doi:10.3969/j.issn.1000-436x.2013.08.021

基于身份公平的匿名多接收者签密方案

庞辽军[1,2]，高璐[2]，裴庆祺[2]，王育民[2]
(1. 西安电子科技大学 生命科学技术学院，陕西 西安 710071；
2. 西安电子科技大学 综合业务网国家重点实验室，陕西 西安 710071)

摘 要：针对 Lal 等人所提出的基于身份的多接收者签密方案中存在的暴露接收者身份信息隐私性和解密不公平的问题，应用拉格拉日插值方法，提出一种满足接收者身份匿名性和解密公平性的新的多接收者签密方案。基于双线性 Diffie-Hellman 问题和计算 Diffie-Hellman 问题，对随机模预言模型下的 IND-sMIBSC-CCA2 和 EUF-sMIBSC-CMA 的安全性进行了证明，验证本方案具有保密性和不可否认性。
关键词：多接收者签密；公平性；匿名性；保密性；不可否认性
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)08-0161-08

Fair and anonymous ID-based multi-receiver signcryption

PANG Liao-jun[1,2], GAO Lu[2], PEI Qing-qi[2], WANG Yu-min[2]
(1.School of Life Sciences and Technology, Xidian University, Xi'an 710071, China;
2.State Key Lab. of Integrated Service Networks, Xidian University, Xi'an 710071, China)

Abstract: In order to solve the identify information exposure problem and the decryption unfairness problem in Lal *et al*'s identity-based multi-receiver signcryption scheme, a novel identity-based multi-receiver signcryption scheme, using the Lagrange interpolation method, was proposed to meet the requirements of the identity anonymity and the decryption fairness. Based on the Bilinear Diffie-Hellman and computational Diffie-Hellman assumptions, the security of IND-sMIBSC-CCA2 and EUF-sMIBSC-CMA was proved formally under the random oracle model, which shows that the proposed scheme can achieve the confidentiality and the unforgeablity required.
Key words: multi-receiver signcryption; fairness; anonymity; confidentiality; unforgeablity

1 引言

1997 年,Zheng[1]首次提出了签密的思想，该方案能够实现对明文消息同时进行签名和加密的功能，并且具有比先签名后加密的传统方法更低的计算成本和通信开销。2003 年，Malone-Lee[2]提出了第一个实用的基于身份的签密方案，然而，人们不再仅仅满足于向一个接收者发送消息。当一则消息需要向多个接收者传送时，传统的加密方案不再有效，所以 Bellare[3]和 Baudron[4]于 2000 年分别提出多接收者加密。在多接收者加密概念基础上，2006 年 Duan[5]等提出了第一个基于身份的多接收者签密方案。多接收者签密方案有非常重要的应用前景。例如，它可以应用于数字音频或视频的定制服务：服务提供商仅需为每个电视节目生成一个密文，然后将该密文发送给所有定制该节目的接收者，每个接收者用各自的私钥进行解密。

自 Duan[5]提出多接收者签密概念后，许多研究人

收稿日期：2012-04-13；**修回日期**：2012-07-03
基金项目：国家自然科学基金资助项目(61103178)；NSFC-广东联合基金资助项目(U0835004)；高等学校博士学科点专项科研基金新教师基金资助项目(20096102120045)；教育部计算机网络与信息安全重点实验室(西安电子科技大学)开放基金资助项目(2008CNIS-07)
Foundation Items: The National Natural Science Foundation of China(61103178); The Key Program of NSFC-Guangdong Union Foundation of China (U0835004); The Research Fund for the Doctoral Program of Higher Education of China (20096102120045); The Open Foundation of the Key Laboratory of Network and Information Security in Xidian University, Ministry of Education of China (2008CNIS-07)

员对其进行了研究，并且提出了一些优秀的方案[6~10]。这些方案各有千秋，但它们普遍存在用户隐私性暴露以及由此导致的解密不公平等问题，难以完全满足实际应用需求。用户隐私问题在实际应用中非常重要，例如定制了敏感的电视节目的接收者或者是用户常常希望当他收看该节目时其他人无法知道他的身份[11,12]。但是，现有方案的密文信息中包含身份列表，故暴露了接收者的身份信息。另外，由于每个接收者的解密过程只需要部分密文，故当传输过程中密文部分出错，则会导致有的接收者可以正确解密，有的则无法解密。这些问题在实际应用中都需要避免。

鉴于以上原因，本文基于 Lal 等的签密方案[10]，提出一种新的多接收者签密方案，以满足接收者匿名性和解密公平性等需求。同时，使得该方案具有较短的密文长度和较高的加密效率。

2 相关工作

2.1 数学知识

2.1.1 拉格朗日插值定理

设 $\sum_{i=1}^{t-1}F_i(x)=\sum_{i=0}^{t-1}a_ix^i$ 为一个 t–1 次多项式（其中 $t-1\geqslant 0$），并且通过 t 个点 $(x_1,y_1),(x_2,y_2),\cdots,(x_t,y_t)$，对 $\forall i$ 有

$$F_i(x)=y_i\prod_{1\leqslant j\neq i\leqslant t}\frac{x-x_j}{x_i-x_j}=\begin{cases}y_i,\text{if } x=x_i\\0,\text{ if } x\in\{x_1,x_2,\cdots,x_t\}-\{x_i\}\end{cases}\quad(1)$$

2.1.2 双线性函数

设 G_1 和 G_2 是 2 个阶数为素数 q 的循环群，P 为 G_1 的生成元。存在双线性映射 e：$G_1\times G_1\to G_2$。它具有以下性质。

1) 双线性性: $\forall P,Q\in G_1$ 及 $a,b\in Z_q^*$ 有 $e(aP,bQ)=e(P,Q)^{ab}$。

2) 非退化性: $\exists P,Q\in G_1$，使 $e(P,Q)\neq 1$。

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

2.2 困难问题

1) 双线性 Diffie-Hellman(BDH)问题

已知 $(P,aP,bP,cP)\in G_1$，其中 $a,b,c\in Z_q^*$，计算 $e(P,P)^{abc}$。

定义 1 在解决 G_1 中双线性 Diffie-Hellman 问题时，定义一个概率多项式时间(PPT)算法 A 的优势

$$Adv_A^{BDH}=\Pr\left[A(P,aP,bP,cP)=e(P,P)^{abc},a,b,c\in Z_q^*\right]\quad(2)$$

BHD 假设为:对任意 PPT 算法 A，优势 Adv^{BDH} 都是可忽略的。

2) 计算 Diffie-Hellman(CDH)问题

已知 $(P,aP,bP)\in G_1$，$a,b\in Z_q^*$，计算 abP。

定义 2 在解决 G_1 计算 Diffie-Hellman 问题时，定义一个概率多项式时间算法 A 的优势

$$`Adv_A^{CDH}=\Pr\left[A(P,aP,bP)=abP,\quad a,b\in Z_q^*\right]\quad(3)$$

CDH 假设为：对任意 PPT 算法 A，优势 Adv^{CDH} 都是可忽略的。

2.3 算法模型

基于身份的多接收者签密方案（MIBAS）包括以下 4 个算法。

1) **Setup** PKG 运用该算法生成主密钥 s 以及公开参数 $params$。

2) **Extract** 输入用户的公开身份 ID_i，PKG 的私钥 s 以及系统公开参数 $params$，输出该用户相应的私钥 d_i，即 $d_i=Extract(\mathrm{ID}_i,s,params)$。

3) **Anony-signcrypt** 输入 PKG 的公开参数，一则明文消息 M，签密者 ID_s 选取一个接收者身份集合 $R=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$，并输入自己的私钥 d_s，运行该算法，输出消息 m 相对应的密文消息 C，即 $C=Anony-signcrypt\ (params,M,R,d_s)$。

4) **De-signcrypt** 输入密文 C，PKG 的公开参数 $params$，接收者 $\mathrm{ID}_i,i\in\{1,2,\cdots,n\}$ 的身份及其相应的私钥 d_i 后，该接收者运行该算法进行解密。如果经验证密文 C 是正确签密或正确签名的消息，则接受该签名，并输出相对应的明文消息 M，即 $M=De-signcrypt\ (C,params,d_i)$，否则输出 $\perp$。

2.4 安全模型

定义 3 和定义 4 分别介绍与本文方案相关的安全属性：消息保密性和不可为造型。

定义 3 选择密文攻击下的选择多身份密文不可区分性安全模型 IND-sMIBSC-CCA (indistinguisha -bility of ciphertexts under selective multi-ID, chosen ciphertext attack)：假设 A 是一个攻击者，定义 Π 是一个基于身份的多接收者匿名签密方案。A 与挑战者 B 的博弈如下。

Setup　挑战者 B 运行该算法，生成主密钥 s 以及系统参数 *params*，将 *params* 给 A，自己秘密保存主密钥 s。收到系统参数以后，A 输出 n 个目标身份 $(\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_n^*)$。

Phase 1　A 向 B 进行如下询问。

私钥提取询问：当 B 收到关于身份 ID_j $(\mathrm{ID}_j \neq \mathrm{ID}_i^*, i=1,2,\cdots,n)$ 的密钥提取询问时，挑战者 B 运行密钥提取算法得到 $d_j = Extract(params, s, \mathrm{ID}_j)$。

匿名签密询问：当 B 收到匿名签密询问 (M,R,ID_i^*)，（其中 $R=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$）以后，计算密文 $C = Anony-signcrypt(params, m, R, d_i^*)$（其中 d_i^* 是被攻击者 ID_i^* 的私钥），并返回给 A。

解签密询问：当 B 收到解签密询问 $(C,\mathrm{ID}_j,\mathrm{ID}_i^*)$（其中 $\mathrm{ID}_j \in R$）。如果 C 是有效的密文，就解密出 $M = Decrypt(params, C, \mathrm{ID}_j, \mathrm{ID}_i^*, d_i)$，并返回给 A，否则输出 $\perp$。

Challenge　A 输出一个目标明文对 (M_0,M_1) 和一个私钥 d_s^*，当 B 收到 (M_0,M_1) 和 d_s^* 时，挑战者 B 随机选择一个参数 $\beta \in \{0,1\}$，并生成一个目标密文 $C^* = Anony-signcrypt(params, R^*, M_\beta, d_s^*)$，然后将 C^* 返回给 A。

Phase 2　A 按 Phase 1 一样进行多次询问，注意私钥提取询问时不可以询问 $(\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_n^*)$ 中的身份信息，解密询问时不可以询问 C^*。

Guess　最终，A 输出其猜测 $\beta' \in \{0,1\}$，如果 $\beta' = \beta$，则赢得这场游戏。

如上所述的 A 被称为 IND-sMID-CCA 攻击者，其优势定义为

$$Adv_{\Pi}^{IND-sMID-CCA}(A) = |\Pr[\beta = \beta'] - \frac{1}{2}| \tag{4}$$

如果对于任意的 IND-sMID-CCA 攻击者 A，在概率时间 τ 内，都存在小于 $Adv_{\Pi}^{IND-sMID-CCA}(A)$ 的优势，则方案 Π 是 (τ,ε)-IND-sMID-CCA 安全的。

定义 4　选择消息攻击下的选择多身份强存在不可伪造模型 SUF-sMIBSC-CMA(strong existential unforgeability under selective ID，chosen message attack)，假设 F 是一个伪造者，定义 Π 是一个基于身份的多接收者匿名签密方案。F 与一个挑战者 B 的博弈如下。

Setup　B 运行该算法,生成主密钥 s 以及系统参数 *params*，将 *params* 给 F，并秘密保存主密钥 s。收到系统参数以后，F 输出目标身份 ID_s^*。

Attack　F 向 B 进行如下询问。

私钥提取询问：当 B 接收到关于身份 $\mathrm{ID}(\mathrm{ID} \neq \mathrm{ID}_s^*)$ 的私钥询问时，就运行算法 Extract 得到。

匿名签密询问：当 B 收到匿名签密询问 (M,R,ID_s)（其中 $R=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$）以后，计算密文 $C = Anony-signcrypt(params, M, R, d_s)$（其中 d_s 是被攻击者 ID_s 的私钥），并返回给 F。

Forgery　F 最终输出一个新的密文消息 C^* 和 n 组接收者的公私钥对 $(\mathrm{ID}_1,d_1),(\mathrm{ID}_2,d_2),\cdots,(\mathrm{ID}_n,d_n)$。如果 C^* 是 ID_s^* 对消息 M 的签名，并可以在集合 $\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$ 中被任何接收者正确解密，那么 C^* 是有效密文，F 赢得这场游戏。此处的限制是 F 不能对身份 ID_s^* 进行私钥提取询问，且 C^* 不能由 *Anony-signcrypt* 算法产生。F 的优势为他胜利的概率。

3　方案描述

3.1　参数生成算法

该算法由 PKG 执行，具体包括以下步骤。

step1　设 G_1 和 G_2 分别是阶为素数 q 的加法群和乘法群，P 是 G_1 的生成元；选择双线性映射 e，满足 $e: G_1 \times G_1 \to G_2$；选择一个随机数 $s \in Z_q^*$ 为主密钥，并随机选择 G_1 中的元素 P_1。

step2　设置 $P_{\mathrm{pub}} = sP \in G_1$。

step3　定义 4 个单向散列函数：$H: \{0,1\}^{\lambda_1} \to Z_q^*$，$H_0: \{0,1\}^{\lambda_1} \to G_1$，$H_1: G_1 \times \{0,1\}^{\lambda_2} \to Z_q^*$，$H_2: G_2 \to \{0,1\}^{\lambda_1+\lambda_2}$，其中 λ_1、λ_2 分别表示身份 ID 和明文的长度。

step4　发送者公开系统参数 $params = \langle G_1, G_2, q, e, P, P_1, P_{\mathrm{pub}}, H, H_0, H_1, H_2 \rangle$ 并秘密保存主密钥 s。

3.2　私钥提取算法

PKG 输入参数 *params*，s 和身份 $\mathrm{ID} \in \{0,1\}^{\lambda_1}$，算法进行以下步骤。

计算 ID 的公钥 $Q_{\mathrm{ID}} = H_0(\mathrm{ID})$，设置 ID 的私钥 $d_{\mathrm{ID}} = s(Q_{\mathrm{ID}} + P_1)$。

3.3　签密算法

签密者输入参数 *params*，消息 M，设 ID_s 是签密者，$\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n$ 是签密者选择的 n 个接收者，算法进行以下步骤。

1) 签名

step1 随机选择整数 $r\in Z_q^*$。

step2 计算 $X=rP$，$h=H_1(M,X)$ 及 $W=hd_s+rQ_s$，这里 $Q_s=H_0(\mathrm{ID}_s)$ 和 $d_s=s(Q_s+P_1)$ 分别为签密者的公钥和私钥。

2) 加密

step1 计算 $V=e(rP_{\mathrm{pub}},P_1)$，$Z=H_2(V)\oplus(\mathrm{ID}_s\|M)$。

step2 计算 $x_i=H(\mathrm{ID}_i)$，$y_i=rQ_i\ (i=1,2,\cdots,n)$，得到 n 组数: $(x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)$。构造拉格朗日函数 $F_i(x)$，满足 x_i 是 $F_i(x)=y_i$ 的根。

step3 对于 $i=1,2,\cdots,n$，计算

$$f_i(x)=\prod_{1\leqslant j\neq i\leqslant n}\frac{x-x_j}{x_i-x_j}=a_{i,1}+a_{i,2}x+\cdots+a_{i,n}x^{n-1}$$

其中，$a_{i,1},a_{i,2},\cdots,a_{i,n}\in Z_q$。

step4 对于 $i=1,2,\cdots,n$，计算 $L_i=\sum_{j=1}^{n}a_{j,i}y_j$。

step5 密文为：$C=<L_1,L_2,\cdots,L_n,X,W,Z>$。

3.4 解签密算法

接收者 ID_i 输入密文 $C=<L_1,L_2,\cdots,L_n,X,W,Z>$，参数 *params*，接收者身份 ID_i 及其私钥 d_i，为了解密 C，算法进行以下步骤。

1) 解密

step1 计算 $x_i=H(\mathrm{ID}_i)$。

step2 计算 $\delta_i=L_1+x_iL_2+\cdots+\left(x_i^{n-1}\bmod q\right)L_n$。

step3 计算 $V'=\dfrac{e(X,d_i)}{e(P_{\mathrm{pub}},\delta_i)}$ 和 $(\mathrm{ID}_s\|M)=H_2(V')\oplus Z$。

step4 输出 (ID_s,M) 和 $\langle X,W\rangle$ 进行以下验证过程。

2) 验证

step1 计算 $h=H_1(M,X)$；判断 $e(P,W)=e(hP_{\mathrm{pub}}+X,Q_s)e(hP_{\mathrm{pub}},P_1)$ 是否成立，如果成立，接受消息 M；否则输出 $\perp$。

4 分析与证明

4.1 正确性分析

定理 1 2.4 节中解密步骤是正确的，即 $V'=V$，消息 M 能被正确解出。

证明 对每一个 $i(1\leqslant i\leqslant n)$，由于 $y_i=rQ_i$，都有

$$\begin{aligned}\delta_i&=L_1+x_iL_2+\ldots x_i^{i-1}L_i+\ldots x_i^{n-1}L_n\\&=(a_{1,1}y_1+\ldots+a_{n,1}y_n)+(x_ia_{1,2}y_1+\ldots x_ia_{n,2}y_n)\\&\quad+\ldots+(x_i^{i-1}a_{1,i}y_1+\ldots+x_i^{i-1}a_{n,i}y_n)+\ldots+\\&\quad(x_i^{n-1}a_{1,n}y_1+\ldots+x_i^{n-1}a_{n,n}y_n)\\&=(a_{1,1}+a_{1,2}x_i+\ldots+a_{1,n}x_i^{n-1})rQ_1+\\&\quad(a_{2,1}+a_{2,2}x_i+\ldots+a_{2,n}x_i^{n-1})rQ_2+\cdots+\\&\quad(a_{i,1}+a_{i,2}x_i+\cdots+a_{i,n}x_i^{n-1})rQ_i+\cdots\\&\quad+(a_{n,1}+a_{n,2}x_i+\cdots+a_{n,n}x_i^{n-1})rQ_n\\&=rQ_i\quad(\text{拉格朗日插值定理})\end{aligned}\tag{5}$$

因此，有下式成立

$$\begin{aligned}V'&=\frac{e(X,d_i)}{e(P_{pub},\delta_i)}\\&=\frac{e(rP,s(Q_i+P_1))}{e(P_{pub},y_i)}\\&=\frac{e(sP,Q_i)^r\,e(sP,P_1)^r}{e(P_{pub},rQ_i)}\\&=\frac{e(P_{pub},Q_i)^r\,e(P_{pub},P_1)^r}{e(P_{pub},Q_i)^r}\\&=e(P_{pub},P_1)^r\\&=V\end{aligned}\tag{6}$$

于是，$(\mathrm{ID}_s\|M)=H_2(V')\oplus Z=H_2(V)\oplus Z$。所以解密过程是正确的。

定理 2 2.4 节中验证过程是正确的，即当所有解密过程正确时，等式 $e(P,W)=e(hP_{\mathrm{pub}}+X,Q_s)\,e(hP_{\mathrm{pub}},P_1)$ 成立。

证明 当正确接收消息 M 时，有

$$\begin{aligned}e(P,W)&=e(P,hd_s+rQ_s)\\&=e(P,s(Q_s+P_1))^h\,e(P,Q_s)^r\\&=e(hP_{\mathrm{pub}},Q_s)\,e(hP_{\mathrm{pub}},P_1)\,e(X,Q_s)\\&=e(hP_{\mathrm{pub}}+X,Q_s)\,e(hP_{\mathrm{pub}},P_1)\end{aligned}\tag{7}$$

综上所述，本方案是正确的。

4.2 安全性证明

定理 3 在 (τ',ε')-BDH 的假设下，改进的公平的基于身份的多接收者匿名签密方案是 $(\tau,q_{ex},q_s,q_d,q_H,q_{H_0},q_{H_1},q_{H_2},\varepsilon)$-IND-sMIBSC-CCA2 安全的，这里有 $\varepsilon'\geqslant\varepsilon-\dfrac{q_{H_2}q_d}{2^k}$，且有 $\tau'\approx\tau+(2q_d+q_s)O(\tau_1)$。($q_{ex},q_s,q_d,q_H,q_{H_0},q_{H_1},q_{H_2}$ 分别指密钥提取询

问，匿名签密询问，解密询问以及对散列函数 H、H_0、H_1、H_2 进行询问的次数。τ_1 是对映射 e 的运算时间)。

证明　假设 IND-sMIBSC-CCA 模型下有攻击者 A 在时间 τ 内具有优势 $Adv_{\Pi}^{IND-sMIBSC-CCA}(A)\geqslant\varepsilon$，这里 Π 表示被提出的方案。假设 A 分别进行了至多 q_{ex} 次密钥提取询问，q_s 次签密询问，q_d 次解密询问以及分别 q_H、q_{H_0}、q_{H_1}、q_{H_2} 次散列函数 H、H_0、H_1、H_2 询问。下面给出算法 B 如何利用 A 在时间 τ' 内以概率 ε' 解决 BDH 问题。

首先，B 得到一个 BDH 问题实例 $\langle P,aP,bP,cP\rangle$，目的是计算 $e(P,P)^{abc}$。B 模拟一个挑战者（如定义 3 中所述）执行每一步过程。

Setup　B 设定 $P_{\text{pub}}=bP$，将 $params=\langle G_1,G_2,q,e,P,P_1,P_{\text{pub}},H,H_0,H_1,H_2\rangle$ 作为系统参数给 A。收到系统参数以后。A 输出目标身份 $(\text{ID}_1^*,\text{ID}_2^*,\cdots,\text{ID}_n^*)$。

其中，H、H_0、H_1、H_2 为随机预言模型，并由 B 控制如下：

对 H、H_0、H_1、H_2 询问的结果分别存储在 $H-\text{list},H_0-\text{list},H_1-\text{list},H_2-\text{list}$ 中。

***H*-query**　向 H 输入一个身份 $\text{ID}_j,j\in\{1,2,\cdots,n\}$，如果 $H-\text{list}$ 中存在 (ID_j,x_j)，则返回 x_j，否则，进行以下步骤。

1) 随机选择一个整数 $x_j\in Z_q^*$。

2) 将 (ID_j,x_j) 存入 $H-\text{list}$。

3) 返回 x_j。

***H*$_0$-query**　向 H_0 输入一个身份 ID_j，$j\in\{1,2,\cdots,n\}$。如果 $H_0-\text{list}$ 中存在 (ID_j,l_j,Q_j)，则返回 Q_j。否则,进行以下步骤。

1) 随机选择一个整数 $l_j\in Z_q^*$。

2) 如果 $\text{ID}_j=\text{ID}_i^*,i\in\{1,2,\cdots,n\}$，计算 $Q_j=l_jP-P_1$，否则计算 $Q_j=l_jP$。

3) 将 (ID_j,l_j,Q_j) 存入 $H_0-\text{list}$。

4) 返回 Q_j。

***H*$_1$-query**　向 H_1 输入一组数 $(M_j,X_j),j\in\{1,2,\cdots,q_{H_1}\}$，如果 $H_1-\text{list}$ 中存在 (M_j,X_j,h_j)，则返回 h_j。否则，进行以下步骤。

1) 随机选择一个整数 $h_j\in Z_q^*$。

2) 将 (M_j,X_j,h_j) 存入 $H_1-\text{list}$。

3) 返回 h_j。

***H*$_2$-query**　向 H_2 输入一个元素 $V_j\in G_2,j\in\{1,2,\cdots,q_{H_2}\}$，如果 $H_2-\text{list}$ 中存在 (V_j,ρ_j)，则返回 ρ_j。否则,进行以下步骤。

1) 随机选择一个字符串 $\rho_j\in\{0,1\}^{\lambda_1+\lambda_2}$。

2) 将 (V_j,ρ_j) 存入 $H_2-\text{list}$。

3) 返回 ρ_j。

Phase 1　A 向 B 进行如下询问。

私钥提取询问：当 B 接收到关于身份 ID_j $(\text{ID}_j\neq\text{ID}_i^*,i=1,2,\cdots,n)$ 的私钥询问时，就在 $H_0-\text{list}$ 中寻找 (ID_j,l_j,Q_j)，如果存在二元组 (ID_j,l_j,Q_j),那么计算其私钥 $d_j=l_jP_{\text{pub}}(=l_jbP=bl_jP=b(l_jP-P_1+P_1)=b(Q_j+P_1))$，并返回给 A。

匿名签密询问：B 收到匿名签密询问 (M,L,ID_s)（其中 $L=\{\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_n\}$）时，此处 $\text{ID}_s\neq\text{ID}_i^*(i=1,2,\cdots,n)$，$B$ 随机选择 $r',h,k\in Z_q^*$，计算 $X=r'P-h(bP)$，$W=r'(l_iP-P_1)$，$P_1=kP$，得到 (M,X,h)，并在 $H_1-\text{list}$ 中查找，使得 (M,X) 没有在 $H_1-\text{list}$ 中出现，否则重新选择 $r',h,k\in Z_q^*$，进行以上过程，B 将符合条件的 (M,X,h) 加入到 $H_1-\text{list}$ 中。B 计算 $V=e(r'P_{\text{pub}},kP)$，在 $H_2-\text{list}$ 中查找 (V,ρ)，计算出 $Z=\rho\oplus(\text{ID}_s\|M)$，然后 B 在 $H-list$ 中查找 (ID_i,x_i)，计算 $y_i=(l_i-k)X,\ i=1,2,\cdots,n$，并由此得到 L_i $(i=1,2,\cdots,n)$。最终，B 得到密文 C，并返回给 A。

解签密询问：当 B 收到一个密文为 $C=<L_1,L_2\cdots,L_n,X,W,Z>$ 和一个身份 $\text{ID}_i,i\in\{1,2,\cdots,n\}$ 的解签密询问以后，寻找 $(\text{ID}_i,x_i)\in H-list$，并计算 $\delta_i=L_1+x_iL_2+\cdots+(x_i^{n-1}\bmod q)L_n$。在 $H_0-\text{list}$ 中寻找 (ID_i,l_i,Q_i)，并计算 $d_i=l_iP_{\text{pub}}=l_ibP$，$V'=\dfrac{e(X,d_i)}{e(P_{\text{pub}},\delta_i)}$，从而可以得到 $(\text{ID}_s\|M)=H_2(V')\oplus Z$。再在 $H_0-\text{list}$ 中寻找 (ID_s,l_s,Q_s)，得到 Q_s。最后验证 $e(P,W)=e(hP_{\text{pub}}+X,Q_s)e(hP_{\text{pub}},P_1)$ 是否成立。如果成立，则 C 是有效的密文，就返回 M 给 A。否则，输出 $\perp$。

Challenge　A 选择一对等长的消息 (M_0,M_1) 和

一个签密者的身份 ID_s。当 B 收到 (M_0, M_1) 和 ID_s 以后，随机选择 $\beta \in \{0,1\}$，对消息 M_β 进行签密。首先，B 查找 $H_0-\text{list}$ 获得与 $\mathrm{ID}_i^*, i \in \{1,2,\cdots,n\}$ 相对应的 l_i^*，并得到它们的公钥 $Q_i = l_i^* P - P_1$，计算出 $y_i^* = rQ_i^* = r\left(l_i^* P - P_1\right)$，得到 $L_i^*, i \in \{1,2,\cdots,n\}$。$B$ 最终生成目标密文 $C =< L_1^*, L_2^*, \cdots, L_n^*, X^*, W^*, Z^* >$，其中有 $X^* = aP$，$W^* = \left(h'b + r'\right) l_s^* P - r' P_1$，$P_1^* = cP$，$Z = H_2(e(r' P_{\text{pub}}, P_1)) \oplus \left(\mathrm{ID}_s \| M_\beta\right)$，并将 C^* 返回给 A。

Phase 2 A 像 Phase 1 中一样进行多次询问，注意私钥提取询问时不可以询问 $\left(\mathrm{ID}_1^*, \mathrm{ID}_2^*, \cdots, \mathrm{ID}_n^*\right)$ 中的身份信息，解密询问时不可以询问 C^*。

Guess 最终，A 输出其猜测 $\beta' \in \{0,1\}$，如果 $\beta' = \beta$，B 从 $H_2-\text{list}$ 选取 (V, ρ)，并输出 V 作为 BDH 问题的解。

分析 在签密询问中，由于 $X = r'P - h(bP) = (r' - bh)P$，所以有 $r = r' - bh$，又因为有 $W = r'(l_i P - P_1) + hbP_1 = (r' - bh)(l_i P - P_1) + bh(l_i P - P_1) + hbP_1 = rQ_i + hd_i$，且存在 $y_i = (l_i - k)X = rP(l_i - t) = r(l_i P - kP) = r(l_i P - P_1) = rQ_i, i = 1,2,\cdots,n$，由此计算出 L_i，从而可以得到目标密文。

在挑战过程中，设置 $X^* = aP$，$P_1 = cP$。已知 $Q_{ID_i^*} = H_0\left(\mathrm{ID}_i^*\right) = l_i^* P - P_1$，可以得到 $y_i' = X^*\left(l_i^* - c\right) = aP\left(l_i^* - c\right) = a\left(l_i^* P - cP\right) = aQ_i$，再通过拉格朗日插值函数得到 L_i^*。因此，C^* 与实际攻击过程中描述的相同。如果 A 的猜测正确，它需要询问随机预言函数 H_2 得到 $V = e\left(rP_{\text{pub}}, P_1\right) = e\left(a(bP), cP\right) = e(P,P)^{abc}$，并将 (V, ρ) 存入 $H_2-\text{list}$，B 从中提取出 $e(P,P)^{abc}$。

由以上讨论可知攻击环境的模拟几乎完美，唯一不足的是当一个合理的密文在解签密询问时遭到拒绝，显然对于 $H_2-\text{list}$ 中的每一对 (V_i, ρ_i) 在 $H_1-\text{list}$ 中恰好存在一个 h_i 提供一个合法的密文。拒绝一个合理密文的概率不大于 $\frac{q^k}{2^k}$。在攻击阶段 A 进行了 q_d 次解签密询问。B 从中 $H_2-\text{list}$ 随机选择 V 做为 BDH 困难问题的结果。有 $\varepsilon' \geqslant \varepsilon - \frac{q_{H_2} q_d}{2^k}$。且 $\tau' \approx \tau + (2q_d + q_s) O(\tau_1)$（其中 τ_1 是对运算 e 的运算时间)。所以，由以上困难问题和安全模型的证明可知，本方案满足消息保密性。

定理 4 在随机预言模型中，如果存在一个 SUF-sMIBSC-CMA 敌手 F 能够在时间 τ 内，以一个不可忽略的优势 ε 赢得游戏(他最多能进行 q_{ex} 次密钥提取询问，q_s 匿名签密询问和 q_H、q_{H_0}、q_{H_1}、q_{H_2} 次对 Hash 函数 H、H_0、H_1、H_2 的询问)，则存在一个算法 B 能够在时间 $\tau' \approx \tau + q_s O(\tau_1)$ 内，以优势 $\varepsilon' \geqslant \varepsilon - \frac{q_{H_2} q_s}{2^k}$ 解决 CDH 问题(τ_1 是对运算 e 的运行时间)。

证明 下面给出算法 B 如何利用 F 在时间 τ' 内以概率 ε' 解决 CDH 问题。

首先，B 得到一个 CDH 问题实例 $\langle P, bP, cP \rangle$，其目标为计算出 bcP。B 模拟一个挑战者进行以下每一步过程。

Setup B 设定 $P_{\text{pub}} = bP$，将 $params = \langle G_1, G_2, q, e, P, P_1, P_{\text{pub}}, H, H_0, H_1, H_2 \rangle$ 作为系统参数给 F。收到系统参数以后，F 输出目标身份 ID_s^*，其中对 H_0、H_1、H_2 的询问如定义 4 中所述。

Attack F 向 B 进行如下询问。

私钥提取询问：当 B 接收到关于身份 $\mathrm{ID}\left(\mathrm{ID} \neq \mathrm{ID}_s^*\right)$ 的私钥询问时，就在 $H_0-\text{list}$ 中寻找 (ID, l, Q)，计算 $S_i = b\left(l_i P + P_1\right)$，并返回给 F。

匿名签密询问 对于一个关于 (M, L, ID_s)(其中 $L = \{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$)的签密询问，$B$ 随机选择 $r' \in Z_q^*$ 和 $P_1' \in G_1$，计算 $X = r'P$。在 $H_1-\text{list}$ 中查找 (M, X', h') 得到 h'，如果没找到就选择一个 $h' \in Z_q^*$，并将 (M, X', h') 存入 $H_1-\text{list}$。在 $H_0-\text{list}$ 中查找 $(\mathrm{ID}_s, l_s, Q_s)$，得到 Q_s；如果找不到，就选择一个 $l_s \in Z_q^*$，并计算 $Q_s = l_s P - P_1$。然后将 $(\mathrm{ID}_s, l_s, Q_s)$ 存入 $H_0-\text{list}$，计算 $W' = h' d_s + r' Q_s = h' b l_s P + r'\left(l_s P - P_1\right) = l_s P(bh' + r') - r' P_1$。再计算 $V' = e(r' bP, P_1')$，在 $H_2-\text{list}$ 中查找 (V', ρ')，如果没找到就选择一个 $\rho' \in \{0,1\}^{2t}$，并将 (V', ρ') 存入，计算 $Z' = \rho' \oplus \left(M \| \mathrm{ID}_s\right)$.$B$ 在 $H-\text{list}$ 中查找 (ID_i, l_i)，并计算 $y_i = X(l_i - k), i = 1,2,\cdots,n$，由此得到 $L_i, i \in \{1,2,\cdots,n\}$。最终，$B$ 得到密文 C，并返回给 F。

Forgery F 生成一个目标密文 $C^* =< L_1^*, L_2^*, \cdots, L_n^*, X^*, W^*, Z^* >$，如果这个伪造是成功的，就有等式 $e\left(P, W^*\right) = e\left(hP_{\text{pub}} + X^*, Q_s\right) e\left(hP_{\text{pub}}, P_1\right)$ 成立。定义

表 1　　签密效率比较

方案	Pa	Add	Mul	Exp	Hash	参数个数	密文长度
方案[6]	1	n+1	n+3	1	2	n+9	3|G_1|+n|ID|+|m|
方案[7]	2	n+1	n+4	2	2	8	(n+2)|G_1|+|m|+n|ID|+|Z_q|
方案[9]	1	1	n+3	1	2	10	(n+2)|G_1|+|G_2|+n|ID|+|m|
方案[10]	0	3n	3n+2	1	3	11	(2n+2)|G_1|+2n|ID|+|m|
本方案	1	1	n+3	1	3	11	(n+2)|G_1|+|ID|+|m|

$c=hl_s$，于是有 $W^*=hd_s+rQ_s=h(bl_sP)+rQ_s=bcP+rQ_s$，这样就很容易提取出 CDH 问题的解 $bcP=W^*-rQ_s$。

下面考虑 B 成功的优势。由于匿名签密询问中，至多进行了 q_{H_1} 次 H_1 询问，故 B 回答失败一个签密询问的概率不大于 $\frac{q_{H_1}q_s}{2^k}$，所以得到优势 $\varepsilon' \geqslant \varepsilon-\frac{q_{H_1}q_s}{2^k}$，且 $\tau' \approx \tau+q_sO(\tau_1)$ (其中 τ_1 是对运算 e 的运算时间)。所以,由以上困难问题和安全模型的证明可知，本方案满足不可伪造性。

4.3　性能与效率分析

首先，考虑本文方案功能优势。与现有的基于身份多接收者签密方案进行比较，本文方案实现了更完善的性能，它改善了现有多接收者签密方案接收者身份隐私泄露和解密不公平等问题。它具有接收者匿名性，密文中不再暴露接收者身份信息，即对每一个接收者对于攻击者以及其他接收者都是匿名的。每个接收者或者攻击者都得不到其他授权的接收者身份。同时具有解密公平性，因为对每个接收者来说，在解密过程中，密文中所有信息都必须用到，即对于每一个授权的接收者，他们所能正确解出密文的概率是相等的。一旦消息在传输过程中部分比特的消息出错或者被破坏，所有接收者都将得不到正确消息。

其次，考虑算法性能，主要从计算成本和通信量(密文长度)2 个方面将本文方案与现有相关签密方案进行比较。由于本文方案采用拉格朗日插值公式实现了接收者匿名性，在乘法运算和加法运算上消耗稍大，但是拉格朗日公式的运算可以放在加密前进行预运算，所以真正在加密步骤中进行的运算将大大缩减。实际上，在本方案中乘法运算只需(2n+4)次 G_1 中的标量乘运算，n 次 G_1 中的加法运算，一次双线性对运算。

表 1 是本文方案和现有方案的性能比较结果。其中，用 Pa 表示对运算，用 Add 表示 G_1 中的加法运算，用 Mul 表示 G_1 中的标量乘运算，用 Exp 表示 G_2 中的指数运算，用 Hash 表示加密步骤中的散列运算。|G_1|：G_1 中元素的长度；|ID|： 身份信息 ID 的长度；|M|：明文消息 M 的长度；n：指定接收者的人数

通过比较可以看出，本文提出的方案在计算成本和密文长度等方面综合起来具有一定的优势；系统公开参数数目相对适中，利于系统存储。

5　结束语

多接收者签密方案有着非常重要的应用前景，它仅通过一次签密可以完成对多个用户发送同一信息。本文提出的新多接收者签密方案解决了现有方案的不足，实现了接收者匿名性和解密公平性，并且与现有的基于身份的多接收者签密方案相比，具有更低的通信量和计算成本消耗。本文方案适用于不安全或者开放的网络环境，可用于无线局域网，无线传感器网络等多种形式的无线及有线网络，实现敏感消息的安全广播。

参考文献：

[1] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption)[A]. CRYPTO 1997[C]. Springer-Verlag, 1977. 165-179.

[2] MALONE-LEE J. Identity based signcryption [EB/OL]. http://eprint.iacr.org/ 2002/098.pdf, 2002.

[3] BELLARE M, BOLDYREVA A, MICALI S. Public-key encryption in a multi-user setting: security proofs and improvements[A]. EUROCRYPT 2000[C]. Springer-Verlag, 2000. 259-274.

[4] BAUDRON O, POINTCHEVAL D, STERN J. Extended notions of security for multicast public key cryptosystems[A]. ICALP 2000[C].

Springer-Verlag, 2000. 499-511.

[5] DUAN S, CAO Z. Efficient and provably secure multi receiver identity based signcryption[A]. ACISP 2006[C]. Springer-Verlag, 2006. 195-206.

[6] SHARMILA S, SREE S, SRINIVASAN R, *et al*. An efficient identity-based signcryption scheme for multiple receivers[A]. IWSEC 2009[C]. Springer-Verlag, 2009. 71-88.

[7] ELKAMCHOUCHI H, ABOUELSEOUD Y. MIDSCYK: an efficient provably secure multirecipient identity-based signcryption scheme [A]. ICNM 2009, Networking and Media Convergence[C]. 2009. 70-75.

[8] CHEN L, MALONE-LEE J. Improved identity-based signcryption [A]. PKC 2005[C]. Springer-Verlag, 2005. 362-379.

[9] YU Y, YANG B, HUANG X. Efficient identity-based signcryption scheme for multiple receivers[A]. ATC 2007[C]. Springer-Verlag, 2007. 13-21.

[10] LAL S, KUSHWAH P. Anonymous ID based signcryption scheme for multiple receivers[EB/OL]. http://eprint.iacr.org/2009/345.pdf, 2009.

[11] FAN C, HUANG L, HO P. Anonymous multireceiver identity-based encryption[J]. IEEE Transactions on Computers, 2010, 59(9): 1239-1249.

[12] 庞辽军, 李慧贤, 焦李成等. 可证明安全的多接收者公钥加密方案设计与分析[J]. 软件学报, 2009, 20(10): 2739-2745.
PANG L J, LI H X, JIAO L L, *et al*. Design and analysis of a provable secure multi-recipient public key encryption scheme [J]. Journal of Software, 2009, 20(10): 2739-2745.

作者简介：

庞辽军（1978-），男，陕西渭南人，博士后，西安电子科技大学副教授，主要研究方向为密码学、安全协议设计与分析等。

高璐（1989-），女，陕西西安人，西安电子科技大学硕士生，主要研究方向为密码学与信息安全。

裴庆祺（1975-），男，广西玉林人，博士后，西安电子科技大学教授，主要研究方向为数字内容保护与无线网络安全。

王育民（1936-），男，北京人，西安电子科技大学教授、博士生导师，主要研究方向为信息论、密码学、编码学等。