基于纠缠交换的分布式量子身份认证方案

刘岳启[1,2],张 琨[2]
LIU Yue-qi[1,2],ZHANG Kun[2]

1.淮阴师范学院 科技处,江苏 淮安 223300
2.南京理工大学 计算机科学与技术学院,南京 220091
1.Department of Science and Technology,Huaiyin Teachers College,Huai'an,Jiangsu 223300,China
2.Department of Computer,Nanjing University of Science and Technology,Nanjing 210094,China
E-mail:hysylyq@126.com

LIU Yue-qi,ZHANG Kun.Quantum authentication protocols based on entanglement swapping in distributed network. Computer Engineering and Applications,2008,44(32):90-92.

Abstract: This paper analyzed the quantum identity authentication technology in the network environment and brought forward a scheme of quantum identity authentication based on the swapping of the EPR entanglement and analyzed its security.Thus a scheme of sharing secret key string between two sides in the distributed network environment was presented.It made use of the entanglement swapping to authenticate the identity.

Key words: quantum cryptography;entanglement swapping;identity authentication

摘 要:分析了在网络环境下的量子身份认证技术,提出了在分布式网络环境下,通信双方共享密钥串,利用纠缠交换技术进行身份认证的方案,并分析了方案的可行性。

关键词:量子密码;纠缠交换;身份认证
DOI:10.3778/j.issn.1002-8331.2008.32.027 **文章编号**:1002-8331(2008)32-0090-03 **文献标识码**:A **中图分类号**:TP918.1

身份认证是指计算机及网络系统确认操作者身份的过程。在数字世界中,一切信息包括用户的身份信息都是由一组特定的数据表示的。计算机只能识别用户的数字身份,给用户的授权也是针对用户的数字身份进行的。而人们生活的现实世界是一个真实的物理世界,每个人都拥有独一无二的物理身份。保证操作者的物理身份与数字身份相对应就是身份认证管理系统所需要解决的问题。

目前量子认证主要包括量子身份认证、量子信道认证和量子消息认证三个方面,这里主要讨论身份认证问题。自从第一个量子密钥分发协议 BB84 协议提出以来,量子密钥分发经过多年的努力取得了丰富的成果[1]。但是,人们对量子认证的认识还刚刚开始[2]。文献[3]首次研究了量子密钥的验证问题,在此基础上,人们进一步探讨了量子身份认证[4-5]、量子签名[6-7]和量子消息确认[8]。在这些身份认证系统中,有基于量子密钥和经典身份论证系统[3,9],有基于经典密钥的量子身份认证系统[10-11]——示证者的个人信息用经典信息表示,认证系统具有量子特征,实现时通过量子系统来实现;还有纯量子身份认证系统,如不依赖于第三方的动态量子身份认证方案[12]。不过,量子认证方面还有很多问题有待进一步的研究。

文献[13]提出基于四粒子 GHZ 态的分布式网络身份认证方案,经证明是安全的。但四粒子 GHZ 粒子的长时间存储和测量的同步等技术问题均有待于解决[14]。

本文提出了在分布式网络环境下采用纠缠交换的方法,并利用层状量子存储器进行量子存储,在分布式系统下进行量子身份认证方案。方案经分析是安全可靠的。

1 分布式客户机/服务器认证结构

如图 1 所示,分布式网络认证结构分为三层,第一层为 1 个根服务器,第二层为 m 个子服务器,根服务器与每个子服务器分别共享 K 个处于 EPR 纠缠态的粒子对序列,$\{[T_1(1),T_1(2)],[T_2(1),T_2(2)],\cdots,[T_k(1),T_k(2)]\}$,其中下标表示每一个 EPR 对在序列中的顺序,1 和 2 表示 EPR 对的两个光子。每个子服务器拥有 $n(n>m)$个客户机,每个子服务器分别与所管辖的每个客户机共享 K 个处于 EPR 纠缠态的粒子对序列$\{[P_1(1),P_1(2)],[P_2(1),P_2(2)],\cdots,[P_k(1),P_k(2)]\}$,则整个网络中的最大 EPR 纠缠对的数量级为 $O(mnK)$。如果网络中的客户机互相共享 K 个 EPR 纠缠对序列,那么整个网络中的最大 EPR 纠缠对的数

基金项目:国家自然科学基金重大项目(the Grand National Natural Science Foundation of China under Grant No.90718021);江苏省淮阴师范学院青年教师基金项目(No.07HSQN004)。

作者简介:刘岳启(1975-),男,南京理工大学计算机科学与技术学院硕士研究生,助理研究员,主要研究领域:信息安全;张琨(1977-),女,博士,副教授,主要研究领域:信息安全。

收稿日期:2008-01-24 **修回日期**:2008-08-28

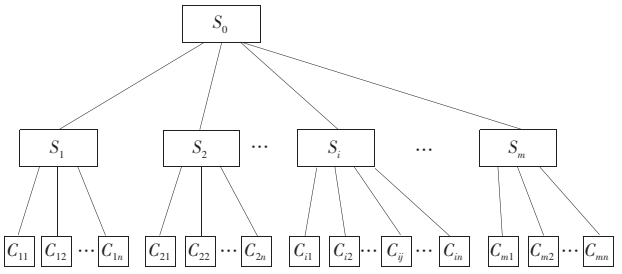

图 1　分布式网络认证结构示意图

量级为 $O((mnK)^2)$，因此，该认证结构大大缓解了网络中的认证密钥的分发问题，也节省了资源[15]。

本章所涉及到的量子存储方式可参考文献[16]。

2　共享密钥串的分布式量子身份认证方案

在分布式系统下，C_{11} 与 C_{ij} 进行身份认证，量子态的制备与发送采用下级制备并向上级发送的方式。

2.1　制备阶段

(1)各客户端 C_{11}，C_{12}，C_{13}，…，C_{mn} 分别制备 EPR 纠缠态粒子对序列 P，如客户端 C_{11} 制备与子服务器 S_1 共享的 EPR 纠缠态粒子对序列为：$\{[P_{111}(1),P_{111}(2)],[P_{112}(1),P_{112}(2)],\cdots,[P_{11k}(1),P_{11k}(2)]\}$，其中下标第一数字表示子服务器 S_1，下标第二个数字表示客户端 C_{11} 在子服务器 S_1 中的位置，下标第三个数字表示每一个 EPR 对在序列中的顺序，1 和 2 表示 EPR 对的两个粒子。C_{11} 从每一个 EPR 对中提取出一个粒子构成一个有序的粒子序列，$\{P_{111}(1),P_{112}(1),\cdots,P_{11k}(1)\}$ 称为 $P_{11}(1)$ 序列，$\{P_{111}(2),P_{112}(2),\cdots,P_{11k}(2)\}$ 称为 $P_{11}(2)$ 序列。

各客户端 C_{ij} 制备与子服务器 S_i 共享的 EPR 纠缠态粒子对序列为$\{[P_{ij1}(1),P_{ij1}(2)],[P_{ij2}(1),P_{ij2}(2)],\cdots,[P_{ijk}(1),P_{ijk}(2)]\}$，其中下标第一数字表示第 i 个子服务器 S_i，下标第二个数字表示 C_{ij} 在子服务器 S_i 中的位置，下标第三个数字表示每一个EPR 对在序列中的顺序，1 和 2 表示 EPR 对的两个粒子；C_{ij} 从每一个 EPR 对中提取一个粒子构成一个有序的粒子序列，$\{P_{ij1}(1),P_{ij2}(1),\cdots,P_{ijk}(1)\}$ 称为 $P_{ij}(1)$ 序列，$\{P_{ij1}(2),P_{ij2}(2),\cdots,P_{ijk}(2)\}$ 称为 $P_{ij}(2)$ 序列。

(2)各客户端 C_{11}，C_{12}，C_{13}，…，C_{mn} 分别将粒子序列 $P_{ij}(1)$ 发送给各子服务器 S_1，S_2，S_3，…，S_m。将粒子序列 $P_{ij}(2)$ 留给自己，并采用量子存储方法存储在量子寄存器中。

(3)各子服务器 S_1，S_2，S_3，…，S_m 制备与根服务器 S_0 共享的 EPR 纠缠态粒子对序列 T，则子服务器 S_1 制备 EPR 纠缠态粒子对序列为：$\{[T_{11}(3),T_{11}(4)],[T_{12}(3),T_{12}(4)],\cdots,[T_{1k}(3),T_{1k}(4)]\}$，其中下标第一数字表示子服务器 S_1，下标第二个数字表示每一个 EPR 对在序列中的顺序，3 和 4 表示 EPR 对的两个粒子。S_1 从每一个 EPR 对中提取出一个粒子构成一个有序的粒子序列，$\{T_{11}(3),T_{12}(3),\cdots,T_{1k}(3)\}$ 称为 $T_1(3)$ 序列，$\{T_{11}(4),T_{12}(4),\cdots,T_{1k}(4)\}$ 称为 $T_1(4)$ 序列。

子服务器 S_i 制备 EPR 纠缠态粒子对序列为：$\{[T_{i1}(3),T_{i1}(4)],[T_{i2}(3),T_{i2}(4)],\cdots,[T_{ik}(3),T_{ik}(4)]\}$，其中下标第一数字表示子服务器 S_i，下标第二个数字表示每一个 EPR 对在序列中的顺序，3 和 4 表示 EPR 对的两个粒子。S_i 从每一个 EPR 对中提取出一个粒子构成一个有序的粒子序列，$\{T_{i1}(3),T_{i2}(3),\cdots,T_{ik}(3)\}$ 称为 $T_i(3)$ 序列，$\{T_{i1}(4),T_{i2}(4),\cdots,T_{ik}(4)\}$ 称为 $T_i(4)$ 序列。

(4)各子服务器 S_1，S_2，S_3，…，S_m 分别将粒子序列 $T_i(3)$ 发送给根服务器 S_0。将粒子序列 $T_i(4)$ 留给自己，并采用量子存储方法存储在量子寄存器中。部分客户端及服务器量子寄存器中所寄存的粒子序列的情况见表 1。

表 1　部分客户端及服务器量子寄存器中所寄存的粒子序列的情况

指针位置	客户端 C_{11}	子服务器 S_1		子服务器 S_0		子服务器 S_i		客户端 C_{ij}
1	$P_{111}(2)$	$P_{111}(1)$	$T_{11}(4)$	$T_{11}(3)$	$T_{i1}(3)$	$T_{i1}(4)$	$P_{ij1}(1)$	$P_{ij1}(2)$
2	$P_{112}(2)$	$P_{112}(1)$	$T_{12}(4)$	$T_{12}(3)$	$T_{i2}(3)$	$T_{i2}(4)$	$P_{ij2}(1)$	$P_{ij2}(2)$
3	$P_{113}(2)$	$P_{113}(1)$	$T_{13}(4)$	$T_{13}(3)$	$T_{i3}(3)$	$T_{i3}(4)$	$P_{ij3}(1)$	$P_{ij3}(2)$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
K	$P_{11k}(2)$	$P_{11k}(1)$	$T_{1k}(4)$	$T_{1k}(3)$	$T_{ik}(3)$	$T_{ik}(4)$	$P_{ijk}(1)$	$P_{ijk}(2)$
粒子序列	$P_{11}(2)$	$P_{11}(1)$	$T_1(4)$	$T_1(3)$	$T_i(3)$	$T_i(4)$	$P_{ij}(1)$	$P_{ij}(2)$

2.2　认证阶段

现假设客户端 C_{11} 要与 C_{ij} 进行通信，在通信之前，先进行量子身份认证。具体步骤如下：

(1)客户端 C_{11} 通过经典信道向子服务器 S_{11} 发送信息 $I_{C_{11}C_{ij}}$，表示 C_{11} 要与 C_{ij} 进行通信。

(2)子服务器 S_1 检查所管辖的客户端，若 C_{ij} 是自己的客户端，则进行(3)的操作，否则进行(3′)的操作。

(3)$C_{ij}=C_{1j}$，子服务器 S_1 将 $P_{11}(1)$ 与 $P_{1j}(1)$ 进行 Bell 基测量，则 $P_{11}(2)$ 与 $P_{1j}(2)$ 通过纠缠交换形成了 EPR 纠缠对，客户端 C_{11} 采用共享密钥串所对应的测量基进行测量，客户端 C_{1j} 也采用共享密钥串所对应的测量基进行测量。

(4)客户端 C_{11} 与 C_{1j} 比较测量结果，若测量结果出错率小于一定阈值，则认证成功。

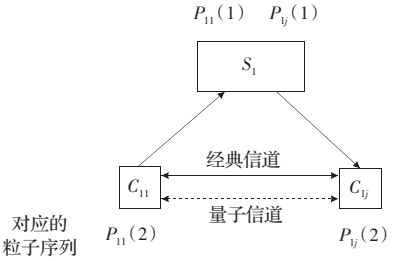

图 2　下级发送粒子时子服务器下客户端认证示意图

(3′)若 $C_{ij}\neq C_{1j}$，子服务器 S_1 向根服务器 S_0 发送信息 $I_{C_{11}C_{ij}}$，S_0 向它所属的子服务器 S_1，S_2，S_3，…，S_m 广播信息 $I_{C_{11}C_{ij}}$，子服务器 S_{ij} 发现 C_{ij} 是自己所管辖的客户端，则 S_{ij} 响应。可采用传统网络路由的方法，提取一条最短的认证路径。

(4′)S_1 将 $P_{11}(1)$ 与 $T_1(4)$ 进行 Bell 基测量，S_0 将 $T_1(3)$ 与 $T_i(3)$ 进行 Bell 基测量，S_i 将 $T_1(4)$ 与 $P_{ij}(1)$ 进行 Bell 基测量，则 $P_{11}(2)$ 与 $P_{ij}(2)$ 通过纠缠交换形成了 EPR 纠缠对序列，客户端 C_{11} 采用共享密钥串所对应的测量基进行测量，客户端 C_{ij} 也采用共享密钥串所对应的测量基进行测量。

(5′)客户端 C_{11} 与 C_{ij} 比较测量结果，若测量结果出错率小于一定阈值，则认证成功。

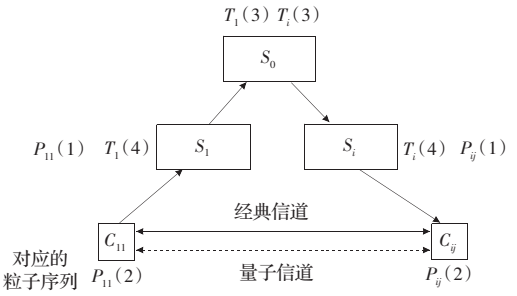

图3 下级发送粒子时根服务器下客户端认证示意图

3 安全性分析

整个协议的安全性取决于子服务器与根服务器之间以及子服务器与所管辖的客户机之间分别成功地共享 EPR 纠缠态。如果子服务器与根服务器之间以及子服务器与所管辖的客户机之间分别成功地共享 EPR 纠缠态，则本协议是完全安全的。量子态的制备与发送采用下级制备并向上级发送的方式，有利于网络的快速查找。整个协议分为两个部分：制备阶段和认证阶段。制备阶段是各服务器和客户端能否共享 EPR 纠缠对的基础。在认证阶段，利用文献[17]中的认证协议（文献[17]详细描述了认证协议的安全性），子服务器可以鉴别申请者是否假冒。如果申请者是真实的，然后可信服务器作纠缠交换操作（操作过程中并没有粒子传输，偷听者得不到任何信息）。在申请者向接收者发送粒子序列时，偷听者也是得不到任何信息的，因为申请者只发送了 EPR 对中的一个，EPR 对的另一个一直在接收者的手中。Eve 不能根据 EPR 对中的一个粒子获取整个 EPR 纠缠态的信息，同时，为了检测偷听，申请者和接收者还随机选取一些 EPR 对测量结果进行错误率估计，这也能检测到 Eve 是否存在。Eve 对传输粒子的偷听，得不到任何信息，只会给传输的粒子造成干扰。

参考文献：

[1] 曾贵华.量子信息安全系统[J].物理,2000,29(4):623-625.
[2] 温巧燕,高飞,朱甫臣.量子密钥分发中身份认证问题的研究现状及方向[J].北京邮电大学学报,2004,27(5):1-6.
[3] Zeng G H,Zhang W P.Identity verification in quantum cryptography[J].Phys Rev A,2000,61(2):022303/1-5.
[4] 曾贵华,王新梅,诸鸿文.可完全脱离信赖第三方的认证系统[J].通信学报,2001,22(8):41-46.
[5] Dusek M,Haderka H,Myski M R.Quantum identification system[J].Phys Rev A,1999,60(1):149-156.
[6] Zeng G H,Keitel C H.An arbitrated quantum signature algorithm[J].Phy Rev A,2002,65(4):042312.
[7] 曾贵华,马文平,王新梅,等.基于量子密码的签名方案[J].电子学报,2001,29(8):1098-1100.
[8] Barnum H,Crepeau C.Authentication of quantum messages[J].Phy Rev A,2002,66(1):021037/1-6.
[9] Dusek M.Quantum identification system[J].Phys Rev A,1999,60:149-156.
[10] 曾贵华,王新梅.用量子效应实现身份认证[J].通信保密,2000,1:1-3.
[11] Ljuuggren D,Bourennane M,Karlsson A.Authority-based user authentication in quantum key distribution[J].Phys Rev A,2000,62:022305.
[12] 曾贵华.不依赖于第三方的动态量子身份认证方案[J].电子学报,2004,32:1148-1151.
[13] 温晓军,刘云.分布式量子通信网络中的身份认证方案[J].铁道学报,2005,27(6):58-61.
[14] Bollinger J J.A 303MHz frequency standard based on trapped Be+Ions[J].IEEE Trans Inst Meas,1997,40:126.
[15] 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):3995-3998.
[16] 吴俊杰,晶菲,潘晓浑,等.基于经典存储器的量子计算机存储系统[J].计算机工程与应用,2006,42(30):98-101.
[17] Ekert A K.Quantum cryptography bases on Bell's theorem[J].Phys Rev Let,1991,67:661-664.

（上接86页）

假设某个入侵者 P_j 选择一个多项式 $f(x)'$，并计算 $v'_j=f'(ID_j) \bmod m$，加密成 (D_j,D'_j) 发送给组中的其他用户 P_j，但是因为入侵者不知道用户 P_j 的私钥，无法伪造有用户 P_i 私钥签名的信息 $\{A_{ic}(c=0,1,2,\cdots,t-1)\}$，所以验证公式 $v_{ij}=f_i(ID_j)G=\sum_{r=0}^{t-1}A_{ir}(ID_j)^r$ 无法通过。秘密重构阶段，入侵者也不能冒充其他用户发送自己的秘密份额，否则验证等式 $e_{ji}=d_jG=PK_j$ 无法通过。

3 结束语

门限秘密共享在信息安全和数据保密中起着非常重要的作用，是设计多方安全协议的基本工具。本文给出了一种基于椭圆曲线密码体制的无可信中心的 (t,n) 门限秘密共享方案，提出了秘密共享矩阵的概念，最后证明了本方案的有效性和安全性。本方案在密钥托管、电子商务及电子选举等应用领域，具有一定的实用价值。

参考文献：

[1] Desmedt Y.Some recent research aspects of threshold cryptography[C]// Lecture Notes in Computer Science:Proc of the 1st Int'l Information Security Workshop.New York:Spring-Verlag,1997:158-173.
[2] Shamir A.How to share a secret[J].Communications of the ACM,1979,22(11):612-613.
[3] Blakley G.Safeguarding cryptographic keys[C]//Proc AFIPS 1979 Natl Conf.New York:AFIPS Press,1979:313-317.
[4] Asmuth C,Bloom J.A modular approach to key safeguarding[J].IEEE Transactions on Information Theory,1983,29:208-210.
[5] Karnin E D,Greene J W,Hellman M E.On secret sharing systems[J].IEEE Transactions on Information Theory,1983,29(1):231-241.
[6] Chang T Y,Yang C C,Hwang M S.A threshold signature scheme for group communications without a shared distribution center[J].Future Generation Computer Systems,2004,20(6):1013-1021.
[7] 周福才.没有SDC的 (t,n) 门限秘密共享方案[J].通信学报,2006,10(10):69-73.
[8] 庞辽军.基于ECC的门限秘密共享方案及其安全性[J].西安电子科技大学学报:自然科学版,2006,8(4):572-575.