一种基于双线性配对的移动自组网密钥协商协议*)

黄清元　王勇军　苏金树
(国防科学技术大学计算机学院　长沙 410073)

摘　要　移动自组网是一种无固定网络基础设施、能量和计算资源有限的分布式动态网络，由于其无线传输链路的开放性，使得它非常需要一种计算和通信开销较小的密钥协商方案。本文基于椭圆曲线上双线性配对的概念，提出了一种适用于移动自组网的可认证密钥协商方案，既实现了邻居节点组成员身份认证的匿名性，也实现了需建立会话的节点之间的可认证密钥协商。分析表明，我们所提出的方案计算和通信开销比较小，安全性较好，非常适合于资源有限的移动自组网。

关键词　双线性配对，密钥协商，移动自组网

A Bilinear Pairing-based Key Agreement Protocol in MANET

HUANG Qing-Yuan　WANG Yong-Jun　SU Jin-Shu
(School of Computer, National University of Defense Technology, Changsha 410073)

Abstract　As a new type of dynamic infrastructure-less networks, mobile Ad Hoc networks are vulnerable to many types of attacks. So the key agreement protocol with mutual authentication between communicators is crucial for the security of MANETs. A key agreement scheme with mutual authentication, which is based on bilinear pairing, is proposed in this paper. This scheme implements two key agreement protocols. One is for the anonymous group member authentication among neighbors. The other is for the session key agreement with mutual authentication. The security and computation cost are analyzed. The results show that the scheme proposed in this paper is very suitable for MANETs.

Keywords　Bilinear pairing, Key agreement, MANET

1　引言

移动自组网是一种无中心的、节点任意移动的网络，这些节点同时具备路由和主机的功能，它们相互协作，通过无线连接构成任意的网络拓扑。由于移动自组网的独特性，如缺乏固定的网络基础设施、节点的移动而导致网络拓扑变化频繁、无线信道的传输范围有限且不可靠、电源和计算能力有限等，使得移动自组网的安全问题显得尤为突出。如何在移动自组网中进行密钥管理和协商，从而对节点身份进行鉴定，并保证数据传输的机密性和完整性，已经成为研究的热点。

近年来，国内外学者已就无线网络的密钥管理和协商机制进行了大量的研究，如文[1～4]等。这些方案主要可以分为两类：一类是采用对称密码体制，如文[1]，但这种体制需要通信双方共享一个长期密钥，或者是存在可信第三方，这对于不存在网络基础设施且动态变化的移动自组网不是很适合。并且，随着网络规模的扩大，密钥管理和可扩展性就成为主要问题。另一类是采用非对称密码学体制。但是，传统基于证书的非对称密码体制的通信、计算和存储开销都非常大，不适合于移动自组网，采用基于阈值密码学的分布式 CA，如 TS-RSA[2]和 TS-DSA[3]，则需要进行大量的交互，效率太低[4]。当前更多的研究集中在将椭圆曲线密码学应用到无线网络设备中[5～10]，由于其密钥长度短、数字签名快、计算数据量小，使得它特别适合于计算资源和存储资源受限的设备。

本文在研究以往移动自组网密钥协商协议的基础上，综合考虑了移动自组网的特点，利用椭圆曲线群上的双线性配对，提出了一种带认证的密钥协商方案。该方案采用匿名的方法来实现邻居节点之间的组成员身份鉴定，只需要一轮交互即可在两个远程通信实体之间建立会话密钥。

2　双线性配对及相关假设

2.1　双线性配对的概念

双线性配对[5]指的是两个循环群之间相对应的线性映射关系。由于椭圆曲线上所有的点形成的集合，在代数几何学上会形成群的关系，因此双线性配对函数的运算正好能应用于椭圆曲线上。其相关参数与符号如：G_1 是一阶数为大质数 q 且生成元为 P 的循环加法群，G_2 则为一阶数同样为大质数 q 的循环乘法群。分别在 G_1 和 G_2 中求解离散对数问题，都是相当困难的。双线性配对函数表示方式为 $\hat{e}:G_1\times G_1\rightarrow G_2$ 且对于 $\forall P,Q\in G_1$ 与 $\forall a,b\in Z_q^*$ 满足下列特性：

- 双线性(Bilinearity)

$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$

$\hat{e}(P_1+P_2,Q)=\hat{e}(P_1,Q)\hat{e}(P_2,Q)$

$\hat{e}(P,Q_1+Q_2)=\hat{e}(P,Q_1)\hat{e}(P,Q_2)$

- 非退化性(Non-degeneracy)

*)本文得到国家自然科学基金项目(No. 90604006)、国家教育部博士点基金(No. 20049998027)资助。**黄清元**　博士研究生，主要研究领域为网络处理器技术与网络安全技术；**王勇军**　副教授，硕士生导师，研究方向为计算机网络通信、信息安全技术；**苏金树**　教授，博士生导师，研究方向为计算机网络通信、信息安全技术。

若 P 是 G_1 的生成元，则 $\hat{e}(P,P)$ 也会是 G_2 的生成元，即 $\hat{e}(P,P)\neq 1$。

· 可计算性(Computability)

对于 $\forall P,Q\in G_1$ 而言，恒有一有效率的算法可在多项式时间内计算 $\hat{e}(P,Q)$。

2.2 安全假设

在密码学的研究领域里，为了符合系统安全的需求，通常会有许多计算难题的假设，并且在安全假设上，要在多项式时间内求解这些问题的机率是可以忽略的。以下针对本文中所要用的数学难题做详细的定义和说明。

· 双线性 Diffie-Hellman 问题(BDHP)

令 $a,b,c\in Z_q^*$ 为未知数，给定 $P,aP,bP,cP\in G_1$，要求 abc 得且满足 $\hat{e}(P,P)^{abc}\in G_2$。

· 双线性 Diffie-Hellman 决定问题(DBDHP)

令 $a,b,c\in Z_q^*$ 为未知数，给定 $P,aP,bP,cP\in G_1$，要决定 $c=ab \bmod q$ 且满足 $\hat{e}(P,P)^c=\hat{e}(P,P)^{ab}\in G_2$。

· GDH 群[6](Gap Diffie-Hellman Group)

存在一种算法，可以在多项式时间内求解 DBDHP 问题；不存在一种算法，在多项式时间内求解 BDHP 问题。这样的群称为 GDH 群。本文我们所使用到的群 G_1 和 G_2 都是 GDH 群。

2.3 安全属性

一般在设计密钥协商协议时，系统必须符合下面五大安全特性。为不失一般性，我们假设 A 和 B 为欲建立秘密通讯的两个成员。

1)已知密钥安全

在这里所谓的密钥指的是共享的会话密钥。已知密钥安全是指当某一次的会话密钥不小心泄漏了，其它次所产生的会话密钥并不会因此而跟着泄漏。已知密钥安全主要是将会话密钥泄漏所产生的安全危害局限在当次的秘密通讯过程内。

2)前向安全

前向安全是指：即使一个或多个使用者生命周期较长的秘密密钥(long-term private key)不小心泄漏了，在此秘密密钥泄漏之前所产生的会话密钥也不会因此而连带泄漏。前向安全主要是对于过去被加密的数据提供完善的机密性保护。若在所有的使用者的秘密密钥全部都泄漏的情形下，系统对于过去所有已被加密的数据尚具有保护作用，也就是无法因为此泄漏情况而推导出先前所产生的会话密钥，我们称此为完美前向安全。

3)密钥泄露模仿

密钥泄漏模仿是指：当 A 的秘密密钥不小心泄漏给了攻击者。在攻击者握有此秘密密钥的情形之下，攻击者只能模仿自己是 A 来欺骗其它人，并无法模仿其它成员欺骗 A。

4)未知密钥分享

在密钥协商协议中，任何人皆不能在 A 不知情的状况下，强迫与 A 分享一把共同会话密钥。而未知密钥分享则是指：当完成密钥协商协议后，A 相信自己与 B 共同分享一会话密钥，但 B 却认为自己是和另一攻击者建立一会话密钥。最后造成在 A 不知情的状况下与攻击者也分享了此共同会话密钥。因此，一个健全的密钥协商协议必须能够抵挡这类型的攻击。

5)密钥控制/支配

密钥控制安全指的是，任何一次的会话密钥建立过程中，会话密钥的产生方式必须由 A 和 B 共同合作建立。密钥控制安全主要是保护会话密钥的产生方式不能为单独一方所决定，以达到安全及公平的原则。

3 密钥协商协议

3.1 方案

本节介绍我们所提出的基于双线性配对计算的移动自组网密钥协商方案。事实上，在移动自组网中，有些节点的身份是需要保密的，并且移动的节点没必要向所有其经过的邻居节点暴露其身份信息，它只需要向其经过的邻居节点证明其组成员身份，然后获取网络的使用权限即可。因此，不同于其它的移动自组网密钥协商方案，我们所提出的方法区分移动自组网中两种不同类型的通信：中继通信和会话通信。所谓中继通信是指由于需要对数据报进行中继转发而引发的两个节点之间的通信，这样的通信通常发生在邻居节点之间，如某一节点请求其邻居节点转发由其它节点发送的数据包。会话通信是指两个节点之间需要完成一次完整的会话所引发的通信，如交换相互的位置信息等。因此，我们也根据这两种不同的通信来协商密钥。

(1)系统初始设置

G_1 是上一节中定义的 q 阶循环加法群，G_2 是上一节定义的 q 阶循环乘法群，$\hat{e}:G_1\times G_1\rightarrow G_2$ 为一双线性配对函数，P 为 G_1 的生成元，系统主密钥 $s\in Z_q^*$ 是密钥产生中心(KGC)的私钥，$P_{pub}=sP$ 是密钥产生中心的公钥，$H_1:\{0,1\}^*\rightarrow G_1$ 是一个单向抗碰撞函数，将任意长度的字符串映射到群 G_1 上的点。$H_2:\{0,1\}^*\rightarrow(0,1)^l$ 是一个单向抗碰撞散列化函数，如 SHA-1，将任意长度的字符串映射到固定长度为 l 位的字符串。公开。

$\langle G_1,G_2,P_{pub},q,\hat{e},H_1,H_2\rangle$

(2)节点密钥提取

每个节点离线向密钥产生中心申请一个私钥/公钥对，密钥产生中心为节点产生的私钥为 $S=sQ$，其中 $Q=H_1(ID)\in G_1$ 是该节点的公钥，ID 是节点的身份标识。由于离散对数求解的困难性，因此给定公钥 Q 和私钥 S，攻击者不能由此而求得系统主密钥 s。假设密钥产生中心为节点 A 和 B 所产生的私钥分别为：$S_A=sQ_A$，其中 $Q_A=H_1$(A 的 ID)；$S_B=sQ_B$，其中 $Q_B=H_1$(B 的 ID)。为了简化表示，以后我们将使用 ID_i 来表示节点 i 的身份标识。为了实现邻居节点之间的匿名组身份验证，密钥产生中心还需要为每个节点提供足够多的笔名 PS，以及与笔名相对应的私钥 $S_{PS}=sH_1(PS)$。除了密钥产生中心，没有节点能够获得该节点的笔名及其真实身份之间的关系。

(3)会话密钥协商

如上面所述，我们区分两种不同类型的通信：中继通信和会话通信。因此，采用两种不同的密钥协商方案，邻居节点之间的匿名密钥协商以及根据上述双线性配对的概念的基于身份的密钥协商。

· 邻居节点之间的匿名密钥协商

在移动自组网中，并不是所有的节点都需要向其邻居节点暴露其身份信息。事实上，大部分的邻居节点认证只是为了获取使用网络的权限，即可以请求邻居节点为其转发数据报文，只有两个真正交换信息的节点之间才需要相互披露真实身份。两个邻居节点 A 和 B 之间的匿名邻居密钥协商过程可以表示如下：

Protocol 1

1)A 从自己的笔名集中随机选取一个笔名 PS_A，以及随机数 a 发送给 B。

2)B 从自己的笔名集中随机选取一个笔名 PS_B，并产生一个随机数 b，计算 $K_{BA}=\hat{e}(H_1(PS_A),sH_1(PS_B))$，然后计算 A 与 B 之间的会话密钥 $K_{S_{AB}}=H_2(K_{BA}\oplus a\oplus b)$，将 PS_B、b 发送给 A。

3)A 计算 $K_{AB}=\hat{e}(sH_1(PS_A),H_1(PS_B))$，然后计算会话密钥 $K_{S_{AB}}=H_2(K_{AB}\oplus a\oplus b)$。

只有当节点 A 和 B 属于同一组的时候，下面的等式才成立：

$$\begin{aligned}K_{BA}&=\hat{e}(H_1(PS_A),sH_1(PS_B))\\&=\hat{e}(H_1(PS_A),H_1(PS_B))^s\\&=\hat{e}(sH_1(PS_A),H_1(PS_B))=K_{AB}\end{aligned}\quad(1)$$

可以看出，每个节点只需要进行一次双线性配对计算、两次 hash 计算，以及一轮通信，就可以完成组成员身份的鉴定。并且，只要在节点初始设置时，密钥产生中心为其产生足够多的笔名和相应的私钥，那么就不用担心节点身份暴露问题。该密钥协商过程只能用于仅需要获取网络使用权限的邻居节点之间。由于该协议不能阻挡中间人攻击，因此需要发起一次完整会话的节点之间，仍然要进行基于身份的密钥协商。

· 基于身份的密钥协商

基于身份的密钥协商不需要可信第三方的参与，我们对文[8]的协议进行改进，使其更安全并适用于移动自组网。两个需要发起一次完整会话的节点 A 和节点 B，需要相互披露彼此的身份信息。节点 A 和 B 首先产生分别产生一个临时密钥 $a,b\in Z_q^*$，然后计算相对应的临时公钥，$T_A=aQ_A$ 和 $T_B=bQ_B$，其中 $Q_A=H_1(ID_A)$，$Q_B=H_1(ID_B)$。其密钥协商的过程可以表示如下：

Protocol 2

1)节点 A 计算 T_A 和 aP_{pub}，然后将它们发送给节点 B。

2)节点 B 计算 T_B 和 bP_{pub}，将它们发送给节点 A，然后计算 $K_{BA}=\hat{e}(T_A+bQ_A,S_B)$，以及会话密钥 $K_{S_{AB}}=H_2(K_{BA}\oplus baP_{pub})$。

3)节点 A 在收到 B 的消息后，计算 $K_{AB}=\hat{e}(S_A,aQ_B+T_B)$，以及会话密钥 $K_{S_{AB}}=H_2(K_{AB}\oplus abP_{pub})$。

当节点 A 和 B 由同一密钥产生中心产生的公钥/私钥时，那么下面的等式成立：

$$\begin{aligned}K_{AB}=\hat{e}(S_A,aQ_B+T_B)&=\hat{e}(sQ_A,aQ_B+bQ_B)\\&=\hat{e}((a+b)Q_A,sQ_B)\\&=\hat{e}(T_A+bQ_A,S_B)=K_{BA}\end{aligned}\quad(2)$$

在上述协议中，每个节点需要进行三次点乘计算、一次双线性配对计算、一次 hash 运算，以及一轮通信即可在两个节点之间协商一个会话密钥。

3.2 方案分析

3.2.1 安全性

Protocol 1 的作用是对邻居节点的组成员身份进行鉴定。也就是说，它只需要能够抵挡来自外部的攻击即可。因此，它的安全性比较低，它满足已知密钥安全和密钥支配安全，不能抵挡来自网络内部的中间人攻击，因此不满足前向安全、密钥泄漏模仿安全以及未知密钥共享安全。下面我们就 Protocol 2 的安全属性进行详细分析。

结论 1(已知密钥安全) Protocol 2 满足已知密钥安全。

在 Protocol 2 中，任何一次会话密钥的产生皆依赖于 K_{AB}，假设攻击者能够以流量监测的方式获取密钥协商中交互的所有信息。要从会话密钥 $K_{S_{AB}}=H_2(K_{AB}\oplus abP_{pub})$ 中破解 K_{AB}，将面临破解单向抗碰撞散列函数 H_2 的难题。因此，丢失当前的会话密钥，影响范围仅限于该次通信。

结论 2(完美前向安全) Protocol 2 是完美前向安全。

在 Protocol 2 中，会话密钥的产生不仅依赖于 K_{AB}，同时依赖于节点 A 和节点 B 所产生的短暂秘密参数 a 和 b。因此，在 A 和 B 节点之间的信息交互中，即使攻击者得到了 K_{AB}，那么在依据 aP 和 bP 获得节点 A 和 B 的临时短暂秘密参数时，仍然面临求解 Diffie-Hellman 计算问题的困难。因此，Protocol 2 满足完美前向安全。

结论 3(密钥泄漏模仿安全) Protocol 2 是密钥泄漏模仿安全的。

在协议 Protocol 2 中，假设节点 A 的密钥 S_A 不小心泄漏给攻击者 E 知道了，E 试图假冒 B 的身份来欺骗 A。如果由节点 A 发起会话请求，A 应该已经知道 B 的真实身份信息，因此，除非攻击者可以在计算 K_{AB} 中消除 B 的身份 Q_B 的影响，否则就无法计算出相同的会话密钥。但是，根据大整数分解的困难性，攻击者无法根据 aP_{pub} 计算出节点 A 的临时秘密 a，所以攻击者无法模仿 B 同 A 通信。如果由节点 B 发起会话请求，B 知道 A 的身份信息，攻击者假冒 B 时，必须将 B 的身份告诉 A，所面临的问题同由 A 发起请求是相同的。因此，Protocol 2 是密钥泄漏模仿安全的。

结论 4(未知密钥共享安全) Protocol 2 是未知密钥共享安全的。

在 Protocol 2 中，由于节点 A 和节点 B 之间只协商了一个会话密钥，因此，该安全问题等价于中间人攻击。会话密钥的计算取决于 A 的身份、B 的身份，以及节点 A 和 B 的长期私钥以及临时秘密参数。攻击者除非能够同时破解节点 A 和 B 的长期私钥以及临时秘密，否则无法假冒协议参与者 A 或者 B 的身份而与其中一方共享密钥，因此 Protocol 2 是未知密钥共享安全的。

结论 5(密钥支配安全) Protocol 2 是密钥支配安全的。

在 Protocol 2 中，每一次通过密钥协商产生的会话密钥，都是由参与秘密通讯的成员 A 和 B 的长期密钥、临时秘密所共同决定。任何一个成员皆无法事先决定所有参与协议成员的安全参数，更无法独立控制整个密钥协商的过程。因此，Protocol 2 是密钥支配安全的。

3.2.1 复杂性

本文我们提出了两种密钥协商方案：邻居节点的匿名认证方案可以实现邻居节点认证时的匿名性，计算开销比较小；而基于身份的方案计算开销比较高，但是安全性相对也比较高。我们将本文所提出的方案同文[7,8]中的方案进行比较，结果如下：

属性	Ref[7]	Ref[8]	Protocol 1	Protocol 2
通信轮数	1	1	1	1
点乘	2	2	0	3
双线性配对	2	1	1	1
Hash 计算	1	1	2	1

其中双线性配对计算的开销最大，点乘其次，hash 计算的开销则比较小。因此，如果在移动自组网中大量的邻居节点需要相互交换信息，而不是仅仅转发数据报文，那么我们所

(下转第 114 页)

上述分析表明，如果协议应答方 R 已经将商品项($item_R$，r_R，key_R)发送给发起方 O，R 能获得来自 O 的 ($item_O$，key_O，r_O)或证词项 $sig_T(m_1, m_2, y_R)$。

对双方串节点路径的分析表明，当一方已发送商品给另一方后，必能获得其所期望的商品项或来自可信方的证词，没有任何一方较另一方处于优势，即 ASW 协议是弱公平的。

结束语 现有的形式化分析研究多集中在认证协议和密钥交换协议。而电子商务协议具有更为复杂的协议结构，如分支结构，或由多个子协议组成，使得难以使用传统的信念逻辑进行分析。本文对串空间逻辑进行了扩展，使之能分析带密文项的电子商务协议。还提出串节点路径分析法，以利用串空间逻辑分析带复杂结构的协议，从而给出了一种较为通用的电子商务协议形式化分析方法。文中成功地对 ISI 支付协议和 ASW 协议进行串空间分析，形式化地证明了 ISI 协议不满足公平性，而 ASW 协议则满足公平性。基于串空间逻辑的复杂协议自动分析器是我们今后研究的方向。

参 考 文 献

1 Asokan N. Fairness in electronic commerce:[PhD thesis]. University of Waterloo, 1998
2 Dolev A, Yao A C. On the security of public-key protocols. IEEE Transactions on Information Theory, 1983, 2(29): 198～208
3 Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1):18～36
4 Kailar R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, 1996, 22(5): 313～328
5 周典萃，卿斯汉，周展飞. Kailar 逻辑的缺陷. 软件学报，1999，10(12):1238～1245
6 Ryan P, Schneider S. Modelling and analysis of security protocols. Addison-Wesley Publishing Co, 2000
7 Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. Software Concepts and Tools, 1996, 17: 93～102
8 Heintze N, Tygar J D, Wing J, et al. Model checking electronic commerce protocols. In: Proc. 2nd USENIX Workshop on Electronic Commerce, 1996. 147～164
9 卿斯汉. 密码学与计算机网络安全. 北京：清华大学出版社，2000. 127～147
10 卿斯汉. 一种新型的非否认协议. 软件学报，2000，11(10)：1338～1343
11 周典萃，卿斯汉，周展飞. 一种分析电子商务协议的新工具. 软件学报，2001，12(9)：1318～1328
12 白硕，隋立颖，陈庆锋，等. 安全协议的验证逻辑. 软件学报，2000，11(2)：213～221
13 陈庆锋，白硕，王驹，等. 电子商务安全协议及其非单调动态逻辑验证. 软件学报，2000，11(2)：240～250
14 Thayer F J, Herzog J C, Guttman J. Strand spaces: Why is a security protocol correct? In: Proc the 1998 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 1998. 160～171
15 Thayer F J, Herzog J C, Guttman J. Honest ideals on strand space. In: Proc. 11th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 1998
16 Thayer F J, Herzog J C, Guttman J. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999, 7(2-3): 191～230
17 Medvinsky G, Neuman B C. Netcash: a design of practical electronic currency on the Internet. In: Proc. ACM Conf. on Computer and Communication Security. New York: ACM Press, 1993. 76～82
18 Asokan N, Schunter M, Waidner M. Optimistic protocols for fair exchange. In: Proc. 4th ACM Conf. on Computer and Communication Security. ACM Press, 1997. 6～17

(上接第 80 页)

提出的方案计算开销就比较高。反之，如果大量的邻居节点认证只是为了获得网络的使用权限，那么我们的方案就可以取得比较好的效果。

结论 本文在分析以往移动自组网密钥协商协议的基础上，综合移动自组网的实际需要，提出了一种适用于移动自组网的密钥协商方案，减轻了节点的计算和通信开销，同时实现了身份认证的功能。本文所提出的方案比较简单，安全性较好，计算和通信开销小，因此非常适合于移动自组网这种能量和计算资源有限的网络。我们下一步的研究目标是结合匿名认证方案和 MPLS 标签交换的局部性来实现移动自组网的匿名安全路由，并结合信任相关的理论来阻挡来自网络的内部的攻击，实现节点回收的功能。

参 考 文 献

1 Zhu S, Xu S, Setia S, et al. Establishing Pair-wise Keys for SecureCommunication in Ad Hoc Networks: A Probabilistic Approach. In: IEEE ICNP, 2003
2 Kong J, Zerfos P, Luo H, et al. Providing Robust and UbiquitousSecurity Support for MANET. In: IEEE ICNP, 2001
3 Narasimha M, Tsudik G, Yi J H. On the Utility of Distributed Cryptography in P2P and MANETs: The Case of Membership Control. In: IEEE ICNP, 2003
4 Jarecki S, Saxena N, Yi J H. An Attack on the Proactive RSA Signature Scheme in the URSA Ad Hoc Network Access Control Protocol. In: ACM SASN, 2004
5 Joux A. A one-round protocol for tripartite Diffie-Hellman. In Algorithmic Number Theory Symposium -ANTS-IV, Springer-Verlag LNCS1838, 2000. 385～394
6 Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham E, ed. Proc. of the Eurocrypt 2003. LNCS 2656, Warsaw: Springer-Verlag, 2003. 416～432
7 Smart N P. An identity-based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 2002, 38: 630～632
8 Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings. CSFW'03, 2003. 219～236
9 Ertaul L, Lu W M. ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (I). In: Boutaba R, Almeroth K, Puigjaner R, et al. eds. Networking 2005. LCNS 3462, Canada: University of Waterloo, Springer-Verlag GmbH, 2005. 102～113
10 Zhang Y, Liu W, Lou W W. Anonymous Communications in Mobile Ad Hoc Networks. IEEE INFOCOM, 2005

(上接第 86 页)

息，可大大减轻可信第三方的负担。

结束语 本文采用基于身份的密码体制作为基础，提出了一套切实可行、安全高效的邮件安全认证方案，该方案系统开销小，安全级别较高，有效地实现了 Web 方式电子邮件系统中的安全认证问题。系统实际运行结果表明，该认证系统结果正确，运行速度较快，运行状况良好。

参 考 文 献

1 Shamir A. Identity-based cryptosystems and signature schemes [J]. In: Advances in Cryptology-CRYPTO84, Vol. 196 of LNCS, Springer-Verlag, 1984. 47～53
2 Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing [C]. Advance in Cryptology-CRYPTO 2001. LNCS 2139, 2001. 213～229
3 Boneh D, Franklin M. Short Signatures from Weil Pairing [C]. Boyd C ASIACRYPT 2001. Berlin: Springer-Verlag, 2001. 514～532
4 Menezes A, Okamoto T, Vanstone S. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field [J]. IEEE Trans on Information Theory, 1993, 39(5): 1639～1646
5 Hess F. Efficient identity based signature schemes based on pairings [C]. In SAC'02: Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography. Springer-Verlag, 2003. 310～324
6 Hankerson D, Menezes A, Vanstone S. Guide to Elliptic Curve Cryptography [M]. Publishing House of Electronics Industry, 2005, 8: 5～20