基于身份的新型广播签密方案

孙 瑾[1,2] 胡予濮[2]
(西安理工大学理学院数学系 西安 710048)[1]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[2]

摘 要 为了适应当前信息传输环境的多样性及多变性,保证传输信息的机密性及权威性,通过借鉴签密方案的优势并结合广播加密模型,提出一种新的身份型广播签密方案。该方案使用哈希运算、环和运算、双线性对运算等多种运算形式,使得新方案中公、私钥长度保持不变,密文长度等于接收用户的个数加1,签密过程与解签密过程均无需双线性对运算,因此具有较低的运算代价及存储代价。详细的安全性证明显示该方案的机密性可归约为弱的BCDH问题,不可伪造性可归约为PSG签名问题,从而使该方案能应用于安全性和实用性要求较高的环境。

关键词 签密,广播签密,基于身份的密码,可证明安全
中图法分类号 TN918.1 **文献标识码** A

Novel Identity Based Broadcast Signcryption Scheme

SUN Jin[1,2] HU Yu-pu[2]
(Department of Application Mathematics, Xi'an University of Technology, Xi'an 710048, China)[1]
(Key Lab of Computer Network and Information Security, Xidian University, Xi'an 710071, China)[2]

Abstract A novel identity based broadcast signcryption scheme was proposed to satisfy the diversity and changeability of the current data transmission environment, and guarantee the confidentiality and authority of the transferred information using the integration of the broadcast encryption, the identity-based cryptography and the signcryption. By means of this scheme, taking the various arithmetic operation such as hash, ring add and bilinear pairing et al., the size of ciphertext is equal to the number of the receiver adding one, and the size of public or private key keeps constant. Simultaneously, the process of signcryption or unsigncryption needs not bilinear pairing operation with high computational cost and storage cost. The detailed proof of security shows that the proposed scheme is not only to be IDN-CCA2 secure under the weak BCDH problem but also to be existentially unforgeable under the EF-ACMA of PSG proposed by Paterson. Furthermore, the proposed scheme is efficient and practical at performance.

Keywords Signcryption, Broadcast signcryption, Identity based cryptography, Provably secure

信息安全研究的一个重要目标就是使消息既保密又认证地传输,能实现这一目标的传统方法是"先签名后加密"或"先加密后签名",它们所需的代价是签名和加密的代价之和,因而效率很低。为了提高效率,Zheng[1]于1997年最先提出签密的概念,它能够在一个逻辑步骤内同时完成签名和加密两项功能,而又保持了较低的计算成本与通信成本。2002年,Baek等[2]给出了规范的签密安全模型的定义。

基于身份的密码系统是1984年由Shamir[3]提出的,其用户的公钥就是他们的身份,而私钥由密钥生成中心(KGC)生成,这样可以很好地解决密钥托管问题;并可以适应更为多样的环境。2002年,第一个基于身份的签密方案由Malone-Lee[4]提出,他还给出了基于身份的签密方案的安全模型,并利用双线性对构造了第一个基于身份的签密方案。Malone-Lee的模型能处理消息的保密性和签名的不可伪造性,随后一系列的基于身份的签密方案[5-10]相继被提出。

广播加密的概念最先由Fiat和Naor提出[11],它应用于将密文发给一组用户的场合。在广播加密系统中,其核心思想是广播者将消息加密通过广播方式发送给大量用户,其中只有拥有授权的合法用户才可以解密并获得真实信息。目前,这种加密方式已成为密码学的一个新研究热点。国内外学者纷纷涉猎于此,很多具有特殊用途的广播加密方案也相继被提出[12-15]。但是,这些方案存在明显的不足,比如,基于的困难问题太强,仅具有Selective-ID安全性或安全性依赖于随机预言机模型等,而此处方法的众多,正表明大家没有形成统一的认识。

在一个群组团队中,当任何一个成员想通过安全渠道给另一部分成员发送消息时,广播方式成为一种重要形式,然而当每个人都可以充当广播者的角色时,待发送的消息及广播者本身的权威性与不可伪造性都会随之提高要求。考虑到上述问题,本文提出一种新的身份型广播签密方案,并给出详细的安全性证明。新方案的机密性可归约为弱的BCDH问题,不可伪造性可归约为PSG[16]签名问题,同时方案的公/私钥

到稿日期:2012-04-02 返修日期:2012-07-11 本文受国家自然科学基金项目(60970119),陕西省教育厅自然科学基金项目(11JK0505)资助。
孙 瑾(1977-),女,博士,讲师,主要研究方向为公钥广播加密方案的设计与分析,E-mail:oksunjin@xaut.edu.cn;胡予濮(1955-),男,博士,教授。

长度保持恒定，双线性运算均可以预计算，不参与签密与解签密过程，因而具有较低的计算代价与存储代价，可运用于效率及安全性要求较高的环境。

1 身份型广播签密的形式化定义及其安全模型

1.1 预备知识

1.1.1 双线性映射

设 G,G_T 是两个素数 p 阶的循环乘法群，g 是 G 的一个生成元，a,b 是 Z_p^* 中的元素。双线性映射 $e(\cdot,\cdot)$ 是 $e:G\times G\to G_T$ 并满足以下性质：

(1)双线性性：$\forall g,h\in G$，$e(g^a,h^b)=e(g,h)^{ab}$。

(2)非退化性：$\exists g,h\in G$，使得 $e(g,h)\neq 1$。

(3)可计算性：$\forall g,h\in G$，存在有效算法计算 $e(g,h)$。

双线性对可以通过有限域上的超奇异椭圆曲线或超奇异超椭圆曲线中的 Weil 对或 Tate 对推导出来[5]。

1.1.2 弱的计算双线性 Diffie-Hellman 问题(weak BCDH)

设$(G_1,+)$和$(G_2,\cdot)$是两个素数 q 阶循环群，p 是 G_1 的一个生成元，$\hat{e}:G_1\times G_1\to G_2$ 是一个双线性对。对于 $a,b,c\in Z_q^*$，给定$(P,aP,bP,cP,\frac{1}{c}P)$，计算$\hat{e}(P,P)^{abc}$是弱的计算双线性 Diffie-Hellman 问题。

1.2 身份型广播签密的形式化定义

基于身份的广播签密方案(IDBSC)允许广播者安全地以广播方式发送消息给授权的用户集合。一个身份型广播签密方案由以下几个算法组成：

系统建立：输入安全参数 λ，输出系统参数 *params* 和密钥生成中心 KGC 的主私钥 *msk*。通常这个算法由 KGC 执行，然后 KGC 公开系统参数 *params* 而秘密保存主私钥 *msk*。

密钥提取：输入系统参数 *params* 及用户身份 $ID\in\{0,1\}^n$，KGC 利用其产生相应的公/私钥对(pk,sk)。

签密(IDBSC)：输入系统参数 *params*、消息 M、发送者的身份 ID_S 及其公/私钥对(pk_S,sk_S)、接收者的身份集合$\{ID_R\}$，其中 $R=\{R_1,R_2,\cdots,R_h\}$及其公钥 PK_{R_i}；输出密文 σ 或者无效符号$\perp$。

解签密(IDBUC)：设接收者 ID_i 是诚实用户，其私钥是 SK_{R_i}，输入系统参数 *params*、密文 σ、发送者身份 ID_S 及其公钥 PK_S、接收者私钥 SK_{R_i}；输出明文 M 或者无效符号$\perp$。

1.3 身份型广播签密的安全模型

Malone-Lee[4] 曾经给出了基于身份的签密方案的安全模型的定义，其安全要求包括：抗适应性选择密文攻击的不可区分性及抗适应性选择消息攻击的不可伪造性。下面仿照它给出身份型广播签密方案的安全模型的定义。

1.3.1 机密性(Confidentiality)

如果不存在多项式时间的敌手以不可忽略的优势完成下列游戏，身份型广播签密方案的机密性即是指适应性选择密文攻击下的密文不可区分性(IND-IDSCMP-CCA2)。设游戏在敌手 A 和挑战者 $\mathcal{R}$ 之间进行，算法如下：

初始化：输入安全参数 λ，挑战者 $\mathcal{R}$ 运行系统建立算法，获得公共参数 *params* 和主私钥 *msk*，随后将 *params* 发送给敌手 A，主私钥 *msk* 自己保存。

阶段 1　敌手 A 适应性提出质询 $q_1,\cdots,q_{n_0}$，每次质询依赖于以前询问的结果。

* 密钥提取质询：敌手 A 询问用户 ID 的密钥，挑战者 $\mathcal{R}$ 计算身份 ID 的公/私钥对(pk,sk)并将其返回给 A。

* 签密质询：当 A 提交发送者身份 ID_S，接收者身份集合 $ID_R(R=\{R_1,\cdots,R_h\})$和消息 M 的签密询问时，挑战者 $\mathcal{R}$ 对消息 M、发送者的私钥 sk_S 和接收者的公钥 pk_R 运行签密算法，并返回所得到的密文 σ。

* 解签密质询：当 A 提交密文 σ、发送者身份 ID_S、接收者身份 ID_R 的解签密询问时，挑战者 $\mathcal{R}$ 对密文 σ、接收者的私钥 sk_R 和发送者的公钥 pk_S 运行解签密算法，并返回相应的结果。

挑战：当敌手 A 决定阶段 1 结束时，选择两个不同的身份$\{ID_S,ID_R\}$和两个等长的消息$\{M_0,M_1\}$，然后挑战者随机选取 $b\in\{0,1\}$，计算 $\sigma^*=Signcrypt(params,M_b,sk_S,ID_R,pk_{R^*})$，并把 σ^* 发送给敌手 A。其中 pk_{R^*} 是挑战者身份 ID_R^* 的公钥。

阶段 2　敌手继续进行询问 $q_{n_0+1},\cdots,q_n$，每一次询问类似于阶段 1。

猜测：最后敌手要输出猜测 γ'。如果 $\gamma=\gamma'$，并满足以下条件，则宣布敌手在游戏中获胜：

(1)A 在任何阶段不能询问挑战者身份 ID_R^* 的私钥。

(2)在第 2 阶段，A 不能询问挑战密文 σ^* 在身份 ID_S^*，ID_R^* 和公钥 pk_{R^*} 下的解签密结果。

定义敌手 A 的优势为：

$$Adv_A^{IND\text{-}CCA2}=2\Pr[b=b']-1$$

定义 1　若不存在多项式时间绑定的敌手 A 以不可忽略的优势赢得上述游戏，则称 IDBSC 方案具有适应性选择密文攻击下的密文不可区分性(IND-IDSCMP-CCA2)。

1.3.2 不可伪造性(Authority)

下面的游戏在敌手 A 与挑战者 $\mathcal{R}$ 之间进行，用来证明身份型广播签密方案的不可伪造性，即适应性选择消息攻击下的存在不可伪造性。交互游戏如下：

初始化：输入安全参数 λ，挑战者 $\mathcal{R}$ 运行系统建立算法获得公共参数 *params* 和主私钥 *msk*，随后将 *params* 发给敌手 A，主私钥 *msk* 自己保存。

质询：敌手 A 选择身份 ID^* 作为挑战对象。然后 A 和机密性游戏中的第二步一样，适应性做多项式有界次质询。包括密钥提取质询、签密质询和解签密质询。

伪造：最后，敌手 A 根据发送者身份 ID_s 和接收者身份 ID_R^* $(R=\{R_1,\cdots,R_h\})$生成一个三维数组(ID_s^*,ID_R^*,σ^*)。需要注意的是，此结果并非来自于游戏环节中的质询过程，ID_s 的私钥也不能公开。如果解签密$(\sigma^*,ID_S^*,pk_{S^*},sk_{R^*})$的结果不是符号$\perp$，且没有询问 ID_{S^*} 的私钥，则敌手 A 赢得上述游戏。

敌手 A 成功的概率 $Succ_A$ 定义为他赢得上述游戏的概率。

定义 2　若不存在多项式时间绑定的敌手 A 以不可忽略的优势赢得上述游戏，则称 IDBSC 方案是不可伪造的，即具有适应性选择消息攻击下的存在性不可伪造性。

2 新的身份型广播签密方案

2.1 方案构造

本节根据文献[7,10]提出一种新的基于身份的广播签密

方案。本方案不需要额外的计算设备(如安全的 MAC 方程),公/私钥长度不变,密文长度仅为接收者集合的长度。方案涉及三方:密钥生成中心 KGC,发送者 ID_S,接收者 ID_R。设所有 $ID\in\{0,1\}^n$,具体算法如下:

系统建立:给定安全参数 1^k,设$(G_1,+)$和$(G_2,\cdot)$是两个素数 q 阶循环群,P 是 G_1 的一个生成元。双线性映射 $\hat{e}$:$G_1\times G_1\to G_2$,目标抗碰撞哈希函数:$H_1:\{0,1\}^{n_1}\to G_1^*$;$H_2:G_2\to\{0,1\}^{n_2}\times\{0,1\}^{n_1}\times G_1^*$;$H_3:\{0,1\}^{n_2}\times\{0,1\}^{n_1}\times\{0,1\}^{hn_1}\to Z_q^*$;$H_4:\{0,1\}^{n_2}\times G_1\to Z_q^*$。其中 n_1 和 n_2 分别表示用户身份和消息的比特长度,H_1,H_2 需要满足一个附加条件:$H_1(0)=\vartheta$,$H_2(1)=0$(其中 ϑ 表示 G_1 中的有限元素)。随后,KGC 随机选择 $s\in Z_q^*$ 作为他的主密钥,并计算 $K_{Pub}=sP$ 作为其公钥。则完整的公共参数为:

$(params,K_{Pub})=\{G_1,G_2,q,n_1,n_2,\hat{e},P,K_{Pub},H_1,H_2,H_3,H_4\}$

密钥提取:设用户集合为$\{ID_i\mid i=1,\cdots,m\}$,$m$ 是最大的用户个数。对于用户 ID_i,其公钥仅为身份的一个简单变形,即 $pk_i=H_1(ID_i)$,而私钥为 $sk_i=s\cdot pk_i$。

签密(IDBSC):发送者 ID_S 为了发送消息 M 给 ID_R,其中 $R=\{R_1,R_2,\cdots,R_h\}$,$h\leqslant m$,执行以下步骤计算:

(1)随机选择 $r\in Z_q^*$,并计算 $X=rP$。

(2)计算 $h_3=H_3(M\parallel ID_s\parallel ID_{R_i})(i=1,\cdots,h)$及 $h_4=H_4(M\parallel X)$。

(3)计算 $V=r^{-1}(h_3P+h_4\cdot sk_s)$。

(4)计算 $pk_{R_i}=H_1(ID_{R_i})$及 $w_i=\hat{e}(K_{Pub},pk_{R_i})^r$。

(5)计算 $h_{2,i}=H_2(w_i)$及 $y_i=M\parallel ID_s\parallel V\oplus h_{2,i}(i=1,\cdots,h)$。

(6)发送密文$(X,y_1,\cdots,y_h)$给 ID_R,其中 $R=\{R_1,R_2,\cdots,R_h\}$。

解签密(IDBUC):收到密文$(X,y_1,\cdots,y_h)$后,接受者 ID_{R_i} 解签密过程如下:

(1)计算 $w_i=\hat{e}(X,sk_{R_i})$,$y_i\oplus h_{2,i}=M\parallel ID_s\parallel V$。

(2)检验 $\hat{e}(X,V)=\hat{e}(p,p)^{h_3}\cdot\hat{e}(K_{Pub},pk_s)^{h_4}$,若不满足,返回符号$\perp$;否则返回消息 M。

2.2 正确性

设$(X,y_1,\cdots,y_h)$是合法的密文,则先计算 $w_i=\hat{e}(X,sk_{R_i})=\hat{e}(rP,sH_1(ID_{R_i}))=\hat{e}(sP,H_1(ID_{R_i}))^r=\hat{e}(K_{Pub},pk_{R_i})^r$,并同时通过计算 $y_i\oplus h_{2,i}=y_i\oplus H_2(w_i)=M\parallel ID_s\parallel V$ 析出 V;然后就很容易验证:

$$\begin{aligned}\hat{e}(X,V)&=\hat{e}(rP,r^{-1}(h_3P+h_4\cdot sk_s))\\&=\hat{e}(P,(h_3P+h_4\cdot s\cdot pk_s))\\&=\hat{e}(P,P)^{h_3}\cdot\hat{e}(P,s\cdot pk_s)^{h_4}\\&=\hat{e}(P,P)^{h_3}\cdot\hat{e}(K_{Pub},pk_s)^{h_4}\end{aligned}$$

而消息 M 就可以从 $y_i\oplus h_{2,i}=y_i\oplus H_2(w_i)=M\parallel ID_s\parallel V$ 中直接提取。

2.3 效率分析

目前的签密方案虽然在同时满足机密性与权威性的基础上效率有所提高,但仍然存在一些问题,如基于的困难问题太强,仅达到 Selective-ID 安全性,选择明文安全,计算与传输代价大等。本文提出的新的身份型签密方案中签密算法、解签密算法均不需要双线性对运算,其中的双线性对运算都可以预计算;解密算法中先验证密文是否有效,合法后返回解密明文,仅需 2 次乘幂运算。虽然方案的密文长度随接受者个数改变,但其依赖于弱的 BCDH 假设可以证明是 IDN-CCA2 安全的,同时依赖于 PSG[16] 签名问题是 EUF-CMA 安全的,具有较高的安全性和实用性。

表 1 将新方案在计算复杂度上与几个著名的签密方案进行了对比。其中符号 mul.,cps. 和 exps. 分别表示乘法运算、双线性对运算和乘幂运算次数,能够被预计算的次数用符号(?)表示。

表 1 新方案与其它方案的计算复杂度对比

方案	签密			解签密/验证		
	mul. in G_1	$\hat{e}$ cps.	exps. in G_2	mul. in G_1	$\hat{e}$ cps.	exps. in G_2
[9]	2	0(2)	0	1	4	0
[10]	3	0(1)	0	1	3	0
[7]	5	0(1)	0	1	3(1)	0
IDBSC	3	0(1)	1	0	2(2)	2

3 安全性分析

本节将陈述新方案的安全性证明过程。其中假设敌手针对 H_i 做 $q_i(i=1,2,3,4)$次质询,q_s,q_u 分别表示敌手所做的签密和解签密质询的次数,n_3,n_4 分别表示 G_1 和 G_2 中元素的比特长度。

定理 1 若敌手 A 能以 $Adv_A^{ef\text{-}acma}(t,p)$的优势成功伪造有效的广播签密(IDBSC)密文,则存在挑战者 $\mathcal{R}$ 能以优势 ξ 伪造有效的 PSG[16] 签名:

$$\xi\geqslant Adv_A^{ef\text{-}acma\text{-}idbsc\text{-}in\text{-}sc}(t,p)+(q_2\cdot q_s)/2^{n_4}+q_u/(2^{n_2}\cdot 2^{2n_1}\cdot 2^{n_3})$$

证明:为了将 IDBSC 方案中的不可伪造性 EF-ACMA 归约为 PSG[16] 签名的不可伪造性 EF-ACMA,定义两个实验:Exp 1 和 Exp 2,其中公/私钥及神谕币的抛掷空间均保持不变,而两个实验的不同在于挑战者提供给敌手的预言机服务规则的不同。

Exp 1

在此试验中,新方案所采用的标准技术是模拟 Hash 方程。众所周知,敌手是不能区分多项式绑定时间环境与真实环境的。设 S_0 表示 EF-ACMA 敌手在 Exp 1 中能够成功地攻击 IDBSC 方案的事件。挑战者 $\mathcal{R}$ 需要创建 4 个初始状态为空的列表 $L_i(i=1,2,3,4)$用来记录相应的哈希 $H_i(i=1,2,3,4)$质询的回答。

初始化:挑战者 $\mathcal{R}$ 首先扮演 KGC 的角色,并运行算法 Setup 1^k 生成完整的公共系统参数$(params,K_{Pub})$及主私钥 s,而后发送$(params,K_{Pub})$给敌手 A。

模拟:下面详细描述挑战者是如何模拟各种不同的质询的:

· $H_1(ID_i)$质询:若记录(ID_i,pk_i,sk_i)在列表 L_1 中,则直接返回 pk_i。否则挑战者 $\mathcal{R}$ 随机选择 $pk_i\in G_1^*$,并计算 $sk_i=s\cdot pk_i$,而后返回 pk_i,并将结果(ID_i,pk_i,sk_i)加入列表 L_1。

· $H_2(w_i)$质询:若记录$(w_i,h_{2,i})$在列表 L_2 中,则返回值 $h_{2,i}$;否则 $\mathcal{R}$ 随机选择 $h_{2,i}\in\{0,1\}^{n_2}\times\{0,1\}^{n_1}\times G_1^*$,并将$(w_i,$

$h_{2,i}$)加入列表 L_2，同时返回 $h_{2,i}$。

• $H_3(M \| ID_s \| ID_{R_i})$质询：挑战者 $\mathcal{R}$ 在列表 L_3 中寻找记录$(M \| ID_s \| ID_{R_i}, h_3)$，若找到则返回 h_3；否则其随机选择 $h_3 \in Z_q^*$，并将$(M \| ID_s \| ID_{R_i}, h_3)$加入列表 L_3，同时返回值 h_3。

• $H_4(M \| X)$质询：挑战者 $\mathcal{R}$ 在列表 L_4 中寻找记录$(M \| X, h_4)$，若找到则返回 h_4；否则其随机选择 $h_4 \in Z_q^*$，并将$(M \| X, h_4)$加入列表 L_4，同时返回值 h_4。

• Extract(ID_i)质询：假设敌手在 Extract(ID_i)质询前已经做过 $H_1(ID_i)$质询。挑战者 $\mathcal{R}$ 在列表 L_1 中寻找对应身份 ID_i 的记录(ID_i, pk_i, sk_i)并返回 sk_i。

• $IDBSC(ID_s, ID_{R_i}, M)$，$IDBUC(ID_s, ID_{R_i}, \delta)$质询：由于所有发送者 ID_s 的公私钥和接受者的公私钥均能被挑战者获取，因此挑战者能够为敌手提供此项质询，其中的哈希方程均使用上述哈希质询后的回答。

Exp 2

在此试验中，签密方案将被归约为 PSG 方案。其中在系统建立阶段，挑战者初始化系统同 Exp 1。模拟阶段，除下面质询外，其他质询同 Expl。

• $IDBSC(ID_s, ID_{R_i}, M)$质询：此阶段中，列表 L_s 将被提供给挑战者来记录敌手提出的质询。

(1)选择唯一的 $r \in Z_q^*$，并计算值 $X=rP$。

(2)计算 $h_3=H_3(M \| ID_s \| ID_{R_i})(i=1,\cdots,h)$，$h_4=H_4(M \| X)$和 $V=r^{-1}(h_3 P+h_4 \cdot sk_s)$。

(3)随机选取 $h_{2,i} \in \{0,1\}^{n_2} \times \{0,1\}^{n_1} \times G_1^*$ 并将$(*, h_{2,i})$ 加入列表 L_2。注意：第一个元素为空，将来会被赋值。

(4)计算 $y_i=M \| ID_s \| V \oplus h_{2,i}$，并将$(X, y_i, V, ID_s, ID_{R_i}, M)$加入列表 L_s，其中 $i=1,\cdots,h$。

(5)输出密文$(X, y_1, \cdots, y_h)$，其中 h_3，h_4 取自相应的哈希质询。

• $GBUC(ID_s, ID_{R_i}, \delta)$质询：

(1)(a)在列表 L_3 中寻找$(* \| ID_s \| ID_{R_i}, *)$，若记录$(M \| ID_s \| ID_{R_i}, h_3)$存在则进入下一步骤，否则返回符号$\perp$。

(b)在列表 L_4 中寻找$(M \| *, *)$，若记录$(M \| X, h_4)$存在则进入下一步骤，否则返回符号$\perp$。

(c)在列表 L_s 中寻找$(X, *, *, ID_s, ID_{R_i}, M)$，若记录$(X, y_i, V, ID_s, ID_{R_i}, M)$存在则进入下一步骤，否则返回错误符号$\perp$。

(2)计算 $w_i=\hat{e}(X, sk_{R_i})$及 $h_{2,i}=y_i \oplus M \| ID_s \| V$。

(3)检验$\hat{e}(X, V)=\hat{e}(p, p)^{h_3} \cdot \hat{e}(K_{Pub}, pk_s)^{h_4}$，若不满足，则返回错误符号$\perp$。

(4)在列表 L_2 中寻找$(*, h_{2,i})$，若记录被找到，则将第一元素定义为 w_i 并返回 M，否则输出错误符号$\perp$。

现在讨论 Exp 1 和 Exp 2 的不同之处。下列情形发生时，敌手可以分辨 Exp 1 和 Exp 2 。首先，在签密质询中，如果敌手 A 已经质询过 $H_2(w_i)$，且其中 w_i 恰好为空值，则此种情形发生的可能性最多为 $q_2/2^{n_4}$。敌手总共做 q_s 次签密质询，所以此种情形发生的可能性最多为 $q_2 \cdot q_s/2^{n_4}$。其次，如果敌手在解签密阶段已经猜出一些密文所对应的明文，则此类情形发生的可能性最多为 $1/2^{n_2} \cdot 2^{2n_1} \cdot 2^{n_3}$，而敌手在解签密质询阶段总共做 q_u 次解签密质询，所以上述情形发生的可能性最多为 $q_u/2^{n_2} \cdot 2^{2n_1} \cdot 2^{n_3}$。

设 S_1 表示敌手能够成功攻击 Exp 2。那么可以得到：

$$|\Pr(S_0)-P_r(S_1)| \leqslant q_2 \cdot q_s/2^{n_4}+q_u/2^{n_2} \cdot 2^{2n_1} \cdot 2^{n_3}$$

定理 2 若存在 IND-IDBSC-CCA2 敌手 A 能够以优势 $Adv_{A^{idbsc\text{-}in\text{-}en}}^{ind\text{-}cca2}(t,p)$成功地攻破 IDBSC 方案，则存在挑战者 $\mathcal{R}$ 能在多项式时间内以优势 ξ 解决弱的 BCDH 问题：$\xi \geqslant Adv_{A^{idsc\text{-}in\text{-}sc}}^{ind\text{-}cca2}(t,p)/(q_1 \cdot q_2)$。

证明 假设存在一个 IND-CCA2 敌手 A 能够攻击本广播签密方案，则利用 A 可以构造一个算法来解决弱的 BCDH 问题。设$(P, aP, bP, cP, \frac{1}{c}P)$是一个待解决的弱的 BCDH 问题的数组。首先，$\mathcal{R}$ 运行 Setup(1^k)算法来生成系统参数 $params$。尽管他不知道主密钥，但 $\mathcal{R}$ 仍可以设定公钥形如 $K_{Pub}=sP$，并发送$(params, K_{Pub})$给敌手 A。

为了记录签密质询的回答，挑战者 $\mathcal{R}$ 除了持有 4 个列表 $L_i(i=1,2,3,4)$外，还需要另外持有一个列表 L_s。

阶段 1

• $H_1(ID_i)$质询：挑战者 $\mathcal{R}$ 先随机选择唯一的 $i_b \in 1,\cdots q_1$，此处假设 A 不能进行重复质询。如果 $i=i_b$，$\mathcal{R}$ 就返回 $H_1(ID_i)=bP$ 并设置 $ID_i=ID_b$。否则挑战者 $\mathcal{R}$ 随机选取唯一的 $k \in Z_q^*$ 并计算 $pk_i=k \cdot P=kP$，$sk_i=k \cdot K_{Pub}$。最后，他存储(ID_i, pk_i, sk_i, k)到 L_1 并返回 pk_i。

• $H_2(w_i)$质询、$H_3(M \| ID_s \| ID_{R_i})$质询、$H_4(M \| X)$质询与定理 3 证明的内容一致。

• Extract(ID_i)质询：假设敌手在 Extract(ID_i)质询前已经做过 $H_1(ID_i)$质询。如果 $ID_i=ID_b$，则 $\mathcal{R}$ 停止质询；否则，对于 ID_i，挑战者 $\mathcal{R}$ 在 L_1 中寻找入口(ID_i, pk_i, sk_i, k)并返回 sk_i。

• $Signcrypt(ID_s, ID_{R_i}, M)$质询：在这一环节，假设敌手在 $Signcrypt(ID_s, ID_{R_i}, M)$质询前已经做过 $H_1(ID_s)$和 $H_1(ID_{R_i})$质询。

场景 1 $ID_i \neq ID_b$

(1)在列表 L_1 中寻找入口(ID_s, pk_s, sk_s, k)。

(2)唯一选择 $r \in Z_q^*$，并计算 $X=rP$。

(3)计算 $h_3=H_3(M \| ID_s \| ID_{R_i})$，$h_4=H_4(M \| X)$ 及 $V=r^{-1}(h_3 P+h_4 \cdot sk_s)$。

(4)计算 $pk_{R_i}=H_1(ID_{R_i})$，$w_i=\hat{e}(K_{Pub}, pk_{R_i})^r(i=1,\cdots,h)$，$h_{2,i}=H_2(w_i)$，$y_i=M \| ID_s \| V \oplus h_{2,i}$。

(5)输出$(X, y_1, \cdots, y_h)(H_i, i=1,2,3,4$ 来自于上述质询)。

场景 2 $ID_i=ID_b$

(1)在列表 L_1 中寻找入口$(ID_{R_i}, pk_{R_i}, sk_{R_i}, k)$。

(2)唯一选择 $r \in Z_q^*$，并计算 $X=rK_{Pub}$。

(3)计算 $h_3=H_3(M \| ID_s \| ID_{R_i})$，$h_4=H_4(M \| X)$ 及 $V=r^{-1}(h_3 \cdot \frac{1}{c}P+h_4 \cdot bP)$。

(4)计算 $w_i=\hat{e}(X, sk_{R_i})$，$h_{2,i}=H_2(w_i)$ 及 $y_i=M \| ID_s \| V \oplus h_{2,i}$。

(5)输出$(X, y_1, \cdots, y_h)(H_i, i=2,3,4$ 来自于上述质询)。

• $Unsigncrypt(ID_s, ID_{R_i}, \varepsilon)$质询：

场景 1 $ID_{R_i} \neq ID_b$

(1)在列表 L_1 中寻找入口$(ID_{R_i}, pk_{R_i}, sk_{R_i}, k)$。

(2)(a)计算 $w_i=\hat{e}(X,sk_{R_i})$，$h_{2,i}=H_2(w_i)$。如果$(w_i,h_{2,i})\notin L_2$，则返回$\perp$；否则计算 $M\|ID_s\|V=y_i\oplus h_{2,i}$。

(b)计算 $h_3=H_3(M\|ID_s\|ID_{R_i})$，如果 $(M\|ID_s\|ID_{R_i},h_3)\notin L_3$，则返回$\perp$。

(c)计算 $h_4=H_4(M\|X)$，如果$(M\|X,h_4)\notin L_4$，则返回$\perp$。

(d)如果 $ID_s=ID_{R_i}$ 或者 $ID_s\notin L_1$，则返回$\perp$；否则计算 $pk_s=H_2(ID_s)$。

(3)检验方程$\hat{e}(X,V)=\hat{e}(P,P)^{h_3}\cdot\hat{e}(K_{Pub},pk_s)^{h_4}$，若不满足，则返回$\perp$；否则返回 M。

场景 2　$ID_{R_i}=ID_b$

通过列表 L_2 中的入口$(w_i,h_{2,i})$进行如下操作：

(1)计算 $M\|ID_s\|V=y_i\oplus h_{2,i}$。

(a) 若 $ID_s=ID_{R_i}$ 或 $ID_s\notin L_1$，则移至列表 L_1 中下一入口并重新开始，否则计算 $pk_s=H_1(ID_s)$。

(b) 若$(M\|ID_s\|ID_{R_i})\in L_3$，则计算 $h_3=H_3(M\|ID_s\|ID_{R_i})$；否则移至列表 L_2 中下一入口并重新开始。

(c) 若 $M\|X\in L_4$，则计算 $h_4=H_4(M\|X)$；否则移至列表 L_2 中下一入口并重新开始。

(2)检验等式$\hat{e}(X,V)=\hat{e}(P,P)^{h_3}\cdot\hat{e}(K_{Pub},pk_s)^{h_4}$，若满足，则返回 M；否则移至列表 L_2 中下一入口并重新开始。

结束 L_2 中的所有步骤后若仍无消息被返回，则返回错误符号$\perp$。

挑战：当 A 决定阶段 1 结束时，提交以下数据：两个不同的身份 ID_s 和 ID_{R_i}，两个等长的消息 M_1 和 M_2。如果 $ID_{R_i}=ID_b$，则停止游戏；否则挑战者对于任意的 $a\in Z_q^*$ 设定 $X^*=aP$，然后随机选取 $\gamma\in\{0,1\}$，$y^*\in\{0,1\}^{n_2}\times\{0,1\}^{n_1}\times G_1^*$，并最终返回 $\delta^*=(X^*,y^*)$给 A 作为挑战密文。

阶段 2　敌手 A 继续进行类似于阶段 1 的询问，唯一的限制是 A 不能在 ID_{R^*} 下进行密钥提取询问，也不能在目标密文 δ^* 下进行解签密质询。

猜测：一旦阶段 2 结束，敌手 A 就输出一个比特 γ'。如果 $\gamma'=\gamma$，则挑战者 $\mathcal{R}$ 输出回答：$w^*=\hat{e}(X^*,sk_{R_i})=\hat{e}(P,P)^{abc}$。此时就暗示挑战者已经成功地解决了弱的 BCDH 问题。

我们来分析一下模拟可能成功的可能性，请注意两个模拟：(1)在挑战阶段，模拟者期望敌手选择 ID_b 作为目标接收身份，这种情形发生的可能性最多为 $1/q_1$。否则当敌手做密钥提取质询 $Extract(ID_b)$时就会出错。(2)在阶段 2 中，若敌手做质询 $H_2(w=\hat{e}(P,P)^{abc})$，则模拟将会失败。不过挑战者可能通过列表 L_2 以 $1/q_2$ 的可能性猜测出弱的 BCDH 问题回答。综上所述，可以推断挑战者最多可以以概率 $Adv_{A^{idbsc\text{-}in\text{-}sc}}^{ind\text{-}cca2}(t,p)/(q_1\cdot q_2)$解决弱的 BCDH 问题。

结束语　考虑到目前安全环境的多样性与多变性，广播加密方案已不能够仅局限在固定广播者与多个接收者之间的信息交互上，而是要求任何人均可以安全地广播消息给一群用户，这样就提高了对方案的权威性与不可否认性要求。基于这些问题，本文提出一种新的身份型广播签密方案，并给出了详细的安全性证明，结果表明，该方案不仅同时具备机密性和不可伪造性特征，而且具有较低的计算代价与传输代价，可运用于安全性要求较高的环境。

参 考 文 献

[1] Zheng Y. Digital signcryption or How to Achieve Cost (Signature Encryption)≤Cost (Signature)+ Cost (Encryption) [C]// CRYPTO'97. LNCS1294, Berlin: Springer-Verlag, 1997: 165-179

[2] Baek J, Steinfeld R, Zheng Y. Formal proofs for the security of signcryption [C]// Public Key Cryp- tography-PKC 2002. LNCS 2274, Berlin: Springer-Verlag, 2002: 80-98

[3] Shamir A. Identity-based cryptosystems and signature schemes [C]// CRYPTO' 84. LNCS 196, Springer-Verlag, 1984: 47-53

[4] Malone-Lee J. Identity Based Signcryption [R]. Report 2002/098. Cryptology e-Print Archive, 2002

[5] Boneh D, Goh E, Nissim K. Evaluating 2-dnf formulas on ciphertexts[C]// Theory of Cryptography. LNCS 3378, Berlin: Springer-Verlag, 2005: 325-342

[6] Lal S, Kushwah P. ID-based generalized signcryption [EB/OL]. Cryptology ePrint Archive, Report 2008/84, http://eprint. iacr. org/ 2008/84. pdf, 2008

[7] Yu G, Ma X, Shen Y, et al. Provable secure identity based generalized signcryption scheme [cs. CR]. Available at arXiv: 1004.1304v1, 2010

[8] Sharmila D S S, Sree Vivek S, Pandu Rangan C. A note on the security identity based online/offline encryption scheme [cs. CR]. Available at: http://eprint. iacr. org/2010/178. 2010

[9] Ji H, Han W, Zhao L. Certificateless generalized signcryption [EB/OL]. Cryptology ePrint Archive, Report 2010/204, http://eprint. iacr. org/ 2010/204. pdf, 2010

[10] Chen L, Malone-Lee. Improved Identity-Based Signcryption[C]// Vaudenay S, ed. Public Key Cryptography-PKC2005. LNCS 3386, Berlin: Springer-Verlag, 2005: 362-379

[11] Fiat A, Naor M. Broadcast encryption [C]// CRYPTO'93. LNCS 773, 1993: 480-491

[12] Zhang L Y, Hu Y P, Mu N B. Identity-based Broadcast Encryption Protocol for Ad Hoc Networks [J]. IEEE Computer Society, 2009: 1619-1623

[13] Mihir B, Waters B, Scott Y. Identity-Based Encryption Secure against Selective Opening Attack [EB/OL]. Cryptology ePrint Archive, Report 2008/84, http://eprint. iacr. org/2010/159

[14] Hu L, Liu Z L, Cheng X H. Efficient identity- based broadcasten cryption without random oracles [J]. Journal of Computers, 2010, 5(3): 331-336

[15] Delerabl'ee C, Paillier P, Pointcheval D. Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys[C]// Takagi T, Okamoto T, Okamoto E, eds., Pairing 2007. LNCS 4575, Springer, Heidelberg, 2007: 39-59

[16] Paterson K G. ID-based signatures from pairings on elliptic curves[J]. Electroniics Letters, 2002, 38(18): 1025-102