基于量子不经意密钥传输的量子匿名认证密钥交换协议

魏春艳[①②] 蔡晓秋[①②] 王天银[②] 苏 琦[④] 秦素娟[①] 高 飞*[①③] 温巧燕[①]

[①](北京邮电大学网络与交换技术国家重点实验室 北京 100876)

[②](洛阳师范学院数学科学学院 洛阳 471934)

[③](鹏程实验室量子计算研究中心 深圳 518055)

[④](密码科学技术国家重点实验室 北京 100878)

摘 要：鉴于量子密码在密钥分配方面取得的巨大成功，人们也在尝试利用量子性质来设计其他各类密码协议。匿名认证密钥交换就是一类尚缺乏实用化量子实现途径的密码任务。为此，该文提出一个基于量子不经意密钥传输的量子匿名认证密钥交换协议。它在满足用户匿名性和实现用户与服务器双向认证的前提下，为双方建立了一个安全的会话密钥。该协议的安全性基于量子力学原理，可以对抗量子计算的攻击。此外，该协议中服务器的攻击行为要么无法奏效，要么能够与外部窃听区分开(从而被认定为欺骗)，因此服务器通常不敢冒着名誉受损的风险来实施欺骗。

关键词：量子保密查询；不经意传输；量子匿名认证密钥交换

中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2020)02-0341-07

DOI: 10.11999/JEIT190679

Quantum Anonymous Authenticated Key Exchange Protocol Based on Quantum Oblivious Key Transfer

WEI Chunyan[①②] CAI Xiaoqiu[①②] WANG Tianyin[②] SU Qi[④]

QIN Sujuan[①] GAO Fei[①③] WEN Qiaoyan[①]

[①](*State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

[②](*School of Mathematical Science*, *Luoyang Normal University*, *Luoyang* 471934, *China*)

[③](*Center for Quantum Computing*, *Peng Cheng Laboratory*, *Shenzhen* 518055, *China*)

[④](*State Key Laboratory of Cryptology*, *Beijing* 100878, *China*)

Abstract: In view of the great success of quantum cryptography in key distribution, people also try to utilize the quantum mechanics to construct many other cryptographic protocols. Anonymous authenticated key exchange is exactly one kind of cryptographic tasks whose practical quantum solution is still awaited so far. To solve this problem, a quantum anonymous authenticated exchange protocol is proposed based on a quantum oblivious key transfer scheme. It not only realizes user anonymity and mutual authentication of the user and server, but also establishes a secure session key between the two parties. Besides, the attacks of the server either fail or can be discriminated with outside eavesdropping (the server is thus caught as a cheater), so the server generally will not cheat at the risk of gaining a bad reputation.

Key words: Quantum private query; Oblivious transfer; Quantum anonymous authenticated key exchange

收稿日期：2019-09-04；改回日期：2019-11-12；网络出版：2019-11-28

*通信作者： 高飞 gaofei_bupt@hotmail.com

基金项目：国家自然科学基金(61672110, 61671082, 61902166, 61572246, 61602232, 61602045)，河南省科技攻关计划项目(182102310930)，河南省高校科技创新研究团队基金(18IRTSTHN014)

Foundation Items: The National Natural Science Foundation of China (61672110, 61671082, 61902166, 61572246, 61602232, 61602045), The Key Scientific and Technological Research Project of Henan Province (182102310930), The Program for Science & Technology Innovation Research Team in Universities of Henan Province (18IRTSTHN014)

1 引言

随着“互联网+”产业的迅猛发展，电子商务与电子政务日益普及。人们逐渐认识到隐私保护的重要性。在很多应用中，人们希望割断自己的身份与行为之间的联系，又希望能够认证通信对象的身份并确保传递信息的完整性和保密性。匿名认证密钥交换就是为实现这类密码任务而提出的[1–3]。它涉及一个服务器及一组合法用户，要求服务器和任意一个合法用户在相互认证身份且不泄露用户身份的前提下共享一个安全的会话密钥，以保证后续通信的安全。在网络服务和通信中，它既能排除非法用户的干扰，又能保护敏感信息传递者的身份。比如，在一个公司的通讯网络中，董事长是服务器方，而公司员工是合法用户。如果某个员工想要向董事长提一些敏感的建议或举报非法信息，他可以与董事长执行匿名认证密钥交换协议来共享一个会话密钥，再将敏感信息用会话密钥加密发送给董事长。通过这种方法，员工能够确保信息提交给了董事长而不是其他人，而董事长能够确定该信息来自公司员工，但无法获知来自哪位员工。目前，匿名认证密钥交换已广泛应用于无线移动网络、云环境等。

在经典密码学中，很多匿名认证密钥交换方案已经陆续被提出。我们知道，经典密码协议大多建立在数学困难问题假设上，随着量子算法的提出，这类协议的安全性面临严峻威胁[4,5]。幸运的是，这一弱点可被安全性基于物理定律的量子密码所克服[6]。鉴于量子密码在密钥分配方面取得的巨大成功，人们也逐步尝试利用量子性质来设计其他各类密码协议，寻找实用安全的量子方法来实现匿名认证密钥交换是其中十分有意义的研究课题。

很多经典匿名认证密钥交换方案是基于“N传1”不经意传输[7,8](即发送者Bob向接收者Alice发送N条信息，Alice仅能选择获得其中一条信息，而Bob不知道Alice获得了哪一条信息)来构造的，因此本文考虑借助不经意传输的量子方法来构造量子匿名认证交换协议。基于量子密钥分配(Quantum Key Distribution, QKD)的量子保密查询(Quantum Private Query, QPQ)是“N传1”不经意传输的一类最具实用潜力的量子方案[9]，它借助现有的量子密钥分配技术就能实现，已经在实现方式[10–16]、经典后处理[17,18]、理论安全性[19,20]、实际安全性[18,21,22]、实验验证[22]等方面都取得了可观的进展。因此，从这类协议出发最有希望设计出实用的量子匿名认密钥交换方案。作为“N传1”不经意传输的一种量子变体，基于QKD的QPQ中发送者Bob拥有一个Nbit的数据库，而接收者(又被称为用户)Alice，可以从数据库中获得自己感兴趣的条目。它通常分为3个步骤：(1)双方借助量子密钥分配来共享一个不对称密钥，使得Bob知道整个密钥而Alice仅知道其中部分比特，且Bob不知道Alice知道了哪些比特；(2)双方对不经意密钥进行压缩得到一个最终密钥，使得Alice在最终密钥中获得1个(或稍多于1个)比特；(3)Bob使用最终密钥加密数据库发送给Alice, Alice利用其得到的那个密钥比特恢复出想要的数据库条目。它本质上仍是“N传1”不经意传输。值得注意的是，双方在前两个步骤中共享了一条不经意密钥，Bob知道整个密钥，而Alice仅获得其中1个(或几个)比特。该过程被称为不经意密钥传输，是实现量子保密查询最核心和关键的环节。本文就是基于这种不经意密钥传输来构造量子匿名认证密钥交换方案的。

事实上，作为不经意传输的量子变体，基于QKD的QPQ(包括其蕴含的量子不经意密钥传输)很少被用于构造其他量子密码方案。这与经典密码学中“不经意传输可被用于实现各类密码任务”[23–25]存在很大差距。一个重要的原因就是不经意传输在量子密码中并不能被完美地实现[26]。首先，接收方Alice通常会获得几条而不是一条信息，这样的信息泄露虽不严重但也导致它难以应用于一些对隐私保护要求较高的密码任务。另一方面，发送方Bob若采用某种攻击试图获知“用户得到了哪一条信息”，其行为一般是在协议结束后才能被Alice以一个非零的概率发现，即对接收方隐私的保护是“非实时”和“欺骗敏感”的。此外，现有不经意传输的量子方案通常忽略对外部攻击进行检测的研究现状，也导致了它们难以适用于很多安全多方计算任务。不难想象，如果不诚实参与者的欺骗行为仅能以非零概率被发现，且不能将其与外部攻击相区分，那么不诚实参与方可以不断实施欺骗并将检测中出现的错误归咎于外部攻击，直至获得对方隐私为止，这显然不安全。本文研究借助量子不经意密钥传输来构造匿名认证密钥交换协议以期取得突破。

2015年，Liu等人[15]基于环回差分相移QKD[14]提出的不经意密钥传输方案具有突出的优点，如Alice能从Bob传送的N个比特中精确地获得1个比特、无失败概率等。本文基于该方案设计了一个量子匿名认证密钥交换协议。该协议能够实现用户和服务器的双向认证，满足用户匿名性和会话密钥安全性。此外，若不诚实服务器方想要获取用户身份，其攻击行为要么无法奏效，要么能够与外部窃听区分开，从而被用户识别并认定为欺骗，因此服务器一般不会冒着名誉受损的风险来实施欺骗。

本文结构和内容安排如下：首先，在第2节中给出具体的量子匿名认证密钥交换协议，然后在第3节中分析其安全性，最后在第4节中进行总结。

2　量子匿名认证密钥交换协议

2015年，Liu等人[15]基于环回差分相移QKD[14]提出了一个量子不经意密钥传输协议，并用其实现了无失败概率的量子保密查询。它最大的优点是接收者只能获得不经意密钥中1个比特，本文的匿名认证密钥交换方案也是基于此协议构造的。

2.1　Liu等人的量子不经意密钥传输协议

(1) Bob随机选择一个$(N+1)$ bit的字符串$S=s_0,s_1,\cdots,s_N$，并根据其制备一个包含$N+1$个脉冲的单光子态$|\Psi_s\rangle=\dfrac{1}{\sqrt{N+1}}\sum_{k=0}^{N}(-1)^{s_k}|k\rangle$发送给Alice。这里$|k\rangle$表示光子在第$k$个脉冲里，$s_k\in\{0,1\}$，$k=0,1,\cdots,N$。

(2) 收到$|\Psi_s\rangle$后，Alice随机选择一个$r\in\{1,2,\cdots,N\}$，再使用一个分束器将脉冲序列分成两路，并将其中一路移动r个脉冲。然后她借助另一个分束器使两路汇合来随机获得$\{s_j\oplus s_{j\oplus_N r}\}_{j=0}^{N}$中的一个值，这里$j\oplus_N r=j+r \bmod (N+1)$，$\oplus$表示模2加。该过程如图1所示，这里$BS_1$, BS_2是50：50分束器；S_1是一个长为$N+1$个脉冲长度的线圈，仅作用于前r个脉冲；S_2是一个长为r个脉冲长度的线圈，作用于所有脉冲；探测器$D_0(D_1)$响应意味着Alice获得的比特值为0(1)。假定Alice最终获得的值是$s_t\oplus s_{t\oplus_N r}$。

(3) Alice公示t，此时他们共享了一个N bit的不经意密钥K：$s_t\oplus s_0$，$s_t\oplus s_1,\cdots,s_t\oplus s_{t-1},s_t\oplus s_{t+1},\cdots,s_t\oplus s_N$。Bob知道整个密钥而Alice仅知道其中一个比特$s_t\oplus s_{t\oplus_N r}$，且Bob不知道Alice获得了哪个比特。

2.2　量子匿名认证密钥交换协议

本文的量子匿名认证密钥交换协议涉及一个服务器和一组合法用户，包含如下3个阶段。

成员的加入阶段：用户向服务器S请求注册成为会员。在确认了该用户身份ID_i的可靠性后，服务器S与用户借助一个安全的量子密钥分配方案(如BB84方案[27])共享一个密钥K_i。服务器S将(K_i,ID_i)存放在用户密钥列表T的第i个位置，然后通知用户其密钥存储地址i。

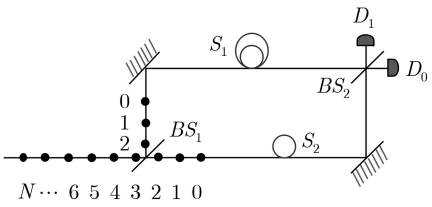

图 1 Liu等人的不经意密钥传输协议

匿名认证密钥交换阶段：假设共有N个合法用户$\{U_j\}_{j=1}^{N}$，每个用户U_j与服务器共享一个密钥K_j，$H:\{0,1\}^*\to\{0,1\}^{2n}$是一个单向哈希函数。用户$U_i$与服务器S可以通过如下步骤实现匿名认证密钥交换。

(1) S作为发送者、U_i作为接收者执行Liu等人的不经意密钥传输协议$m+2n$次，这样双方共享了$m+2n$条长度为N的不经意密钥，S完全得到每条密钥而U_i仅得到每条密钥中的1个比特，且S不知道U_i获得了哪一个比特。

(2) U_i随机挑选m条不经意密钥$K_1',K_2',\cdots,K_m'$。对于$u=1,2,\cdots,m$，若U_i获得了K_u'的第k个比特，他要求S给出K_u'的第k个比特在每个用户密钥K_j中的一种查找方式$(j_1,j_2,\cdots,j_t)$。假设S发现K_u'中第k个比特为0，他对所有用户密钥$\{K_j\}_{j=1}^{N}$构造比特0的查询方式。如对K_i=(0 0 1 0 1 1 1 0 0 $\cdots$ 0 1)，他随机选择一个比特为0的位置，如第8个位置，然后将8转化为二进制1000，再在K_i中随机挑选4个比特值分别为1, 0, 0, 0的位置，如7, 9, 4, 1，最后将查询办法$(i_1,i_2,\cdots,i_t)=(7,9,4,1)$返回给用户。用户$U_i$收到所有用户密钥$\{K_j\}_{j=1}^{N}$中该不经意密钥比特的查询方式后，从中找出自己的密钥K_i对应的查询方法(7, 9, 4, 1)，然后查找密钥K_i第7, 9, 4, 1个位置得到1000及其十进制值8，最后查询K_i的第8个位置得到比特0。若U_i查得的密钥比特与在第(1)步中得到的K_u'中第k个比特不符，协议终止。

显然，只有第(1)步中量子不经意密钥传输中没有外部窃听且服务器不是假冒攻击者时，U_i对这m条不经意密钥的检验才能全部通过。

(3) U_i对余下的$2n$条密钥各声明一个移位，使得移位后他知道每条密钥的第i个比特。这$2n$条密钥第$j(j=1,2,\cdots,N)$个位置上的比特组成了一个长为$2n$的比特串M_j，则S获得N个比特串$\{M_j\}_{j=1}^{N}$，而U_i仅获得其中第i个比特串M_i，且S不知道U_i获得了哪个比特串。

(4) S将$\{M_j\}_{j=1}^{N}$中各比特的异或和$\{q_j\}_{j=1}^{N}$发送给U_i。U_i检查自己得到的M_i，若其各比特的异或和与收到的q_i不一致，则认定服务器S欺骗，协议终止。

(5) S随机选择一个长度为$2n$的比特串$M=b_1b_2b_3b_4\cdots b_{2n}$，然后对$j=1,2,\cdots,N$，计算$m_j=M\oplus M_j\oplus H(K_j\|M_j)$并将其发送给$U_i$。对于收到的$m_1,m_2,\cdots,m_N$，$U_i$从中取出$m_i$，然后计算$M=m_i\oplus M_i\oplus H(K_i\|M_i)$。

(6) S发送一列随机处于$|0\rangle, |1\rangle, |+\rangle, |-\rangle$4个量子态之一的量子比特序列给$U_i$。$U_i$随机使用$\{|0\rangle, |1\rangle\}$基或$\{|+\rangle, |-\rangle\}$基来测量收到的量子比特，然后声明在哪些位置上没有测到结果。双方将未测到的量子比特记录丢弃。这里$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, $|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$。

(7) S声明一个序列$(i_1, i_2, \cdots, i_n)$，使得他在第i_k个位置发送的量子比特处于量子态$|\varphi_k\rangle$。这里$|\varphi_k\rangle$由M中的比特$b_{2k-1}b_{2k}$决定，即当$b_{2k-1}b_{2k}=00\,(01, 10, 11)$时，$|\varphi_k\rangle=|0\rangle\ (|1\rangle, |+\rangle, |-\rangle)$。

(8) U_i根据自己的测量结果和M来检查$(i_1, i_2, \cdots, i_n)$是否正确。比如，当$b_{2k-1}b_{2k}=00$时，U_i若在第i_k个位置上测得结果$|1\rangle$，则他知道S实施了欺骗或者在第(6)步的量子比特传输中存在外部窃听，协议终止。若$(i_1, i_2, \cdots, i_n)$中每个位置均未出错，U_i接受S为合法服务器。

(9) 双方丢弃检测量子比特记录。U_i声明一个序列$(j_1, j_2, \cdots, j_n)$，使得他在第j_k个位置测得的结果为$|\varphi_k\rangle$。S根据自己发送的量子态和M检查$(j_1, j_2, \cdots, j_n)$是否正确。比如，若S在第j_k个位置发送的是$|1\rangle$态而$b_{2k-1}b_{2k}=00$，则他知道U_i欺骗或第(6)步的量子态传输中存在外部窃听，协议终止。若$(j_1, j_2, \cdots, j_n)$中每个位置均未出错，则S接受U_i是合法用户。

(10) 双方丢掉用于检测的量子比特记录。S声明余下每个量子比特所处的基是$\{|0\rangle, |1\rangle\}$还是$\{|+\rangle, |-\rangle\}$，然后U_i对照自己使用的测量基，声明在哪些位置上选用了正确的测量基。最后双方根据这些位置上传送的量子态来共享会话密钥，即$|0\rangle$和$|+\rangle$对应密钥比特0，而$|1\rangle$和$|-\rangle$对应比特1。

成员的撤销阶段：假设要撤销第j个用户的成员资格，服务器S只需任选一个比特串K^*，用$(K^*, -)$来覆盖列表T中第j个位置的密钥(K_j, ID_j)，标记j以便有新成员加入时该位置可以被重新使用。

3 安全性分析

3.1 双向认证性和抗假冒攻击

本文的协议实现了用户和服务器的双向认证。首先，除了S之外的任何人由于不知道用户U_i的密钥K_i，也就无法给出第(2)步中不经意密钥查询方式，无法通过用户的检验。且由于$M=m_i\oplus M_i\oplus H(K_i\|M_i)$，除了S之外的任何人由于不知道用户$U_i$的密钥$K_i$，所以无法获知$U_i$提取出来的$M$，也就无法伪装成为服务器在第(7)步中声明正确位置序列$(i_1, i_2, \cdots, i_n)$通过用户的认证。此时，若S声明的i_k处发送的量子态与$b_{2k-1}b_{2k}$不符，至少会有1/4的概率被用户发现。比如，当$b_{2k-1}b_{2k}=00$时，若S在i_k处发送的量子态为$|1\rangle$，则当用户使用$\{|+\rangle, |-\rangle\}$基测量时不能发现S发送的量子态有误，而当他使用$\{|0\rangle, |1\rangle\}$基测量时会发现出错，即被发现的概率为1/2；若S在该处发送的量子态为$|+\rangle$或$|-\rangle$，则当用户使用$\{|+\rangle, |-\rangle\}$基测量时不能发现S发送的量子态有误，而当他使用$\{|0\rangle, |1\rangle\}$基测得$|1\rangle$时发现错误，即被发现的概率为1/4。此时，n个位置均通过用户检验的概率不超过$(3/4)^n$。

另一方面，由于不知道用户密钥K_i，外部攻击者也无法得到正确的M以便在第(9)步中声明正确的位置序列$(j_1, j_2, \cdots, j_n)$来通过服务器S的验证。当然，外部攻击者可能尝试根据第(7)步中S声明的$(i_1, i_2, \cdots, i_n)$来设法找出合适的$(j_1, j_2, \cdots, j_n)$提交给服务器。比如，若外部攻击者在第i_k处若测得$|+\rangle$，他就找另一个测得$|+\rangle$的位置来作为j_k。这种方法虽然能降低被发现的概率，但仍难以成功。比如，若$b_{2k-1}b_{2k}=00$，则S在i_k处发送$|0\rangle$。若外部攻击者使用$\{|+\rangle, |-\rangle\}$基测得$|+\rangle$(或$|-\rangle$)，此时他声明另一个测得$|+\rangle$(或$|-\rangle$)的位置作为j_k，而该位置S发送的量子态可能是$|+\rangle, |0\rangle, |1\rangle$(或$|-\rangle, |0\rangle, |1\rangle$)。当该位置S发送的是$|1\rangle$时，可以判定出错，这种错误发生的概率为1/8。此时，n个位置均通过服务器检验的概率不超过$(7/8)^n$，随着n的增大，这一概率快速趋于0。

因此，本文的协议具有双向认证性，能够抵抗假冒攻击。

3.2 用户匿名性

本文的协议能实现用户匿名性，即合法用户在向服务器证实自己的成员资格时可以隐藏自己的身份信息。服务器S以“提取用户身份”为目的的攻击要么无法奏效，要么能被用户发现并认定为欺骗。

首先，S可以在第(1)步不经意密钥传输中试图发送假态来猜测用户获得了哪个比特，从而推测用户的索引i来比对T表获取用户身份。这种攻击可以分为如下两种情形。

(1) 单粒子假态攻击：根据文献[15]中的分析，只要发送者S发送单粒子假态来试图获取“U_i获得了哪个比特”的信息，他将无法提供正确的密钥比特给接收者U_i，也就无法通过第(2)步的检验。

(2) 纠缠-测量攻击：值得注意的是，根据文献[15]中的分析，如果发送方S采用纠缠-测量攻击，他的欺骗是无法被实时发现的。具体来说，在不经意密钥传输的(1)中，服务器S制备纠缠态

$$|\Psi\rangle=\sum_{\mathrm{i}=1}^{2^N}\lambda_i|\Lambda_i\rangle_B\left[\frac{1}{\sqrt{N+1}}\sum_{k=0}^{N}(-1)^{s_{ik}}|k\rangle\right]_A \tag{1}$$

这里，$\langle\Lambda_i/\Lambda_j\rangle=\begin{cases}0, i\neq j\\ 1, i=j\end{cases}\sum_{i=1}^{2^N}|\lambda_i|^2=1, s_{ik}\in\{0,1\}$。然后S发送子系统A给用户，自己保存子系统B。若S对子系统B实施某种其他测量能以一定概率推测出“用户获得了哪个比特”，但这种攻击也会使得S无法获得准确的密钥比特值；而若他推迟测量，在第(2)步中使用$\{\Lambda_i\}$基测量子系统B就可以获知s_{ik}的值来得到正确的不经意密钥，从而能够逃避协议中第(2)步的检测。幸运的是，将Liu等人的协议为量子匿名认证密钥交换的基础构件时，服务器的这种欺骗行为还是可以被实时发现并与外部攻击区分开的。比如，若S在不经意传输的第(1)步中制备纠缠态

$$|\psi\rangle=\frac{1}{\sqrt{2^N(N+1)}}\sum_{s_0,s_1,\cdots,s_N=0}^{1}|s_0\rangle_0|s_1\rangle_1\cdots|s_N\rangle_N\cdot\left[\sum_{k=0}^{N}(-1)^{s_k}|k\rangle\right]_A \tag{2}$$

然后发送系统A给U_i代替合法的载体态，而自己保存其余$N+1$个粒子。当在第(2)步中，用户要求S声明某个不经意密钥比特的构造时，S使用$\{|0\rangle,|1\rangle\}$基来测量相应的纠缠态中前$N+1$个粒子确定相应的s_k值就能推导出该密钥比特，这样不会被发现欺骗。当第(2)步结束后，S再测量对应于剩余密钥的$N+1$个粒子来推测用户获得了哪个密钥比特，进而获取用户身份。容易得出，当用户在第t个脉冲处测得密钥比特0时，S存储的系统将演化为

$$\frac{1}{\sqrt{2}}\left(|+\rangle_t|-\rangle_{t\oplus_N r}+|-\rangle_t|+\rangle_{t\oplus_N r}\right)\bigotimes_{\substack{i=0,\mathrm{i}\neq t\\ i\neq t\oplus_N r}}^{N}|+\rangle_i \tag{3}$$

而当用户U_i在第t个脉冲处测得密钥比特1时，S存储的系统将演化为

$$\frac{1}{\sqrt{2}}\left(|+\rangle_t|-\rangle_{t\oplus_N r}-|-\rangle_t|+\rangle_{t\oplus_N r}\right)\bigotimes_{\substack{i=0,i\neq t\\ i\neq t\oplus_N r}}^{N}|+\rangle_i \tag{4}$$

由式(3)、式(4)容易看出，若S用$\{|+\rangle,|-\rangle\}$基来测量存储的粒子，将有1/2的机会获得t(当测量结果为$|-\rangle$的位置有1/2的概率是t)，但同时也就无法判断出用户得到的生密钥比特究竟是0还是1，会有1/2的概率给出错误的值。这将导致S在第(4)步中会有1/2的概率会发送错误的异或和q_i给U_i。由于在第(2)步中没有发现错误，因此在此前的量子通信中不存在外部窃听且服务器方S是真实的。若q_i出错只能是S的欺骗引起的，因此可以认定服务器S欺骗。也就是说，在本文的匿名认证密钥交换方案中，服务器方的这类欺骗能被实时检测，也能与外部攻击区分开来。在这种情形下，服务器一般不敢冒着被发现的风险实施欺骗，那将损害其荣誉，造成严重的损失。

最后，S可能会选择给不同的用户设置不同的比特串M以便在第(9)步根据用户声明的$(j_1,j_2,\cdots,j_n)$和自己发送的态来推测M并判断用户身份。比如S在第j_k个位置发送$|0\rangle$，那么所有满足$b_{2k-1}b_{2k}=01$(即测量结果为$|1\rangle$)的M值对应的用户将被排除出去，S在猜测用户身份上获得一定优势。幸运的是，S需在此前(即第(7)步中)根据M声明位置序列，如果S不知道M，其声明的位置序列将无法通过验证，协议将提前终止，S不能得到任何优势。

3.3 用户密钥安全性

在本文的协议中，用户的密钥被很好地保护。首先，对外部攻击者来说，若要获得密钥相关信息，有两种途径。一是从第(2)步中服务器S给出的查询方法中获得密钥K_i的信息，由于比特0和1分别占据了K_i中约1/2的位置，因此它们均具有很多构造方式。外部攻击者在不知道S选择哪个构造方式时很难从S声明的$(i_1,i_2,\cdots,i_t)$中获取任何密钥比特；二是设法获取哈希值$H(K_i\|M_i)=m_i\oplus M_i\oplus M$并从中得到密钥$K_i$的部分信息。对外部攻击者来说，只可能截留第(6)步传输的量子态并发送一个假态代替，然后通过第(7)和第(9)步中声明的位置来推测M，这种攻击会干扰量子比特从而在认证身份时被发现。而且，在外部敌手看来，M中任两个比特$b_{2j-1}b_{2j}$对应的量子态均处于完全混合态

$$\frac{I}{2}=\frac{1}{4}\left(|0\rangle\langle 0|+|1\rangle\langle 1|+|+\rangle\langle +|+|-\rangle\langle -|\right) \tag{5}$$

且即便他测量截获的量子态后也不能确定$b_{2j-1}b_{2j}$的任何信息。比如，若测量结果为$|-\rangle$，则该量子比特可能为$|0\rangle,|1\rangle,|-\rangle$3个态，即$b_{2j-1}b_{2j}$可能为00, 01或11，无法确定其中任何一个比特。因此，外部攻击者无法获得M，也就无法获得哈希值$H(K_i,M_i)=m_i\oplus M_i\oplus M$，更无法获得密钥$K_i$的信息。

另一方面，假如某个不诚实合法用户U_i想获得另一个用户U_j的密钥K_j的有关信息，则他需要获取与K_j相关的哈希值$H(K_j\|M_j)$。注意到$H(K_j\|M_j)=m_j\oplus M_j\oplus M$, U_i需要获取M_j和M才能得到这个哈希值。若U_i要获取M，就需要诚实执行协议获得M_i，然后根据自己的密钥计算出$M=m_i\oplus M_i\oplus H(K_i\|M_i)$，此时他将无法获知$M_j$；反之，如果$U_i$要获取$M_j$，就无法获得$M_i$来推导出$M$。也就是说，

U_i只能获得M_j和M中一个值，无法求出$H(K_j \| M_j) = m_j \oplus M_j \oplus M$，也就更无法获得密钥$K_j$的信息。

3.4 会话密钥安全性

在本文的协议中会话密钥的生成过程与BB84协议[27]类似，不同之处在于BB84协议中双方随机选择一些量子比特来判断是否存在外部窃听，而在本文的方案中，在双方声明的位置$(i_1, i_2, \cdots, i_n)$和$(j_1, j_2, \cdots, j_n)$处，双方分别根据M和量子态/测量结果来对对方身份的合法性进行检验。由于外部窃听势必会干扰量子态，从而使得测量结果发生改变。因此，若检验通过，说明测量结果并未出错，也就排除了外部窃听的存在，最终双方共享的会话密钥是安全的。

4 结束语

本文基于Liu等人[15]提出的量子不经意密钥传输方案，设计了一个量子匿名认证密钥交换协议。该协议实现了用户和服务器之间的双向认证，满足用户匿名性和会话密钥安全性，且能够方便地加入和撤销成员。值得注意的是，由于量子不经意传输中对发送方的攻击是欺骗敏感的，作为其应用，本文的量子匿名认证密钥交换协议中对服务器方的攻击也是欺骗敏感的。这就要求必须要将服务器的欺骗与外部攻击区分开来，否则服务器可以不断实施攻击直至获得用户身份信息，而当检测出错时就将错误归咎为外部攻击来逃避追责，这显然是不安全的。在方案的第(2)步中，只有没有外部窃听且S确实知道用户密钥时才能给出正确应答。如果通过检验，那就说明此前的量子传输中无外部窃听的存在，且服务器方身份为真。因此，如果在第(4)步检测出错，那只能是由于服务器S想要非法获得用户的身份进行欺骗引起的，此时可以判定服务器方欺骗。鉴于这种内外攻击的可区分性，服务器方一般不敢冒着名誉受损的风险实施欺骗。本文的结果表明，尽管不够理想，不经意传输的量子方案在量子密码中依然可以发挥出基础构建和基础工具的作用，相信将来它还可以被用于构造其他的量子密码协议。

参 考 文 献

[1] VIET D Q, YAMAMURA A, and TANAKA H. Anonymous password-based authenticated key exchange[C]. The 6th International Conference on Cryptology in India, Bangalore, India, 2005: 244–257. doi: 10.1007/11596219_20.

[2] HU Xuexian, ZHANG Jiang, ZHANG Zhenfeng, *et al*. Universally composable anonymous password authenticated key exchange[J]. *Science China Information Sciences*, 2017, 60(5): 52107. doi: 10.1007/s11432-016-5522-z.

[3] LI Xiong, IBRAHIM M H, KUMARI S, *et al*. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks[J]. *Computer Networks*, 2017, 129: 429–443. doi: 10.1016/j.comnet.2017.03.013.

[4] SHOR P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]. The 35th Annual Symposium on Foundations of Computer Science, Santa Fe, USA, 1994: 124–134. doi: 10.1109/SFCS.1994.365700.

[5] GROVER L K. A fast quantum mechanical algorithm for database search[C]. The 28th Annual ACM Symposium on Theory of Computing, Philadelphia, USA, 1996: 212–219. doi: 10.1145/237814.237866.

[6] GISIN N, RIBORDY G, TITTEL W, *et al*. Quantum cryptography[J]. *Reviews of Modern Physics*, 2002, 74(1): 145–195. doi: 10.1103/RevModPhys.74.145.

[7] EVEN S, GOLDREICH O, and LEMPEL A. A randomized protocol for signing contracts[J]. *Communications of the ACM*, 1985, 28(6): 637–647. doi: 10.1145/3812.3818.

[8] BRASSARD G, CREPEAU C, and ROBERT J M. All-or-Nothing Disclosure of Secrets[M]. Berlin, Heidelberg: Springer, 1987: 234–238. doi: 10.1007/3-540-47721-7_17.

[9] GAO Fei, QIN Sujuan, HUANG Wei, *et al*. Quantum private query: A new kind of practical quantum cryptographic protocol[J]. *Science China Physics, Mechanics & Astronomy*, 2019, 62(7): 70301. doi: 10.1007/s11433-018-9324-6.

[10] JAKOBI M, SIMON C, GISIN N, *et al*. Practical private database queries based on a quantum- key-distribution protocol[J]. *Physical Review A*, 2011, 83(2): 022301. doi: 10.1103/PhysRevA.83.022301.

[11] SCARANI V, ACÍN A, RIBORDY G, *et al*. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations[J]. *Physical Review Letters*, 2004, 92(5): 057901. doi: 10.1103/physrevlett.92.057901.

[12] GAO Fei, LIU Bin, WEN Qiaoyan, *et al*. Flexible quantum private queries based on quantum key distribution[J]. *Optics Express*, 2012, 20(16): 17411–17420. doi: 10.1364/OE.20.017411.

[13] ZHANG Jiali, GUO Fenzhuo, GAO Fei, *et al*. Private database queries based on counterfactual quantum key distribution[J]. *Physical Review A*, 2013, 88(2): 022334. doi: 10.1103/physreva.88.022334.

[14] SASAKI T, YAMAMOTO Y, and KOASHI M. Practical quantum key distribution protocol without monitoring signal disturbance[J]. *Nature*, 2014, 509(7501): 475–478. doi: 10.1038/nature13303.

[15] LIU Bin, GAO Fei, HUANG Wei, *et al*. QKD-based

quantum private query without a failure probability[J]. *Science China Physics, Mechanics & Astronomy*, 2015, 58(10): 100301. doi: 10.1007/s11433-015-5714-3.

[16] WEI Chunyan, GAO Fei, WEN Qiaoyan, *et al*. Practical quantum private query of blocks based on unbalanced-state Bennett-Brassard-1984 quantum-key -distribution protocol[J]. *Scientific Reports*, 2014, 4(1): 7537. doi: 10.1038/srep07537.

[17] PANDURANGA RAO M V and JAKOBI M. Towards communication-efficient quantum oblivious key distribution[J]. *Physical Review A*, 2013, 87(1): 012331. doi: 10.1103/PhysRevA.87.012331.

[18] GAO Fei, LIU Bin, HUANG Wei, *et al*. Postprocessing of the oblivious key in quantum private query[J]. *IEEE Journal of Selected Topics in Quantum Electronics*, 2015, 21(3): 98–108. doi: 10.1109/jstqe.2014.2358192.

[19] WEI Chunyan, WANG Tianyin, and GAO Fei. Practical quantum private query with better performance in resisting joint-measurement attack[J]. *Physical Review A*, 2016, 93(4): 042318. doi: 10.1103/PhysRevA.93.042318.

[20] YU Fang, QIU Daowen, SITU Haozhen, *et al*. Enhancing user privacy in SARG04-based private database query protocols[J]. *Quantum Information Processing*, 2015, 14(11): 4201–4210. doi: 10.1007/s11128-015-1091-0.

[21] WEI Chunyan, CAI Xiaoqiu, LIU Bin, *et al*. A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure[J]. *IEEE Transactions on Computers*, 2018, 67(1): 2–8. doi: 10.1109/TC.2017.2721404.

[22] CHAN P, LUCIO-MARTINEZ I, MO Xiaofan, *et al*. Performing private database queries in a real-world environment using a quantum protocol[J]. *Scientific Reports*, 2014, 4(1): 5233. doi: 10.1038/srep05233.

[23] YAO A C C. How to generate and exchange secrets[C]. The 27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 1986: 162–167. doi: 10.1109/SFCS.1986.25.

[24] KILIAN J. Founding crytpography on oblivious transfer[C]. The 20th Annual ACM Symposium on Theory of Computing, Chicago, USA, 1988: 20–31. doi: 10.1145/62212.62215.

[25] NIELSEN J B, NORDHOLT P S, ORLANDI C, *et al*. A new approach to practical active-secure two-party computation[C]. The 32nd Annual Cryptology Conference, Santa Barbara, USA, 2012: 681–700. doi: 10.1007/978-3-642-32009-5_40.

[26] LO H K. Insecurity of quantum secure computations[J]. *Physical Review A*, 1998, 56(2): 1154–1162. doi: 10.1103/PhysRevA.56.1154.

[27] BENNETT C H and BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[J]. *Theoretical Computer Science*, 2014, 560: 7–11. doi: 10.1016/j.tcs.2014.05.025.

魏春艳：女，1982年生，副教授，研究方向为量子密码与量子信息.
蔡晓秋：女，1980年生，副教授，研究方向为量子密码与量子计算.
王天银：男，1979年生，教授，研究方向为量子密码与量子信息.
苏　琦：男，1985年生，副研究员，研究方向为量子密码与量子计算.
秦素娟：女，1979年生，副教授，研究方向为量子密码与量子计算.
高　飞：男，1980年生，教授，研究方向为量子密码与量子计算.
温巧燕：女，1959年生，教授，研究方向为密码学与信息安全.