



基于可信控制中心的量子密钥中继方案^{*}

蒋韶生, 池瑞楠, 温晓军

(深圳职业技术学院计算机工程学院 深圳 518055)

摘 要:提出了一种利用可信控制中心以及可信量子中继服务器进行量子密钥中继传输的实现方案。在设计可信中继点协议上采用了量子密钥一次一密的加密算法,在组建可信中继网络时,利用可信控制中心来保证接入中继的可信性与安全性,并把用户地址隐藏于已加密的量子信息数据中,只有合法的可信用户才能解密并进行信息传输。实验结果表明,用户之间即使没有量子信道直接相连,仍然可以利用可信中继网络进行量子密钥长距离的安全传输,该量子密钥中继方案是可行的。安全性分析表明,在传输过程中,攻击者无法获取到真正有用的量子密钥信息。

关键词:量子密钥;可信中继;可信控制中心;可信量子中继服务器

doi: 10.3969/j.issn.1000-0801.2014.06.016

Quantum Key Relay Scheme Based on Trusted Control Center

Jiang Shaosheng, Chi Ruinan, Wen Xiaojun

(School of Computer Engineering, Shenzhen Polytechnic, Shenzhen 518055, China)

Abstract: A transmit quantum key relay scheme based on trusted control center and trusted quantum relay server was proposed. The quantum key one-time pad encryption algorithm was used in the design of trusted relay protocol. Upon the establishment of trusted relay network, the trusted control center was used to ensure the credibility and security of access relay, and the user's IP address was hidden in the quantum information data that had been encrypted only for the legal user to decrypt and transmit credible information. The security analysis shows, users who do not connect with the quantum channel can still use the trusted relay network to transmit quantum key securely in a long-distance transmission while attackers can not obtain useful quantum key information from the network.

Key words: quantum key, trusted relay, trusted control center, trusted quantum relay server

1 引言

量子安全通信网络是以量子密钥分发为基础,结合量子密钥分配网络和经典通信技术而形成的安全的信息传输系统。由于量子密码的两个基本特征——对窃听的可检测性和无条件安全性,保证了量子安全通信网络的无条件安全性^[1],因此该网络是下一代安全通信的重要发展方向。

然而,在远距离量子通信系统中,由于光子极易被信道吸收,造成信号随通信距离指数衰减、误码率提高,进而导致通信失败。所以量子通信的距离被限制在 100 km 的量级,试验距离也不过 200 km^[2]。因此,建立一种类似于传统通信中的中继器来补偿因信号衰减造成的损失,最终实现大规模的远距离量子通信,成为当前研究的热点,许多国家都在建立相关的实验保密通信网络。美国早在 2005 年

^{*} 广东省自然科学基金资助项目(No.S2013010015471),深圳市基础研究计划基金资助项目(No.JCYJ20120617140737337, No.JCYJ20130331151803073)



$$K_i = \{k_i^1, k_i^2, \dots, k_i^l, \dots, k_M^l\} (i=1, 2, \dots, R; R=N-L) \quad (7)$$

步骤 5 通过经典信道, Alice 和 QRS 对原始密钥 K_i 中的 Q bit 再次进行公开比较, 假定其中出错率 $\varepsilon \leq \varepsilon_0$ (ε_0 为错误率阈值) 就采用 K_i 做原始密钥, 否则放弃 K_i 。如果采用, 则将 Q bit 从原始密钥 K_i 中删除并进行校验位处理。假定校验位处理后需放弃 P bit, 则最后局部共享密钥 K_i 为:

$$K_i = \{k_i^1, k_i^2, \dots, k_i^l, \dots, k_M^l\} (i=1, 2, \dots, M; M=N-L-Q-P) \quad (8)$$

步骤 6 同上述步骤 1~步骤 5, Bob 与 QRS 进行量子通信, 产生局部共享密钥 K_2 。

第二阶段: 初始密钥的加解密与传送。

步骤 1 Alice 与 QRS 约定用手中的局部密钥 K_1 作为传输的量子密钥, 即 $K=K_1$ 。

步骤 2 QRS 将得到的传输密钥 K_1 的每一位与 K_2 的对应位进行异或加密得到 C_2 , 然后通过经典信道将 C_2 传送给 Bob。 C_2 表示如下:

$$C_2 = \{c_1^2, c_2^2, \dots, c_i^2, \dots, c_M^2\} (i=1, 2, \dots, M) \quad (9)$$

式 (9) 中: $c_1^2 = k_1^1 \oplus k_1^2, c_2^2 = k_2^1 \oplus k_2^2, \dots, c_i^2 = k_i^1 \oplus k_i^2, \dots, c_M^2 = k_M^1 \oplus k_M^2$ 。

步骤 3 Bob 接收到 C_2 后则使用 K_2 的每一位对 C_2 的对应位进行异或解密得到 K_1 (传输密钥 K), 即 $k_1^1 = c_1^2 \oplus k_1^2, k_2^1 = c_2^2 \oplus k_2^2, \dots, k_i^1 = c_i^2 \oplus k_i^2, \dots, k_M^1 = c_M^2 \oplus k_M^2$ 。

需要说明的是, 第三方可以作为 QRS 是有一个前提的, 就是它必须是可信的第三方, 因为 QRS 在整个过程中同样也掌握着传输密钥 K 。因此在网络中, 需要设计可信中继节点, 确保 QRS 的可信性, 即为 TQRS, 这对于在网络中任意两个用户之间进行量子密钥的传输是相当重要的条件。

3 可信中继网络的设计

有了 TQRS, 就可以基于它与邻近的用户建立相应的量子信道, 实现相应的量子密钥传输中继功能。但网络中的两个用户若暂时不能实现同时共享一个 TQRS, 则可以组建基于 TCC 控制下的树型网络, 网络中的 TQRS 为中继交换中心节点, 由 TCC 保证中继交换中心节点的合法性与安全性, 即为可信中继。通过可信中继, 可以实现任意两个用户的间接相连, 并通过间接相连中的 TQRS 实现两用户的量子密钥共享功能。可信中继网络设计如图 2 所示。

数据线路为用户之间传递已加密数据的传输线路。量子信道, 主要负责量子密钥的产生与中继传输。

鉴于量子通信的距离被限制在 100 km 量级的特性^[2],

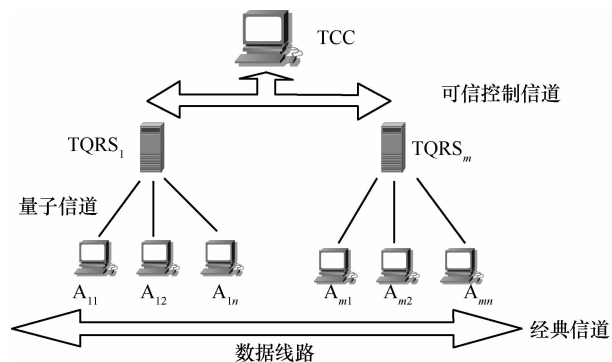


图 2 TCC 控制下的量子密钥可信中继传输

可以在需要量子密钥共享的区域设置若干个 TQRS, 然后根据规模设计相应的可信控制线路, 并由 TCC 控制中心保证 TQRS 及网络的可信程度。这其中的设计过程超出了本文的研究范围, 在此不再论述。

从图 2 中可以看出, 网络中的同一可信中继 TQRS 群里的用户都能通过与可信中继 TQRS 建立量子信道, 并采用前述的中继点协议完成任意两用户间的量子密钥共享。当用户属于不同群时, 如分属于 TQRS₁ 和 TQRS_m 两个群中时, 就牵涉量子密钥在 TCC 控制下的可信控制线路的传输问题, 在实际应用中常常会有这方面的需求, 下面阐述它们的传输协议。

4 网络中量子密钥的安全传输协议

量子网络中数据的保密传输通常是采用单向加密解密 (即单边链) 的模式进行。一般都是首先利用局部共享密钥进行加密, 传到下一个节点后用该密钥解密, 并利用另一对局部密钥再次进行加密, 再到下一个节点时进行解密, 从而获取保密数据。只要中继节点知道密钥传送的目标地址, 这种基于经典可信节点的中继方式很容易得到实现和验证。但在经典网络中, TQRS 则必须考虑传送的安全问题, 因为经典网络中没有量子网络中传递密钥时的无条件安全性作为保障, 非法用户若能获取目标网络地址, 则有进一步窃取并复制密钥数据的机会。因此在传送量子密钥的整个过程中, 设计引入了目标用户 IP 地址需同步加解密的机制, 可信中继必须在解密之后根据获取的目标用户网络地址传递量子密钥, 而接收到量子密钥的目标用户只要在解密之后, 即可事先得知共享量子密钥的对方用户网络地址, 则可以有效加强网络中的数据安全传输。下面提出一个网络中任意两个用户之间进行量子密钥安全传输的协议过程, 如图 3 所示。

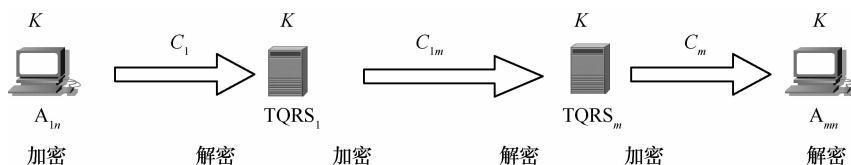


图 3 任意中继用户量子密钥安全传输过程

图 3 描述的是用户 A_{in} 希望与用户 A_m 之间共享密钥 K , 它们分属于不同的 TQRS 群, 密钥的传输过程设计如下。

步骤 1 用户 A_{in} 按照 BB84 协议与 $TQRS_1$ 进行量子通信, 双方获取局部共享量子密钥 K_1 , 并以此作为将与用户 A_m 共享的量子密钥 K 。过程如同前述中继点协议第一阶段所示, 在此不再复述。

步骤 2 A_{in} 用户将需要传输的用户地址 $A_m - A_{in}$ 按照协议约定组合成 K_0 。目前经典网络主要使用 IPv4 地址, 表达一个地址共需 32 bit, 因此可以组合为:

$$K_0 = \{k_0^{in}, k_1^{in}, \dots, k_i^{in}, \dots, k_{31}^{in}, k_0^{ln}, k_1^{ln}, \dots, k_j^{ln}, \dots, k_{31}^{ln}\} (i, j = 0, 1, \dots, 31) \quad (10)$$

然后用量子密钥 K_1 的每一位与 K_0 的对应位进行异或加密得到 C_1 , 即:

$$C_1 = \{c_1^1, c_2^1, \dots, c_i^1, \dots, c_j^1, \dots, c_{64}^1\} (i = 1, 2, \dots, 32; j = 33, 34, \dots, 64) \quad (11)$$

式 (11) 中: $c_1^1 = k_1^1 \oplus k_0^{in}, \dots, c_i^1 = k_i^1 \oplus k_i^{in}, \dots, c_j^1 = k_j^1 \oplus k_j^{ln}, \dots, c_{64}^1 = k_{64}^1 \oplus k_{31}^{ln}$ 。如果 K_1 不足 64 bit, 则不足位数再从 K_1 开始循环取数。随后 A_{in} 用户将 C_1 通过经典信道传输给 $TQRS_1$ 。

步骤 3 $TQRS_1$ 接收到 C_1 后首先利用 K_1 的每一位与 C_1 的对应位进行异或解密得到 K_0 , K_0 的各位为 $k_1^0 = k_1^1 \oplus c_1^1, \dots, k_i^0 = k_i^1 \oplus c_i^1, \dots, k_{64}^0 = k_{64}^1 \oplus c_{64}^1$ 。从而分离出需要共享量子密钥用户的地址 $A_m - A_{in}$, 规则同式 (2), 分离方法如下:

$$A_m = \{A_0^{in}, A_1^{in}, \dots, A_i^{in}, \dots, A_{31}^{in}\} (A_m \subset K_0; A_i^{in} \in \{k_1^0, \dots, k_{32}^0\}) \quad (12)$$

$$A_{in} = \{A_0^{ln}, A_1^{ln}, \dots, A_j^{ln}, \dots, A_{31}^{ln}\} (A_{in} \subset K_0; A_j^{ln} \in \{k_{33}^0, \dots, k_{64}^0\}) \quad (13)$$

$TQRS_1$ 在获取目的用户 A_m 的地址后, 则通过可信控制线路向 TCC 申请与用户 A_m 所属的 $TQRS_m$ 共享传输密钥。

步骤 4 TCC 收到申请后, 向 $TQRS_1$ 及 $TQRS_m$ 分发局部共享密钥 K_{lm} (在可信控制线路内有效, 且一次一密)。

步骤 5 $TQRS_1$ 将需要传输的量子密钥 K_1 以及需要传送的地址 $A_m - A_{in}$ 按照协议约定组合成 K_0 , 即:

$$K_0 = \{k_0^{in}, \dots, k_i^{in}, \dots, k_{31}^{in}, k_0^{ln}, \dots, k_j^{ln}, \dots, k_{31}^{ln}, k_1^1, \dots, k_h^1, \dots, k_M^1\} \quad (h = 1, 2, \dots, M; i, j = 0, 1, \dots, 31) \quad (14)$$

然后用 TCC 分发的 K_{lm} 的每一位与 K_0 的对应位进行异或加密得到 C_{lm} , 加密的规则同步骤 2。 C_{lm} 形式如下:

$$C_{lm} = \{c_1^{lm}, c_2^{lm}, \dots, c_i^{lm}, \dots, c_N^{lm}\} (i = 1, 2, \dots, N; N = M + 64) \quad (15)$$

随后 $TQRS_1$ 将 C_{lm} 通过经典信道传输给 $TQRS_m$ 。

步骤 6 $TQRS_m$ 接收到 C_{lm} 后则首先利用 TCC 分发的 K_{lm} 的每一位与 C_{lm} 的对应位进行异或解密得到 K_0 , 解密的规则同步骤 2。得到 K_0 后, 先分离出需要传送共享密钥的目标用户 A_m 的地址, 如同式 (12)。

步骤 7 $TQRS_m$ 按照 BB84 协议与用户 A_m 进行量子通信, 双方获取局部共享量子密钥 K_m 。

步骤 8 $TQRS_m$ 用局部共享量子密钥 K_m 的每一位与 K_0 的对应位进行异或加密得到 C_m , 方法同步骤 5。随后 $TQRS_m$ 将 C_m 通过经典信道传输给用户 A_m 。

步骤 9 用户 A_m 接收到 C_m 后, 用局部共享量子密钥 K_m 的每一位与 C_m 的对应位进行异或解密得到 K_0 , 解密的规则同步骤 2。得到 K_0 后, 首先分离出需共享量子密钥用户 A_{in} 的地址, 同式 (13), 然后获取共享量子密钥 K , 如式 (16):

$$K = \{K_1, K_2, \dots, K_i, \dots, K_M\} (K \subset K_0; K_i \in \{k_{65}^0, \dots, k_{64+M}^0\}) \quad (16)$$

步骤 10 用户 A_{in} 与用户 A_m 此时均已知需要保密通信的双方用户地址, 可以建立相应的安全通信传输机制, 然后利用双方共享的量子密钥 K 对需传输的数据进行加解密操作并在经典网络上传输 (注: 量子密钥 K 仍需一次一密, 每次数据传输都必须获取新的共享量子密钥 K)。

5 实验结果及其分析

实验的搭建是基于可信中继网络的设计来进行的。测试环境: 2 台 Windows XP 操作系统的计算机作为用户使用的带有量子信道的计算机, 3 台 Windows7 操作系统的带有 TPM 安全芯片的可信计算机分别作为可信网络中的 1 台 TCC 和 2 台 TQRS, 1 台基于 IEEE 802.1x 技术的交换机以及 2 套量子密码生成终端实验系统。



实验中,假定两台带有量子信道的计算机分别代表用户 A_m 和 A_n ,按照上述量子网络中量子密钥的安全传输协议,将 A_m 的量子密钥经过 2 台 TQRS 安全传送给 A_n 。传输过程中 TCC 保证 2 台 TQRS 节点的合法性与安全性,且向其随机分发共享密钥,最终实现量子密钥在可信网络的安全传输。

为了分析量子密钥在网络中的安全传输效率,在量子密码生成终端实验系统里特地设计了密钥传输统计模块进行密钥传输效率统计。当用户 A_m 最终获取到量子密钥 K 后,则向分离出需共享量子密钥用户 A_n 的地址按照 TCP/IP 发送收到信号,用户 A_n 确认后,双方将该次传输的量子密钥存入自己相应的量子密钥数据池,作为双方通信的可以使用的共享量子密钥,接着继续进行下一轮的量子密钥安全传输。如果用户 A_m 最终未获取到量子密钥 K 或者两个用户之间没有成功确认该轮量子密钥的安全传输,则此次需共享的量子密钥作废,重新进行下一轮的量子密钥安全传输。

在用户 A_n 中,用密钥传输统计模块进行统计后的曲线如图 4 所示。

图 4 中统计曲线的统计信息分为两个部分,上部曲线是指经过可信中继传输后的两个用户之间量子密钥相同率,即经过用户 A_m 确认的成功传输的量子密钥占用户 A_n 传输出去的量子密钥总和的比率,从图中可以看出量子密钥最终能成功传输的比率大概为 98% 左右。

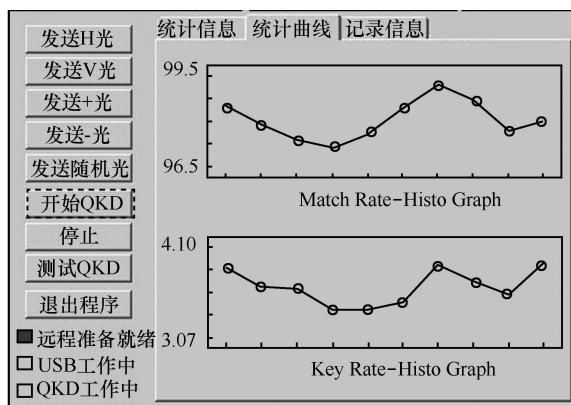


图 4 量子密钥成码情况统计曲线

多次试验验证,只要量子密钥损失率低于 5%,则可以进行的量子密钥加解密信息传递。下部曲线是最终两个用户间成功传输的量子密钥增长速率,从图中可以看出量子密钥增长速率大概为 4 kbit/s 左右,该速率符合本实验系统中量子密码生成终端实验系统的性能范围指标。用户 A_n 的量子密钥传输相应的统计数据信息如图 5 所示。

在图 5 中,经过安全传输用户之间可用的量子密钥达到了近 200 kbit 左右,由于还有未经验证确认的量子密钥正在可信中继网络不断地安全传输,因此可用的量子密钥量还将不断增长。当双方进行安全通信时,必须使用量子密钥池里的量子密钥进行加解密传输,使用后的量子密钥

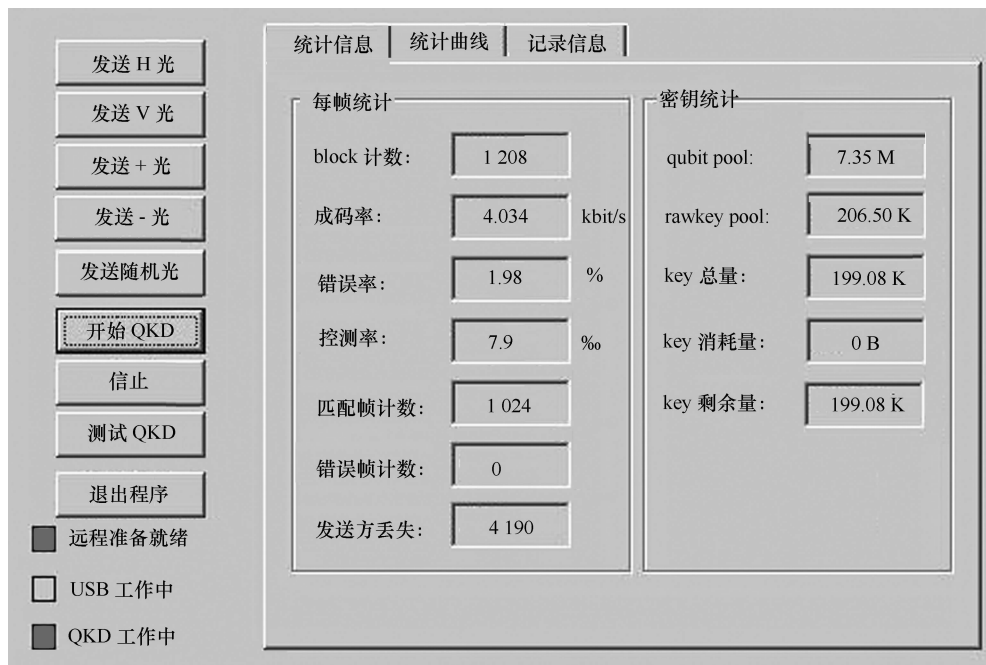


图 5 量子密钥传输统计数据

将会被抛弃,并记录进量子密钥的消耗量中。

由上述试验可见,通过本文设计的可信中继网络和量子密钥的安全传输协议,没有量子信道直接相连的两用户间完全可以进行量子密钥中继传输。为了保证量子密钥的安全性,该中继传输方案必须在 TCC 控制下的可信网络中进行。

6 安全性

在安全性上,本文中用户与 TQRS 中继点协议设计中量子密钥的生成与共享是按照 BB84 协议来完成的,这已经被证明是无条件安全的^[6];在量子密钥的使用上,即便攻击者在经典信道中通过任何手段获取了某段加密数据,但由于本文采用的是一次一密的加解密传输方式,攻击者采用的任何破解手段均不能影响整个加密数据传输的安全性;对于 TQRS,由 TCC 按照可信网络连接的方案接入可信中继者,按照该方案,可信网络能够转移攻击者带来的风险,且无法在可信中继网络中伪装成中继者完成协议的运行^[4],密钥的中继传输得到了安全性保证;在可信中继网络的设计上,共享量子密钥在经典可信控制网络中仅为两用户所属的 TQRS 之间加密传输,攻击者若想获取量子密钥,至少要满足两个条件之一方可获取,一是冒充中继者获取加密密钥,但前面已证明在可信控制网络中是无法冒充中继者获取的。二是明确知道量子密钥的传输目标并设法截取加密后的量子密钥,但本文在设计中引入了目标用户 IP 地址同步加解密的机制,攻击者无法提前获知共享量子密钥的传输目标,因此无法获取量子密钥;在量子密钥的使用上,采用一次一密的加密使用机制,因此攻击者即便在经典网络中获取了含量子密钥的片段加密内容,也无法分析出其他部分内容所使用的量子密钥。

7 结束语

本文提出了一种在可信网络中利用可信中继服务器传输量子密钥的实现方案。通过量子密钥中继点协议的设计以及在树型结构可信网络中设置 TCC、TQRS 的方法,实现了量子密钥在网络中任意两用户间的安全共享。结合在所有密钥的传输过程中均使用一次一密的加密算法,将目标用户地址隐藏于已加密的量子信息数据中等信息安全设计思想,进一步保证了量子密钥中继传输过程的安全性。安全性证明,在量子密钥产生到传输的各个阶段,攻击

者无法获取有用的量子密钥信息。未来进一步加上身份识别等环节,即可成为一个完善实用的在可信网络中进行量子密钥中继传输的系统。

参考文献

- 1 Schiff J, Poirier B. Communication: quantum mechanics without wavefunctions. *Journal of Chemical Physics*, 2012, 136 (3): 031102~031105
- 2 Shamsolah S, Shahram M. An error-free protocol for quantum entanglement distribution in long-distance quantum communication. *Chinese Science Bulletin*, 2011,56(7):618~625
- 3 Chen T Y, Liang H, Liu Y, *et al.* Field test of a practical secure communication network with decoy-state quantum cryptography. *Optics Express*, 2009,17(8):6548~6549
- 4 Yu Y S. Extended research on trusted network connection under Web environment. *Journal of East China Normal University (Natural Science)*, 2009(4):137~140
- 5 Jose C, Carlos R. Optimum design for BB84 quantum key distribution in tree-type passive optical networks. *Journal of the Optical Society of America B*, 2010,27(6):A146~A151
- 6 Peter W, John P. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 2000,85 (2): 441~444
- 7 Wen X J, Liu Y, Zhang P Y. Digital multi-signature based on the controlled quantum teleportation. *Wuhan University Journal of Natural Sciences*, 2007, 12(1):29~32
- 8 Wen X J, Tian Y, Niu X M. A group signature scheme based on quantum teleportation. *Physica Scripta*, 2010, 81(5):055001~055006
- 9 Wen X J. An E-payment system based on quantum group signature. *Physica Scripta*, 2010, 82(6):065403~065407

[作者简介]



蒋韶生,男,深圳职业技术学院工程师,主要研究方向为数据库与信息安全。

池瑞楠,男,深圳职业技术学院副教授,主要研究方向为计算机网络。

温晓军,男,博士,深圳职业技术学院教授,主要研究方向为量子密码。

(收稿日期:2014-05-28)