle|}, \tag{6}$$

$$A_? = 1 - A_\psi - A_\phi, \tag{7}$$

式中 $A_?$ 表示非确定性算符.这种情况下,非确定性结果(*inconclusive result*)为

$$|\langle\psi|\phi\rangle| = \cos 2\theta, \tag{8}$$

式中 θ 为两个非正交量子态的夹角,$0 < \theta < \pi/4$.上式说明错误结果为 $\cos 2\theta$,这种方法也不能精确区分量子态为 $|\psi\rangle$,$|\phi\rangle$.研究表明,由于这两个量子态的不可区分性,即使采用最好的测量方法,出错率仍为 17% [10] .以上说明了非正交量子态是不可区分的.这种不可区分性在量子密码中有重要的价值,实际上,量子密码的根本点就是非正交量子态不可区分性,因为这种不可区分性使得未知量子态不可克隆.本文将利用这种不可区分性来实现量子密钥的验证问题.

3. 协议描述

按照惯例,通信者用 Alice 和 Bob 表示,假设 Alice 和 Bob 间有共享信息 K_1(认证密钥),本文提出的协议描述如下:

第一步,Alice 和 Bob 将认证密钥 K_1 转换成测量基序列.当 Alice 和 Bob 需要验证各自的身份时,他们根据预先的约定,秘密地将保存的共享密钥 K_1 转化为量子态的测量基矢序列.例如,如果 Alice 和 Bob 采用极化光子态的测量基,这种情况下有两种测量基矢:rectilinear 和 diagonal 测量基,则可让‘0’对应 rectilinear 基,让‘1’对应 diagonal 基.为方便我们用符号 $\oplus$ 表示 rectilinear 测量基,$\odot$ 表示 diagonal 测量基,这时我们可将 K_1 转化为由 rectilinear 和 diagonal 测量基组成的测量基序列.例如,若 K_a = 00110,则对应的测量基序列为$\odot\odot\oplus\oplus\odot\oplus$.

第二步,Alice 和 Bob 建立量子信道.当 Alice 和 Bob 希望进行量子通信时,他们需要建立一个量子信道.量子信道中传输的量子态可以是各种,在本协议中采用非正交量子态.Alice 每次随机地从非正交量子态 $|\psi\rangle$,$|\phi\rangle$ 选取一个,测量她的粒子,记录结果,然后发送给 Bob.

第三步,Bob 测量收到的量子比特串.Bob 用两个测量算符 M 和 M_{K_1} 随机测量所收到的量子态,其中 M 用于获取新的认证密钥,M_{K_1} 用于当前通信中通信者的身份认证.

第四步,检测窃听者.Bob 随机地从测量算符 $M 所测的粒子中选取部分结果,将这些结果告之 Alice,然后根据 Bennett 的理论[11] 检测窃听者存在与否.

第五步,Bob 用 K_1 加密其用测量算符 M_{K_1} 测量的结果.虽然 Bob 不知道 Alice 的测量结果,但这并不影响身份验证,实际上,正是这样才避免了 Bob 的假冒.下面讨论加密过程:

设 Bob 收到的用于认证的量子态序列为

$$|\Psi\rangle = \{|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_n\rangle\}, \tag{9}$$

式中 $|\psi_i\rangle$ 表示 Bob 的一个粒子量子态.必须注意,上式中的量子态序列 Bob 并不知道.Bob 对量子态 $|\Psi\rangle$ 测量后获得结果

$$|\Phi\rangle = M_{K_1}|\Psi\rangle, \tag{10}$$

式中

$$|\Phi\rangle = \{|\phi_1\rangle, |\phi_2\rangle, \cdots, |\phi_n\rangle\},$$
$$|\phi_i\rangle = M^i_{K_1}|\Psi\rangle. \tag{11}$$

按照约定将 $|\Phi\rangle$ 转化为 m 比特串,然后用 K_1 加密 m 和量子态 $|\psi\rangle$ 对应的序列号 N,得到密文

$$y = E_{K_1}(m, N). \tag{12}$$

Bob 将密文 y 送给 Alice.

第六步,Alice 验证 Bob 的身份.收到 Bob 送来的密文 y 后,Alice 用 K_1 解密密文 y

$$m', N = D_{K_1}(y), \tag{13}$$

然后与自己的结果进行比较,从而 Alice 得到测量基 M_{K_b},如果 $K_b = K_1$,于是断定 Bob 的身份是真.

第七步,Bob 验证 Alice 的身份.Alice 获得 m' 后,将 m' 送给 Bob.若 $m' = m$,则断定 Alice 的身份是真.

第八步,Alice 和 Bob 放弃认证密钥 K_1,并获得

新的认证密钥.身份验证完成后,K_1 完成了它的使命,Alice 和 Bob 不再使用 K_1,他们从测量算符 M 的测量结果中获得密钥,并获得新的认证密钥,方法与 B92 协议相同.

4. 安全性分析

本协议可能存在的安全性问题有:1)密钥的首次获取;2)认证密钥 K_1 的安全性.下面分析这些可能的安全问题在本协议中是否存在.

安全问题 1)涉及所谓的 Catch22 问题[12],这是密码学中存在的基本问题.本协议中,我们采用公钥密码体制解决,方法为:通信者利用经典密码学中的公钥体制获得密钥实现首次认证,然后在有效时间内进行量子通信,获得量子密钥,并放弃原来由公钥体制所得到的密钥.必须说明的是,量子密钥的获得须在公钥体制的有效时间内,例如:若公钥体制需要一年才能破译,则可在由公钥体制获得密钥后小于一年或或更短的时间内获得量子密钥,并放弃由公钥体制所获得的密钥[1)].

对于认证密钥 K_1,我们认为是安全的,理由如下.一方面 K_1 的获取是由上次通信中采用量子密钥分发的方式,其安全性与量子密钥分发协议的安全性相同,另一方面,K_1 只使用一次,是一个动态密钥.

综上可知,本协议防止了假冒问题;同时,重放攻击也不可能成功,因为密钥仅使用一次;量子攻击也是无效的,理由与 B92 协议相同.本协议的安全性与 Bennett 于 1992 年提出的 B92 协议相同,因此该协议具有无条件安全性.

5. 结　论

本文利用非正交量子态提出了一个量子密钥验证协议,该协议能有效地验证所获得密钥的可靠性和真实性,从而保证了信息交换时的安全性.由于非正交量子态的不可区分性,该协议是无条件安全的.

[1] Bennett C H and Brassard G 1984 *Advances in Cryptology*: *Proceedings of Crypto* 84 (Springer-Verlag) pp475—480

[2] Zeng G 1999 *Summarization of Postdoctoral Research* (Xi'an: Xidian university) (in Chinese)

[3] Zeng G 2000 *Physics* **29** 623 (in Chinese) [曾贵华 2000 物理 **29** 623]

[4] Bennett C H and Shor P W 1998 *IEEE Trans. Inf. Theory* **44** 2724

[5] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptology* **5** 3

[6] Dusek M, Haderka O, Hendrych M and Myski R 1999 *Phys. Rev.* A **60** 149
Zeng G and Guo G 2000 *Preprint* quant-ph/0001046

[7] Zeng G and Zhang W 2000 *Phys. Rev.* A **61** 022303

[8] Gong S 2000 *Chin. Phys.* **9** 94

[9] Shi M G, Du J F and Zhu D P 2000 *Acta Phys. Sin.* **49** 825 (in Chinese) [石名俊、杜江峰、朱栋培 2000 物理学报 **49** 825]

[10] Bose S, Vedral V and Knight P L 1998 *Phys. Rev.* A **57** 822

[11] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[12] Zeng G 1999 *Tongxin Baomi* **10** 1 (in Chinese)

1) 现有的公钥体制在量子计算机出现后将不在安全,但是可以肯定,将来必有针对量子计算机的公钥密码体制.

Quantum key verification scheme based on non-orthogonal quantum states *

Zeng Gui-Hua Zhu Hong-Wen

(*Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai* 200030, *China*)

(Received 30 September 2000; revised manuscript received 11 October 2001)

Abstract

The reliability of the obtained quantum key is investigated, and a quantum key verification scheme based on non-distinguishability of unknown two-nonorthogonal states is proposed.

Keywords: quantum key verification, quantum cryptography, quantum physics, cryptography

PACC: 0367, 0365

* Project supported by the National Natural Science Foundation of China (Grant No. 69803008).