高效的基于双线性对和身份的广义签密方案 *

张洪礼, 赵 静, 刘文远
(燕山大学 信息科学与工程学院 计算机系, 河北 秦皇岛 066004)

摘 要: 为解决目前基于身份的广义签密方案效率不高的问题,利用双线性对,结合广义的思想,提出了一个高效的基于身份的广义签密方案。在随机预言机模型下给出了该方案的安全性证明,证明结果表明该方案满足抗适应性选择密文攻击下的机密性、不可伪造性和不可否认性。与目前惟一的一个基于身份的广义签密方案相比,本方案减少了两个对运算,是目前效率最高的基于身份和对映射的广义签密方案。

关键词: 签密; 广义签密; 基于身份; 双线性对; 随机预言机
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)02-0678-04
doi:10.3969/j.issn.1001-3695.2010.02.076

Efficient pairing-based and identity-based generalized signcryption scheme

ZHANG Hong-li, ZHAO Jing, LIU Wen-yuan
(*Dept. of Computer, School of Information Science & Engineering, Yanshan University, Qinhuangdao Hebei* 066004, *China*)

Abstract: To improve the efficience, this paper proposed a new efficient identity-based generalized signcryption scheme using the bilinear pairings and the ideas of generalization. Proved the proposed scheme to be message confidentiality non-repudiation and unforgeability under the random oracle model. As compared with the only-one identity-based gernalized signcryption scheme to date, the proposed scheme decreases two pairing operations, and is more efficient.

Key words: signcryption; generalized signcryption; identity-based; bilinear pairings; random oracle

0 引言

签密在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能。如今签密技术已经得到了广泛的应用,如防火墙、电子现金支付和密钥分配等。虽然签密在需要提供加密和认证功能的场合效率比较高,但当系统只需要机密性或认证性时,普通的签密方案就不再适用了。系统必须切换到其他的加密或签名算法才能满足需要,这将增加额外的开销。为了解决这个问题,2006 年,韩益亮等人[1]提出了广义签密的概念,即具有更强适应性的签密体制,它能实现三种功能。当要求同时满足机密性和认证性时能够提供加密和签名双重功能,当仅要求机密性或认证性时,无须任何修改和附加计算就可以单独提供加密或签名功能。他们也提出了一个基于椭圆曲线数字签名标准 ECDSA(elliptic curve digital signature algorithm,椭圆曲线数字签名算法)的广义签密方案 SC-ECDSA,但是没有给出完整的安全性定义。为了简化密钥的管理,Shamir[2] 于 1984 年提出基于身份的密码体制。由于双线性对是构造基于身份的密码体制的很好工具,近几年来,利用双线性对构造基于身份的方案成为密码学界的研究热点。2008 年,文献[3]首次提出了基于对映射和身份的广义签密方案,但该方案从签密到解签密总共花费了四次对运算,效率比较低。基于身份的广义签密将基于身份的签密推广到只要求机密性或认证性的场合,有着更广阔的应用前景。

本文利用双线性对提出了一个高效的基于身份的广义签密方案,并对方案的安全性给出了证明。本文的方案仅需两个对运算,与文献[3]中提出的至今惟一一个基于身份的广义签密方案相比,本文方案效率更高。

1 预备知识

本节简要介绍双线性对的基础知识及其相关困难问题。

令 G_1 是阶为 q 的循环加法群,G_2 是 q 阶循环乘法群,P 是 G_1 的生成元,映射 $e: G_1 \times G_1 \to G_2$。

双线性对:若映射 e 满足下列三个性质则就是双线性对。

1)双线性 对任意 $P, Q \in G_1$, $a, b \in Z_q^*$ 有等式 $e(aP, bQ) = e(P, Q)^{ab}$ 成立。

2)退化性 对于 $\forall P \in G_1$,当且仅当 $Q \in G_1$ 且 $P = O$ 时,存在 $e(P, Q) = 1$ 成立。

3)可计算性 对于 $\forall P, Q \in G_1$, 都存在有效的算法计算 $e(P, Q)$。

本文提出的签密方案依赖于以下困难问题。

定义 1 对于任意 $a, b, c \in Z_q^*$,由 (P, aP, bP, cP) 计算 $e(P, P)^{abc}$ 就是 BDH 问题(这里并不知道具体的 a、b、c 的值)。注意:椭圆曲线中的 BDH 问题是数学领域公认的难题。目前大部分基于身份和对映射的密码学方案都是基于 BDH 难题假设。

2 基于身份的广义签密定义

本章描述基于身份的广义签密方案的算法组成及其安全

收稿日期: 2009-06-05; **修回日期**: 2009-07-06 **基金项目**: 国家火炬计划资助项目(国科发计[2008]658 号)

作者简介:张洪礼(1962-),男,黑龙江人,副教授,主要研究方向为信息安全(zisaimingzhu@126.com);赵静(1984-),女,硕士研究生,主要研究方向为密码学;刘文远(1968-),男,黑龙江密山人,教授,主要研究方向为电子商务、信息安全.

性概念。

2.1　基于身份的广义签密的算法组成

在基于身份的广义签密中存在三种模式,即签密、签名和加密。

定义 2　一个基于身份的广义签密由以下四个算法组成:

a)系统密钥的生成(setup)。由 PKG 完成,输入安全参数,密钥生成中心(PKG)输出主密钥 s 和系统参数 params。保密 s,公开 params。

b)用户私钥的生成(extract)。输入一个用户身份 ID_U 和主密钥 s,PKG 计算相应 ID_U 的私钥 S_U,并通过安全方式发送给这个用户。

c)广义签密(GSC)。该签密有三种可能模式,但每次广义签密只有一种模式发生。

(a)签密。若 Alice(ID_A)需要既机密又认证地发送一个消息 m 给 Bob(ID_B)。Alice 的输入需为(S_A,ID_B,m),广义签密算法生成密文 $\sigma = GSC(m, S_A, ID_B)$。

(b)签名。若 Alice 只需签名一个消息 m,则不需要特定的接收方 Bob 的信息。Alice 的输入为(S_A,$ID_\varnothing$,m),其中 $ID_\varnothing$ 为身份空的情况。广义签密算法生成密文 $\sigma = GSC(m, S_A^-, ID_\varnothing)$。此时的广义签密就相当于签名。

(c)加密。若某个用户只需要机密地向 Bob 发送消息 m,则无须知道 Alice 的信息。输入为($S_\varnothing$,ID_B,m)。其中 $S_\varnothing$ 表示用户的身份为 $ID_\varnothing$ 时对应的用户私钥。广义签密算法生成密文 $\sigma = GSC(S_\varnothing, ID_B, m)$,此时的广义签密就相当于加密。

c)解广义签密(DGSC)。无论是解签密、签名验证还是解密都会执行如下操作:

若密文 σ 是有效的密文,则 Bob 解签后返回消息 m、Alice 对 m 的签名,否则返回 $\perp$ 表示解签密失败。

注意:只有满足基于身份的广义签密方案的正确性验证,即当且仅当 $m = DGSC(\sigma, ID_A, S_B)$ 成立时才会有 $\sigma = GSC(m, S_A, ID_B)$ 是合法的密文。

2.2　安全性概念

根据攻击者是否包括执行协议的两方,又可分为内部安全和外部安全。当攻击者包括执行协议的两方时的安全性称为内部安全性,否则称为外部安全性,内部安全性更强[4]。本节所定义的安全性都是指内部安全性。

1)机密性　因为只有在加密模式和签密模式下才会涉及到机密性的概念,而签名模式则无须考虑机密性问题。所以广义签密机密性的攻击游戏和定义如下:

游戏(签密或加密)

初始化阶段

C 运行 setup(1^k)返回 params 给 A,保密 s。

游戏第一阶段如下:

a)签密(或加密)询问 A 提交一个签名者的身份、一个接收者的身份和消息(或只提交接收者的身份和消息)给 C,C 返回对消息的签密(或密文)。

b)解签密(或解密)询问 A 提交密文和接收者的身份给 C,C 用接收者的私钥解密;然后验证解密的结果与签名是不是合法的消息/签名对。若是则 C 返回明文消息、该消息的签名和签名者的身份,否则返回 $\perp$ 表示拒绝(或 A 提交密文和接收者的身份给 C,C 用接收者的私钥解密并返回明文消息)。

c)Extract 询问。A 提供一个身份 ID_U,C 返回相应的私钥 S_U 给 A。

d)A 输出两个身份$\{ID_A, ID_B\}$和两个消息$\{m_1, m_0\}$,A 不允许对 ID_B 进行 extract 询问。这里 $ID_B \neq ID_\varnothing$,否则考虑机密性就没有意义了。C 随机选取 $b \in \{0,1\}$。当 $ID_A \neq ID_\varnothing$ 时,C 计算 $\sigma = GSC(m_b, S_A, ID_B)$ 或当 $ID_A = ID_\varnothing$ 时,C 计算 $\sigma = GSC(m_b, S_\phi, ID_B)$,返回 σ 给 A。

游戏第二阶段如下:

(a)A 像第一阶段那样执行多项式有界次询问。但是不允许对 ID_B 进行 extract 询问,也不允许用 ID_B 对 σ 进行解签密询问。

最后阶段如下:

A 返回 b',若 $b' = b$ 则 A 获胜。

定义 3　令 A 表示进行上面游戏的攻击者,若 A 在攻击中的优势 $adv[A] = 2P_r[b = b'] - 1$ 是可忽略的,则称一个基于身份的广义签密方案是抗适应性选择密文攻击(IND-IBGSC-CCA2)安全的。

2)不可伪造性　因为只有在签名模式和签密模式下才会涉及到伪造性,机密模式时无须考虑伪造性。在内部安全性[4]的意义下,签密的伪造者为密文的接收者(Bob)和第三方攻击者,接收者知道自己的私钥,他具有最强的伪造能力。给定一个签密密文给接收者(Bob),它能够用自己的私钥解签密,对签密的伪造就是对签名的伪造。因此,广义签密的不可伪造性与签名的不可伪造性相同,即在签名模式中适应性攻击者(包括接收者)冒充发送方伪造一则签密文在计算上是不可行的,则称一个基于身份的广义签密方案满足不可伪造性。

攻击游戏

初始化　C 运行 setup(1^k)返回给 A。

询问 A　像定义 3 那样执行多项式有界次询问。

最后,A 输出一个新的三元组(σ^*,ID_A,ID_B)或(σ^*,ID_A,$ID_\varnothing$),且这个元组不是由签密预言机产生,也没有对 ID_A 执行 extract 询问。如果解广义签密(σ^*,ID_A,ID_B)或(σ^*,ID_A,$ID_\varnothing$)成功,则 A 赢得游戏。

定义 4　如果没有任何多项式有界的敌手以一个不可忽略的优势(A 获胜利的概率就是他的优势)赢得以上游戏,则称一个基于身份的广义签密方案在适应性选择消息攻击下不可伪造。

3)不可否认性　与 2)类似,如果在签名和签密模式下,发送方想要否认他曾发出的签密文时,第三方进行仲裁在计算上是可行的,则称一个基于身份的广义签密方案满足不可否认性。

3　基于身份的广义签密方案

根据定义 2 知基于身份的广义签密最关建的就是区分签密、签名、加密这三个模式。在基于身份的密码学中,签名消息需要特定的发送者的信息,加密消息需要特定的接收者的信息,签密消息则既要知道特定的发送者又要知道特定的接收者的信息。因此,协议双方的身份就可以用来区分这三种模式。当输入者的身份不存在时,令其公钥为 0 表示的二进制串来区分三个模式;采用异或加密方式来控制是否屏蔽加密功能。

方案的具体描述如下:

a)Setup。令G_1是阶为q的循环加法群,G_2是q阶循环乘法群,P是G_1的生成元。$e:G_1\times G_1\to G_2$为双线性映射。定义四个函数$H_1:\{0,1\}^*\to G_1$,$H_2:\{0,1\}^*\to Z_q$,$H_3:G_1\to Z_q$,$H_4:G_2\to\{0,1\}^n$为安全的hash函数,而且令$H_4(1)$输出的为n bit的0串。PKG随机选择一个主密钥$s\in Z_q^*$,计算密PKG的公钥$P_{pub}=sP$。$\{G_1,G_2,n,e,P,P_{pub},H_1,H_2,H_3,H_4\}$是PKG公开的系统参数,保密主密钥$s$。

b)Extract。给定一个用户U的ID_U,PKG计算U的私钥$S_U=sQ_U$。其中$Q_U=H_1(ID_U)$为U的公钥。在这里设Alice的身份为ID_A,公钥为Q_A,私钥为S_A。Bob的身份为ID_B,公钥为Q_B,私钥为S_B。对于签名或加密模型,由于接收者或者发送者不存在,令$ID_\varnothing$是与ID_U同样长度的0串,并令$ID_U=ID_\varnothing$,则有$S_U=S_\varnothing=O$,$Q_U=Q_\varnothing=O$。其中$Q_\varnothing$是用户身份为$ID_\varnothing$时对应的公钥。

c)广义签密。

(a)签密　输入(S_A,ID_B,m),为了发送一个消息给Bob,Alice执行

①随机选取$k\in Z_q^*$。

②计算,$R=kP$,$S=k^{-1}(H_2(m)\cdot P_{pub}+H_3(R)\cdot S_A)$。

③计算$w=e(P_{pub},Q_B)^k$和$c=H_4(w)\oplus m$。

④发送密文$\sigma=(c,R,S)$给Bob。

(b)签名　输入$(S_A,ID_\varnothing,m)$

①和②与签密相同。

③计算$w=e(P_{pub},Q_B)^k=e(P_{pub},O)^k=1$,然后计算$c=H_4(w)\oplus m=H_4(1)\oplus m=m$。

④发送密文$\sigma=(c,R,S)=(m,R,S)$给Bob。

(c)加密

①与签密相同。

②计算$R=kP$,$S=k^{-1}(H_2(m)\cdot P_{pub})$。

③和④与签密相同。

d)解广义签密。当收到密文σ时,Bob执行

①计算$w=e(R,S_B)$,恢复消息$m=c\oplus H_4(w)$。

②若等式$e(R,S)=e(P,P_{pub})^{H_2(m)}\cdot e(P_{pub},Q_A)^{H_3(R)}$成立,Bob接收这个消息,否则认为$\sigma$不合法。

广义签密方案的正确性验证:

$$\begin{aligned}e(R,S)&=e(kP,k^{-1}(H_2(m)\cdot P_{pub}+H_3(R)\cdot S_A))=\\&e(P,H_2(m)\cdot P_{pub}+H_3(R)\cdot S_A)=\\&e(P,H_2(m)\cdot P_{pub}+H_3(R)\cdot sQ_A)=\\&e(P,P_{pub})^{H_2(m)}\cdot e(P,sQ_A)^{H_3(R)}=\\&e(P,P_{pub})^{H_2(m)}\cdot e(P_{pub},Q_A)^{H_3R}\end{aligned}$$

4　安全性分析

1)机密性

定理1　在随机预言模型中,若存在一个IND-IBSC-CCA2攻击者A能够在t时间内,以ε的优势赢得定义1的游戏(A最多能进行q_i次H_i询问($i=1,2,3,4$),q_s次签密询问(或q_e次加密询问),q_u次解签密询问(或q_d次解密询问)),则存在一个区分者C,能够在$t'<t+(q_s+4\cdot q_u)\cdot t_e$或$t'<t+(q_e+4\cdot q_d)\cdot t_e$时间内,以$\varepsilon'>\varepsilon\cdot(1/q_1q_4)$的优势解决BDH问题。其中$t_e$表示计算一次双线性对运算所需要的时间。

证明　区分者接收随机的BDH问题实例(P,aP,bP,cP),它的目标是计算出$e(P,P)^{abc}$。区分者则扮演C的角色,把A作为子程序并扮演IND-IBSC-CCA2游戏中向C提出挑战的攻击者。游戏一开始,C发送系统参数给A。其中$P_{pub}=cP$(C并不知道c,c扮演PKG的主密钥)。C维护L_1、L_2、L_3、L_4、L_s或L_e、L_u或L_d六张列表,这些列表开始均为空,L_1,L_2,L_3,L_4分别用于跟踪A对预言机H_1、H_2、H_3、H_4的询问,L_s用于模拟签密预言机(或L_e于来模拟加密预言机),L_u用于模拟解签密预言机(或L_d用来模拟解密预言机)。这些列表的建立详细解释如下:

a)H_1询问。C首先从$\{1,2,\cdots,q_1\}$中选取一个随机数i_b。假设A不会作重复询问。对于A的第i次H_1询问,若$ID_U=ID_\varnothing$,C计算$Q_U=0$,$P=O$,$S_U=0$,$P_{pub}=O$,并添加$(ID_\varnothing,O,O,0)$到L_1中,回答$H_1(ID_\varnothing)=O$。若$i=i_b$,回答$H_1(ID_U)=bP$并设置$ID_b=ID_U$;否则从Z_q^*中随机选取x,计算$Q_U=xP$,$S_U=xP_{pub}$,并添加(ID_U,Q_U,S_U,x)到L_1中,回答$H_1(ID_U)=Q_U$。

b)H_2询问。若(m,h_2)在L_2中,返回h_2;否则从Z_q^*中随机选取h_2,添加(m,h_2)到L_2中,返回h_2。

c)H_3询问。若(R,h_3)在L_3中,返回h_3;否则从Z_q^*中随机选取h_3,添加(R,h_3)到L_3中,返回h_3。

d)H_4询问。若(w,h_4)在L_4中,返回h_4;若$w=1$,令h_4为0构成的二进制串,并添加(w,h_4)到L_4中;否则,从$\{0,1\}^n$中随机选取h_4,添加(w,h_4)到L_4中,返回h_4。

e)Extract询问。假设A在对执行extract询问前已经执行过H_1询问了。若$ID_U=ID_b$,终止模拟;否则在表L_1中查找ID_U对应的条目(ID_U,Q_U,S_U,x),返回S_U。

f)签密(或加密)询问。假设A在ID_1对ID_2和执行此询问前已经执行过H_1询问了。

①$ID_1\neq ID_b$

表L_1中查找到条目(ID_1,Q_1,S_1,x),然后从Z_q^*中随机选取k并计算$R=kP$。

计算$h_2=H_2(m)$　($H_2(m)$可以从上述的H_2询问获得)。

计算$h_3=H_3(R)$　$H_3(R)$(可以从上述的H_3询问获得)。

计算$S=k^{-1}(h_2P_{pub}+h_3S_1)$。

计算$Q_2=H_1(ID_2)$。

计算$w=e(P_{pub},Q_2)^k$。

计算$c=H_4(w)\oplus m$($H_4(w)$可从上述H_4询问获得)。

返回(c,R,S)。

②$ID_1=ID_b$

从Z_q^*中随机选取k并计算$R=kP_{pub}$。

计算$h_2=H_2(m)$　($H_2(m)$可以从上述的H_2询问获得)。

计算$h_3=H_3(R)$　($H_3(R)$可以从上述的H_3询问获得)。

计算$S=k^{-1}(h_2P+h_3bP)$,在表L_1中查找到条目(ID_2,Q_2,S_2,x),然后计算$w=e(R,S_2)$。

计算$c=H_4(w)\oplus m$($H_4(w)$可从上述H_4询问获得)。

返回(c,R,S)。

g)解签密(或解密)询问。输入(c,R,S),假设A在对ID_2执行此询问前已经执行过H_1询问了。

①$ID_2\neq ID_b$

在表L_1中查找到条目(ID_2,Q_2,S_2,x)。

计算$w=e(R,S_2)$。若$w\notin L_4$返回符号"$\perp$";

当为dec询问还需考虑:若$ID_1=ID_2$或$ID_1\notin L_1$,返回符号"$\perp$";否则在表L_1中查找到条目$(ID_\varnothing,O,O,0)$返回$Q_1=$

O。否则继续执行后面步骤。

计算 $m = c \oplus H_4(w)$。

若 $ID_1 = ID_2$ 或 $ID_1 \notin L_1$,返回符号“⊥”;否则计算 $Q_1 = H_1(ID_1)$。

若 $m \notin L_2$,返回符号“⊥”;否则计算 $h_2 = H_2(m)$。

若 $R \notin L_3$,返回符号“⊥”;否则计算 $h_3 = H_3(R)$。

若 $e(R,S) \neq e(P, P_{pub}^{h_2} \cdot e(P_{pub}, Q_1)^{h_3})$,则返回符号“⊥”;否则返回 m。

②$ID_2 = ID_b$

按以下的步骤遍历表 L_4 中的条目(w,h_4)。

当为解签密询问时还需考虑:若 $ID_1 = ID_b$,移到表 L_4 中的下一个条目并且重新开始。若 $ID_1 \in L_1$,找到 L_1 中的 Q_1 和;否则移到表 L_4 中的下一个条目且重新开始。否则继续执行后面步骤。

计算 $m = c \oplus H_4(w)$。

若 $m \in L_2$,计算 $h_2 = H_2(m)$;否则移到表 L_4 中的下一个条目且重新开始。

若 $R \in L_3$,计算 $h_3 = H_3(R)$;否则移到表 L_4 中的下一个条目且重新开始。

若 $e(R,S) = e(P, P_{pub})^{h_2} \cdot e(P_{pub}, Q_1)^{h_3}$ 成立,返回消息 m;否则移到表 L_4 中的下一个条目且重新开始。

若遍历完 L_4 中所有的条目还是没有消息返回,则返回符号“⊥”。

在经过多项式有界次上述询问后,A 输出两个希望挑战的身份$\{ID_A, ID_B\}$和两个消息$\{m_0, m_1\}$。若 $ID_B \neq ID_b$(或 $ID_B \neq ID_b$ 或者 $ID_A \neq ID_\varnothing$),C 终止这个模拟;否则随机选取 $S^* \in G_1$,$b \in \{0,1\}$,令 $R^* = aP$,w(w 从 H_4 中随机选取作为 BDH 问题的候选答案),计算 $c^* = m_b \oplus H_4(w)$,然后返回挑战密文 $\sigma^* = (c^*, R^*, S^*)$给 A。A 经过第二轮的询问,这些询问同第一轮相同。在第二阶段模拟结束时,A 输出一个 b'作为对 b 的猜测。若 $b' = b$,C 就能输出 $w = e(P,P)^{abc}$作为 BDH 问题的答案,即 C 解决了 BDH 问题;否则 C 没有解决 BDH 问题。

现在考虑第一阶段失败的情况:从 A 的角度来看,A 和 C 之间的询问与 A 和真正的预言机的询问如果出现不同,就说发生错误了。很显然,对 H_1、H_2、H_3 的模拟和真正的语言机是不可区分的。此时,对 H_4 的询问只是在 A 或 B 需要时才发生,所以对 H_4 的模拟也是和真正的随机预言机不可区分的。对签密询问的模拟是不可能失败的。最后是 extract 模拟。看一下 H_1 的模拟就会发现,A 选择一个 H_1 询问,并用一个待解决的 BDH 实例的群元素 bP 作为响应。在挑战中,模拟器身份是 A 选择作为接收者的身份的最小概率是 $1/q_1$。若不是这种情况,则就说错误发生在 extract 阶段。因为若 A 对身份进行 extract 时,模拟会终止。

第二阶段失败的情况:所有上述错误都可能发生,另外,若 A 对 $w = e(P,P)^{abc}$执行 H_4 询问那么 C 会失败。但是,若 A 有 ε 的优势攻击成功,则 A 就不能失败。那么 A 就必须对 $w = e(P,P)^{abc}$执行 H_4 询问。一旦 A 进行询问,L_4 中必会有足够的信息让 C 解决 BDH 问题。C 解决 BDH 问题的概率是 $1/q_4$。所以 C 成功解决 BDH 问题的概率最少为 $\varepsilon \cdot (1/q_4 q_1)$。证毕。

2)不可伪造性　本文的方案在适应性选择消息攻击下能抗存在性伪造。若一个敌手能伪造一个本文的签名,则他也能够伪造下面的一个签名方案,这个签名方案是 Paterson 方案[6]的一个变体。

a)签名。签名者随机选取 $k \in Z_q^*$,计算 $R = kP$ 和 $S = k^{-1}(H_2(m) \cdot P_{pub} + H_3(R) \cdot S_A)$。消息 m 的签名为 $\sigma = (R,S)$。

b)验证。当收到 m 的签名 σ 时,验证者检验 $e(R,S) = e(P, P_{pub})^{H_2(m)} \cdot e(P_{pub}, Q_A)^{H_3(R)}$是否成立,当且仅当该等式成立时接受此签名。由于 Paterson 方案在适应性选择消息攻击下能抗存在性伪造,本文的方案也同样能抗存在性伪造。

3)不可否认性　既然本文的方案是不可伪造的,若 Alice 确实签密过一个消息,他就不能够否认。

5　效率分析

由于对运算比乘法群中的指数运算、加法群中的标量成运算耗时的多,对基于双线性对的密码学方案来说,影响整个方案效率的主要因素就是对运算的使用个数,即不可与计算的对运算使用个数越少,效率越高。

表 1 给出了本文方案与目前存在的基于身份和双线性对的广义签密方案效率比较。用 e、m、p 分别表示G_2 中的指数运算个数、G_1 中的标量乘运算个数、对运算个数。

表 1　签密功能的性能比较

	文献[3]	本文方案
签名	$3m + p$	$4m$
验证	$m + 3p$	$2p$
加密	$2m + p$	$3m$
解密	$m + 3p$	$2p$
签密	$3m + p$	$e + 4m$
解签密	$m + 3p$	$2e + 2p$

通过比较可见本文提出的方案无论是用做签名方案、加密方案还是签密方案,效率都比较高。

6　结束语

本文基于 BDH 难题假设提出了目前效率最高的基于身份和对运算的广义签密方案,它满足内部安全性意义抗适应性选择攻击下的机密性、不可伪造性和不可否认性,减少了计算比较耗时的对运算的使用个数。但本文方案假设在 PKG 完全可信的情况下,对于如何防止不可信的 PKG 情况,还仍然是值得研究的问题。

参考文献:

[1] 韩益亮, 杨晓元. ECDSA 可公开验证广义签密[J]. 计算机学报, 2006,29(11):2003-2012.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Advances in Cryptology-CRYPTO'84. Berlin: Springer-Verlag, 1984:47-53.

[3] LAL S, KUSHWAH P. ID based generalized signcryption[R/OL]. (2008-08-04). http://eprint.iacr.org/.

[4] AN J H, DODIS Y, RABIN T. On the security of joint signature and encryption[C]//Advances in Cryptology EUROCRYPT'2002. Berlin:Springer-Verlag,2002:83-107.

[5] PATERSON K G. ID-based signatures from pairings on elliptic curves [J]. Electronics Letters,2002,38(18):1025-1026.

[6] ZHENG Y. Digital signcryption or how to achieve cost (signature&encryption cost(signature) + cost (encryption)[C]//Advances in Cryptology-CRYPTO'97. Berlin: Springer-Verlag,1997:165-179.