文章编号：2095-4980(2020)06-1098-05

一种无证书的跨域量子密钥协商协议

马　骁，施运梅*，宋　莹，孟　坤

(北京信息科技大学 计算机学院，北京 100101)

摘　要：针对传统跨域密钥协商协议安全性不足问题，提出一种新的跨域量子密钥协商协议。在无证书密钥协商体系下，采用量子密钥协商与经典密码算法结合的方案，提高了协议适应现有通信网络架构的能力。密钥协商过程使用三粒子量子隐形传态，利用量子态不可克隆定理保障协商过程中密钥的安全性。与其他方案相比，本协议具有较高的量子比特效率，并且可以抵抗中间人攻击、重放攻击等多种内部和外部攻击手段。

关键词：量子密钥协商；量子隐形传态；共享密钥；无证书

中图分类号：TN929.11　　**文献标志码：**A　　**doi：**10.11805/TKYDA2019222

A certificateless cross-domain quantum key agreement protocol

MA Xiao，SHI Yunmei*，SONG Ying，MENG Kun

(School of Computer，Beijing Information Science and Technology University，Beijing 100101，China)

Abstract：Aiming at the problem of insufficient security of traditional cross-domain key agreement protocol，a new cross-domain quantum key agreement protocol is proposed. In the certificateless key negotiation system，the combination of quantum key negotiation and classical cryptographic algorithm is adopted to improve the ability of the protocol to adapt to the existing communication network architecture. The key negotiation process uses three-particle quantum teleportation，and the quantum state non-cloning theorem can guarantee the security of the key during the negotiation process. Compared with other schemes，the proposed protocol has higher quantum bit efficiency and can resist various internal and external attacks such as man-in-the-middle attacks and replay attacks.

Keywords：quantum key agreement；quantum teleportation；shared key；certificateless

量子密码学的安全性由量子力学的基本原理确定，如海森堡测不准定理、量子的不可克隆性等，这些原理使量子密码在理论上拥有无条件安全性。随着量子技术的快速发展，人们提出许多有借鉴意义的量子密码协议，其中，量子密钥协商协议允许参与者通过量子信道协商一个经典的共享密钥，而且在协商过程中非授权用户很难成功窃听并不被发现。相对于传统的密码体系，它拥有更高的安全性。但量子信道在实际环境下会受到种种限制，因此有一种做法是把量子密钥协商协议与经典密码算法结合，构成混合密码系统。

2004 年，ZHOU[1]等提出第一个量子密钥协商协议，该协议以量子隐形传态技术为基础，但该协议不能抵抗参与者攻击，存在着一定的缺陷。2005 年，杨宇光[2]等提出一种多用户量子身份认证和密钥分配方案，该方案实现了网络中用户之间的身份认证和密钥分配。随后，国内外研究者提出了更多种类的量子密钥协商协议，如多方量子密钥协商协议[3-5]、基于 BB84 协议[6]的两方量子密钥协商协议、集体噪声信道下容错的量子密钥分配协议[7]等。现有的量子密钥协商协议多是在单一网络环境下设计，通信双方使用相同的通信服务工具进行信息交互，在这种情况下，量子密钥协商协议可以有效地保证用户信息的安全。但在实际网络通信中，通信双方可能使用不同的通信服务工具，这种情况称为跨域密钥协商，由于不同域内的验证或协商方式可能存在差异，通信双方无法直接使用各自的密钥协商协议协商出共享密钥。所以跨域协商过程中依然存在着信息遭到监听、

收稿日期：2019-06-20；**修回日期：**2019-08-04

基金项目：国家重点研发计划:私有云环境下服务化智能办公系统平台(2018YFB1004100)；中央引导地方专项“量子通信技术创新与行业应用”(Z171100004717002)

作者简介：马　骁(1994–)，男，在读硕士研究生，主要研究方向为网络安全、密码学。email:1540730779@qq.com

***通信作者：**施运梅　email:sym@bistu.edu.cn

泄露的风险。目前主流的跨域通信协议有基于口令的跨域密钥协商协议[8]、Kerberos 跨域认证协议[9]等。基于口令的密钥协商协议已被证明存在安全隐患，该协议无法抵抗字典攻击。Kim 等[10]指出了协议的问题并提供了改进版本，不过改进版本也被指出存在中间人攻击的隐患[11]。而 Kerberos 协议存在系统开销较大，对口令复杂程度要求高，时间同步困难等问题。

为更好地解决上述协议存在的问题，引入量子密钥。量子密钥可有效对抗字典攻击、重放攻击、中间人攻击等多种攻击方式。量子密钥的真随机特性在域服务器不完全可信时，依然可以保证密钥的安全。因此，本文基于无证书密钥协商体系，提出一种跨域量子密钥协商协议。协议采用三粒子量子隐形传态协商会话密钥，通过无证书的密钥协商体系进行身份认证并保障会话密钥安全传递给用户。无证书密钥协商体系[12−15]选取用户的身份作为公钥，私钥由可信私钥生成中心生成，不涉及证书管理问题，可以很好地配合量子密钥的协商过程。

1　预备知识

本文协议采用三粒子 A、B、C 的任意自旋态 χ 作为信源，即：

$$|\chi\rangle = a|000\rangle_{ABC}+b|001\rangle_{ABC}+c|010\rangle_{ABC}+d|011\rangle_{ABC}+e|100\rangle_{ABC}+f|010\rangle_{ABC}+g|110\rangle_{ABC}+h|111\rangle_{ABC} \tag{1}$$

其中，系数满足：

$$|a|^2+|b|^2+|c|^2+|d|^2+|e|^2+|f|^2+|g|^2+|h|^2=1 \tag{2}$$

把作为量子信道的六粒子(1,2,3,4,5,6)制备在三纠缠态的直积上：

$$\begin{aligned}\chi\rangle_{123456}&=|\varphi^+\rangle_{12}\otimes|\varphi^+\rangle_{34}\otimes|\varphi^+\rangle_{56}=\\&\frac{1}{2\sqrt{2}}(|010101\rangle_{123456}+|010110\rangle_{123456}+|011001\rangle_{123456}+|011010\rangle_{123456}+|100101\rangle_{123456}+\\&|100110\rangle_{123456}+|101001\rangle_{123456}+|101010\rangle_{123456})\end{aligned} \tag{3}$$

粒子 1,3,5 发送给通信发起方，粒子 2,4,6 发送给通信响应方。此时，粒子 A,B,C,1,2,3,4,5,6 总体系的量子态为 $\chi\rangle_{ABC}\otimes|\chi\rangle_{123456}$，通信发起方在 Bell 基下对粒子{A,1},{B,3},{C,5}进行测量，可以得到 64 种可能结果。相应地，通信响应方手中的粒子 2,4,6 将变换到对应的量子态上。

2　跨域量子密钥协商协议

2.1 使用的符号

表 1 列出了相关符号的具体含义。

表 1 符号含义

Table1 Symbols meaning

symbols	description	symbols	description
QCA_1,QCA_2	Quantum Certificate Authority with different Trust Domains	$PriKey_A()$	signing data using *A*'s private key
R_i	random number *i*	*exchange*()	QKM began to entanglement distribution
qk	quantum keys	*T*	time stamp
Hash()	Hash calculation of data	*P*	cross-domain identifier
$A\rightarrow B\{M\}$	*A* sends a message *M* to *B*	*H*	Quantum Key Distribution Request Identification
ID	identity information	QKMC	Quantum Key Management Center
$PubKey_A()$	encryption of data using *A*'s public key		

2.2 通信流程

如图 1 所示，协议包含 2 个终端用户 Alice(发起方)和 Bob(响应方)、位于不同信任域的量子认证机构 QCA_1 和 QCA_2、负责分发量子密钥的量子密钥管理中心 QKMC，协议的通信流程如图 2 所示。

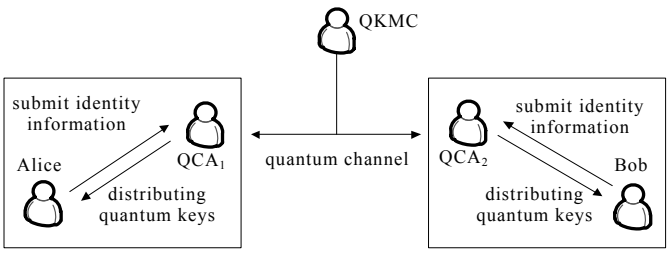

Fig.1 Relationship among protocol participants

图 1 协议参与者关系图

基本假设：只有 QCA_1,QCA_2 和 QKMC 结点可以使用量子信道，其他各个用户之间依然使用经典信道，所有用户共享一个 *n* 位二进制秘值 $L(L=k_1,k_2,k_3\cdots,k_m$，$k$=0 或 1），只有拥有 *L* 的用户被视为合法用户。

协议步骤的具体描述如下：

1) Alice→QCA_1\{$PriKey_{Alice}$(ID_{Bob},R_A)\}

Alice 向 Bob 发送随机数 R_A 以及用户 Bob 的 ID，使用 Alice 的私钥对信息签名，向 QCA_1 表明 Alice 要与 Bob 通信。

2) QCA_1→Alice\{R_1,$PriKey_{QCA1}$($Hash(ID_{QCA1},R_1)$),ID_{QCA1},P\}

QCA_1 收到 Alice 的请求，使用 Alice 的公钥检查消息是否被篡改，随后选择一个随机数 R_1 和跨域通信标识符 P，计算 R_1 和 QCA_1 的 ID 的哈希验证码，并使用自己的私钥签名，然后发送给 QCA_1。

3) QCA_1→QCA_2\{ID_{Alice},ID_{Bob},H\}

QCA_1 找到 Bob 对应的其他信任域服务器 QCA_2，将 Alice 和 Bob 的 ID、量子密钥分发请求标识 H 发送给 QCA_2。

4) QCA_2→Bob\{R_2,$PriKey_{QCA2}$($Hash(ID_{QCA2},R_2)$),ID_{QCA2},P\}

QCA_2 收到 QCA_1 的请求，QCA_2 计算 QCA_2 的 ID 和随机数 R_2 的哈希验证码并签名，与 QCA_2 的 ID、随机数 R_2 和跨域通信标识符 P 用私钥签名后一并发给 Bob。

5) Bob→QCA_2\{$PriKey_{Bob}$(ID_{Bob},R_B)\}

Bob 向 QCA_2 发送随机数 R_B 以及 Bob 的 ID，使用 Bob 的私钥对信息签名，向 QCA_2 证明身份。

6) QKMC→QCA_1\{$exchange()$,qk\}；QKMC→QCA_2\{$exchange()$,qk\}

QCA_2 收到 Bob 的身份信息，检查确定无误后，QCA_1 和 QCA_2 与用户身份认证完成。QCA_2 通知 QKMC 制备足够多的量子源。QKMC 制备数量为 q_1 的量子源用于密钥分发，数量为 q_2 的量子源用于窃听检测。q_1 与 q_2 的量子态为 $|\chi\rangle_{ABC}\otimes|\chi\rangle_{123456}$。

QKMC 将 q_1 中(A,1),(B,3),(C,5)粒子编成序列 n_1，2,4,6 粒子编成序列 n_2。QKMC 将 q_2 的所有粒子随机分别加入 n_1 和 n_2 中，并记录加入位置和粒子状态。

QKMC 将序列 n_2 发送给 QCA_1，序列 n_1 发送给 QCA_2。确认发送成功后，QKMC 公布 q_2 在各序列中的位置和状态，随后 QCA_1 和 QCA_2 对粒子序列进行 Bell 测量，测量序列中 q_2 的状态，若测量误差低于预期，说明信道安全；否则，放弃本次通信。

在确认信道安全后，QCA_1 和 QCA_2 将序列中剩余粒子视为量子密钥 qk。QCA_2 通过经典信道将测量结果发送给 QCA_1。

7) QCA_1→Alice\{$PriKey_{QCA1}$($PubKey_{Alice}$(qk,R_A)),T\}；QCA_2→Bob\{$PriKey_{QCA2}$($PubKey_{Bob}$(qk,R_B)),T\}

QCA_1 和 QCA_2 同时向 Alice 和 Bob 发放 qk，qk 使用 Alice 和 Bob 各自的公钥加密并签名，用户解密后即可得到 qk；然后，Alice 和 Bob 根据秘密值 L 的第 S 位，开始对 qk 进行下面的操作，直到 S+2 位停止(S 为通信双方通信次数乘以 3，S 的初始值为 1)：

a) k_s=1，将 qk 分成两部分，后半部分与前半部分对调位置；若 k_s=0，不做任何动作。

b) k_{s+1}=1，将 qk 分成两部分，前半部分与后半部分进行异或运算，然后将后半部分与异或运算的部分连接在一起作为结果；若 k_{s+1}=0，对 qk 进行非运算。

c) k_{s+2}=1，不做任何动作；若 k_{s+2}=1，将 qk 分成两部分，后半部分与前半部分对调位置。

Alice 和 Bob 使用处理后的 qk'作为会话密钥进行接下来的通信。

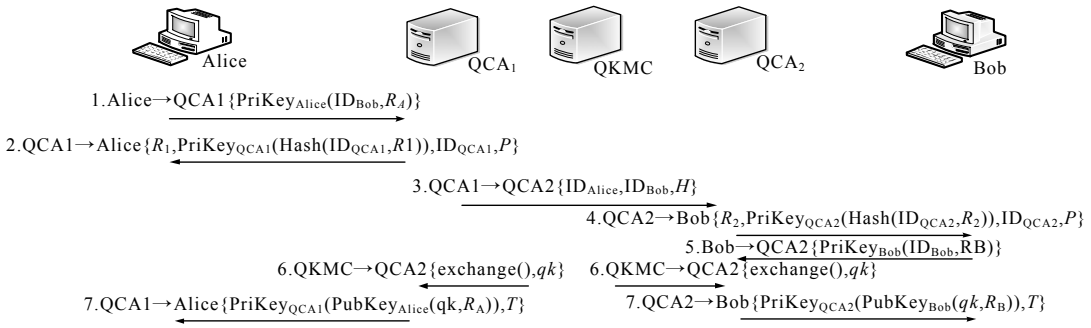

Fig.2 Protocol workflow

图 2 协议工作流程图

3 安全分析

假设 Eve 是一个想窃取共享密钥的攻击者，攻击的可能方法有外部攻击和内部攻击。

3.1 外部攻击

3.1.1 重放攻击：

在协议通信流程中，攻击者可以重放经典信道下的消息 1 和 5：

消息 1：Alice→QCA$_1${$PriKey_{\mathrm{Alice}}$(ID$_{\mathrm{Bob}}$,R_{A})}

消息 5：Bob→QCA_2{$PriKey_{\mathrm{Bob}}$(ID$_{\mathrm{Bob}}$,R_{B})}

QCA 在收到重放消息后无法判断信息是否新鲜，重放是有效的。QCA 收到重放消息，验证消息有效后会重新发送消息 2 和消息 4 给攻击者。

消息 2：QCA$_1$→Alice{R_1,$PriKey_{\mathrm{QCA1}}$($Hash$(ID_{QCA1},R_1)),ID_{QCA1},P}

消息 4：QCA$_2$→Bob{R_2,$PriKey_{\mathrm{QCA2}}$($Hash$(ID_{QCA2},R_2)),ID_{QCA2},P}

消息 2 和消息 4 仅用于表达 QCA 的身份信息，并且使用了 QCA 的私钥和哈希函数对 QCA 的身份进行保护，攻击者得到这些信息对破解会话密钥毫无意义，也无法对消息进行篡改或伪造。同时消息 1 和消息 5 均使用用户的私钥进行签名，攻击者也无法从这些消息中获得有利信息。

攻击者还可以对量子密钥分发中序列 n_1 和 n_2 进行测量−重发攻击，不过攻击者的测量会影响序列 q_2 中的粒子状态，攻击者有一定几率使误码率低于阈值，从而得出分发的量子密钥，但是缺少秘密值 L，攻击者依然无法破解通信双方的通信流程。

总之，攻击者在无法解决非对称加密体系和量子的物理特性情况下，无法从重放攻击中获得会话密钥，故本系统有能力抵抗重放攻击。

3.1.2 密钥猜测攻击：

攻击者试图使用已知会话密钥推导未知会话密钥。根据量子密钥的真随机性等物理特性，任意的量子密钥均无联系，攻击者无法根据规律得出未知密钥。而且根据协商流程，攻击者需要拥有或计算出秘密值 L 才能掌握对 qk 的动作，然而 L 同样是一组随机数，每一位之间没有依赖关系，根据通信双方的通信次数，使用的位置也不同，所以攻击者无法推导出任何有助于破解未知会话密钥的信息，也无法干预通信双方以后的会话过程。

3.2 内部攻击

中间人/冒充攻击：攻击者冒充用户 Alice 和 Bob。因为协议需要用户和 QCA 的私钥对身份 ID 等信息进行签名，攻击者无法在未知私钥的情况下完成双向认证的过程。即使攻击者使用截获的消息进行重发，获得服务器的重发消息也无法获得破解量子密钥所需的信息。使用时间戳和用户公钥加密的量子密钥信息也有效防止攻击者根据历史信息重构会话。因此本系统对中间人攻击有很高的抵抗性。

若攻击者伪装成 QCA，用户使用私钥签名的消息 1 可以被攻击者伪装的 QCA 接收到。由于任何人均可得到用户的公钥，攻击者可以解密消息 1 的内容，但接下来消息 2 必须使用 QCA 的私钥进行签名，攻击者伪装的 QCA 在没有获得私钥的情况下无法伪造签名信息，也就不可能完成与用户的双向认证，更得不到通信双方的会话密钥，所以攻击者的伪装一定会被识破。

4　效率分析

本协议的特点在于使用三粒子隐形传态分发会话密钥，同时使用经典信道进行身份认证，最终把密钥传递给通信双方。沿用 Cabello[16]的量子比特效率公式 $\eta=c/q$ 来判断协议的效率，其中 c 表示双方协商的经典比特数，q 表示所使用的量子比特数。本协议中，用于传递的量子比特数量为 $3n$，插入量子序列的诱骗态比特数量为 $3n$，共计用到的量子比特数量为 $3n+3n=6n$，最终获得共享密钥的长度为 $2n$，量子比特效率为 33.33%。将本协议与几种典型量子密钥协议进行比对，见表 2。从表 2 可知，本协议有较高的量子比特效率。

表 2 协议对比

Table2 Protocols comparison

protocols	quantum state	quantum bit efficiency
Shukla[17]'s protocol	Bell state	16.7%
Chong[18]'s protocol	Bell state	16.7%
Huang[19]'s protocol	Bell state	25%
He[20]'s protocol	four-particle cluster state	26.67%
protocol in this paper	three-particle spin state	33.33%

5　结论

本文提出了一种无证书的跨域量子密钥协商协议，使用量子信道与经典信道配合的方式协商密钥，解决了传统跨域密钥协商协议的部分安全隐患。安全分析表明，该协议可以抵挡来自内部和外部的攻击，并且拥有较高的量子比特效率。下一步将深入开展本协议对信道噪声抗干扰性的研究。

参考文献：

[1] ZHOU N,ZENG G,XIONG J. Quantum key agreement protocol[J]. Electronics Letters, 2004,40(18):1149-1150.

[2] 杨宇光,温巧燕,朱甫臣. 一种网络多用户量子认证和密钥分配理论方案[J]. 物理学报, 2005,54(9):3995-3999. (YANG Yuguang,WEN Qiaoyan,ZHU Fuchen. A theoretical scheme for multi-user quantum authentication and key distribution in a network[J]. Acta Physica Sinica, 2005,54(9):3995-3999.)

[3] 周南润,宋汉冲,龚黎华,等. 基于 GHz 态的三方量子确定性密钥分配协议[J]. 物理学报, 2012,61(21):225-231. (ZHOU Nanrun,SONG Hanchong,GONG Lihua,et al. Tripartite quantum deterministic key distribution based on GHz states[J]. Acta Physica Sinica, 2012,61(21):225-231.)

[4] 胡钰安,叶志清. 基于四粒子 GHz 态的可控量子双向隐形传态及安全性[J]. 光子学报, 2014,43(8):182-186. (HU Yu'an, YE Zhiqing. Controlled two-way quantum teleportation via GHz quadripartite entangled state and security[J]. Acta Photonica Sinica, 2014,43(8):182-186.)

[5] HE Y F,MA W P. Quantum key agreement protocols with four-qubit cluster states[J]. Quantum Information Processing, 2015,14(9):3483-3498.

[6] CHONG S K,HWANG T. Quantum key agreement protocol based on BB84[J]. Optics Communications, 2010,283(6):1192-1195.

[7] 高昊,陈晓光,钱松荣. 集体噪声信道下容错的量子密钥分配协议[J]. 太赫兹科学与电子信息学报, 2017,15(6):921-927. (GAO Hao,CHEN Xiaoguang,QIAN Songrong. Fault-tolerant quantum key distribution protocols under collective noise channel[J]. Journal of Terahertz Science and Electronic Information Technology, 2017,15(6): 921-927.)

[8] BYUN J W,JEONG I R,LEE D,et al. Password-authenticated key exchange between clients with different passwords[C]// International Conference on Information and Communication Security. Singapore:[s.n.], 2002:134-146.

[9] GANESAN R. Yaksha:augmenting Kerberos with public key cryptography[C]// Network and Distributed System Security Symposium. San Diego,CA:[s.n.], 1995:132-143.

[10] KIM J,KIM S,JIN K,et al. Cryptanalysis and improvement of password authenticated key exchange scheme between clients with different passwords[C]// International Conference on Computational Science and Its Applications. Assisi,Italy:[s.n.], 2004:895-902.

[11] YOON E J,YOO K Y. A secure password-authenticated key exchange between clients with different passwords[C]// International Conference on Advanced Web and Network Technologies, and Applications. Harbin,China:Springer-Verlag, 2006:659-663.

[12] 杨小东,安发英,杨平,等. 基于无证书签名的云端跨域身份认证方案[J]. 计算机工程, 2017(11):134-139,151. (YANG Xiaodong,AN Faying,YANG Ping,et al. Cross-domain identity authentication scheme in cloud based on certificateless signature[J]. Computer Engineering, 2017(11):134-139,151.)

[13] GHOREISHI S M,RAZAK S A,ISNIN I F,et al. New secure identity-based and certificateless authenticated key agreement protocols without pairings[C]// International Symposium on Biometrics and Security Technologies. Kuala Lumpur,Malaysia: IEEE, 2015:188-192.

[14] 李晓伟,杨邓奇,陈本辉,等. 基于生物特征和口令的双因子认证与密钥协商协议[J]. 通信学报, 2017,38(7):89-95. (LI Xiaowei,YANG Dengqi,CHEN Benhui,et al. Two-factor authenticated key agreement protocol based on biometric feature and password[J]. Journal on Communications, 2017,38(7):89-95.)

[15] 张全领,陆阳. 无证书两方认证密钥协商协议攻击及改进[J]. 信息技术, 2015,39(7):1-4. (ZHANG Quanling,LU Yang. Attack and improvement of a certificateless two-party authenticated key agreement protocol[J]. Journal on Communications, 2017,38(7):1-4.)

[16] CABELLO A. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000,85(26):5635-5638.

[17] SHUKLA C,ALAM N,PATHAK A. Protocols of quantum key agreement solely using Bell states and Bell measurement[J]. Quantum Information Processing, 2014,13(11):2391-2405.

[18] CHONG S K,TSAI C W,HWANG T. Improvement on "Quantum Key Agreement Protocol with Maximally Entangled States"[J]. International Journal of Theoretical Physics, 2011,50(6):1793-1802.

[19] HUANG W,WEN Q Y,LIU B,et al. Quantum key agreement with EPR pairs and single-particle measurements[J]. Quantum Information Processing, 2014,13(3):649-663.

[20] HE Y F,MA W P. Quantum key agreement protocols with four-qubit cluster states[J]. Quantum Information Processing, 2015,14(9):3483-3498.