可证明安全的群组匿名认证密钥协商协议

冯 涛[1,2,3]，刘媛媛[1,4]，马建峰[3]

(1. 兰州理工大学计算机与通信学院 兰州 730050; 2. 福建师范大学网络安全与密码技术重点实验室 福州 350007;
3. 西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071; 4. 经济日报社技术处 北京 宣武区 100054)

【摘要】基于BDH困难问题，借鉴环签密方案的思想，提出了一种有效的群组匿名认证密钥协商方案。该方案首先在实现群组成员认证的前提下，协商出安全的会话密钥；对群组内外实现了不同程度的匿名，即群组之外的用户完全不能获悉参与协商的成员组成，群组内的成员了解参与协商的成员组成，但不能识别成员的身份信息；支持节点的动态群组密钥更新，实现了群组密钥的前向保密与后向保密；仅通过一轮交互确定会话密钥，降低了计算复杂性、减小了存储开销。

关 键 词 认证协议； 匿名技术； 群组技术； 密钥协商协议； 网络安全； 网络协议
中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.02.023

Provably Secure Anonymous Authentication Key Agreement Protocol for Multicast Group

FENG Tao[1,2,3], LIU Yuan-yuan[1,4], and MA Jian-feng[3]

(1. School of Computer and Communication, Lanzhou University of Technology Lanzhou 730050;
2. Key Lab of the Network Security and Cryptology, Fujian Normal University Fuzhou 350007;
3. Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University Xi'an 710071;
4. Technical Equipment Department, Economic Daily Xuanwu Beijing 100054)

Abstract With the idea of ring signcryption, an efficient anonymous group key agreement scheme is presented based on the Bilinear Diffie-Hellman (BDH) assumption. The scheme establishes a secure group key under the premise of authenticating group members. For both internal and external group members the scheme achieves different degree of anonymity, that is, the external users can absolutely not learn any information about the internal membership structure, and the internal users only can find out the member composition but cannot recognize the identity of any member. In order to achieve the forward security and backward security of group key, new scheme supports group members to renew their group key when the external nodes join the group or the internal members leave the group. The proposed scheme can establish the group session key through only one round, and therefore, its computation complexity and storage cost are efficiently reduced.

Key words authentication; anonymity; group technology; key agreement; network security; network protocols

随着面向群组的应用日益普及，群组通信的安全和群组成员的隐私保护问题逐渐成为用户关注的焦点。群组成员之间共享的会话密钥是群组成员间实现正常安全通信的保证，而匿名技术[1]则可以隐藏通信方的身份或通信关系，从而更好地保护群组成员利益，解决隐私保护问题。

目前，群组密钥的生成方式大致可以分为群组密钥分配和群组密钥协商两类。群组密钥分配协议存在单点(群组服务器)失陷问题，并且群组服务器需要比较强大的运算能力支持群组密钥的计算及更新。群组密钥协商协议是贡献式的密钥协商机制，群组会话密钥由群组成员协同运算产生，群组成员计算量和通信开销基本相同，在某些特定网络环境下显得重要且有实际意义。

为了解决密钥协商中用户的隐私保护问题，通常使用匿名的密钥协商方案[2-6]。如文献[2]使用消息认证码函数实现认证，协商过程通过网络服务器与群组成员来完成；文献[3-4]中协商过程由用户和归属网络或者访问网络完成，是非贡献式的密钥协商方案；文献[5]是两个不同群组(会话发起群组和会话

收稿日期： 2009 – 09 – 12；修回日期： 2009 – 12 – 03
基金项目：国家863计划(2007AA01Z429)；国家自然科学基金(60702059,60972078)；甘肃省自然科学基金(2007GS04823)；网络安全与密码技术福建省高校重点实验室开放课题(09A006)
作者简介：冯 涛(1970 –)，男，博士，主要从事可证明安全协议理论、无线和移动网络安全等方面的研究.

响应群组)各自的一个成员实现两成员之间的密钥协商；文献[6]实现了单边匿名，协商的两方中只有一方是匿名的。

文献[7]首次提出了基于身份的匿名群组密钥协商方案。该方案假设存在会话发起者U_1，由其选择参与会话的成员U_2、U_3、…、U_n，并在协商之前为每个成员分配一个假名Nym_i，i=1,2,…n，然后将串($U_1\|U_2\cdots\|U_n\|\mathrm{Nym}_1\|\cdots\|\mathrm{Nym}_n\|\mathrm{SIG}_1$)用列表中每个内成员的公钥加密后发送出去。所有成员收到U_1发送的信息，利用自己的私钥解密密文，解密成功后，根据自己的身份对应找到自己的假名。最后所有解密得到假名的成员利用假名进行群组密钥协商。文献[7]实现了针对群组之外的匿名，对于群组内成员，无法实现匿名，并且一旦敌手获悉任意一条发起者发送给群组成员的消息，则匿名性也将完全丧失，原因在于通过查询身份和假名列表就可以将身份与假名一一对应。

本文借鉴基于身份的环签密[8]思想，提出了一种有效的匿名群组密钥协商方案。方案在协商出安全的会话密钥的同时，实现了群组成员的身份认证，更重要的是，该方案结合环签密的匿名思想实现了对于群组内外不同程度的匿名，保护了用户的隐私。可针对网络节点加入或退出问题，实现群组密钥更新，满足组密钥前向保密与后向保密。本文方案仅通过一轮交互就能确定会话密钥，降低了计算复杂性和存储开销。

1 背景知识

定义 1 双线性Diffie-Hellman(BDH)问题：设P为G_1的一个生成元，已知$(P,aP,bP,cP)\in G_1$，其中$a,b,c\in Z_q^*$，来计算$e(P,P)^{abc}\in G_2$。

定义 2 BDH假设：不存在一种算法能够在期望的多项式时间内以不可忽略的概率解决(G_1,G_2,e)中的BDH问题。

2 匿名群组密钥协商方案

2.1 主要参数选择

Setup：给定一个安全参数k，PKG选择阶为q的加法群G_1和乘法群G_2，以及G_1的一个生成元P、一个双线性映射[9]$e:G_1\times G_1\to G_2$，还有3个密码学哈希函数H、H_1和H_2。其中$H:\{0,1\}^*\to G_1$，$H_1:\{0,1\}^*\to Z_q^*$，$H_2:\{0,1\}^*\to G_2$。$(E_k(\cdot),D_k(\cdot))$是一对安全的公钥加解密算法。PKG随机选择$x\in_R Z_q^*$并且保存它作为系统私钥，计算对应的系统公钥$P_{\mathrm{pub}}=xP$，得到系统参数为$\{G_1,G_2,e,q,P,P_{\mathrm{pub}},H,H_1,H_2\}$。

Extract：PKG根据用户身份ID计算用户的公私钥对$Q_{\mathrm{ID}}=H(\mathrm{ID})\in G_1$和$S_{\mathrm{ID}}=xQ_{\mathrm{ID}}$，并通过一个安全信道将私钥安全地发送给用户。

2.2 匿名群组密钥协商协议

存在会话发起者，不妨假设为A_1想要与一组用户$A=\{A_1,A_2,\cdots,A_n\}$协商一个会话密钥，他们的身份集合为$l=(\mathrm{ID}_1\|\mathrm{ID}_2\|\cdots\|\mathrm{ID}_n)$。$A_1$分别使用列表内成员的公钥$Q_i$，$i=1,2,\cdots,n$，将身份列表加密$L_i=E_{Q_i}(l)$得到并广播$\bigcup_{i=1}^{n}\{L_i\}$。

收到该消息，成员使用自己的私钥对$\bigcup_{i=1}^{n}\{L_i\}$进行解密，查看自己是否是被选择要协商密钥的成员，假设有A_j成功解密密文L_j，并且在列表里找到ID_j(即$\mathrm{ID}_j\in l$)。列表中所有在列成员的操作如下：

不失一般性，设成员A_j选择消息m_j如下操作：

1) 分别使用列表内成员的公钥Q_i，$i=1,2,\cdots,n$，对要发送的消息m_j，身份列表加密$M_i=E_{Q_i}(m_j\|l)$得到$\bigcup_{i=1}^{n}\{M_i\}$；

2) 随机选择$U_{i\in R}G_1\forall i\in\{1,2,\cdots,n\}\setminus\{j\}$，计算$h_i=H_1(U_i\|m_j\|l)$；随机选择$r'_{j\in R}Z_q^*$，计算$U_j=r'_jQ_j-\sum_{i\neq j}\{U_i+h_iQ_i\}$，$h_j=H_1(H_j\|m_j\|l)$；

3) 广播$\left\{\bigcup_{i=1}^{n}\{U_i\}\right\},\left\{\bigcup_{i=1}^{n}\{M_i\}\right\}$，不失一般性，假设群组成员$A_b$(即$\mathrm{ID}_b\in l$)收到来自于$A_j$的消息；

4) 使用自己的私钥S_b，从$\bigcup_{i=1}^{n}\{M_1\}$中解密得到$m_j\|l=D_{S_b}(M_b)$；

5) 计算$h_i=H_1(U_i\|m_j\|l)\forall i\in\{1,2,\cdots,n\}$；

同理，也可以接收来自A_f($\mathrm{ID}_f\in l$)的消息$\left\{\bigcup_{i=1}^{n}\{V_i\}\right\},\left\{\bigcup_{i=1}^{n}\{M_i\}\right\}$，并解密得到$m_f\|l=D_{S_b}(M_b)$，计算$o_i=H_1(V_i\|m_f\|l)\forall i\in\{1,2,\cdots,n\}$。

当A_b收到来自其他所有成员的n–1个消息时，计算会话密钥:

$$K=H_2(e((r'_b+x_b)S_b,\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i)))$$

2.3 节点加入事件的群组密钥更新协议

设节点 A_k ($\mathrm{ID}_k \notin l$)加入群组，所有成员更新身份列表为 $l'=\{\mathrm{ID}_1\|\mathrm{ID}_2\|\cdots\|\mathrm{ID}_n\|\mathrm{ID}_k\}$，将串 $\left\{\sum_{i=1}^{n}(W_i+x_iQ_i)\left\|\sum_{i=1}^{n}(U_i+h_iQ_i)\right\|\cdots\left\|\sum_{i=1}^{n}(V_i+o_iQ_i)\right\|l'\right\}$ 使用 A_k 的公钥 Q_k 加密后发送给 A_k，A_k 收到n个 $M=E_{Q_k}\left\{\sum_{i=1}^{n}(W_i+x_iQ_i)\left\|\sum_{i=1}^{n}(U_i+h_iQ_i)\right\|\cdots\left\|\sum_{i=1}^{n}(V_i+o_iQ_i)\right\|l\right\}$ 并检验是否相同，若相同，则 A_k 重复上述协商过程1)～3)。计算新密钥：

$$K'=H_2(e((r_k'+k_k)S_k,\sum_{i=1}^{n}(W_i+x_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i)))$$

同理其他成员收到 $\left\{\bigcup_{i=1}^{n}Y_i\right\},\left\{\bigcup_{i=1}^{n}M_i\right\}$，依据上述密钥计算过程计算新的会话密钥 K'，密钥更新成功。

2.4 节点离开事件的群组密钥更新协议

设群组成员 $A_b=\mathrm{ID}_b(1\leqslant b\leqslant n)$ 离开群组，所有群组成员更新身份列表为 $l'=\{\mathrm{ID}_1\|\mathrm{ID}_2\|\cdots\|\mathrm{ID}_n\,(b\notin\{1,2,\cdots,n\})\}$，剩余群组成员组成新群组，新群组中的任意成员假定为A_j，$\mathrm{ID}_j(1\leqslant j\leqslant n)$处于不繁忙状态，重复协商过程中1)～3)步，发送 $\left\{\bigcup_{i=1}^{n}\{U_i'\}\right\},\left\{\bigcup_{i=1}^{n}\{M_i'\}\right\}$ 给剩余成员，成员依据上述密钥计算过程计算新密钥，密钥更新成功。

3 安全性定义与分析

3.1 方案安全性定义

文献[10]提出了一种形式化分析密钥协商协议模型(简记为CK模型)，采用了不可区分性的方法[11]定义安全。根据CK模型，对群组密钥协商协议敌手攻击能力以及协议的安全属性进行定义。

定义 3 敌手攻击能力：假设敌手μ知道协议的运行过程，以及群组内的所有公开信息(比如公钥信息等)，敌手μ能够截获并读取组成员之间的消息，也可以伪造消息，但是μ不能控制组成员，也不能读取他们的秘密信息(比如私钥信息等)。

定义 4 匿名群组密钥协商协议的安全属性：如果满足下面3个条件，则协议是安全的。

1) 正确性：如果未被攻陷的参与者完成了匹配的会话，它们将输出相同的会话密钥。

2) 不可区分性：对于所有的概率多项式时间敌手μ，其优势可以忽略，特别是在1-out-of-n认证性中，对于不了解参与者私钥的敌手想要获知新鲜会话密钥的优势是可以忽略的。

3) 匿名性：对于群组外敌手猜出参与协商密钥成员组成的概率可以忽略，对于任意敌手猜出消息发送者真实身份的概率不超过1/n，n为参与协议的总人数。

3.2 方案安全性分析

协商协议正确性、不可区分性和匿名性分别由定理1、定理2和定理3保证。

定理 1 协商协议满足正确性。

证明

$$K=H_2(e((r_b'+x_b)S_b,\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i)))=H_2(e((r_b'+x_b)Q_b,\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i))^s)=$$

$$H_2(e((r_b'Q_b+x_bQ_b),\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i))^s)=$$

$$H_2(e(U_b+\sum_{i=1,i\neq b}^{n}(W_i+x_iQ_b)+x_bQ_b,\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i))^s)=$$

$$H_2(e(\sum_{i=1}^{n}(W_i+x_iQ_i),\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i))^s)$$

在公钥加密体制安全的假设下，密钥协商过程中，所有参与方都未被攻陷且完成了协议的执行，那么它们就能够得到相同的会话密钥。所以该协议满足了定义4的第一个要求，即实现了方案正确性。

定理 2 在BDH假设下，协商协议可以实现不可区分性。

证明：用反证法证明。该协议满足定义4的第2个条件。假设敌手μ在概率多项式时间内能够以一个不可忽略的优势ε区分会话密钥K和一个随机数，那么μ一定能够以一个不可忽略的概率计算会话密钥K。这是因为μ如果不能够以一个不可忽略的概率计算会话密钥，则μ不能够在概率多项式时间内区分会话密钥与随机数。因为：

$$K=H_2(e((r_b'+x_b)S_{A_b},\sum_{i=1}^{n}(U_i+h_iQ_{A_i}),\cdots,$$

$$\sum_{i=1}^{n}(V_i+o_iQ_{A_i})))\tag{1}$$

$$K=H_2(e(\sum_{i=1}^{n}(W_i+x_iQ_i),\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i))^s)\tag{2}$$

根据式(1)计算会话密钥意味着需要攻陷计算者A_b，了解其选择的随机数r_b'和私钥S_{A_b}，这与敌手攻击能力定义中敌手μ不能控制群组成员，也不能读取他们的秘密信息的假设相矛盾。

根据式(2)计算会话密钥意味着敌手μ在已知$\left\{\sum_{i=1}^{n}(W_i+x_iQ_i),\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i)\right\}$而系统私钥$s$未知的情况下计算$e\left(\sum_{i=1}^{n}(W_i+x_iQ_i),\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i)\right)^s$，这与BDH假设矛盾。

因此敌手μ无法以一个不可忽略的概率来区分会话密钥与一个随机数。所以协议实现了不可区分性，满足定义4中的第2个条件。

定理 3 协议可以提供1-out-of-n无条件匿名。

证明：首先，分析协商过程，会话发起者A_1使用列表内成员的公钥Q_i，i=1,2,⋯,n，将身份列表加密$L_i=E_{Q_i}(l)$得到并广播$\bigcup_{i=1}^{n}\{L_i\}$。在公钥加密体制安全的假设下，群组外无法获知有哪些参与者参加会话这样的信息，也就是说协议对于群组外实现了完全匿名。

其次，分析成员信息发送过程，每个成员所发送的信息均为$\left\{\bigcup_{i=1}^{n}\{U_i\}\right\},\left\{\bigcup_{i=1}^{n}\{M_i\}\right\}$，信息包含以下两部分：

1) $\bigcup_{i=1}^{n}\{U_i\}$中$U_{i\in R}G_1$是发送者随机选择的，每个U_i均匀地分布在G_1上，$r_j'\in_R Z_q^*$也是在Z_q^*上随机选择的，所以均不包含身份信息；

2) $\bigcup_{i=1}^{n}\{M_i\}$是对同一消息经过n次加密后得到的n个消息，加密密钥是群组内每个成员的公钥，加密之前的消息和加密使用的密钥均不包含身份信息，不具备特殊性。

因此，任何接收者都无法从得到的消息中获取消息发送者身份的相关信息，从而实现1-out-of-n无条件匿名，满足定义4中的第3个条件。

综上所述，根据定义4，该协议实现了匿名群组密钥协商协议的安全属性定义，因此是安全的、匿名的。

定理 4 密钥更新协议满足后向保密性。

证明：节点A_k($\mathrm{ID}_k\notin l$)加入群组，所有列表成员更新身份列表为$l'=\{\mathrm{ID}_1\|\mathrm{ID}_2\|\cdots\|\mathrm{ID}_n\|\mathrm{ID}_k\}$，原群组成员都使用$A_k$的公钥$Q_k$加密并发送消息$M=E_{Q_k}\left\{\sum_{i=1}^{n}(W_i+x_iQ_i)\left\|\sum_{i=1}^{n}(U_i+h_iQ_i)\right\|\cdots\left\|\sum_{i=1}^{n}(V_i+o_iQ_i)\right\|l\right\}$给$A_k$，$A_k$收到$n$个发送来的消息用自己的私钥$S_k$解密后检验是否相同，若$n$个消息都相同，则进行保存。

通过$\sum_{i=1}^{n}(W_i+x_iQ_i)\left\|\sum_{i=1}^{n}(U_i+h_ih_iQ_i)\right\|\cdots\left\|\sum_{i=1}^{n}(V_i+o_iQ_i)\right\|l'$，$A_k$无法在概率多项式时间内区分会话密钥与一个随机数。如果A_k可以在概率多项式时间内区分会话密钥与一个随机数，则意味着A_k可以在概率多项式时间内计算原会话密钥，即在已知$\left\{(\sum_{i=1}^{n}(W_i+x_iQ_i),\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i)\right\}$而未知系统私钥$s$的情况下计算$e(\sum_{i=1}^{n}(W_i+x_iQ_i),\sum_{i=1}^{n}(U_i+h_iQ_i),\cdots,\sum_{i=1}^{n}(V_i+o_iQ_i))^s$，这与BDH假设相矛盾。

之后A_k重复上述协商过程1)～3)，计算新鲜会话密钥。新的群组可以得到新的会话密钥，实现了成员加入后群组密钥的更新，保证了协议的后向保密性。该过程与最初协商密钥的过程相同，此处不再赘述。

定理 5 密钥更新协议满足前向保密性。

证明：群组成员A_b，ID_b($1\leqslant b\leqslant n$)离开，所有成员更新身份列表为$l'=\{\mathrm{ID}_1\|\mathrm{ID}_2\|\cdots\|\mathrm{ID}_n$ $(b\notin\{1,2,\cdots,n\})\}$，剩余群组成员组成新群组。新群组中的任意成员假定为A_j，ID_j($1\leqslant j\leqslant n$)处于不繁忙状态，重复协商过程中1)～3)步骤。A_j发送$\left\{\bigcup_{i=1}^{n}\{U_i'\},\bigcup_{i=1}^{n}\{M_i'\},\right\}$给剩余成员，因为新的身份列表中不存在$\mathrm{ID}_b$，所以信息列表中也不存在$M_b$这一项。即使$A_b$接收到所发送信息，在公钥加密体制安全假设下也不能解密密文，因此也就无法得到m_j'，进而

也就无法继续计算新的会话密钥。之后剩余成员依据上述密钥计算过程，计算新的群组密钥，实现成员离开后群组密钥的更新，保证了协议的前向保密性。

4 性能分析与比较

本文主要通过通信开销、计算量和存储开销等将本文方案与文献[7]中的方案进行比较，如表1所示。本文方案在群组规模增大时，通信开销、计算量和存储开销都有很大的改进。

表1 本文方案与相关方案的比较

方案	通信			对运算	存储
	轮数	单播	组播		
文献[7]方案	3	$3n$	n	$2n$	$n+2$
本文方案	1	$n-1$	n	n	n

其中，轮数表示确定会话密钥所需的通信轮数；单播表示通信中总的单播次数；组播表示通信中总的组播次数；对运算表示确定会话密钥总的对运算；存储表示每个成员需要存储的消息条数；n为组成员数。

文献[7]使用假名实现了针对群组之外的匿名，即群组之外无法获悉参与者身份，对于群组内成员，则无匿名可言；并且一旦敌手获悉任意一条发起者发送给群组成员的消息，则匿名性也将完全丧失。

本文方案避免了假名概念，发起者发送给群组成员的只有身份列表。在公钥加密体制安全的假设下，实现了对于群组之外的完全匿名；对于群组内成员来说，也仅能了解参与成员的组成，无法将参与者行为与具体成员身份对应起来。组内窃听者无法对用户的信息进行跟踪，也无法了解用户的行为或通信对象，从而避免了许多潜藏的不安全因素。另外，即使敌手截获发起者发送的成员列表，获悉参与成员的组成，也无法跟踪成员行为和窃听成员隐私。与文献[7]比较，本文方案的匿名性增强。

5 结 束 语

本文分析了现有的基于身份的群组密钥协商方案后，发现绝大多数方案没有实现对用户的隐私保护。针对该问题，提出了一种有效的基于身份的匿名群组密钥协商方案，不仅延续了基于身份密码系统的优点，而且仅需一轮交互就能协商出安全有效的群组会话密钥。方案强调成员身份的公平性，具有计算量、存储开销和通信开销小，以及安全性和效率较高的特点。更重要的是，方案还实现了对群组内外不同程度的匿名，保护了群组成员隐私。匿名群组密钥协商协议将在更多需要用户隐私保护的群组内应用，在协同工作、电话会议、多媒体远程教育等领域中发挥重要作用。

本文的研究工作得到兰州理工大学博士基金(BS14200901)的资助，在此表示感谢。

参 考 文 献

[1] MICHAEL K R, AVIEL D R. Crowds: anonymity for web transactions[J]. ACM Transactions on Information and System Security (TISSEC), 1998, 1(1): 66-92.

[2] 万仁福, 李方伟, 朱江. 匿名双向认证与密钥协商新协议[J]. 电子科技大学学报, 2005, 34(1): 61-64.
WAN Ren-fu, LI Fang-wei, ZHU Jiang. An efficient anonymity mutual authentication protocol[J]. Journal of University of Electronic Science and Technology of China, 2005, 34(1): 61-64.

[3] 冯国柱, 李超, 吴翊. 一个高效的无线匿名认证和密钥协商协议[J]. 计算机工程与应用, 2006, 42(19): 3-7.
FENG Guo-zhu, LI Chao, WU Yi. An efficient anonymous authentication and key agreement protocol[J]. Computer Engineering and Application, 2006, 42(19): 3-7.

[4] 邓所云, 胡正名, 钮心忻, 等. 一个无线双向认证和密钥协商协议[J]. 电子学报, 2003, 31(1): 135-138.
DENG Suo-yun, HU Zheng-ming, NIU Xin-xin, et al. A wireless mutual authentication and key agreement protocol[J]. Acta Electronica Sinica, 2003, 31(1): 135-138.

[5] SHERMAN S M. Chow and kim-kwang raymond choo, strongly-secure identity-based key agreement and anonymous extension[C]//ISC 2007, LNCS 4779. Berlin: Springer-Verlag, 2007: 203-220.

[6] CHENG Z, CHEN L, COMLEY R, et al. Identity-based key agreement with unilateral identity privacy using pairings [C]//ISPEC 2006, LNCS 3903. Berlin: Springer-Verlag, 2006: 202-213.

[7] WAN Zhi-guo, REN Kui, LOU Wen-jing, et al. Anonymous ID-based group key agreement for wireless networks[C]//Wireless Communications and Networking Conference. [S.l]: IEEE, 2008: 2615-2620.

[8] LI Fa-gen, SHIRASE M, TAKAGI T. Analysis and improvement of authenticatable ring signcryption scheme[J]. Journal of Shanghai Jiaotong University: Science, 2008, 13(6): 679-683.

[9] 李兴华, 马建峰, 文相在. 基于身份密码系统下Canetti-Krawczyk模型的安全扩展[J]. 中国科学(E辑): 信息科学, 2004, 34(10): 1185-1192.
LI Xing-hua, MA Jian-feng, WEN Xiang-zai. Security extension for the canetti-krawczyk model in identity-based systems[J]. Science in China, (Series E), 2004, 34(10): 1185-1192.

[10] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]// Eurocrypt 2001, LNCS 2045. Berlin: Springer-Verlag, 2001: 453-474.

[11] GOLDWASSER S, MICALI S. Probabilistic encryption[J]. JCSS, 1984, 28(2): 270-299.

编 辑 蒋 晓