一种新的基于身份的动态群签名方案

欧海文[1],王佳丽[1,2]
OU Hai-wen[1],WANG Jia-li[1,2]

1.北京电子科技学院 信息安全与保密重点实验室,北京 100070
2.西安电子科技大学 通信工程学院,西安 710071
1.Key Lab of Information Security and Secrecy,Beijing Electronic Science and Technology Institute,Beijing 100070,China
2.College of Communication Engineering,Xidian University,Xi'an 710071,China
E-mail:breashjiali@163.com

OU Hai-wen,WANG Jia-li.New ID-based dynamic group signature scheme.Computer Engineering and Applications,2010,46(6):96-97.

Abstract: In order to solve the problem that KGC can not be trusted in ID-based group signature,a new ID-based dynamic group signature scheme is proposed.The new verify and open algorithms make sure the scheme can against forgery attack.Additional,this scheme can delete members simply and efficiently without changing the group public key and the other group members' key.At the same time,the sizes of signature and key are independent on the numbers of the group members.
Key words: group signature;ID-based;dynamic

摘 要:为了解决在基于身份的群签名中 KGC 不可信的问题,提出了一种新的基于身份的动态群签名方案。新的验证和打开算法确保了该方案可以抵抗伪造攻击。另外该方案可以简单有效地删除群成员,而不改变群公钥和其他群成员的密钥,签名和密钥的长度不依赖于群成员的个数。
关键词:群签名;基于身份;动态
DOI:10.3778/j.issn.1002-8331.2010.06.027 **文章编号:**1002-8331(2010)06-0096-02 **文献标识码:**A **中图分类号:**TN918.1

1 引言

1993 年,Park,Kim 和 Won 首次提出了基于身份的群签名方案[1],但是该方案效率非常的低,群公钥和签名长度随着群成员个数的增多而线性增加。此后多种基于身份的群签名方案被提出。1998 年,Mao 和 Lim[2]证明了该方案不满足匿名性。同年,Tseng 和 Jan[3]提出了另一个基于身份的群签名方案,声称解决了群成员的加入和删除对过去签名影响的问题,而且效率高,其安全性是依赖于模复合整数 n 的离散对数求解的困难性。然而,文献[4-6]指出了该方案是不安全的,存在多处漏洞。2003 年,Chen、Zhang 和 Kim[7]提出了由双线性对构造的无可信 PKG 的基于身份的签名方案。在该方案中,不诚实 PKG 不能伪造用户进行签名,而且该方案还解决了固有的密钥托管问题。2008 年杨学俊等人[8]指出 Chen 等人的方案在 KGC 不可信的情况下,不能有效地保证签名的安全性。在分析了多种基于身份的群签名方案的优缺点后,提出了一种新的基于身份的动态的群签名方案。

2 Gap Diffie_Hellman 群(GDH 群)和双线性映射

2.1 Gap Diffie_Hellman 群

设 G 是一个循环加群,阶为素数 q,生成元为 P。若:

(1)给定元素 $P,Q\in G$,找到一个 $n\in Z_q^*$,使得 $Q=nP$,则称其为 DLP。

(2)给定元素 P,aP,bP,其中 $a,b\in Z_q^*$,计算 abP,则称其为计算性 Diffie-Hellman 问题(Computational Diffie-Hellman Problem,CDHP)。

(3)给定元素 P,aP,bP,其中 $a,b,c\in Z_q^*$,计算是否 $c\equiv ab \bmod q$,则称其为判定性 Diffie-Hellman 问题(Decisional Diffie-Hellman Problem,DDHP)。

如果群 G 对于 DDHP 能在多项式时间内解决,而 DLP 和 CDHP 不能在多项式时间内解决,则称 G 为 Gap Diffie-Hellman 群(GDH 群)。

2.2 双线性映射

令 G_1 是一个由 P 生成的循环加法群,阶为素数 q,G_2 是一

基金项目:北京市自然科学基金(the Natural Science Foundation of Beijing of China under Grant No.4063040);北京电子科技学院信息安全与保密重点实验室基金项目(the Program of Key Lab of Information Security and Secrecy,Beijing Electronic Science and Technology Institute under Grant No.YZDJ0421)。
作者简介:欧海文(1963-),男,教授,硕士生导师,主要研究方向为密码编码理论及其技术应用;王佳丽(1984-),女,硕士生,主要研究方向为信息安全。
收稿日期:2008-09-01 **修回日期:**2008-11-03

个阶为素数 q 的循环乘法群。令 $a,b\in Z_q^*$ 假设群 G_1 和 G_2 中的离散对数问题是困难的。双线性对是一个映射 $e:G_1\times G_2\to G_2$,具有下面的性质:

(1)双线性性:$e(aP,bQ)=e(P,Q)^{ab}$,其中 $P,Q\in G_1$。

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

(3)可计算性:对于 $P,Q\in G_1$,存在一个有效的算法可以计算 $e(P,Q)$。

3 基于身份的动态群签名方案

下面给出一种新的基于身份的群签名方案,该方案在 KGC 不可信的情况下依然能保证签名的安全性,并且可以有效地删除群成员,而不改变 KGC 和其他群成员密钥,签名的长度不依赖于群成员的个数。

3.1 系统初始化

设 G_1 是一个 GDH 群,生成元为 P,阶为素数 q,G_2 是一个乘法循环群,阶为 q,e 为双线性映射:$G_1\times G_2\to G_2$。H_1,H_2,H_3 和 H_4 为单向哈希函数,$H_1:\{0,1\}^*\to G_1$,$H_2:\{0,1\}^*\times G_1\to Z_q^*$,$H_3:\{0,1\}^*\to Z_q^*$,$H_4:\{0,1\}^*\times G_1\to G_1$。

KGC 随机选择 $s\in Z_q^*$,并计算 $P_{pub}=sP$,系统公开参数$\{G_1,G_2,P,q,H_1,H_2,H_3,H_4,e,P_{pub}\}$,系统主密钥为 s。在群公告板里公告时间 T 和所有群成员的 $H_3(ID_i)$ 乘积,记作 $E=\prod H_3(ID_i)$。

3.2 成员加入

(1)成员 U_i 随机选取 $r_i\in Z_q^*$,并计算 r_i^{-1},r_iP,$Q_{ID_i}=H_4(ID_i,r_iP)$,U_i 把自己的身份信息 ID_i,$H_3(ID_i)$,$r_iQ_{ID_i}$ 和 r_iP 交给 KGC。

(2)KGC 计算 $sr_iQ_{ID_i}$,保留$(ID_i,H_3(ID_i),r_iP)$,并把 $sr_iQ_{ID_i}$ 交给 U_i,同时更新 $E'=H_3(ID_i)E$。

U_i 的签名密钥为 $sr_iQ_{ID_i}$ 和 r_i,公钥为 Q_{ID_i}。

3.3 成员删除

若要删除成员 U_j,KGC 只需更新时间 T 和 E 即可。T 时刻对应的 $E=H_3(ID_j)^{-1}\prod H_3(ID_i)$。

3.4 签名

U_i 对消息 m 进行签名,U_i 随机选取 $k_i\in Z_q^*$ 并计算 k_i^{-1} 及以下数值:

$$A=k_ir_i^{-1}P,B=r_iH_1(m)$$

$$C=H_2(m,B)k_i^{-1}sr_iQ_{ID_i},D=H_2(m,r_iP)H_3(ID_i)$$

则 U_i 对消息 m 的签名为(A,B,C,D,r_iP,t),其中 t 为签名时间。

3.5 验证

验证者 U_j 收到签名(A,B,C,D,r_AP,t)后,根据时间 t 与 T 的比较,选取相应的 E。U_j 计算:$H_1(m)$,$H_2(m,B)$,$H_2(m,r_i,P)$。U_j 验证 D 是否整除 $H_2(m,r_i,P)E$,若不整除则说明签名无效,否则签名者是群中的成员,并继续验证以下两个等式是否成立。

(1)$e(A,C)=e(H_2(m,B)Q_{ID_i},P_{pub})$

(2)$e(B,P)=e(H_1(m),r_iP)$

等式(1)成立说明签名者拥有签名密钥 $sr_iQ_{ID_i}$,等式(2)成立说明签名者拥有 r_iP 对应的签名密钥 r_i。

3.6 打开

因为身份信息 ID_i 只有签名者本人和 KGC 知道,并且 KGC 保留有$(ID_i,H_3(ID_i),r_iP)$,所以当发生争议时 KGC 计算 $H=H_2(m,r_iP)^{-1}D$,查找 ID_i 使之与 H 和 r_iP 相匹配。即使伪造者伪造的签名通过了验证算法,但是根据此打开算法依然可以分析出伪造者的身份。

4 安全性分析

4.1 伪造攻击

(1)非群成员伪造

因为签名者的身份信息 ID_i 只有签名者本人和 KGC 知道,所以非群成员伪造的签名中的 D 就不能整除 $H_2(m,r_iP)E$,伪造签名无效被拒绝。

(2)KGC 伪造成员 Alice 的签名

情况 1 KGC 首先选择 $r_A',k_A'\in Z_q^*$,并计算 $r_A'^{-1}$,$k_A'^{-1}$ 及以下数值:

$$A=k_A'r_A'^{-1}P,B=r_A'H_1(m)$$

$$C=H_2(m,B)k_A'^{-1}sr_AQ_{ID_A},D=H_2(m,r_AP)H_3(ID_A)$$

从而形成签名(A,B,C,D,r_AP,t)。

若要使签名有效则需:

$$e(A,C)=e(H_2(m,B)Q_{ID_A},P_{pub})$$

即 $e(k_A'r_A'^{-1}P,H_2(m,B)k_A'^{-1}sr_AQ_{ID_A})=e(H_2(m,B)Q_{ID_A},sP)$

即 $r_A'^{-1}$ 和 r_A 的乘积为单位元,也就是说 $r_A=r_A'$,但是 $r_A=r_A'$ 的概率为 $1/q$,由此可得 KGC 伪造的签名无效。

情况 2 KGC 选取合适的 r,k,使用 Alice 的身份信息 $H_3(ID_A)$ 和 Q_{ID_A},伪造出一个签名(A,B,C,D,rP,t),并且此签名可以通过验证算法,但是当此签名出现争议时,打开算法也可以分析出此签名的伪造者是 KGC。这是因为 KGC 保存了$(ID_A,H_3(ID_A),r_AP)$,且只有 Alice 和 KGC 知道 ID_A,而 rP 和 $H_3(ID_A)$ 所对应的 r_AP 不相等。

情况 3 KGC 选取合适的 r,k,用成员 Bob 的身份信息和 Alice 的 Q_{ID_A} 伪造 Alice 的签名从而陷害 Bob。

情况 1 伪造成功的概率只有 $1/q$,所以情况 2 和情况 3 出现的概率可忽略。

(3)成员 Bob 伪造成员 Alice 的签名

Bob 不知道 Alice 的签名密钥 $sr_AQ_{ID_A}$ 和 $H_3(ID_A)$ 所以无法伪造成功。即使 Bob 伪造签名成功了,也只能用自身的 $H_3(ID_B)$ 进行伪造,同样打开算法可以揭示签名是 Bob 伪造的。

(4)KGC 和成员 Bob 联合陷害 Alice

KGC 提供 $H_3(ID_A)$,Bob 提供用其自身的 r_B 和 $sr_BQ_{ID_B}$ 进行签名,从而得到签名(A,B,C,D,r_BP,t),虽然此签名可以通过验证算法,但是当产生争议时,打开算法可以断定此签名是 KGC 和 Bob 联合陷害 Alice 的。这是因为 $H_3(ID_A)$ 对应的是 ID_A 而 r_BP 对应的是 ID_B,而 Bob 是不知道 $H_3(ID_A)$ 的,只能是 KGC 向 Bob 提供了 $H_3(ID_A)$。

(下转 115 页)