无可信中心的基于身份的广义签密

周才学

(九江学院信息科学与技术学院 九江 332005)

摘 要 广义签密可以只用一个算法实现加密、签名和签密3种功能。提出了无可信中心的基于身份的广义签密体制的形式化定义,并定义了其较为全面的安全模型,进而利用双线性对提出一个具体方案。在BDH和CDH困难问题假设下,证明了方案在随机预言机模型下的安全性。效率比较表明,方案是高效的。

关键词 广义签密,基于身份,无可信中心,双线性对,随机预言机模型

中图法分类号 TP309 **文献标识码** A

ID-based Generalized Signcryption without Trusted Party

ZHOU Cai-xue

(School of Information Science and Technology, University of Jiujiang, Jiujiang 332005, China)

Abstract GSC(Generalized signcryption) can realize encryption, signature and signcryption with only one algorithm. The formal definitions of identity based generalized signcryption without trusted party and the complete security model were proposed. A concrete scheme was presented by using the bilinear pairings. Its confidentiality and unforgeability were proved in ROM under BDH assumption and CDH assumption. Compared with other ID-based GSC schemes, the new scheme is also efficient.

Keywords Generalized signcryption, Identity-based, Without trusted party, Bilinear pairings, Random oracle model

1 引言

基于身份的公钥密码是Shamir[1]于1984年提出的,目的是简化公钥证书的管理。2001年Boneh和Franklin[2]利用椭圆曲线上的双线性对构造了第一个基于身份的加密方案。此后,基于身份的密码成为研究热点。但基于身份的密码体制天生就具有密钥托管的缺陷,为克服这种缺陷,人们提出了不同的解决方案。2003年,Al-Riyami和Paterson[3]提出了无证书公钥密码体制CLPKC(Certificateless Public Key Cryptography),成功地解决了密钥托管问题,但CLPKC一般只能达到Girault[4]所定义的Level 2安全性,即如果KGC(Key Generation Center)替换了用户的公钥,则CLPKC仍然存在密钥托管问题[5]。同年,陈晓峰等人[6]提出无可信中心的基于身份的密码方案,其也消除了密钥托管问题,而且能达到Girault[4]所定义的Level 3安全性,此后许多无可信中心方案被提出[7-10]。

签密是Zheng[11]于1997年提出的概念,它能在一个逻辑步骤内既加密又认证,其效率要高于"先签名后加密"的传统实现。在一些需要同时实现加密和认证的网络环境下,签密发挥了巨大的作用。然而,在某些应用中,当系统同时需要实现签密、加密和签名3种功能时,普通签密方案便失去其优势。Zheng建议将算法切换到另外的签名和加密算法,于是系统至少要实现3个方案才能满足要求,这势必会增加相应的计算和实现复杂性,特别对一些资源受限的环境如智能卡系统和无线传感器网络等会造成沉重的负担。为解决这种不足,韩益亮等人[12,13]于2006年提出了广义签密的概念,它能只用一个算法根据输入的不同实现3种功能:签密、加密和签名,从而简化了实现,非常适合于如电子邮件和资源受限的环境使用,比如无线多播网络[14]、Ad hoc网络[15]等。此后,出现了许多广义签密方案[16-22]。2008年,Lal和Kushwah[23]将广义签密的概念推广到基于身份的密码系统中,并提出一个具体方案。2010年,Yu Gang等人[24]给出了比以前安全模型更加完整的基于身份的广义签密安全模型,并指出在这种模型中[23]是不安全的。此后,Kushwah和Lal[25]又对文献[24]的安全模型进行了简化。

在无可信中心的基于身份的广义签密方面,赵静[26]首先提出一个方案。据我们所知,目前再无其它方案。实际上赵静的方案不是语义安全的,且其没有给出无可信中心的基于身份的广义签密的安全模型。本文参考杜红珍[5]的可追踪的基于身份的签名的安全模型、刘景伟[27]的基于ID的无证书签名方案的安全模型、文献[25]的基于身份的广义签密的安全模型,首次给出较全面的无可信中心的基于身份的广义签密的安全模型和形式化定义,并参考文献[28]提出一个具体方案。由于文献[29]指出文献[28]是不安全的,因此对文献[28]作了一些改进。方案达到了Girault[4]所定义的Level 3安全,在随机预言机模型中证明了方案的安全性,对方案的效率也进行了分析。

2 一些基本概念

2.1 双线性对

设G_1是素数q阶加法循环群,G_2是同阶乘法循环群。

到稿日期:2012-06-20 返修日期:2012-10-11

周才学(1966—),男,硕士,副教授,CCF会员,主要研究方向为密码学与网络信息安全,E-mail:charlesjjjx@126.com。

映射 $e:G_1\times G_1\to G_2$ 称作双线性对，如果该映射具有以下 3 个性质：

双线性性：对任意的 $P,Q\in G_1$，$a,b\in Z_q$，都有 $e(aP,bQ)=e(P,Q)^{ab}$；

非退化性：存在 $P,Q\in G_1$，满足 $e(P,Q)\neq 1_{G_2}$；

可计算性：对任意的 $P,Q\in G_1$，存在一个有效的算法计算 $e(P,Q)$。

2.2 困难问题

定义 1 对任意 $a,b,c\in Z_q^*$，由 (P,aP,bP,cP) 计算 $e(P,P)^{abc}$ 就是 BDH(Bilinear Diffie-Hellman)问题(这里并不知道具体的 a,b,c 的值)。

定义 2 在 G_1 中给定 (P,aP,bP)，$a,b\in Z_q$ 未知，要求计算 $abP\in G_1$ 就是 CDH(Computational Diffie-Hellman)问题。

3 无可信中心的基于身份的广义签密体制

3.1 定义

定义 3 一个无可信中心的基于 ID 的广义签密由 6 个算法构成：系统初始化、用户密钥生成、部分私钥解析、广义签密、解广义签密和追踪算法。

系统初始化(Setup)：一个全局初始化算法，以安全参数 1^k 为输入，输出一个主密钥 s 和系统全局参数 $Params$。该算法由 KGC 运行，保密 s，公开 $Params$。

用户密钥生成(User-Key-Generation)：该算法输入一个用户身份 ID 和公开参数 $Params$，输出一个秘密值 x_{ID} 和一个公钥 R。该算法由用户运行得到一个公钥和一个秘密值，该秘密值用于构造完整私钥。

部分私钥解析(Partial-Key-Extract)：该算法输入一个用户身份 ID、用户秘密值 x_{ID} 的使用期限 T、用户公钥 R、系统主密钥 s 和全局参数 $Params$，输出相应于该 ID 的部分私钥 D_{ID}。该算法由 KGC 运行，验证完用户身份后运行。

广义签密(GSC)：有 3 种可能模式，但每次只有一种模式发生(根据输入的身份是否为空)。

(a)签密。若 $ID_A\notin\phi$，$ID_B\notin\phi$，则对应签密模式。$\sigma=GSC(m,ID_A,ID_B)=signcrypt(m,ID_A,ID_B)$。

(b)签名。若 $ID_A\notin\phi$，$ID_B\in\phi$，则对应签名模式。$\sigma=GSC(m,ID_A,\phi)=sign(m,ID_A)$。

(c)加密。若 $ID_A\in\phi$，$ID_B\notin\phi$，则对应加密模式。$\sigma=GSC(m,\phi,ID_B)=encrypt(m,ID_B)$。

解广义签密(UGSC)：对应 3 种模式中的一种(根据输入的身份是否为空)。

(a)解签密。若 $ID_A\notin\phi$，$ID_B\notin\phi$，则对应解签密。m or $\perp=UGSC(\sigma,ID_A,ID_B)=unsigncrypt(\sigma,ID_A,ID_B)$。

(b)签名验证。若 $ID_A\notin\phi$，$ID_B\in\phi$，则对应签名验证。T or $\perp=UGSC(\sigma,ID_A,\phi)=verify(\sigma,ID_A)$。

(c)解密。若 $ID_A\in\phi$，$ID_B\notin\phi$，则对应解密。m or $\perp=UGSC(\sigma,\phi,ID_B)=decrypt(\sigma,ID_B)$。

追踪算法(Trace)：如果 KGC 用两个或两个以上的私钥来绑定同一个用户的 ID，从而伪造用户的广义签密，用户可以生成证据提交给仲裁者 TA，TA 通过检验证据可以判断 KGC 是否诚实。

3.2 安全模型

文献[24]定义了基于身份广义签密体制较为全面的安全模型，攻击者能得到 7 种预言机服务，即 Extract、Sign、Verify、Encrypt、Decrypt、Signcrypt、Unsigncrypt。文献[25]对其进行了简化。本文对文献[25]稍作修改，再参考杜红珍[5]的可追踪的基于身份的签名的安全模型、刘景伟[27]的基于 ID 的无证书签名方案的安全模型，定义了无可信中心的基于身份的广义签密体制的安全模型。

在一个无可信中心的基于身份的广义签密方案中，KGC 可能扮演 3 种角色。

1)可信的：KGC 是诚实的，不会与他人合谋；

2)消极不诚实：KGC 有可能将用户的部分私钥泄漏给敌手；

3)积极不诚实：KGC 伪造用户的秘密值，从而用两个或两个以上的私钥来绑定一个用户的 ID，然后泄漏给敌手。

根据 KGC 的行为，定义 3 种类型的敌手。

类型 I：敌手没有用户的部分私钥，但可以知道用户的秘密值。

类型 II：敌手知道用户的部分私钥，但没有用户的秘密值。

类型 III：敌手有用户秘密值及部分私钥，但该秘密值是 KGC 伪造的，与用户真正的秘密值不同。

注意，在机密性游戏中只需考虑广义签密在签密和加密模式下的情形，在不可伪造性游戏中，只需考虑签密和签名模式下的情形。

定义 4 一个无可信中心的基于身份的广义签密体制，在加密或签密模式下，被称作是抗适应性选择密文和身份攻击安全的(IND-IDGSC-CCA2)，如果不存在任何多项式有界的攻击者(类型 I 或 II)以不可忽略的概率赢得下面定义的游戏：

游戏 1

初始化：挑战者 C 运行 Setup(1^k)，生成系统公开参数 $params$ 和主密钥 s。返回 $params$ 给 A，如果 A 是类型 II 攻击者，则另外返回 s 给 A。

阶段 1 攻击者 A 适应性地进行至多多项式有界次的以下询问：

(a)部分私钥解析询问(仅适用于类型 I 攻击者)：输入身份 ID，预言机返回相应的部分私钥 D_{ID}。

(b)秘密值解析询问：对 ID 的秘密值的访问，C 返回 x_{ID} 给 A。

(c)公钥询问：输入身份 ID，预言机返回相应公钥。

(d)广义签密询问。输入 (m,ID_A,ID_B)，预言机返回对消息 m 的广义签密 σ。这里，ID_A 或 ID_B 可以为空。如果 ID_A 为空，则相当于加密预言机；如果 ID_B 为空，则是签名预言机；如果都不空，则是签密预言机。

(e)解广义签密询问。输入 (σ,ID_A,ID_B)，预言机解广义签密，返回 m 或 $\perp$。这里，ID_A 或 ID_B 可以为空。如果 ID_A 为空，则是解密预言机；如果 ID_B 为空，则是签名验证预言机，如果都不空，则是解签密预言机。

挑战阶段：A 输出两个身份 $\{ID_A^*,ID_B^*\}$ 和两个等长不同消息 $\{m_0,m_1\}$，要求 $ID_B^*\notin\phi$(否则无意义)。C 随机取 $b\in\{0,1\}$，计算 $\sigma^*=GSC(m_b,ID_A^*,ID_B^*)$ 并返回给 A。

阶段 2 A 继续适应性地进行像阶段 1 中的多项式有界次的询问，但不允许用 ID_A^* 和 ID_B^* 对 σ^* 进行解广义签密询

问。

最后 A 返回对 b 的猜测 b'，若 $b=b'$ 且满足以下条件，则 A 获胜。A 在攻击中的优势定义为 $Adv[A]=|2\Pr[b=b']-1|$。

对类型 I 敌手，不能对 ID_B^* 作部分私钥解析询问；对类型 II 敌手，不能对 ID_B^* 作秘密值解析询问。

以上挑战阶段 ID_A^* 如果为空，对应加密模式；ID_A^* 不空，对应签密模式。所以加密和签密模式共用同一个游戏。

定义 5 一个基于身份的广义签密体制，在签密或签名模式下，被称作是在适应性选择消息和身份攻击下不可伪造的(UF-IDGSC-CMA)，如果不存在任何多项式有界的攻击者(类型 I 或 II)以不可忽略的概率赢得如下定义的游戏：

游戏 2

初始化阶段和阶段 1：同游戏 1。

伪造：最后，A 输出一个新的三元组 $(\sigma^*, ID_A^*, ID_B^*)$，要求 $ID_A^* \notin \phi$(否则无意义)且该三元组不是由广义签密预言机产生，如果解广义签密 σ^*, ID_A^*, ID_B^* 不是失败，且满足以下条件，则 A 赢得游戏。

对类型 I 敌手，不能对 ID_A^* 作部分私钥解析询问；对类型 II 敌手，ID_A^* 没有经过秘密值解析询问。

以上伪造阶段 ID_B^* 如果为空，对应签名模式；ID_B^* 不空，对应签密模式。所以签名和签密模式共用同一个游戏。

4 具体方案

Setup：设 G_1 为由 P 生成的循环加法群，阶为 q，G_2 为具有相同阶的循环乘法群，$e: G_1 \times G_1 \to G_2$ 为一个双线性映射。定义 4 个安全的散列函数 $H_1: \{0,1\}^* \times G_1 \to G_1$，$H_2: \{0,1\}^* \to \{0,1\}^{n+k_1}$，$H_3: \{0,1\}^* \to G_1$，$H_4: \{0,1\}^* \to G_1$，其中 n、k_1 分别是消息比特长度和 G_1 中元素比特长度。密钥生成中心 KGC 随机选择一个主密钥 $s \in Z_q^*$，计算 $P_{Pub}=sP$，保密 s。系统公开参数 $\{G_1, G_2, e, q, P, P_{Pub}, H_1, H_2, H_3, H_4\}$。定义一个特殊函数 $f(ID)$。当 $ID \in \phi$，$f(ID)=0$；else $f(ID)=1$。

User-Key-Generation：用户选取一个随机数 $x \in Z_q^*$ 作为秘密值，计算 $R=xP$ 作为公钥。

Partial-Key-Extract：用户把公钥 R、x 的使用期限 T 和他的身份 ID 送给 KGC。KGC 验证其身份后，计算 $Q_{ID}=H_1(ID \| T, R)$ 并公开，计算 $D_{ID}=sQ_{ID}$，将 D_{ID} 通过一个安全信道送给用户。这样用户的公钥是 $\{R, Q_{ID}\}$，私钥是 $\{x, D_{ID}\}$。如果 $ID \in \phi$，则公钥是 $\{\vartheta, \vartheta\}$，私钥是 $\{0, \vartheta\}$，ϑ 代表 G_1 中的无穷远点。

$GSC(m, ID_S, ID_R)$：

(1)计算 $f(ID_S)$，$f(ID_R)$，如果都为 0，则无意义并终止；

(2)随机选取 $r \in Z_q^*$，计算 $U=rP$；

(3)计算 $H=H_3(U, m, ID_R)$；

(4)计算 $H'=H_4(U, m, ID_R)$；

(5)计算 $S=f(ID_S)D_S+rH+f(ID_S)x_S H'$；

(6)计算 $w=e(P_{Pub}, Q_R)^{r f(ID_R)}$；

(7)计算 $h=f(ID_R)H_2(U, w, rR_R, ID_S, ID_R)$；

(8)计算 $V=m \| S \oplus h$；

(9)输出 $\sigma=(U, V)$

$UGSC(U, V, ID_S, ID_R)$：

(1)计算 $f(ID_S)$，$f(ID_R)$，如果都为 0，则无意义并终止；

(2)计算 $w'=e(U, D_R)^{f(ID_R)}$；

(3)计算 $h'=f(ID_R)H_2(U, w', x_R U, ID_S, ID_R)$；

(4)计算 $m \| S=V \oplus h'$；

(5)计算 $H=H_3(U, m, ID_R)$；

(6)计算 $H'=H_4(U, m, ID_R)$；

(7)判断 $e(P_{Pub}, Q_S)^{f(ID_S)} e(U, H) e(R_S, H')^{f(ID_S)}=e(P, S)$ 是否成立，成立则返回 m，否则返回 $\perp$。

Trace：若某广义签密能在声称是 A 的另外一对公钥 $\{R', Q'_{ID}\}$ 下通过验证，则 A 可以提供证据给仲裁方 TA，以证明是主密钥 s 泄漏或是 KGC 不诚实。首先，A 把公钥 R 递交给 TA，然后证明 A 知道对应的部分私钥 $D_{ID}=sH_1(ID \| T, R)$。证明如下：TA 选取一个随机数 $a \in Z_q^*$，把 aP 给 A，A 计算 $S=e(D_{ID}, aP)$ 并将 S 发给 TA，TA 计算 $e(aQ_{ID}, P_{Pub})$ 是否等于 S，若成立，则 TA 可以判定是系统主密钥 s 泄漏或是 KGC 不诚实，因为身份 ID 同时对应了两对公钥 $\{R, Q_{ID}\}$ 和 $\{R', Q'_{ID}\}$，而主密钥 s 只有 KGC 知道。

说明：

(1)如果 $ID_S \notin \phi$，$ID_R \in \phi$，算法工作于签名模式：这时 $f(ID_R)=0$，$h=0$，$V=m \| S \oplus h=m \| S$，所以最后发送的密文 $\sigma=(U, V)=(U, m \| S)$，即 (U, S) 为 m 的签名。

(2)如果 $ID_S \in \varphi$，$ID_R \notin \phi$，算法工作于加密模式：这时 $f(ID_S)=0$，$S=rH$，验证等式变成 $e(U, H)=e(P, S)$。

(3)如果 $ID_S \notin \varphi$，$ID_R \notin \phi$，算法工作于签密模式：这时 $f(ID_S)=1$，$f(ID_R)=1$。

5 方案分析

5.1 安全性分析

限于篇幅，本文只给出定理 1 的安全性证明。

定理 1 在随机预言机模型中，在加密模式或签密模式下，若存在一个 PPT 敌手 A(类型 I 攻击者)以不可忽略的优势 ε 攻击本文方案的 IND-IDGSC-CCA 安全，则存在一个算法 B 利用 A 以以下优势解决 BDH 问题：

$$\varepsilon' > (\varepsilon / q_{T1} q_{T2})(1 - q_{GSC}(q_{GSC} + q_{UGSC} + q_3 + 1)/2^k)(1 - q_{UGSC}/2^k)$$

其中 $q_{T1}=q_1+q_E+2q_{GSC}+2q_{UGSC}+2$，$q_{T2}=q_2+q_{GSC}+q_{UGSC}$。$q_1$、$q_2$、$q_3$、$q_E$、$q_{GSC}$ 和 q_{UGSC} 分别表示攻击者能进行的对 H_1、H_2、H_3、部分私钥解析、广义签密和解广义签密的最大询问次数。

证明：当收到 BDH 挑战元组 (Γ, aP, bP, cP) 时，P 是生成元，算法 B 设置 $P_{Pub}=aP$。B 随机选取 ID_l $(1 \leqslant l \leqslant q_{T1})$ 作为挑战身份。

(a)H_1 询问。输入是 (ID, R, T)，如果 L_1 中已经包含元组 (ID, R, T, y) 或 $(ID, R, T, -)$，则返回 yP 或 bP；否则，如果 $ID=ID_l$，把 $(ID, R, T, -)$ 加入 L_1 并返回 bP；否则，B 随机取 $y \in Z_q^*$，返回 yP，并把 (ID, R, T, y) 加到 L_1 中。

(b)H_2 询问。如果 L_2 中已经包含元组 (U, w, R, ID_A, ID_B, h)，则返回该 h；否则 B 返回一个随机的 h，并把元组 (U, w, R, ID_A, ID_B, h) 加入 L_2。

(c)H_3 询问。如果 L_3 中已经包含元组 (U, m, ID_R, t, tP)，则返回 tP；否则 B 生成一个随机的值 $t \in Z_q^*$，把 (U, m, ID_R, t, tP) 加入 L_3，返回 tP。

(d)H_4 询问。如果 L_4 中已经包含元组 $(U, m, ID_R, t', t'P)$，则返回 $t'P$；否则 B 生成一个随机的值 $t' \in Z_q^*$，把 $(U,$

$m, ID_R, t', t'P$)加入 L_4，返回 $t'P$。

(e)公钥询问。输入是 ID，如果 L_{PK} 中已经包含元组 (ID,R,x)，则返回 R；否则 B 随机选取 $x\in Z_q^*$ 作为 A 的秘密值，计算 $R=xP$，把 (ID,R,x) 加入 L_{PK} 并返回 R。

(f)部分私钥解析询问。输入是 ID，如果 $ID=ID_l$，B 失败并终止模拟；否则 B 调出 L_1 中的元组 (ID,R,T,y)，返回 $D=yaP$(如果 L_1 中不含该元组，则先作 H_1 询问，以后类似情况作相同处理，不再另作说明)。

(g)秘密值解析询问。输入是 ID，如果 L_{PK} 中已经包含元组 (ID,R,x)，则返回 x；否则 B 随机选取 $x\in Z_q^*$ 作为 A 的秘密值，计算 $R=xP$，把 (ID,R,x) 加入 L_{PK} 并返回 x。

(h)广义签密询问。对每一个新的元组 (m, ID_S, ID_R) 的询问，若 $ID_S\in\phi$，$ID_R\notin\phi$，对应加密，只需公开参数，所以 B 只需简单地按正常方式进行加密。以下考虑 $ID_S\notin\phi$，分两种情况：

Case1　$ID_S\neq ID_l$。由于可以得到两个私钥，因此 B 只需简单地按正常方式进行广义签密。

Case2　$ID_S=ID_l$。B 随机选取 $u,v\in Z_q^*$，设置 $U=vaP, H=v^{-1}(uP-bP)$，把 $(U,m,ID_R,\perp,H)$ 加入 L_3，如果 L_3 中已经包含该元组，则失败并终止模拟；否则，B 在 L_4 中查找元组 $(U,m,ID_R,t',t'P)$ 得到 t'，在 L_{PK} 中查找 ID_S 得到 R_S，计算 $S=uaP+t'R_S$。在 L_1 中查找 ID_R 得到 y_R，在 L_{PK} 中查找 ID_R 得到 x_R，计算 $w=e(U,y_RP_{pub}), R=x_RU$。在 L_2 中查找元组 (U,w,R,ID_S,ID_R,h)，用该 h 计算 $V=(m\parallel S)\oplus(f(ID_R)h)$。最后，返回 $\sigma=(U,V)$。注意，这是一个正确的广义签密，因为 $S=D_S+rH+x_SH'=abP+vav^{-1}(uP-bP)+x_St'P=uaP+t'R_S$。

(I)解广义签密询问。对每一个新的元组 (U,V,ID_S,ID_R) 的询问，若 $ID_S\notin\phi$，$ID_R\in\phi$，对应签名验证，只需公开参数，B 按正常方式进行。以下考虑 $ID_R\notin\phi$，分两种情况：

Case1　$ID_R\neq ID_l$。由于可以得到 ID_R 的完整私钥，B 按正常方式完成解广义签密。

Case2　$ID_R=ID_l$。B 遍历 L_2 中的所有含 ID_l 的元组 (U,w,R,ID_S,ID_l,h)，使用 h 计算 $m\parallel S=V\oplus h$，然后判断验证等式 $e(P_{Pub},Q_S)^{f(ID_S)}e(U,H)e(R_S,H')^{f(ID_S)}=e(P,S)$ 是否成立，其中 H、H'、Q_S 和 R_S 都可从相应询问获得，成立则返回 m，否则移到 L_2 中下一条目重新开始。如果遍历完 L_2 中的条目没有消息返回，则返回 $\perp$。

最终，A 输出两个等长的不同消息 (m_0,m_1) 和两个身份 ID_S^* 和 ID_R^*。若 $ID_R^*\neq ID_l$，B 失败并终止模拟；否则 B 如下处理。设置 $U^*=cP$，随机取 $V^*\in\{0,1\}^{n+k_1}$，提交挑战密文 $\sigma^*=(U^*,V^*)$ 给 A。

第二阶段，这些询问与第一阶段相同，对 A 的限制同游戏 1。最终，A 输出他的猜测。A 不知道 $\sigma^*=(U^*,V^*)$ 不是一个正确的密文，除非 A 用挑战元组 $(U^*,w^*,R^*,ID_S^*,ID_l)$ 询问 H_2。如果这种情况发生，由于 $w^*=e(P_{pub},Q_R^*)^r=e(aP,bP)^c=e(P,P)^{abc}$，则 BDH 问题的候选答案将被保存在 L_2 中，B 忽略 A 的猜测，随机从 L_2 中选择一个 w^* 作为 BDH 问题的答案，B 从这可以成功解决 BDH 问题。下面分析 B 成功的概率，由于 L_1 中最多含有 q_{T1} 个元素，因此 ID_l 被选为挑战身份的概率为 $1/q_{T1}$。B 随机从 L_2 中选择 w^* 作为 BDH 问题的解，正确的概率是 $1/q_{T2}$。在广义签密阶段，L_3 冲突 B 将失败，由于 L_3 最大值为 $q_{GSC}+q_{UGSC}+q_3+1$，冲突的概率为 $q_{GSC}(q_{GSC}+q_{UGSC}+q_3+1)/2^k$；解广义签密阶段，$B$ 拒绝有效密文的概率小于 $q_{UGSC}/2^k$。

在挑战阶段，ID_S^* 可以为空，如果 ID_S^* 为空，则对应加密模式；如果 ID_S^* 不为空，则对应签密模式。所以加密模式和签密模式共用同一个游戏。

定理 2　在随机预言机模型中，在加密模式或签密模式下，若存在一个 PPT 敌手 A(类型 II 攻击者)以不可忽略的优势 ε 攻击本文方案的 IND-IDGSC-CCA 安全，则存在一个算法 B 利用 A 以以下优势解决 CDH 问题：

$$\varepsilon'>(\varepsilon/q_{T1})(1-q_{GSC}(q_{GSC}+q_{UGSC}+q_3+1)/2^k)(1-q_{UGSC}/2^k)$$

其中 $q_{T1}=q_1+2q_{GSC}+2q_{UGSC}+2$。$q_1$、$q_3$、$q_{GSC}$ 和 q_{UGSC} 的表示同前。

定理 3　在随机预言机模型中，在签名或签密模式下，若存在一个 PPT 敌手 A(类型 I 攻击者)以不可忽略的优势 ε 攻击本文方案的 UF-IDGSC-CMA 安全，则存在一个算法 B 利用 A 以以下优势解决 CDH 问题：

$$\varepsilon'>(\varepsilon/q_{T1})(1-(q_{GSC}(q_{GSC}+q_{UGSC}+q_3+1)+2)/2^k)(1-q_{UGSC}/2^k)$$

其中 $q_{T1}=q_1+q_E+2q_{GSC}+2q_{UGSC}+1$。$q_1$、$q_3$、$q_E$、$q_{GSC}$ 和 q_{UGSC} 的表示同前。

定理 4　在随机预言机模型中，在签名或签密模式下，若存在一个 PPT 敌手 A(类型 II 攻击者)以不可忽略的优势 ε 攻击本文方案的 UF-IDGSC-CMA 安全，则存在一个算法 B 利用 A 以以下优势解决 CDH 问题：

$$\varepsilon'>(\varepsilon/q_{T1})(1-(q_{GSC}(q_{GSC}+q_{UGSC}+q_3+1)+2)/2^k)(1-q_{UGSC}/2^k)$$

其中 $q_{T1}=q_1+2q_{GSC}+2q_{UGSC}+1$。$q_1$、$q_3$、$q_{GSC}$ 和 q_{UGSC} 的表示同前。

定理 5　如果 KGC(类型 III 攻击者)冒充某个合法用户伪造了广义签密，该用户能向仲裁者证明 KGC 是不诚实的。

定理 5 的证明类似本文方案的 Trace 算法。

5.2　效率分析

计算开销和密文长度是影响效率的两个主要方面。在计算开销方面，主要考虑双线性对运算、G_1 中的点乘运算和 G_2 中的指数运算。表 1 列出本方案与其它方案的比较。其中 P 表示对运算(括号表示可以预计算)，E 表示指数运算，M 表示点乘运算。可以看出，本文方案的密文长度最短，方案是高效的。

表 1　与其它基于身份的广义签密方案的比较

方案	密文长度	加密、签名			解密、验证		
		E	M	P	E	M	P
方案[15]	$2\|G_1\\|+\|m\|+\|ID\|$	0	5	1	0	1	3
方案[23]	$2\|G_1\\|+\|m\|+\|ID\|$	0	4	1	0	1	3
方案[24]	$2\|G_1\\|+\|m\|+\|ID\|$	1	3	0(+1)	2	0	2(+2)
方案[25]	$2\|G_1\\|+\|m\|+\|ID\|+\|G_2\|$	2	3	0	1	2	2
方案[26]	$2\|G_1\\|+\|m\|+2\|q\|$	1	2	0(+1)	1	0	3(+1)
本方案	$2\|G_1\\|+\|m\|$	1	4	0(+1)	0	1	4(+1)

结束语　结合无可信中心和基于身份的广义签密的概念，本文首次给出了无可信中心的基于身份的广义签密方案的形式化定义及安全模型，并给出一个具体方案，在随机预言机中证明了方案的安全性。效率比较表明，方案是高效的。

广义签密在一般签密方案能同时提供机密性和认证性的基础上，可以只实现机密性或认证性一种功能，在节约时间和成本的基础上满足了不同的需求环境，因而具有更广泛的应用前景。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceeding of Crypto'84, LNCS196. Berlin: Springer-Verlag, 1984: 47-53

[2] Boneh D, Frankklin M. Identity Based Encryption From the Weil Pairing [C] // Proceeding of Crypto' 01, LNCS2139. Berlin: Springer-Verlag, 2001: 213-229

[3] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C]// Proceeding of ASIACRYPT 2003, LNCS2894. Berlin: Springer-Verlag, 2003: 452-473

[4] Girault M. Self-certified public keys[C]// Proceeding of Eurocrypt '91, LNCS547. Berlin: Springer-Verlag, 1991: 490-497

[5] 杜红珍. 数字签名技术的若干问题研究[D]. 北京：北京邮电大学，2009

[6] Chen Xiao-feng, Zhang Fang-guo, Kim K. A New ID-based Group Signature Scheme from Bilinear Pairings [C] // Proceedings of WISA'03. 2003: 585-592

[7] Liao Jian, Xiao Jun-fang, Qi Ying-hao, et al. ID-based signature scheme without trusted PKG [C] // Proceeding of CISC 2005, LNCS3822. Berlin: Springer-Verlag, 2005: 53-62

[8] 周亮，李大鹏，杨义先. 基于身份的无需可信任 PKG 的签名方案[J]. 通信学报，2008，29(6)：8-12

[9] Liu Jing-wei, Sun Rong, Kou Wei-dong, et al. Efficient ID-based Signature Without Trusted PKG[EB/OL]. http://eprint.iacr.org /2007/135, 2007-04-17

[10] 徐玲玲. 基于身份的无可信 PKG 的签名体制[D]. 济南：山东大学，2008

[11] Zheng Yu-liang. Digital signcryption or how to achieve cost (signature & encryption)<<cost (signature)+cost (encryption) [C] // Proceeding of Crypto' 97, LNCS1294. Berlin: Springer-Verlag, 1997: 165-179

[12] 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

[13] Han Yi-liang. Generalization of signcryption for resources-constrained environments[J]. Wireless Communication and Mobile Computing, 2007, 7(7): 919-931

[14] Han Yi-liang, Gui Xiao-lin. Adaptive secure multicast in wireless networks[J]. International Journal of Communication Systems, 2009, 22(9): 1213-1239

[15] 魏靓，张串绒，郑连清. 基于广义签密的移动 Ad hoc 网络密钥管理方案[J]. 计算机工程与应用，2010，46(32)：6-9

[16] 杨晓元，李秀广，郝斌，等. 基于广义签密和 DWT 技术的图像水印算法[J]. 计算机工程与应用，2007，43(36)：86-88

[17] Yang Xiao-yuan, Li Mao-tang, Wei Li-xian, et al. New ECDSA-Verifiable Multi-Receiver Generalization Signcryption [C]// The 10th IEEE International Conference on High Performance Computing and Communications. 2008: 1042-1047

[18] Han Yi-liang, Gui Xiao-lin. BPGSC: Bilinear pairing based generalized signcryption scheme[C]// 2009 Eighth International Conference on Grid and Cooperative Computing. 2009: 76-82

[19] 杨晓元，黎茂堂，魏立线. ECDSA 可公开验证广播签密[J]. 解放军理工大学学报：自然科学版，2009，10(4)：324-328

[20] Zhang Chuan-rong, Zhang Yu-qing. Secure and Efficient Generalized Signcryption Scheme Based on a Short ECDSA[C]// Proc of IIH-MSP'2010. 2010: 466-469

[21] 冀会芳，韩文报，刘连东. 标准模型下多个 PKG 的基于身份广义签密[J]. 电子与信息学报，2011，33(5)：1204-1210

[22] 冀会芳，韩文报，刘连东. 高效的无证书广义签密方案[J]. 四川大学学报：工程科学版，2011，43(5)：133-139

[23] Lai S, Kushwah P. ID-based generalized signcryption[EB/OL]. http://eprint.iacr.org/2008/084, 2008-02-26

[24] Yu Gang, Ma Xiao-xiao, Shen Yong, et al. Provable secure identity based generalized signcryption scheme[J]. Theoretical Computer Science, 2010, 411(40-42): 3614 -3624

[25] Kushwah P, Lai S. An efficient identity based generalized signcryption scheme[J]. Theoretical Computer Science, 2011, 412 (45): 6382-6389

[26] 赵静. 高效的基于身份和对映射的广义签密方案的研究[D]. 秦皇岛：燕山大学，2010

[27] 刘景伟，孙蓉，马文平. 高效的基于 ID 的无证书签名方案[J]. 通信学报，2008，29(2)：87- 94

[28] Barbosa M, Farshim P. Certificateless signcryption[C]// ACM Symposium on Information, Computer and Communications Security-ASIACCS 2008. ACM, 2008: 369-372

[29] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing[EB/OL]. http://eprint.iacr.org/2009/298, 2009-06-22

(上接第 110 页)

[3] Topcuoglu H, Hariri S, Wu M Y. Performance-effective and low-complexity task scheduling for heterogeneous computing[J]. IEEE Trans. Parallel and Distributed Systems, 2002, 13(3): 260-274

[4] Kwok Y-K, Ahmad I. Dynamic Critical-Path Scheduling: An Effective Technique for Allocating Task Graphs to Multiprocessors[J]. Parallel and Distributed Systems, 1996(7): 506-521

[5] Darbha S, Agrawal D P. Optimal Scheduling Algorithm for Distributed-Memory Machines[J]. IEEE Trans. Parallel and Distributed Systems, 1998, 9(1): 87-95

[6] Liu Zhen-ying, Fang Bin-xing, Zhang Yi. TSA-OT, An Algorithm Scheduling An Out-Tree DAG[J]. Chinese Journal of Computers, 2001, 24(4): 1-5

[7] 张建军，李庆华，瞿勇. 基于任务复制的调度算法[J]. 计算机工程与设计，2009，30(8)：1896-1899

[8] Omara F A, Arafa M M. Genetic Algorithms for Task Scheduling Problem[J]. Journal of Parallel and Distributed Computing, 2010, 70(1): 13-22

[9] Zhong Yi-wen, Yang Jian-gang, Qia Heng-nian. Hybrid Genetic Algorithm for Tasks Scheduling in Heterogeneous Computing Systems[C]// Proceedings of the Third International Conference on Machine Learning and Cybernetics. Shanghai. 2004(8): 26-29

[10] Darbha S, Agrawal D P. A task duplication based scalable scheduling algorithm for distributed memory systems[J]. Journal of parallel and Distributed Computing, 1997, 46(1): 15-27

[11] Yang Jia-dong, Xu Hua, Jia Pei-fa. Task Scheduling for Heterogeneous Computing based on Bayesian Optimization Algorithm [C]// 2009 International Conference on Computational Intelligence and Security. 2009: 112-117