一种基于身份的群签名方案

董 亮 肖国镇

(西安电子科技大学 ISN 综合业务网国家重点实验室 西安 710071)

摘 要 基于身份的密码系统(Identity-based Cryptosystem)是为了简化基于证书的密码系统繁琐的密钥管理过程而提出的。群签名能对签名者提供很好的匿名性,它在电子商务、匿名电子选举等方面有重要应用。本文利用双线性对的性质构造了一种新的基于身份的群签名方案。对该方案的安全性及其效率的分析表明,方案是安全有效的。

关键词 基于身份,双线性映射,群签名

An ID-based Group Signature Scheme

DONG Liang XIAO Guo-Zhen

(Information Security and Privacy Institute in ISN, Xidian University, Xi'an 710071)

Abstract Identity-based (ID-based) cryptosystem can simplify key management procedures of certificate-based cryptosystem. Group signature is very useful to provide the signer's anonymity, so it is plays an important role in building e-commerce, anonymous electronic voting etc. In this paper, we propose a new ID-based group signature scheme based on the bilinear pairings. The analysis shows that our scheme has higher safety and better efficiency.

Keywords ID-based, Bilinear map, Group signature

1 引言

1984 年 Shamir[1] 为了简化电子邮件系统中的证书管理问题,提出了基于身份的密码系统(IBC)。系统中每个用户都有一个身份,其中身份可以是姓名、住址、电子邮件地址等,用户的公钥可以由任何人根据其身份计算出来,而私钥则由可信第三方生成,这里,可信第三方称为私钥生成器 PKG (Private Key Generator)。IBC 系统不需要保存每个用户的公钥证书,避免了使用证书带来的存储和管理开销的问题,简化了基于证书的密码系统繁琐的密钥管理过程。最近,利用椭圆曲线上的 Weil 对的双线性性质,一些基于身份的加密[2]、签名方案[3~7]相继被构造出来。

群签名能对签名者提供很好的匿名性,它可以由可信中心协助执行,中心掌握各签名人与所签名之间的相关信息,并为签名人匿名签字保密;在有争执时,可以由可信中心打开签名而识别出签名人,所以群签名在电子商务、匿名电子选举及网上投标等场合有重要应用。本文是在 SOK-IBS (Sakai-Ogishi-Kasahara Identity Based Signature)[6] 的基础上,利用椭圆曲线上的 Weil 对的双线性性质,构造了一种新的基于身份的群签名方案。

2 双线性映射和 GDH 群

在文[2~7]的加密和签名系统中使用了双线性映射和 GDH 群,下面简要介绍它们的定义及性质。

2.1 双线性映射

设 G_1 是一个由 P 产生的循环加法群,其阶为 q,G_2 是一个阶为 q 的循环乘法群,a,b 是 Z_q^* 的元素,我们假定 DLP 问题在 G_1 和 G_2 上是困难的。e 是由椭圆曲线上的 Weil 对产生的,双线性映射 $e:G_1\times G_2\rightarrow G_2$ 具有以下性质:

(1)双线性:对任意的 $P,Q,R\in G_1$,$e(P,Q+R)=e(P,Q)e(P,R)$,$e(P+Q,R)=e(P,R)e(Q,R)$。对于任意的 $a\in Z_q^*$,用 aP 表示 P 自加 a 次,则对任意的 $a,b\in Z_p^*$,有 $e(aP,bQ)=e(P,Q)^{ab}$。

(2)非退化性:存在 $P,Q\in G_1$,使得 $e(P,Q)$ 不等于 1。

(3)可计算性:存在一个高效的算法计算 $e(P,Q)$,其中 $P,Q\in G_1$。

2.2 GDH 群

设 G 是一个由 P 生成的阶为素数 q 的加法循环群,假定在 G 上乘法和逆在单位时间内可以计算出来,$a,b,c\in Z_q^*$。则:

(1)CDHP(计算上的 Diffie-Hellman 问题):已知(P,aP,bP),计算 abP。

(2)DDHP(决定性的 Diffie-Hellman 问题):已知(P,aP,bP,cP),判断 $c=ab \bmod q$ 是否成立。

(3)CDH 假设:不存在有效的多项式时间算法可以解决 CDHP。

(4)GDH 群:在素数阶循环群 G 上,DDHP 在多项式时间内能被解决,但没有算法可以解决 CDHP,即 CDH 假设成

9 Wallner D M, Harder E J, Agee R C. Key management for multicast: Issues and architectures. Internet draft, Sept. 1998
10 Wong C K, Gouda M, Lam S S. Secure group communications using key graphs. IEEE/ACM Trans. Networking, Feb. 2000, 8: 15~36. Also In: Proc. ACKM SIGCOMM '98, Vancouver, BC, Canada, Sept. 1998
11 Gallager R. Information Theory and Reliable Communication. New York: Wiley, 1968
12 Harney H, Muckenhirn C. GKMP architecture. Request for Comments(RFC), 1997, 2093
13 戴宗坤,罗万伯. 密钥管理. 信息系统安全. 电子工业出版社, 2002
14 冯登国. 计算机通信网络安全. 清华大学出版社, 2001
15 Stallings W 著. 杨明,等译. 密码编码学与网络安全. 电子工业出版社, 2001

立，则称 G 为一个 GDH 群。

3 基于身份的数字签名方案

一个基于身份的数字签名方案由四个算法组成：系统初始化，密钥提取，签名和验证。系统中包括三方：可信中心、签名者和验证者。这里给出 SOK-IBS (Sakai-Ogishi-Kasahara Identity Based Signature)[6] 方案，它的安全性是建立在 CDHP 的困难性假设基础之上的，可证明在随机预言(random oracle)模型下是安全的。

系统初始化：设 G_1 是阶为素数 q 的 GDH 群，P 为生成元；G_2 是阶为 q 的循环乘法群，e 是 $G_1\times G_1$ 到 G_2 的一个双线性映射。设 ID 是一个表示用户身份的字符串，H_1 和 H_2 是公开的加密哈希函数，$H_1:\{0,1\}^*\rightarrow\{0,1\}^k$ (k 为常数)，$H_2:\{0,1\}^*\rightarrow G_1$。可信中心 PKG 随机选取一个整数 $s\in Z_q^*$，计算 $P_{pub}=sP$，s 称为系统主密钥，系统中所有用户的私钥均由它产生。系统公开参数为 $(G_1,G_2,e,q,P,P_{pub},H_1,H_2)$ 以及系统中用户的身份信息 $ID\in\{0,1\}^*$，严格保密主密钥 s。

密钥提取：用户向 PKG 递交身份 ID 进行认证，PKG 在验证了用户的身份后给出用户身份对应的私钥。PKG 计算 $Q_{ID}=H_1(ID)$，用户的解密私钥 $S_{ID}=sQ_{ID}$。然后通过安全信道把 S_{ID} 发送给用户。用户的密钥对为 (Q_{ID},S_{ID})。

签名：为了签名一个消息 m，签名者随机选取一个整数 $r\in Z_q^*$ 并计算：$U=rP$；$H=H_2(ID,m,U)$；$V=S_{ID}+rH$。对 m 的签名是 (U,V)。

验证：验证者计算 $Q=H_1(ID)$，$H=H_2(ID,m,U)$，检查验证等式 $e(P,V)=e(P_{pub},Q)e(U,H)$ 是否成立。如果验证等式成立，接受签名；否则，拒绝该签名。

4 基于身份的群签名方案的构造

4.1 定义

一个基于身份的群签名系统，它包括以下五个过程：

创建：输入安全系数 k，通过某种多项式时间概率算法输出群公钥和群管理员私钥。

加入：群管理员和用户之间的交互式协议，执行该协议使用户成为群成员，产生群成员的私钥和成员证书。

签名：该概率算法输入群公钥，成员证书，成员私钥和信息 m，输出对 m 的群签名。

验证：该算法输入群公钥，对消息 m 的签名，输出 1 或 0，确定签名是否有效。

打开：该算法在输入消息 m、对消息 m 的签名、群私钥后可以确定签名人的身份。

4.2 方案实现

下面描述基于第 3 节的数字签名方案的一个群签名方案，我们假设 PKG 就是群管理员。

创建：系统参数的选取除 S_{ID} 外和上述方案相同。用户随机选取一个整数 $r\in Z_q^*$ 作为他的长期私钥，PKG 计算 $Q_{ID}=H_1(ID)$，$S_{ID}=sH_2(Q_{ID},rP)$，然后通过安全信道把 S_{ID} 发送给用户。用户的私钥对为 (S_{ID},r)，公钥为 Q_{ID}。

加入：当一个用户想成为一个群成员时，他和 PKG 之间执行以下交互式协议：

(1)用户随机选取 $x_i\in Z_q^*$，$i=1,2,\cdots,k$，并把 ID,S_{ID},rP,x_iP 和 rx_iP 发送给 PKG；

(2)如果 $S_{ID}=sH_2(Q_{ID},rP)$ 并且 $e(rx_iP,P)=e(x_iP,rP)$，PKG 把 $S_i=sH_2(T,rx_iP)$ 发送给用户，T 是 r 的生存周期，用户在 T 之后需要更换私钥对。否则协议终止；

(3)用户的群成员证书是 (S_i,rx_iP)，签名私钥是 rx_i；

(4)PKG 把 ID,rP,x_iP 和 rx_iP 加入成员列表，该用户成为合法的群成员。

签名：为了签名消息 m，签名者随机选择一个签名密钥和相应的群成员证书，作以下计算：

(1)$U=rx_iP$；

(2)$V=rx_iH_2(Q_{ID}\|T,U)$；

(3)$H=H_2(m,V)$；

(4)$W=S_1+rx_iH$。

(U,V,W,T) 是对消息 m 的签名。

验证：如果 T 是有效的时间，验证者作以下计算：

(1)$Q=H_2(T,rx_iP)$；

(2)$H=H_2(m,V)$；

(3)检查验证等式 $e(P,W)=e(P_{pub},Q)e(U,H)$ 是否成立。如果验证等式成立，则接受签名；否则，拒绝该签名。

验证算法的正确性如下：

$$\begin{aligned}e(P,W)&=e(P,S_i+rx_iH)=e(P,S_i)e(P,rx_iH)\\&=e(sP,H_2(T,rx_iP))e(rx_iP,H)\\&=e(P_{pub},Q)e(U,H)\end{aligned}$$

打开：如果是一个合法签名，PKG 根据成员列表很容易从 rx_iP 得到该群成员的 ID，从而恢复出签名者的身份。

5 安全性分析

上述的基于身份的群签名方案满足群签名的所有安全性要求。

(1)不可伪造性：只有合法的群成员才具有有效的群成员证书 (S_i,rx_iP)，代表该群组产生合法的群签名。任何人如果不知道该成员的私钥 S_{ID}，就无法通过 PKG 的验证。更进一步，我们也不能从签名 (U,V,W,T) 中计算出群成员的私钥，因为 SOK-IBS (Sakai-Ogishi-Kasahara Identity Based Signature)[6] 在 CDHP 的困难性假设下是安全的。

(2)匿名性：给定某个消息的有效群签名，除了可信第三方 PKG 外，任何其他人要确定签名者的身份在计算上是不可行的。因为 x_i 是任意选取的，rx_iP 不能显示有关用户身份的任何信息。

(3)不可关联性：给定 rx_iP 和 rx_jP，在不知道 x_iP 和 x_jP 的情况下，确定它们是否源于同一个 rP 在计算上是困难的。

(4)可开脱性：任何一个群成员包括 PKG 都不能代表另一个群成员产生有效的群签名。假设一个不诚实的 PKG 或与一个不诚实用户合谋想陷害另一个合法群成员，作如下计算：

PKG 随机选取 $r'\in Z_q^*$，，计算 $Q'=H_2(T,r'P)$；然后对消息 m 执行签名协议，输出签名 (U',V',W',T)。因为 $e(P,W')=e(P_{pub},Q')e(U',H)$ 可以通过验证，所以 PKG 可以伪造一个合法的签名。

然而，该群成员能够提供一个证据证明这个签名是 PKG 伪造的。首先，他发送 rP 给仲裁者，然后提供他知道 $S_{ID}=sH_2(Q_{ID},rP)$ 的知识证明：仲裁者任意选取一个秘密整数 $a\in Z_q^*$，然后把 aP 发送给该成员，该成员计算 $e(S_{ID},aP)$。如果 $e(S_{ID},aP)=e(H_2(Q_{ID},rP),P_{pub})^a$ 成立，则说明该成员确实知道 S_{ID}，但主密钥 s 只有 PKG 自己知道，由此仲裁者可以断

定该签名是PKG伪造的，则该群成员不必为他人产生的群签名承担责任。

(5)可跟踪性：PKG可以打开任何有效的群签名以确定签名者的身份，签名者不能否认他的签名。因为PKG能提供证据证明该签名的确是该群成员的签名，因为：

$e(rx_iP,P)=e(x_iP,rP)$；

$e(S_{ID},P)=e(H_2(Q_{ID},rP),P_{pub})$。

(6)防合谋攻击：群管理员PKG知道所有群成员的私钥，群成员合谋子集不能产生一个有效的群签名，使得群管理员不能将签名与其中的一个群成员的身份联系起来。

(7)效率：传统的群签名方案中，群公钥的大小和群签名的长度与群成员的数量成正比，因此对于比较大的群或动态性很强的群效率很低。而本方案中群公钥的大小和群签名的长度是常数，不依赖于群成员的数量，群签名的算法和协议是有效的。

结论 基于身份的密码系统可以简化基于证书的密码系统繁琐的密钥管理过程。本文是在基于身份的数字签名方案的基础上，利用双线性映射的特殊性质，构造了一种新的基于身份的群签名方案，该方案是安全有效的。基于身份的签名方案能够降低证书管理开销，具有较高的执行效率，因此具有更广泛的现实意义。

参 考 文 献

1 Shamir A. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto 1984, LNCS 196, Springer-Verlag, 1984. 47～53

2 Boneh D, Franklin M. Identity-based encryption from the Weil pairing. Advances in Cryptology-Crypto 2001, LNCS 2139, Springer-Verlag, 2001. 213～229

3 Cha J, Cheon J H. An identity-based signature from gap Diffie-Hellman groups. Public Key Cryptography-PKC 2003, LNCS 2567, Springer-Verlag, 2003. 18～30

4 Hess F. Exponent Group Signature Schemes and Efficient Identity Based Signature Schemes Based on Pairings. Cryptology ePrint Archive, Report 2002/012

5 Chen Xiaofeng, Zhang Fangguo, Kim K. A New ID-based Group Signature Scheme from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/116

6 Bellare M, Namprempre C, Neven G. Security Proofs for Identity-Based Identification and Signature Schemes. Advances in Cryptology-Eurocrypt 2004, LNCS 3027, Springer-Verlag, 2004. 268～286

7 Xu Jing, Zhang Zhenfeng, Feng Dengguo. ID-Based Proxy Signature Using Bilinear Pairings. Cryptology ePrint Archive, Report 2004/206

第六届中国Rough集与软计算学术研讨会（CRSSC2006）

征 文 通 知

由中国人工智能学会粗糙集与软计算专业委员会和中国计算机学会人工智能与模式识别专业委员会主办、浙江师范大学承办的“第六届中国Rough集与软计算学术研讨会”(CRSSC2006)拟定于2006年10月30日至11月3日在浙江金华召开。

Rough集理论自1982年由波兰数学家Zdzisław Pawlak教授提出以来，其理论模型得到不断完善和发展，并渗透到很多学科，成为研究数据挖掘、知识约简和粒计算的理论基础。Rough集理论自身也已成为完整、独立的科学领域。此外，Rough集理论与其它一些软计算理论，诸如Fuzzy集、粒计算、神经网络、遗传算法等均已经成为当前国内计算机及相关专业的研究热点。

自2001年在重庆成功召开“第一届中国Rough集与软计算学术研讨会(CRSSC2001)”以来，我国每年的CRSSC系列研讨会在规模和质量上均呈良好的增长趋势，在此领域的研究工作发展很快。2003年成立了中国人工智能学会粗糙集与软计算专业委会，Rough集的研究队伍也更加壮大，研究成果在深度和广度上有了更大的发展。

现将有关征文事宜通知如下，欢迎各界人士踊跃投稿。

一、征文范围

Rough集理论及应用；计算智能；机器学习；文字计算；Fuzzy集理论及应用；粒计算；软计算及其应用；演化计算；Petri网；软计算的逻辑基础；非经典逻辑；神经网络；计算复杂性；空间推理；统计与概率推理；智能Agent；多准则决策分析；决策支持系统；知识发现与数据挖掘；多Agent技术；近似推理与不确定性推理；网络智能；集成智能系统；数据仓库；模式识别与图像处理生物信息与生物计算；认知信息学；其他有关领域

二、征文要求

a) 未公开发表过，一般不超过6000字。

b) 论文包括中英文题目，作者姓名、单位、地址、邮编、E-mail地址、联系电话，中英文摘要（一般不超过200字）、关键词、正文和参考文献。

c) 论文请用Word排版，A4纸打印，一式两份，欢迎通过会议网站在线投稿或通过EMAIL投稿。

d) 录用论文将由《计算机科学》杂志专辑出版。

e) 征文请寄：浙江省金华市浙江师范大学信息科学与工程学院 吴小红 收 邮政编码：321004，
电子版投稿请送：crssc2006@zjnu.cn 会议网站：http://cs.cqupt.edu.cn/crssc/crssc2006

三、重要日期 截稿日期（收到）：2006年4月31日 录用日期（发出）：2006年6月10日
论文清样付印和论文注册截止日期（收到）：2006年7月10日

四、联系方式 联系人(联系电话)：梁久祯(0579-2298258)；王基一(0579-2283436)；吴小红(0579-2298903)
电子信箱：liangjz@zjnu.cn（梁久祯），xx51@zjnu.cn（王基一）