第 54 卷 第 9 期 2005 年 9 月
1000-3290/2005/54(09)/3995-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.9,September,2005
©2005 Chin. Phys. Soc.

一种网络多用户量子认证和密钥分配理论方案*

杨宇光[1)†] 温巧燕[1)] 朱甫臣[2)]

[1)](北京邮电大学理学院,北京 100876)

[2)](现代通信国家重点实验室,成都 610041)

(2004 年 12 月 19 日收到;2005 年 2 月 2 日收到修改稿)

提出了一种网络多用户量子认证和密钥分配理论方案.类似于现代密码学中的网络认证体系结构提出了一种基于网络中用户与所属的可信服务器之间共享 Einstein-Podolsky-Rosen(EPR)纠缠对进行身份认证和密钥分配的分布式客户机/服务器体系结构.基于该体系结构实现网络中任意用户之间的身份认证和密钥分配.可信服务器只提供用户的身份认证以及交换粒子之间的纠缠使得两个想要秘密通信的用户的粒子纠缠起来.密钥的生成由发起请求的用户自己完成.网络中的用户只需和所属的可信服务器共享 EPR 纠缠对通过经典信道和量子信道与服务器通信.用户不需要互相共享 EPR 纠缠对,这使得网络中的 EPR 对的数量由 $O(n^2)$ 减小到 $O(n)$.

关键词:量子认证,量子密钥分配,客户机/服务器,纠缠交换

PACC:0365

1. 引 言

当 Alice 和 Bob 坐在网络的两端想要秘密通信,他们如何秘密交换密钥呢?他们中的每一个人又能如何确信是在和对方通信而不是和第三方通信呢?现代密码学提供了解决方案,如 Wide-Mouth Frog 协议、Yahalom 协议、Otway-Rees 协议、Needham 和 Schroeder 协议、Kerberos 协议和 CCITTX.509[1] 等都能解决这一问题.这些协议都是基于对称密码和公开密钥密码提出的.由于它们的安全性取决于计算复杂性以及数学难题,随着量子计算机的研究,这些基于数学难题或计算复杂性的协议的安全性存在潜在的危险.

自从 Wiesner[2] 以及随后的 Bennett 和 Brassard[3] 发现利用量子效应可以在公开的量子信道上传送秘密信息,人们对量子密码学投入越来越多的关注,提出了许多量子密钥分配协议[4—21] 并对所提出的 QKD 协议的窃听问题进行了研究[22—25].其中提出的许多协议属于两方之间的点对点的密钥分配.然而 QKD 实际的实现要求网络中任意用户之间的密钥分配.人们已研究了利用单光子的多用户 QKD 方案[15,19].也提出了使用非正交基的多用户 QKD 方案[20].

另外,即使不需要进行量子密钥分配,在点对点通信中或量子密码网络中也需要验证用户的身份[26].本文提出了一种网络多用户量子认证和密钥分配理论方案.该方案利用了一种分布式客户机/服务器结构.基于该结构实现网络中任意用户之间的身份认证和密钥分配.可信服务器只提供用户的身份认证而不参与用户的密钥分配.网络中的用户只需和所属的可信服务器共享 Einstein-Podolsky-Rosen(EPR)纠缠对作为量子认证密钥且通过经典信道和量子信道与服务器通信.采用量子密钥作为认证密钥的目的是提高认证的安全性以避免现代密码学中经典密钥带来的安全性问题.用户不需要互相共享 EPR 纠缠对,这使得网络中的 EPR 对的数量由 $O(n^2)$ 减小到 $O(n)$.

本文提出了一种网络多用户量子认证和密钥分配理论方案;描述了分布式客户机/服务器认证结构;详细描述了网络多用户量子认证和密钥分配理论方案;分析了协议的安全性.

2. 网络多用户量子认证和密钥分配理论方案

一个最大 EPR 纠缠对处于下面四个 Bell 态

* 国家自然科学基金(批准号:60373059)和教育部博士点基金(批准号:20040013007)资助的课题.

† E-mail:yangyang7357@sina.com.

之一：

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \quad (1)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle), \quad (2)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle), \quad (3)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle), \quad (4)$$

2.1. 分布式客户机/服务器认证结构

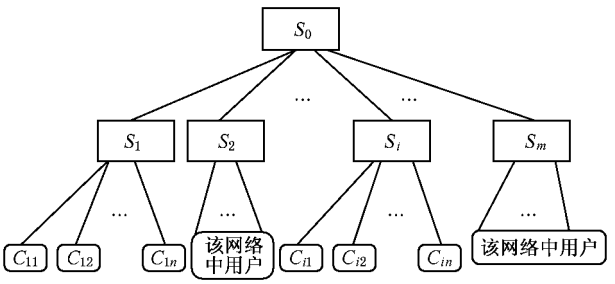

图 1 分布式客户机/服务器认证结构

如图 1 的认证结构分为三层.第一层为一个根服务器,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 N 个处于 $|\Phi^+\rangle$ 态的粒子对,每个子服务器之间分别共享 N 个处于 $|\Phi^+\rangle$ 态的粒子对.每个子服务器拥有 $n(n \gg m)$ 个客户机,每个子服务器分别与所管辖的每个客户机共享 N 个处于 $|\Phi^+\rangle$ 态的粒子对,则整个网络中的最大 EPR 纠缠对的数量级为 $O(nmN)$.如果网络中的客户机互相共享 N 个最大 EPR 纠缠对,那么整个网络中的最大 EPR 纠缠对的数量级为 $O((nmN)^2)$,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.

该认证结构中,子服务器之间可以进行交叉认证,下面描述的量子认证和密钥分配协议就是基于子服务器之间的交叉认证来设计的.

2.2. 网络多用户量子认证和密钥分配理论方案

先介绍纠缠交换的概念[27].假设两个相距遥远的 Alice 和 Bob 共享初始纠缠态 $|\Phi_{12}^+\rangle$ 和 $|\Phi_{34}^+\rangle$,Alice 拥有下标为 1 和 4 的粒子,对量子位 1 和 4 实施 Bell 基测量,Bob 拥有下标为 2 和 3 的粒子,对量子位 2 和 3 实施 Bell 基测量.总状态以 1/4 等概投影到,$\{|\Phi_{23}^+\rangle\otimes|\Phi_{14}^+\rangle, |\Phi_{23}^-\rangle\otimes|\Phi_{14}^-\rangle, |\Psi_{23}^+\rangle\otimes|\Psi_{14}^+\rangle, |\Psi_{23}^-\rangle\otimes|\Phi_{14}^-\rangle\}$,之前的粒子 1 和 2 之间的纠缠与粒子 3 和 4 之间的纠缠交换为粒子 2 和 3 之间的纠缠与粒子 1 和 4 之间的纠缠.不同的初始状态具有不同的测量结果,总结见表 1.

表 1 不同的初始态得到的测量结果

	$\|\Phi_{34}^+\rangle$	$\|\Phi_{34}^-\rangle$	$\|\Psi_{34}^+\rangle$	$\|\Psi_{34}^-\rangle$
$\|\Phi_{12}^+\rangle$	1	+ −	$\Phi\Psi$	both
$\|\Phi_{12}^-\rangle$	+ −	1	both	$\Phi\Psi$
$\|\Psi_{12}^+\rangle$	$\Phi\Psi$	both	1	+ −
$\|\Psi_{12}^-\rangle$	both	$\Phi\Psi$	+ −	1

“1”表示 $\{\{|\Phi_A^+\rangle, |\Phi_B^+\rangle\}, \{|\Phi_A^-\rangle, |\Phi_B^-\rangle\}, \{|\Psi_A^+\rangle, |\Psi_B^+\rangle\}, \{|\Psi_A^-\rangle, |\Psi_B^-\rangle\}\}$;

“+ −”表示 $\{\{|\Phi_A^+\rangle, |\Phi_B^-\rangle\}, \{|\Phi_A^-\rangle, |\Phi_B^+\rangle\}, \{|\Psi_A^+\rangle, |\Psi_B^-\rangle\}, \{|\Psi_A^-\rangle, |\Psi_B^+\rangle\}\}$;

“$\Phi\Psi$”表示 $\{\{|\Phi_A^+\rangle, |\Psi_B^+\rangle\}, \{|\Phi_A^-\rangle, |\Psi_B^-\rangle\}, \{|\Psi_A^+\rangle, |\Phi_B^+\rangle\}, \{|\Psi_A^-\rangle, |\Phi_B^-\rangle\}\}$;

“both”表示 $\{\{|\Phi_A^+\rangle, |\Psi_B^-\rangle\}, \{|\Phi_A^-\rangle, |\Psi_B^+\rangle\}, \{|\Psi_A^+\rangle, |\Phi_B^-\rangle\}, \{|\Psi_A^-\rangle, |\Phi_B^+\rangle\}\}$.

在下面的协议中假定经典信道是公开的,只能监听不能篡改.而量子信道则可以被偷听者操纵进行攻击.

协议如下：

1) 通过经典信道,子服务器 $S1$ 所管辖的客户机 $C11$ 发送消息给 $S1$,他想要和 Cij 进行秘密通信,$S1$ 利用文献[28]中的认证协议鉴别 $C11$ 的身份.

2) 在认证开始前,$C11$ 和 $S1$ 分别把他们的粒子态旋转 θ,旋转算子为

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \quad (5)$$

最大纠缠态 $|\Phi_A^+\rangle$ 在两边的旋转操作下不变.该操作的目的是防止偷听者的假冒.然后 $S1$ 制备 $K(K < N)$ 个处于任意态的粒子 γ_S^i：$|\psi_i\rangle = a_i|0\rangle + b_i|1\rangle, i = 1,2,\cdots,K$.其中 $|a_i|^2 + |b_i|^2 = 1$,a_i, b_i 是随意选择的复数.$S1$ 把挑战粒子 γ_S^i 发送给 $C11$.

3) $C11$ 使用纠缠对中的相应粒子 β_{C11}^i 和粒子 γ_S^i 进行 C-NOT 操作(β_{C11}^i 是控制位,γ_S^i 是目标位),三个粒子的态变为

$$|\Psi_i\rangle = \frac{1}{\sqrt{2}}(a_i|000\rangle + b_i|001\rangle + a_i|111\rangle + b_i|110\rangle), \quad (6)$$

然后 $C11$ 把 γ_S^i 发送回 $S1$,$S2$ 使用他的相应粒子 β_{S1}^i(β_{S1}^i 与 β_{C11}^i 纠缠)和 γ_S^i 进行 C-NOT 操作(β_{S1}^i 是控

制位,γ_S^i 是目标位),则三粒子的态变为

$$|\Psi_i'\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |11\rangle) \otimes a_i|0\rangle + b_i|1\rangle$$
$$= |\Phi^+\rangle \otimes |\Psi_i\rangle, \quad (7)$$

$S1$ 在基 $\{|\psi_i\rangle, |\psi_i\rangle^\perp\}$ 上测量 γ_S^i,如 γ_S^i 的态为 $|\psi_i\rangle$,表明 $C11$ 是真实的,继续步骤 4),否则表明 $C11$ 是假冒的,协议终止.

4) 如果 $S1$ 发现 Cij 为自己管辖的客户机,执行步骤 5),否则执行步骤 5 ').

5) $S1$ 分别对所拥有与 $C11$ 纠缠的粒子序列和与 Cij 纠缠的粒子序列作 Bell 基测量,并通过经典信道告知 $C11$ 和 Cij,他已进行了 Bell 基测量.

6) $C11$ 对自己的每个粒子分别随机地选取 $\{U_0, U_1, U_2, U_3\}$ 之一作幺正操作:

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad (8)$$
$$U_1 = \sigma_Z = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad (9)$$
$$U_2 = \sigma_X = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad (10)$$
$$U_3 = i\sigma_\gamma = |0\rangle\langle 1| - |1\rangle\langle 0|. \quad (11)$$

这些操作分别对应于 00,01,10,11. 然后把它们发送给 Cij.

7) Cij 在收到 $C11$ 发送的粒子序列之后,与自己的粒子序列分别进行 Bell 基测量.

8) $S1$ 告知 $C11$ 和 Cij 他的测量结果.

9) 根据表 1,$S1$ 的测量结果以及自己的测量结果,Cij 可以推断出 $C11$ 的操作,从而得到一个密钥序列.为了检测在粒子序列传输过程中是否存在偷听,$C11$ 和 Cij 随机选取一个 EPR 纠缠对子集,对传输中的错误率进行估计.实际上,在粒子序列传输中,Eve 仅仅对传输的粒子序列造成干扰,而得不到任何信息,因为他仅仅得到了 EPR 对中的一个粒子.

10)如果错误率低于某一门限值,$C11$ 和 Cij 进行错误纠正,获得最终秘密密钥,协议结束.

5 ') $S1$ 发现 Cij 为 Si 管辖的客户机,$S1$ 分别对所拥有与 $C11$ 纠缠的粒子序列和与 Si 纠缠的粒子序列作 Bell 基测量,这样 $C11$ 的粒子序列和 Si 的粒子序列纠缠起来.同时 $S1$ 通过经典信道告知 Si 自己的客户机 $C11$ 想要和 Cij 秘密通信.

6 ') Si 分别对所拥有与 $C11$ 纠缠的粒子序列和与 Cij 纠缠的粒子序列作 Bell 基测量,这样 $C11$ 和 Cij 的粒子序列纠缠起来.

7 ')类似于步骤6),$C11$对自己的每个粒子分别随机地选取 $\{U_0, U_1, U_2, U_3\}$ 之一作幺正操作,然后把它们发送给 Cij.

8 ') Cij 在收到 $C11$ 发送的粒子序列之后,与自己的粒子序列分别进行 Bell 基测量.

9 ') $S1$ 和 Si 通过经典信道告知 $C11$ 和 Cij 他们的测量结果.

10 ')根据表 1,$S1$ 和 Si 的测量结果以及自己的测量结果,Cij 可以推断出 $C11$ 的操作,从而得到一个密钥序列.为了检测在粒子序列传输过程中是否存在偷听,$C11$ 和 Cij 随机选取一个 EPR 纠缠对子集,对传输中的错误率进行估计.

11 ')如果错误率低于某一门限值,$C11$ 和 Cij 进行错误纠正,获得最终秘密密钥,协议结束.

2.3. 安全性分析

整个协议的安全性取决于子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最大 EPR 纠缠态.如果子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最大 EPR 纠缠态,则所建议的协议是完全安全的.整个协议分为两个部分:认证阶段和密钥分配阶段.密钥分配阶段是基于认证阶段的,没有认证阶段,密钥分配阶段不能实施.在认证阶段,利用文献[28]中的认证协议(文献[28] 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.每一个被发送粒子的态均为 $\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,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.

另外,在所建议的方案中,可信服务器的作用只是用来对客户机进行身份认证,并不参与客户机的密钥分配,因此即使某一服务器被偷听者控制,偷听者也不能获取到密钥的信息,如果他想获取密钥的信息,只会在申请者和接收者选取一些 EPR 对进行偷听检测时被检测到.

3. 结 论

本文提出了一种网络多用户量子认证和密钥分配理论方案.该方案利用了一种分布式客户机/服务器结构.基于该结构实现网络中任意用户之间的身份认证和密钥分配.可信服务器只提供用户的身份认证而不参与用户的密钥分配.网络中的用户只需和所属的可信服务器共享 EPR 纠缠对作为量子认证密钥且通过经典信道和量子信道与服务器通信.采用量子密钥作为认证密钥的目的是提高认证的安全性以避免现代密码学中经典密钥带来的安全性问题.用户不需要互相共享 EPR 纠缠对,这使得网络中的 EPR 对的数量由 $O(n^2)$ 减小到 $O(n)$.

所建议的方案实践的可行性可借鉴使用 Bell 基测量的实验诸如隐形传态[29] 和纠缠交换[30] . Pan 等[30] 实施的实验使用了四个由 UV 脉冲产生的光子以及通过在一个分束器处干涉两个光子来实施 Bell 测量.为了实施所建议的方案,需要事先在子服务器和客户机上分别共享最大 EPR 纠缠对,并且需要保存一段时间,这可能在目前的技术看来有些困难.

[1] Bruce Schneier 1994 *Applied Cryptography-Protocols, Algorithms, and Source Code in C*(John Wiley & Sons,Inc.) p36—38

[2] Wiesner S 1983 *Sigact News* **15** 78

[3] Bennett C H, Brassard G, Breidbart S and Wiesner S 1982 *Advances in Cryptology*:*Proceedings of Crypto* **82** 267

[4] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* 175

[5] Ekert A 1991 *Phys. Rev. Lett.* **67** 661

[6] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[7] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881

[8] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239

[9] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863

[10] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383

[11] Bruβ D 1998 *Phys. Rev. Lett.* **81** 3018

[12] Hwang W Y, Koh I G and Han Y D 1998 *Phys. Lett.* A **244** 489

[13] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635

[14] Cabello A 2000 *Phys. Rev.* A **61** 052312 – 1

[15] Phoenix S J D, Barnett S M, Townsend P D and Blow K J 1995 *J. Modern Optics* **42** 1155

[16] Lo H K, Chan H F and Ardehali M arViv:quant-ph/0011056

[17] Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238

[18] Cabello A 2001 *Phys. Rev.* A **64** 024301

[19] Townsend P D 1997 *Nature* **385** 47

[20] Xue P, Li C F and Guo G C 2002 *Phys. Rev.* A **65** 022317

[21] Yang L, Wu L A and Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese) [杨 理、吴令安、刘颂豪 2002 物理学报 **51** 2446]

[22] Yang L, Wu L A and Liu S H 2002 *Acta Phys. Sin.* **51** 961 (in Chinese) [杨 理、吴令安、刘颂豪 2002 物理学报 **51** 961]

[23] Zhang Q, Tang C J and Zhang S Q 2002 *Acta Phys. Sin.* **51** 1439 (in Chinese) [张 权、唐朝京、张森强 2002 物理学报 **51** 1439]

[24] Zhang Q and Zhang E Y 2002 *Acta Phys. Sin.* **51** 1684 (in Chinese) [张 权、张尔扬 2002 物理学报 **51** 1684]

[25] Liu J F, Tang Z L, Liang R S *et al Acta Phys. Sin.* (in Chinese) (accepted) [刘景锋、唐志列、梁瑞生等 物理学报 (已接受)]

[26] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651

[27] Daegene Song arXiv:quant-ph/0305168

[28] Zhang Y S, Li C F, Guo G C arViv:quant-ph/ 0008044

[29] Boschi D, Branca S, De Martini F, Hardy L and Popescu S 1998 *Phys. Rev. Lett.* **80** 1121

[30] Pan J W, Bouwmeester D, Weinfurter H and Zeilinger A 1998 *Phys. Rev. Lett.* **80** 3891

A theoretical scheme for multi-user quantum authentication and key distribution in a network*

Yang Yu-Guang[1)†] Wen Qiao-Yan[1)] Zhu Fu-Chen[2)]

[1)] (*Science School, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

[2)] (*State Key Laboratory for Modern Communication, Chengdu* 610041, *China*)

(Received 19 December 2004; revised manuscript received 2 February 2005)

Abstract

A theoretical scheme for multi-user quantum authentication and key distribution in a network is proposed. Similar to the authentication architecture of the network in classical cryptography, a distributed client/server architecture with the shared Einstein-Podolsky-Rosen(EPR) entangled pairs between each user and his trusted server used for the authentication and key distribution is proposed. Based on this architecture, any-to-any multi-user quantum authentication and key distribution is realized. The trusted server only provides the authentication between users and swaps the entanglement between the particles so as to entangle the particles of the two users who want to communicate secretly. The key generation is performed by the requesting user. Each user in a network only shares Einstein-Podolsky-Rosen entangled pairs with the trusted server and communicates with the trusted server through the classical channel and quantum channel. Users need not share EPR entangled pairs with each other so that the number of EPR pairs in the network is reduced from $O(n^2)$ to $O(n)$.

Keywords: quantum authentication, quantum key distribution, client/server, entanglement swapping

PACC: 0365

* Project supported by the National Natural Science Foundation of China (Grant No. 60373059) and by the Doctoral Fund of Education Ministry of China (Grant No. 20040013007).

† E-mail: yangyang7357@sina.com