一种改进的椭圆曲线安全代理签名方案 *

胡兰兰[a,b,c], 郑康锋[a,b,c], 李 剑[a,b], 胡正名[a,b,c], 杨义先[a,b,c]

(北京邮电大学 a. 网络与交换技术国家重点实验室 信息安全中心; b. 网络与信息攻防技术教育部重点实验室; c. 灾备技术国家工程实验室, 北京 100876)

摘 要: 为解决基于椭圆曲线的代理签名方案的安全问题,提出一种改进的抗伪造攻击的代理签名方案。该方案通过改进代理签名私钥生成方式和相应的代理签名验证等式的方法,提高了基于椭圆曲线的代理签名方案的安全性。分析表明,新方案解决了以往方案中存在的原始签名者伪造问题,满足强代理签名方案所必须的六种性质,具有无须安全通道的优点并且更为高效。分析结果说明,新方案比以往方案具有更好的安全性和更高的实用性。

关键词: 代理签名; 椭圆曲线; 椭圆曲线离散对数问题

中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)02-0685-04

doi:10.3969/j.issn.1001-3695.2010.02.078

Improved secure proxy signature scheme based on elliptic curve

HU Lan-lan[a,b,c], ZHENG Kang-feng[a,b,c], LI Jian[a,b], HU Zheng-ming[a,b,c], YANG Yi-xian[a,b,c]

(*a. Information Security Center, State Key Laboratory of Networking & Switching Technology, b. Key Laboratory of Network & Information Attack & Defence Technology of MOE, c. National Engineering Laboratory for Disaster Backup & Recovery, Beijing University of Posts & Telecommunications, Beijing* 100876, *China*)

Abstract: To overcome the secure weakness of the existing proxy signature scheme based on elliptic curve, this paper presented an improved proxy signature scheme that could avoid forgery attack. Enhanced the security of the proxy signature scheme based on elliptic curve by improving on the generate form of the private key and the corresponding verification equation of proxy signature. The analysis showed that the new scheme resolved secure problems in the former schemes, met the six aspects of security features needed by strong proxy signature scheme, did not need the support of the secure channel, and was more efficient. The analytic results prove that the new scheme is more secure and practicable.

Key words: proxy signature; elliptic curve; elliptic curve discrete logarithm problem (ECDLP)

0 引言

1996 年 Mambo 等人[1]提出了代理签名的概念并给出了一种代理数字签名方案,此后基于离散对数和素因子分解的代理数字签名方案[2,3]纷纷涌现。代理签名是指原始签名者将其签名权(部分)授予代理者,代理者可以代表原始签名者来行使他的签名权。通过对以往代理签名研究的归纳总结,可以认为,一个可被实际应用的典型代理签名方案应是具备以下特性的强代理签名方案[4,5]:

a)可验证性。对于有效的代理签名,验证者能够确信这个签名是原始签名者认可的数字签名,即不但能验证代理签名者生成的代理签名,也能验证原始签名者的授权。

b)强可区分性。由代理签名者所签署的代理签名与原始签名者所产生的签名是有区别的,不同的代理签名者生成的代理签名之间也有明显区别。

c)强不可伪造性。除代理签名者外,任何人(包括原始签名者)都不能生成有效的代理签名。

d)强可鉴别性。对于有效的代理签名,原始签名者和任何验证者都能够确定代理签名者的身份。

e)强不可否认性。代理签名者一旦生成一个有效的代理签名,事后不能否定对这个代理签名的建立。

f)可控性或阻止滥用。原始签名者能够有效控制代理签名者的代理权限,包括代理者的身份、代理有效时间、代理签署消息范围等。代理签名密钥不能用于其他目的。

1 基于椭圆曲线代理签名方案的优越性及相关研究

Koblitz 等人在 1985 年将椭圆曲线群引入公钥密码理论中,提出了基于椭圆曲线的公钥密码体制 ECC(elliptic curves cryptosystem),椭圆曲线公钥密码的安全性主要是建立在基于椭圆曲线离散对数问题(ECDLP)求解的困难性[6,7]。从目前的研究结果看,椭圆曲线上的离散对数问题比有限域上的离散对数问题更加难以处理,具有更高的安全性,还具有密钥短小、

收稿日期: 2009-05-04; **修回日期**: 2009-06-15 **基金项目**: 国家"973"计划资助项目(2007CB310704); 国家自然科学基金资助项目(90718001,60821001,U0835001)

作者简介:胡兰兰(1979-),女(回族),河南开封人,博士后,主要研究方向为信息安全、网络安全和电子商务(hulanlan@126.com);郑康锋(1975-),男,山东莒县人,讲师,博士,主要研究方向为网络安全、数据挖掘;李剑(1976-),男,陕西西安人,副教授,博士,主要研究方向为信息安全、电子商务和人工智能;胡正名(1931-),男,湖北荆沙人,教授,博导,主要研究方向为信息理论与编码密码;杨义先(1961-),男,四川绵阳人,教授,博导,主要研究方向为信息安全、网络安全.

运算速度快等优点，$GF(2^{160})$上的椭圆曲线系统就可以达到1 024 bit的RSA系统同样的安全性[8]。因此，基于ECDLP的代理签名方案比基于有限域上离散对数问题的相应方案具有优越性。

在对基于椭圆曲线的代理签名的研究中，文献[9, 10]给出了两种典型的基于椭圆曲线离散对数问题的代理签名方案。但文献[11]指出这两种方案都存在着原始签名人的伪造攻击，即原始签名人能够伪造代理签名。文献[12]在改进椭圆曲线数字签名算法的基础上提出了一种新的椭圆曲线代理签名方案。文献[13]指出该方案同样存在着上述伪造问题。2007年，左为平等人[14]指出以上方案还存在着另外一种原始人伪造攻击，即原始签名者可以成功地把一个代理签名伪造成代理签名者自己的普通签名。为了抵御原始签名者对代理签名进行伪造攻击，左为平等人提出了一种新的基于椭圆曲线的安全代理签名方案(以下简称ZL方案)。但经笔者进一步分析发现，ZL方案依然存在着原始签名人的伪造攻击。为此，本文借鉴文献[15]中代理签名私钥构造方法，在ZL方案基础上提出了一个新方案。新方案能有效抵御伪造攻击，保护代理签名者的合法利益。与已有方案相比，新方案更安全、更实用。

2　Z L方案及其不足

ZL方案包括系统初始化、签名委托、签名产生和签名验证过程四个阶段。方案的协议方为原始签名者、代理签名者和签名验证者。

2.1　初始化

$GF(q)$：定义的有限域；

q：有限域的元素个数，其中$q=p$(p是一大素数)或$q=2^m$；

E：定义在有限域$GF(q)$上的安全椭圆曲线；

P：E上的一个阶为素数n的公开基点，其中$P\in E(GF(q))$；

n：素数，是P的阶，$n>2^{160}$且$n>4q^{1/2}$；

h：$\{0,1\}^*\rightarrow\{0,1\}^{160}$是美国NIST和NSA设计的一种安全hash函数；

(x_A,Y_A)：原始签名者A的私钥公钥对，其中，$Y_A=x_AP$，x_A保密，Y_A公开；

(x_B,Y_B)：代理签名者B的私钥公钥对，其中，$Y_B=x_BP$，x_B保密，Y_B公开；

m_w：授权证书，主要包含原始签名者A和代理签名者B的身份以及授权范围和期限等信息。

2.2　代理签名委托

1)原始签名者A随机选取一个整数$k_A\in[1,n-1]$，计算$G=k_AP=(x_G,y_G)$，$r_A=x_G \bmod n$，$e_1=h(m_w,r_A)$，$s_A=x_Ae_1+k_A \bmod n$，然后将(m_w,G,s_A)秘密地发送给代理签名者B。这里(G,s_A)实质上是A对m_w的签名值。

2)代理签名者B验证授权签名的合法性

B收到(m_w, G, s_A)后，首先检查授权证书m_w，之后计算：$r_A=x_G \bmod n$，$e_1=h(m_w,r_A)$，然后验证等式$s_AP=Y_Ae_1+G$是否成立，若成立则说明授权合法。

2.3　代理签名生成

对某个消息m，B代表A生成代理签名的过程如下：

B首先计算代理签名之私钥$x=s_A+x_BY_B \bmod n$，然后随机选取一个整数$k_B\in[1,n-1]$，计算$Q=k_BP=(x_Q,y_Q)$，$r=x_Q \bmod n$，$e_2=h(m,r)$，$s=xe_2+k_B \bmod n$，则将(m, m_w,G,Q,s)作为代理签名，并将(m,m_w,G,Q,s)发送给签名验证者。

2.4　代理签名验证

验证者收到代理签名(m,m_w,G,Q,s)后，利用原始签名者A和代理签名者B的公钥验证代理签名的过程如下：

计算$r_A=x_G \bmod n$，$r=x_Q \bmod n$，$e_1=h(m_w,r_A)$，$e_2=h(m,r)$，然后验证等式$sP=Q+e_2(G+Y_BY_B+e_1Y_A)$是否成立，如果等式成立则认为$B$代理$A$所做的代理签名有效，否则无效。

2.5　Z L方案安全性分析

证明ZL方案存在原始签名人的伪造攻击如下：

a)原始签名者A随机选取一个整数$k_A\in[1,n-1]$，计算$G=k_AP-Y_BY_B=(x_G, y_G)$，$r_A=x_G \bmod n$，$e_1=h(m_w,r_A)$，$s_A=x_Ae_1+k_A \bmod n$。

b)对某个消息m，A随机选取一个整数$k_B\in[1,n-1]$，计算$Q=k_BP=(x_Q,y_Q)$，$r=x_Q \bmod n$，$e_2=h(m,r)$，$s=s_Ae_2+k_B \bmod n$，则将(m,m_w,G,Q,s)作为代理签名，并将(m,m_w,G,Q,s)发送给签名验证者。

c)验证者计算$r_A=x_G \bmod n$，$r=x_Q \bmod n$，$e_1=h(m_w,r_A)$，$e_2=h(m,r)$，然后验证等式$s_P=Q+e_2(G+Y_BY_B+e_1Y_A)$是否成立，若等式成立则认为$(m,m_w,G,Q,s)$是$B$代理$A$所做的有效代理签名。以下证明上述等式成立：

$$Q+e_2(G+Y_BY_B+e_1Y_A)=Q+e_2(k_AP-Y_BY_B+Y_BY_B+e_1Y_A)=$$
$$Q+e_2(k_AP+e_1x_AP)=Q+e_2(k_A+e_1x_A)P=k_BP+e_2s_AP=(k_B+e_2s_A)P=sP$$

由以上分析可见，原始签名者A伪造的代理签名(m,m_w,G,Q,s)能通过签名验证者的验证，被认为是B代理A所做的有效代理签名，从而证明了ZL方案存在原始签名人的伪造攻击。

3　新的安全代理签名方案

系统初始化过程、签名委托过程同ZL方案，参见2.1、2.2节。以下仅叙述与ZL方案不同的签名产生过程和签名验证过程。

3.1　代理签名生成

对某个消息m，B代表A生成代理签名的过程如下：

B首先计算代理签名之私钥$x=s_Ax_B-1 \bmod n$，然后随机选取一个整数$k_B\in[1,n-1]$，计算$Q=k_BY_B=(x_Q,y_Q)$，$r=x_Q \bmod n$，$e_2=h(m,r)$，$s=xe_2+k_B \bmod n$，则将(m,m_w,G,Q,s)作为代理签名，并将(m,m_w,G,Q,s)发送给签名验证者。

3.2　代理签名验证

验证者收到代理签名(m,m_w,G,Q,s)后，首先检查授权证书m_w，之后利用原始签名者A和代理签名者B的公钥验证代理签名的过程如下：

计算$r_A=x_G \bmod n$，$r=x_Q \bmod n$，$e_1=h(m_w,r_A)$，$e_2=h(m,r)$，然后验证等式$sY_B=Q+e_2(G+e_1Y_A)$是否成立，如果等式成立则认为B代理A所做的代理签名有效，否则无效。

等式的正确性证明如下：

已知$s=xe_2+k_B \bmod n$，$x=s_A\ x_B-1 \bmod n$，$Q=k_BY_B$，$s_A=x_Ae_1+k_A \bmod n$，则

$$sY_B=(xe_2+k_B)Y_B=(s_A x_B^{-1}e_2+k_B)Y_B=s_A x_B^{-1}e_2Y_B+k_BY_B=e_2s_A x_B^{-1}x_BP+Q=e_2(x_Ae_1+k_A)P+Q=e_2(e_1x_AP+kAP)+Q=e_2(e_1Y_A+G)+Q=Q+e_2(G+e_1Y_A)$$

由此可知等式 $sY_B=Q+e_2(G+e_1Y_A)$ 成立。

4　新方案分析

4.1　安全分析

4.1.1　可验证性

根据代理签名 (m,m_w,G,Q,s),验证者利用原始签名者 A 和代理签名者 B 的公钥验证等式 $sY_B=Q+e_2(G+e_1Y_A)$ 是否成立,若等式成立则能够确信该签名是 B 代理 A 所生成的有效代理签名。由授权证书 m_w 及代理签名等式验证过程中内含的对授权证书签名值 (G,s_A) 的检查(内含验证等式 $s_AP=Y_Ae_1+G$ 是否成立),验证者能够确信这个签名是原始签名者授权认可的代理签名。

4.1.2　强可区分性

代理签名 (m,m_w,G,Q,s) 中包含授权证书 m_w,在形式上明显不同于普通签名,因而与原始签名者所产生的签名可以很容易区分开。如果有多个代理人或者对同一代理人进行了多次不同的授权,则因为在每次代理签名委托过程中 k_A 是随机选择的,所以每次的代理授权参数 G 不同,再加上授权证书 m_w 中的授权信息的不同,从而可以很容易地将不同代理人的代理签名和同一代理人根据不同授权进行的代理签名逐一区分开。

4.1.3　强不可伪造性

代理私钥 $x=s_A x_B^{-1} \bmod n$ 中包含代理签名者 B 的私钥 x_B,其他任何人(包括原始签名者)由于不知道 x_B 都不能假冒代理签名者 B 生成这个代理签名;又其中授权参数 $s_A=x_Ae_1+k_A \bmod n$ 中又包含原始签名者 A 的私钥 x_A,只有 A 授权的代理签名者 B 才能生成有效的代理签名。以下分析新方案对常见的几种伪造攻击的可抵抗性:

a)原始签名者普通签名的不可伪造性。在代理签名方案中,代理签名者 B 无法从代理委托请求 (m_w,G,s_A) 中求出原始签名者 A 的私钥 x_A。这是因为,$G=k_AP=(x_G,y_G)$,$r_A=x_G \bmod n$,$e_1=h(m_w,r_A)$,$s_A=x_Ae_1+k_A \bmod n$。其中包含 x_A 的等式中 s_A 的值已知,e_1 的值可计算得出,若想计算出 x_A 需要知道 k_A 的值,而在等式 $G=k_AP$ 中试图根据 G 计算出 k_A 时将面临求解椭圆曲线离散对数问题。因此 B 不可能利用代理签名方案中的信息伪造 A 的普通数字签名。进而可知其他攻击者也都难以伪造 A 的普通数字签名。

b)代理签名者普通签名的不可伪造性。新方案中代理签名私钥 $x=s_A x_B^{-1} \bmod n$,对于原始签名者 A 而言,在不知道随机数 k_B 的情况下,已知 $s=xe_2+k_B \bmod n=s_A x_B^{-1}e_2+k_B \bmod n$,用 ZL 方案指出的攻击方法计算 $s'=s-s_Ae_2=s_A x_B^{-1}e_2+k_B-s_Ae_2 \bmod n$,$s'$ 显然不等于 Schnorr 签名算法体制下代理签名者 B 的普通签名 $s_B=x_Be_2+k_B \bmod n$。因此,新方案中不存在 ZL 方案中指出的原始签名者可利用代理签名伪造代理签名者普通签名的安全缺陷。

c)代理签名的不可伪造性。新方案中代理签名验证等式为 $sY_B=Q+e_2(G+e_1Y_A)$,伪造代理签名等价于求 (s,Q,G,e_1,e_2) 使得上述等式成立。由于哈希函数的单向性,攻击者必须先确定哈希函数所有参数 (m_w,r_A,m,r) 的值。其中 $r_A=x_G \bmod n$,$r=x_Q \bmod n$,x_G、x_Q 分别为点 Q,G 的横坐标,从而必须先确定 (Q,G) 的值。又由于验证等式中的 Y_B 不像 ZL 方案那样和 G 或 Q 处于相同的构成项位置,因而无法通过构造 G 或 Q 的值消去。一旦 (m_w,m,Q,G) 的值确定了,则 e_1,e_2 的值就确定了,从而验证等式 $sY_B=Q+e_2(G+e_1Y_A)$ 等号右边的值就确定了,求解 s 将面临求解椭圆曲线离散对数问题。其他任何人(即使是原始签名者)也不能伪造代理签名。

4.1.4　强可鉴别性

对于有效的代理签名 (m,m_w,G,Q,s),授权证书 m_w 中包含代理签名者的身份信息,代理签名验证时要用到代理签名者 B 的公钥 Y_B,原始签名者和任何验证者在验证代理签名时都能够确定代理签名者的身份,因此方案具有强可鉴别性。

4.1.5　强不可否认性

从上面强不可伪造性可知,只有经授权的代理签名者才能生成这个代理签名,代理签名者一旦生成一个有效代理签名,事后不能否定对这个代理签名的建立,因此方案具有强不可否认性。

4.1.6　可控性或阻止滥用

原始签名者能够通过授权证书 m_w 有效控制代理签名者的代理权限,包括代理者的身份、代理有效时间、代理签署消息范围等。因 m_w 受安全 hash 函数的保护,最终的代理签名验证等式中要用到 $e_1=h(m_w,r_A)$,对 m_w 的窜改会导致代理签名不能通过验证从而使其无效。因此,代理签名者 B 只能在规定的授权范围和期限内代表原始签名者 A 进行签名,且即使 B 将代理权限转交给第三方 C,C 也不可能代表原始签名者 A 进行签名。所以代理签名密钥不能用于其他目的,方案具有较好的可控性。

4.1.7　无须安全信道

方案中代理授权为 (m_w,G,s_A),其中 (G,s_A) 实质上是原始签名者 A 对授权证书 m_w 的签名值,m_w 中明确了 A、B 的身份及代理关系,s_A 是由原始签名者的私钥 x_A 和 m_w 决定的。由于代理私钥 $x=s_A x_B^{-1} \bmod n$。其中包含了由 A 的私钥来保证不可窜改的授权参数 s_A,由哈希值 e_1 来保证不可窜改的授权证书 m_w,以及 B 的私钥 x_B,窃听者 D 即使截获了代理授权值,也无法冒充代理签名者 B 生成代表 A 的代理签名,也无法将代理签名者改为自己生成代表 A 的代理签名。因而方案不需要安全传输信道的支持。

4.2　效率分析

由于新方案系统初始化过程、签名委托过程同 ZL 方案,仅需比较与 ZL 方案不同的签名产生过程和签名验证过程的效率。

本文所描述方案的签名产生过程由两部分组成:一是代理签名私钥的生成,二是用代理签名私钥进行签名。新方案与 ZL 方案在用代理签名私钥进行签名方面的运算过程类似,计算量的差异存在于代理签名私钥生成过程。ZL 方案代理签名私钥生成需一次椭圆曲线乘法和一次模加运算,新方案需一次模逆和一次模乘运算。其中最费时的是椭圆曲线乘法,其他运算与椭圆曲线乘法运算相比几乎可忽略不计。因而新方案更为高效。

签名验证过程中,ZL 方案需两次哈希、四次椭圆曲线乘法

和三次椭圆曲线加法运算;新方案需两次哈希、三次椭圆曲线乘法和两次椭圆曲线加法运算。显然,新方案的效率要高于ZL方案。

5 结束语

本文首先介绍了文献[14]提出的基于椭圆曲线的代理签名方案并构造了针对该方案的原始签名人伪造攻击;然后提出新的方案,并验证了新的安全代理签名方案避免了以往方案所存在的安全问题,满足引言中所列出的典型代理签名方案应具备的六个方面的安全特性。新方案具有椭圆曲线密码体制安全性高、密钥短小、运算速度快等优点,具备强代理签名方案所应有的性质,且无须安全信道,具有更强的抗攻击性和更高的实用价值。

参考文献:

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans on Fundamentals of Electronics Communications and Computer Sciences, 1996, E79A(9): 1338-1354.

[2] 祁明, HARN L. 基于离散对数的若干新型代理签名方案[J]. 电子学报, 2000,28(11):114-115.

[3] SHAO Zu-hua. Proxy signature schemes based on factoring[J]. Information Processing Letters, 2003,85(3): 137-143.

[4] LEE B, KIM H, KIM K. Strong proxy signature and its applications [C]//Proc of Symposium on Cryptography and Information Security. Oiso, Japan :[s. n.], 2001:603-608.

[5] 杨伟强, 徐秋亮. 典型代理签名方案的分析与改进[J]. 计算机工程与应用, 2004,40(9): 152-154.

[6] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation,1987,48(1): 203-209.

[7] MILLER V S. Use of elliptic curve in cryptography[C]//Proc of Advances in Cryptology-Crypto'85. New York: Springer-Verlag, 1986: 417-426.

[8] CAELLI W J, DAWSON E P, REA S A. PKI, elliptic curve cryptography, and digital signatures [J]. Computers and Security, 1999, 18(1): 47-66.

[9] CHEN T S, LIU T P, HWANG G S, *et al*. An improvement of proxy-protected proxy multi-signature scheme[C]//Proc of the 13th International Conference on Information Management. 2002:33-40.

[10] CHEN T S, CHUNG Y F, HWANG G S. Efficient proxy multi-signature schemes based on the elliptic curve cryptosystem[J]. Computers & Security,2003,22(6):527-534.

[11] 曹天杰,林东岱,薛锐. 基于椭圆曲线的代理多签名方案的安全性分析[J]. 小型微型计算机系统,2006,27(5):798-801.

[12] 纪家慧,李大兴.新的代理多签名体制[J].计算机研究与发展, 2004,141(14):715-719.

[13] 吴旭辉,沈庆浩.一种代理多签名体制的安全性分析[J].通信学报, 2005,26(7):119-122.

[14] 左为平, 李海峰. 一种安全的椭圆曲线代理签名方案[J]. 佳木斯大学学报:自然科学版, 2007,25(4): 495-497.

[15] CHANG M H, CHEN I T, CHEN M T. Design of proxy signature in ECDSA[C]//Proc of the 8th International Conference on Intelligent Systems Design and Applications. Kaohsiung City, Taiwan:[s. n.], 2008: 17-22.

(上接第 684 页)其需要将欲发送的消息分别用各子组的公钥进行加密后连接起来广播出去,消息总长度大约为 2 *tn*。

5 结束语

设计动态高效的分布式组密钥管理协议是 DPG 组播通信需要重点考虑的问题。本文在文献[6]的基础上,提出了一个新的基于 Merkle 身份树的 DPG 密钥协商方案,实现了任意多个子组之间的保密通信,而无须经过 KGCs 的转发,避免了其翻译组播消息时所引起的延迟,具有较高的灵活性。子组成员之间以及子组与子组之间,在协商密钥或通信时都是相互独立的,充分体现了分布式的特点。使用一组并行工作的 KGCs,也大大降低了单个 KGC 的工作负担,避免了单点故障的产生,提高了组播系统的健壮性。

密钥托管(key escrow)是基于身份的密码系统所固有的缺点,本文方案同样存在这个问题,即 KGCs 可以计算出所有子组的公、私钥。近年来提出的无证书密码系统[7,8]在传统的基于证书的公钥密码系统和基于身份的公钥密码系统之间进行了适当的折中,取得了较好的效果。下一步的工作将考虑应用无证书的密码系统,以期构造一个更安全的密钥协商方案。

参考文献:

[1] MA Chun-bo, AO Jun, LI Jian-hua. A novel verifier-based authenticated key agreement protocol[C]//Proc of International Conference on Intelligent Computing. Heidelberg: Springer, 2007: 1044-1050.

[2] YOON E J, YOO K Y. A new key agreement protocol based on chaotic maps[C]//Proc of the 2nd International Symposium on Agents and Multi-agent Systems: Technologies and Applications. Heidelberg: Springer, 2008: 897-906.

[3] SVEN L, SYLVAIN P. SAS-based group authentication and key agreement protocols[C]//Proc of International Conference on Theory and Practice of Public-Key Cryptography. Heidelberg: Springer, 2008: 197-213.

[4] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security,2007,6(4): 213-241.

[5] CHIEN Hung-yu. ID-based key agreement with anonymity for Ad hoc networks[C]//Proc of IFIP International Conference on Embedded and Ubiquitous Computing. Heidelberg: Springer, 2007: 333-345.

[6] WANG Li-ming, WU Chuan-kun. Efficient key agreement for large and dynamic multicast groups[J]. International Journal of Network Security,2006, 3(1): 11-20.

[7] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology. Heidelberg: Springer, 2003: 452-473.

[8] MANDT T K, TAN C H. Certificateless authenticated two-party key agreement protocols[M]. Heidelberg: Springer, 2007: 37-44.

[9] BONEH D, FRANKLIN M K. Identity-based encryption from the Weil pairing[C]//Proc of the 21st Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer, 2001: 213-229.