doi:10.11959/j.issn.1000-436x.2016122

高效的无证书多接收者匿名签密方案

秦艳琳，吴晓平，胡卫
（海军工程大学信息安全系，湖北 武汉 430033）

摘 要：针对已有的基于身份的多接收者签密方案存在的密钥托管问题，研究了无证书多接收者签密安全模型，进而基于椭圆曲线密码体制，提出一个无证书多接收者签密方案，并在随机预言机模型下证明方案的安全性建立在计算 Diffie-Hellman 问题及椭圆曲线离散对数问题的困难性之上。该方案无需证书管理中心，在签密阶段和解签密阶段均不含双线性对运算，且可确保发送者和接收者的身份信息不被泄露，可以方便地应用于网络广播签密服务。
关键词：无证书公钥密码；多接收者匿名签密；计算 Diffie-Hellman 问题；椭圆曲线离散对数问题；随机预言机
中图分类号：TP309 **文献标识码**：A

Efficient certificateless multi-receiver anonymous signcryption scheme

QIN Yan-lin, WU Xiao-ping, HU Wei
(Department of Information Security, Naval University of Engineering, Wuhan 430033, China)

Abstract: To solve the private key escrow problem of identity-based multi-receiver signcryption schemes, the security model for multi-receiver signcryption scheme was constructed, and then a certificateless multi-receiver signcryption scheme based on ECC was proposed. Furthermore, the security of the scheme in the random oracle was based on the computational Diffie-Hellman assumption and elliptic curve discrete logarithm assumption was proved. Meanwhile, the scheme was free from certificate management center and needed no bilinear paring operation in both signcryption and decryption phases. It can also protect both the sender and receivers' identity from leaking out. So the scheme can be applied conveniently to broadcast signcryption in network environment.
Key words: certificateless cryptography, multi-receiver anonymous signcryption, computational Diffie-Hellman problem, elliptic curve discrete logarithm problem, random oracle

1 引言

签密机制是由 Zheng[1]首次提出的一种使用户同时实现对消息的签名及加密功能的密码应用算法，该方案所消耗的通信和计算代价远小于“先签名，后加密”的传统方案。在实际应用中，学者将签密思想与不同的应用场景结合，设计了多种具有特殊性质的签密算法。如在具体的网络应用中，某些消息的发布者或软件的提供商通常需要对消息（软件）进行签密后分发给特定的多个接收者，付费或授权的接收者可以对接收到的签密消息进行解密验证，过滤掉其中的无用信息，获得需要的服务或信息。针对此种实际应用，众多学者利用传统公钥密码体制和基于身份的公钥密码体制提出了多接收者签密方案[2~9]，文献[3]利用基于身份的公钥密码体制设计了一种多接收者匿名签密方案，用户私钥完全由 KGC 产生，导致恶意的 KGC 可以伪造合法用户的私钥，即存在密钥托管问题。文献[4]提出一种基于门限解密的多接收者签密方案，该方案同样是由基于身份的公钥密码体制构建，因此存在密钥

收稿日期：2016-01-18；**修回日期**：2016-06-03
基金项目：国家自然科学基金青年基金资助项目（No.61100042）；海军工程大学自然科学基金项目（No.20150437）
Foundation Items: The National Natural Science Foundation of China (Project for Youth) (No.61100042), The Natural Science Foundation of Naval University of Engineering (No.20150437)

托管问题，并且方案声称能实现接收者的匿名性，但实际上在传递的密文中必须包含与各接收者身份信息对应的列表才能实现正确解密，故无法保护接收者的身份隐私，同时方案中没有明确签密者身份信息是以何种方式传递给接收者，若为默认的明文传输，则无法确保签密者身份的匿名性。文献[5]提出一种基于身份的多接收者签密方案，存在密钥托管问题，且算法的验证等式中没有使用签密者的身份信息，导致无法确定签密消息的来源，同时密文中仍包含了接收者身份信息列表，无法实现接收者的匿名性。文献[6]提出 2 种基于身份的广播签密方案，存在密钥托管问题，并且所提 2 种算法在签密阶段和解签密阶段均使用了系统主密钥，与基于身份的签密方案的基本构造违背，同时文献[7]指出这 2 种方案均存在签密密文伪造，难以实现消息的机密性和认证性；在密文中虽然没有接收者的身份信息，但是每个接收者在恢复原始消息时实际上需要用到其他用户的身份信息，因此无法确保接收者身份的匿名性，同时该算法中没有明确给出签密的验证算法，解签密算法还包含了复杂的双线性对运算。文献[8,9]中的多接收者签密方案均利用基于身份的公钥密码体制构建，且文献[9]并未给出具体的签密算法。文献[10]中的多接收者签密方案基于传统公钥密码构建，但传统公钥密码体制中公钥证书的管理需要巨大的通信、存储开支，不方便大规模的网络应用。为突破上述 2 类公钥密码体制的局限性，Alriyami 等[11]提出了无证书公钥密码学，文献[12]提出一种基于多变量公钥密码体制的无证书多接收者签密方案，该方案具有较高的运算效率，消除了密钥托管的隐患，密文中对接收者的身份信息进行了加密处理，使攻击者无法从中得到接收者的身份，但是方案没有对签密者的身份进行保护且接收群组内的成员可以获知其他接收者的身份，这在某些情境下也不利于用户隐私的保护。

针对上述问题，本文基于无证书公钥密码，在对前人提出的不使用双线性对的无证书签密方案[13~15]进行分析研究的基础上，借鉴文献[3]中保护接收者匿名性的思想，设计了一个无证书多接收者签密方案，并在随机预言机模型下证明了方案的安全性，方案能同时保护签密者和接收者的身份隐私，而且由于方案中没有使用双线性对运算，因此与同类方案相比具有较高的运行效率。

2 背景知识

2.1 无证书签密方案的构成

无证书签密方案由签密方（ID_A）、接收方（ID_B）及密钥生成中心(KGC)通过执行以下算法构成。

设置系统参数：以安全参数η作为输入，KGC 设置公开的系统参数，产生系统主密钥 w 并严格保密。

设置用户部分公、私钥：以系统参数、主密钥 w 和用户身份 ID_{u} 作为输入，KGC 设置用户的部分公、私钥（$D_{\mathrm{u}}, W_{\mathrm{u}}$）。

设置用户秘密值：以系统参数、用户身份 ID_{u} 作为输入，签密用户设置自己的秘密值 u_{u}。

设置用户私钥：以系统参数、用户身份 ID_{u}、部分私钥 W_{u}、秘密值 u_{u} 作为输入，签密用户设置自己的完整私钥 SK_{u}。

设置用户公钥：算法由签密用户执行。以系统参数、用户身份 ID_{u}、部分公钥 D_{u}、秘密值 u_{u} 作为输入，设置自己的完整公钥 PK_{u}。

签密算法：该算法以系统参数、明文消息 m、签密者身份 ID_A、签密者私钥 SK_A、接收者身份 ID_B、接收者公钥 PK_B 作为输入，签密方最终输出对消息 m 的签密密文 σ 。

验证签密算法：该算法以系统参数、密文 σ 、签密者身份 ID_A、公钥 PK_A、接收者身份 ID_B、接收者私钥 SK_B 作为输入，接收方进行验证，最终输出解密消息 m，或者“拒绝”。

2.2 困难问题

计算性 Diffie-Hellman 问题（CDLP）：设 G 是由椭圆曲线上的点构成的阶为素数 q 的加法循环群，P 为 G 中的一个生成元，已知 $aP,bP\in G$，计算 abP。

椭圆曲线离散对数问题（ECDLP）：设 G 是由椭圆曲线上的点构成的阶为素数 q 的加法循环群，P 为 G 中的一个生成元，已知 $aP\in G$，求解 a。

3 无证书多接收者签密安全模型

文献[4]给出了基于身份的门限解密多接收者签密方案的安全模型，文献[14]给出了无证书签密方案的安全模型，本节在对文献[4,14]中的 2 类安全模型进行分析研究的基础上给出无证书多接收者签密的安全模型。首先，攻击无证书签密方案的敌手目前主要分为 2 类：一类敌手可以任意替换用户的公开密钥，但是无法得到系统主密钥，将该

类敌手标记为 A_{I}；另一类敌手可以得到系统主密钥，但是不能对用户公钥进行替换，将该类敌手标记为 A_{II}。

一个安全的无证书签密方案通常应满足选择消息攻击下密文的机密性和签名的不可伪造性。本文利用一个由敌手（包括 A_{I} 和 A_{II}）和挑战者 F 参与的游戏来定义无证书多接收者签密的安全模型。

定义 1　假设攻击者为第一类敌手 A_{I}，如果 A_{I} 在概率多项式时间内不能以不可忽略的优势在以下设置的游戏中胜出，则称无证书多接收者签密方案在适应性选择密文攻击下满足不可区分性。

参数设置：挑战者 F 设置系统主密钥和公共参数，并将系统公共参数传递给 A_{I}。在接收到系统公共参数后，A_{I} 输出 k 个目标身份 $L^*=(ID_1^*,ID_2^*,\mathrm{L}\ ,ID_k^*)$。$A_{\mathrm{I}}$ 向挑战者 F 发起以下几种询问。

散列询问：A_{I} 就输入的任意散列值进行询问。

部分私钥生成询问：A_{I} 向 F 发送对身份 ID 的部分私钥生成询问，F 生成该身份 ID 的部分私钥 W_{ID}，进而返回给 A_{I}。

秘密值生成询问：A_{I} 向 F 发送对身份 ID 的秘密值生成询问，F 生成该身份 ID 的秘密值 u_{ID}，并返回给 A_{I}。

公钥生成询问：A_{I} 向 F 发送对身份 ID 的公钥生成询问，F 生成用户 ID 的公钥 PK_{ID}，并返回给 A_{I}。

用户公钥替换：对任意身份 ID，A_{I} 可以选择一个新公钥来替换用户 ID 原有的公钥 PK_{ID}。

签密询问：A_{I} 选取消息 m，接收者身份 $L=(ID_1,ID_2,\cdots,ID_k)$及签密者身份 ID_{u}，向 F 进行签密询问，F 分别生成接收者 $ID_i\in L$ 的公钥 PK_i 和签密者 ID_{u} 的私钥 SK_{u}。计算σ=Signcrypt($params$, m, L, SK_{u})，并返回给 A_{I}。

解签密询问：F 收到该询问后，计算接收者 $ID_i\in L$ 的私钥 SK_i 和 ID_{u} 的公钥 PK_{u}。由解签密算法计算 Unsigncrypt($params$, σ,PK_{u},SK_i)，返回明文 m 或“拒绝”给 A_{I}。

挑战：A_{I} 选择 2 个等长的消息 m_0、m_1 和一个希望挑战的身份 ID_{u}^*，F 计算 ID_{u}^* 的私钥 SK_{u}^*，随机选择 $b\in\{0,1\}$,计算 $\sigma^*=\mathrm{Signcrypt}(params,\ m_b,L^*,\ SK_{\mathrm{u}}^*)$，将 σ^* 发送给 A_{I}。

猜测：A_{I} 像询问阶段一样进行多次询问（注意不允许对 $ID_i^*\in L^*$ 进行部分私钥生成询问和私钥生成询问，也不能对 σ^* 进行解签密询问）。最后，输出一个 b' 作为对 b 的猜测，如果 $b'=b$，则 A_{I} 在此游戏中胜出，其优势为

$$Adv^{\text{IND-CCA2}}(A_{\mathrm{I}})=\left|\Pr[b'=b]-\frac{1}{2}\right|$$

定义 2　假设攻击者为第二类敌手 A_{II}，如果 A_{II} 在概率多项式时间内不能以不可忽略的优势在以下设置的游戏中胜出，则称无证书多接收者签密方案在适应性选择密文攻击下具有不可区分性。

参数设置：挑战者 F 设置系统主密钥和公共参数，并将系统公共参数传递给 A_{II}。在接收到系统公共参数后，A_{II} 输出 k 个目标身份 $L^*=(ID_1^*,ID_2^*,\mathrm{L}\ ,ID_k^*)$。

询问：A_{II} 进行类似于定义 1 中的散列询问、部分私钥询问、秘密值询问、签密询问和解签密询问，但不能进行“用户公钥替换”。

挑战和猜测阶段与定义 1 相同。

定义 3　A_{I} 敌手攻击下的不可伪造性。假设攻击者为第一类敌手 A_{I}，如果 A_{I} 在概率多项式时间内不能以不可忽略的优势在以下设置的游戏中胜出，则称无证书多接收者签密方案在适应性选择消息攻击下具有不可伪造性。

参数设置：挑战者 F 设置系统主密钥和公共参数，并将系统公共参数传递给 A_{I}。在接收到系统公共参数后，A_{I} 输出一个目标身份 ID_{u}^*。

询问阶段与定义 1 中相同。

伪造：A_{I} 输出伪造的签密消息$(\sigma^*,ID_{\mathrm{u}}^*,L)$，如果 A_{I} 没有对 ID_{u}^* 进行部分私钥查询和秘密值查询，σ^* 不是经过签密询问产生，且 σ^* 可以通过接收者集合 L 中的任意一个接收者的解密验证，则说 A_{I} 在这个游戏中胜出。

定义 4　A_{II} 敌手攻击下的不可伪造性。假设攻击者为第二类敌手 A_{II}，如果 A_{II} 在概率多项式时间内不能以不可忽略的优势在以下设置的游戏中胜出，则称无证书多接收者签密方案在适应性选择消息攻击下具有不可伪造性。

系统参数设置及询问阶段与定义 2 中相同。

伪造：A_{II} 输出伪造的签密消息$(\sigma^*,ID_{\mathrm{u}}^*,L)$，如果 A_{II} 没有对 ID_{u}^* 进行部分私钥查询和秘密值查询，σ^* 不是经过签密询问产生，且 σ^* 可以通过接收者集合 L 中的任意一个接收者的解密验证，则说 A_{II} 在这个游戏中胜出。

4 无证书多接收者签密方案

1) 设置系统参数

KGC 设定一个系统安全参数η，生成符合安全要求的大素数 q, 选择阶为素数 q 的椭圆曲线加法循环群 G，选取 P 为加法群 G 的一个生成元；定义如下 4 个安全的散列函数。

H_0：$\{0,1\}^*\times G\times G\rightarrow Z_q^*$

H_1：$G\times\{0,1\}^*\times G\rightarrow Z_q^*$

H_2：$G\rightarrow\{0,1\}^*$

H_3：$\{0,1\}^*\rightarrow Z_q^*$

随机选择整数 $w\in Z_q^*$作为系统主密钥，计算 $P_{\text{sys}}=wP$ 作为系统公钥，对外公开系统参数(q,P_{sys}, H_0, H_1, H_2, H_3)，严格保密系统主密钥 w，设定待签密消息 m 为任意长的二进制序列。

2) 设置用户秘密值

用户 ID_i 随机选择整数 $u_i\in Z_q^*$，严格保密并作为自己的秘密值，计算 $U_i=u_iP$，将 $U_i||ID_i$ 安全传递给 KGC。

KGC 在收到消息 $U_i||ID_i$ 以后，随机选择整数 $d_i\in Z_q^*$，并计算

$$D_i=d_iP,\ W_i=d_i+wH_0(ID_i,D_i,U_i)$$

进而通过安全渠道将 $W_i||D_i$ 返回给用户 ID_i，用户收到 KGC 的回复信息后，提取部分私钥 W_i，将自己的完整私钥设置为(u_i,W_i)，提取部分公钥 D_i ，将自己的完整公钥设置为(U_i,D_i)。用户可进一步验证等式 $D_i+H_0(ID_i,D_i,U_i)P_{\text{sys}}=W_iP$ 是否成立来判断 KGC 发送给自己的部分私钥的真实性。

3) 签密算法

签密者身份为 ID_A，接收者身份集合为 $\{ID_1,ID_2,\cdots,ID_k\}$，签密者执行以下步骤对消息 m 进行签密。

①随机选择整数 $r_1\in Z_q^*$，计算 $T=r_1P$ 和 $h=H_1(T+U_A, ID_A, m, D_A)$，$s=\dfrac{r_1+u_A}{u_A+hW_A}$。

②计算 $h_i=H_0(ID_i,D_i,U_i)$，随机选择整数 $r_2\in Z_q^*$，计算 $R=r_2P$，$C=H_2(R)\oplus(m||ID_A||s)$。

③计算 $x_i=H_3(ID_i),1\leqslant i\leqslant k$，计算拉格朗日差值多项式 $f_i(x)=\prod\limits_{1\leqslant j\neq i\leqslant k}\dfrac{x-x_j}{x_i-x_j}=c_{i1}+c_{i2}x+\text{L}\ c_{ik}x^{k-1}$，其中，$c_{i1},c_{i2},\cdots,c_{ik}\in Z_q^*$。

④计算 $Y_i=r_2(U_i+D_i+h_iP_{\text{sys}}),V_i=\sum\limits_{j=1}^{k}c_{ji}Y_j$,$1\leqslant i\leqslant k$。

⑤签密者将密文$\sigma=(V_1,V_2,\cdots,V_k,T,C)$分别发送给接收者 $ID_1,ID_2,\cdots,ID_k$。

4) 验证签密算法

接收者 $ID_i(1\leqslant i\leqslant k)$执行以下步骤对接收到的签密密文$\sigma=(V_1,V_2,\cdots,V_k,T,C)$进行解密并验证签名。

①利用自己的身份信息计算 $x_i=H_3(ID_i)$，$Y_i'=V_1+x_iV_2+\text{L}\ x_i^{k-1}(\text{mod}\,q)V_k$，计算 $R'=(u_i+W_i)^{-1}Y_i'$，恢复原始消息及签名 $(m\,||\,ID_A||s)=H_2(R')\oplus C$。

②从恢复的消息中得到发送者的身份信息 ID_A，进而计算 $h'=H_1(T+U_A,ID_A,m,D_A)$ 和 $h_A'=H_0(ID_A,D_A,U_A)$；最后利用发送者的公钥信息(U_A,D_A)验证 $h'=H_1(s(U_A+h'(D_A+h_A'P_{\text{sys}})),\ ID_A,m,D_A)$ 是否成立，如果成立，接收者确认收到的签密消息为来自 ID_A 的真实签密，否则拒绝该签密。

下面对签密算法的正确性和匿名性进行证明。

$$\begin{aligned}
Y_i' &= V_1+x_iV_2+\text{L}\ x_i^{k-1}(\text{mod}\,q)V_k\\
&=\sum_{j=1}^{k}c_{j1}Y_j+x_i(\sum_{j=1}^{k}c_{j2}Y_j)+\text{L}\ +x_i^{k-1}(\sum_{j=1}^{k}c_{jk}Y_j)\\
&=(\sum_{j=1}^{k}c_{1j}x_i^{j-1})\ Y_1+(\sum_{j=1}^{k}c_{2j}x_i^{j-1})\ Y_2+\text{L}\\
&\quad(\sum_{j=1}^{k}c_{ij}x_i^{j-1})\ Y_i+\text{L}\ +(\sum_{j=1}^{k}c_{kj}x_i^{j-1})\ Y_k\\
&=f_1(x_i)Y_1+f_2(x_i)Y_2+\text{L}\ +f_i(x_i)Y_i=Y_i\\
R' &= (u_i+W_i)^{-1}Y_i'\\
&=(u_i+W_i)^{-1}r_2(U_i+D_i+h_iP_{\text{sys}})\\
&=(u_i+W_i)^{-1}r_2(u_i+d_i+h_iw)\ P\\
&=(u_i+W_i)^{-1}r_2(u_i+W_i)\ P\\
&=r_2P\\
h' &= H_1(s(U_A+h'(D_A+h_A'P_{\text{sys}})),ID_A,m,D_A)\\
&=H_1((\frac{r_1+u_A}{u_A+hW_A})(U_A+h(D_A+h_AP_{\text{sys}})),ID_A,m,D_A)\\
&=H_1((\frac{r_1+u_A}{u_A+hW_A})(u_A+hW_A)P,ID_A,m,D_A)\\
&=H_1((r_1+u_A)P,ID_A,m,D_A)\\
&=H_1(T+U_A,ID_A,m,D_A)=h
\end{aligned}$$

上述无证书多接收者签密方案中，对消息发送者的身份信息 ID_A 与消息 m 一起进行了加密处理，非合法接收者无法获知发送方的身份信息，由此确

保了发送方身份的匿名性。同时，借鉴文献[3]中的思想，利用拉格郎日插值多项式将各个接收者的身份信息隐藏在 $(V_1,V_2,\cdots,V_k)$ 中，密文中无需加入接收者身份与相关密文的关联信息，每个接收者在对签密消息进行解密的过程中只需要利用公共的密文信息$\sigma=(V_1,V_2,\cdots,V_k,T,C)$和自己的身份信息即可，不需要利用其他接收者的身份信息，因此方案可以确保接收者身份不外泄，即使同一接收群组中的成员也无法获知其他成员的身份信息。

5　安全性证明

本节通过以下4个定理在随机预言机模型下证明第 4 节中所提无证书多接收者签密方案的安全性。

定理 1　A_1敌手攻击下的不可区分性。在随机预言机模型中，如果有敌手 A_1 以不可忽略的概率辨别密文，挑战者 F 可以利用该敌手解决一个特定的CDHP。

证明　F 是 CDHP 挑战者。散列函数 H_0、H_1、H_2 和 H_3 是随机预言机，给定$\{P, vP, fP\}$，F 期望通过 A_1 辨别密文的过程计算出 vfP。为了达到挑战目的，F 需要设置系统参数：$P_{sys}=vP$ 及 $(G,q,P,P_{sys},H_0,H_1,H_2,H_3)$。$F$ 把设置好的系统参数发送给 A_1。A_1 输出 k 个目标身份 $L^*=(ID_1^*,ID_2^*,\mathrm{L}\ ,ID_k^*)$，并执行 H_0，H_1，H_2，H_3 散列询问、部分私钥询问、秘密值询问、公钥代替询问、签密询问和解签密询问，具体询问过程如下。

H_0-散列询问：A_1 提出针对身份 ID_j 的 H_0-散列询问，如果列表 L-H_0 中存在记录（ID_j，D_j，U_j，h_j），则返回 h_j。否则，F 选择随机数 h_j，将（ID_j，D_j，U_j，h_j）存入 L-H_0，并返回 h_j 给 A_1。

H_1−散列询问：A_1 提出针对（T_j+U_j ,ID_j, m_j,D_j）的 H_1−散列询问，如果列表 L-H_1 中存在记录 $(T_j+U_j,ID_j,m_j,D_j,\delta_j)$，则返回 δ_j。否则，F 选择随机数 $\delta_j\in Z_q^*$，将 $(T_j+U_j,ID_j,m_j,D_j,\delta_j)$ 存入 L-H_1，并返回 δ_j 给 A_1。

H_2−散列询问：A_1 提出针对 R 的 H_2-散列询问，如果列表 L-H_2 中存在记录 (R,ξ)，则返回 ξ。否则，F 选择随机数 $\xi\in Z_q^*$，将 (R,ξ) 存入 L-H_2，并返回 ξ 给 A_1。

H_3−散列询问：A_1 提出针对身份 ID_j 的 H_3-散列询问，如果列表 L-H_3 中存在记录（ID_j，x_j），则返回 x_j。否则，F 选择随机数 $x_j\in Z_q^*$，将（ID_j，x_j）存入 L-H_3，并返回 x_j 给 A_1。

阶段 I：A_1 向 F 进行以下各项询问。

1) 公开密钥询问：A_1 提出针对身份 ID_j 的公开密钥询问，如果（ID_j，D_j，U_j）在 L-PK 中，则返回 $PK_j=(D_j,U_j)$，否则，分 2 种情况进行回复。① 如果 $ID_j\neq ID_j^*$，F 随机选择 W_j，h，$u_j\in Z_q^*$，计算 $D_j=W_jP-hP_{sys}$，$U_j=u_jP$，然后，将（ID_j，D_j，U_j，h）、（ID_j，u_j，W_j）和（ID_j，D_j，U_j）分别加入 L-H_0、L-SK 和 L-PK 中，最后，F 返回 $PK_j=(D_j,U_j)$给敌手 A_1。② $ID_j=ID_j^*$，F 随机选择 u_j，d_j，$W_j\in Z_q^*$，计算 $U_j=u_jP$，$D_j=d_jP$，然后将(ID_j,u_j,W_j)加入 L-SK 中，将（ID_j，D_j，U_j）加入 L-PK 中，并返回 $PK_j=(D_j,U_j)$给 A_1。

2) 秘密值询问：A_1 提出针对身份 ID_j 的秘密值询问，F 首先执行公开密钥询问，在 L-PK 中得到记录（ID_j，D_j，U_j），进而查询 L-SK 得到（ID_j，u_j，W_j），最后，返回 u_j 给 A_1。

3) 部分私钥询问：A_1 提出针对身份 ID_j 的部分私钥询问，F 执行公开密钥询问，在 L-PK 中得到记录（ID_j, D_j, U_j），若 $ID_j\neq ID_j^*$，则查询 L-SK 得到（ID_j, u_j, W_j），并返回 W_j 给 A_1。否则，返回“拒绝”信息并停止游戏。

4) 公钥替换询问：对于身份 ID_j，A_1 选择新的公钥 (ID_j,D_j',U_j') 并提供给 F，F 将(ID_j,D_j,U_j)替换为新公钥 (ID_j,D_j',U_j')。

5) 签密询问：A_1 提出针对身份$(m, L=(ID_1, ID_2,\cdots,ID_k),ID_u)$的签密询问，$F$ 做出如下回应。①如果 $ID_u\neq ID_j^*$，F 可以通过查询 L-SK 得到(u_u, W_u)，继而执行签密算法得到$(V_1,V_2,\cdots, V_k,T,C)$，并将$((m,L,ID_u,V_1,V_2,\cdots,V_k,T,C)$加入 L-SC 中，最后,返回$(V_1,V_2,\cdots,V_k,T,C)$给 A_1。②若 $ID_u=ID_j^*$，$ID_j\neq ID_j^*$，j=1,2, $\cdots$,k，F 随机选择整数 $h',s',r_2'\in Z_q^*$，令 $T'=s'(U_u+h'(D_u+h_uP_{sys}))-U_u$，计算 $R'=r_2'P$，$C'=H_2(R')\oplus(m\,\|\,ID_u\|s')$；在 L-H_3 中查找（ID_j, x_j），j=1,2,$\cdots$,k，计算 $Y_j=r_2(U_j+D_j+h_jP_{sys})$，进而计算得到 V_i' (i=1,2,$\cdots$,k)，将签密密文 $(m,L,ID_u,V_1',V_2',\mathrm{L}\ ,V_k',T',C')$ 加入 L-SC，将 $(T'+U_u,ID_u,m,D_u,\delta')$ 和 (R',ξ') 分别加入 L-H_1 和 L-H_2，最后返回 $(V_1',V_2',\mathrm{L}\ ,V_k',T',C')$ 给 A_1。

6) 解签密询问：对$(V_1,V_2,\cdots,V_k,T,C)$和身份

ID_i (i=1,2,…,k)进行解签密询问，在 L-H_3 中找到(ID_i， x_i)， i=1,2,…,k，并计算 $Y_i'=V_1+x_iV_2+\mathrm{L}\ x_i^{k-1}(\mathrm{mod}\,q)V_k$，在 L-SK 中查找（ID_i，u_i，W_i），计算 $R'=(u_i+W_i)^{-1}Y_i'$，恢复 $(m\|ID_\mathrm{u}\|s)=H_2(R')\oplus C$，再在 L-PK 中查找（ID_u, D_u, U_u），计算 $h=H_1(T+U_\mathrm{u},ID_\mathrm{u},m,D_\mathrm{u})$ 和 h_u=$H_0(ID_\mathrm{u},D_\mathrm{u},U_\mathrm{u})$，并验证 $h=H_1(s(U_\mathrm{u}+h(D_\mathrm{u}+h_\mathrm{u}P_\mathrm{sys})),ID_\mathrm{u},m,D_\mathrm{u})$ 是否成立，若成立，则(V_1,V_2,…,V_k,T,C)为有效密文，返回 m 给 A_I；否则，返回“拒绝”。

挑战阶段：A_I 输出签密用户身份 ID_u 和 2 个长度相等的明文(p_0, p_1)。F 随机选取 s^*,h^*， $l\in Z_q^*$，$\theta\in\{0,1\}$，令 $T^*=s^*(U_\mathrm{u}+h^*(D_\mathrm{u}+h_\mathrm{u}P_\mathrm{sys}))-U_\mathrm{u}$，并计算 R^*=lP，$C^*=H_2(R^*)\oplus(p_\theta\|ID_\mathrm{u}\|s^*)$，在 L-H_3 中找到与 ID_j^* 对应的 x_j^*，计算 $Y_j^*=l(U_j^*+D_j^*+h_j^*P_\mathrm{sys})$，并得到 V_i^*，最后，将(V_1^*,V_2^*,L ,V_k^*,T^*,C^*)返回给 A_I。

A_I 经过执行类似于第一阶段中的询问后（但不能询问 $L^*=(ID_1^*,ID_2^*,\mathrm{L}\ ,ID_k^*)$ 的私钥，也不能对(V_1^*,V_2^*,L ,V_k^*,T^*,C^*)进行解签密询问），输出 θ' 作为对 θ 的猜测，如果猜测与实际吻合，则以极大的概率对 R^*进行了 H_2-散列询问，F 可以从 L-H_2 中查找到(R^*,ξ^*)，并输出 $l^{-1}(u_j^*+W_j^*)R^*-U_j^*-D_j^*=h_j^*vP$，从而 F 利用敌手 A_I 对密文的辨别解决了一个特定的 CDHP。

定理 2 A_II 敌手攻击下的不可区分性。在随机预言机模型中，如果有敌手 A_II 以不可忽略的概率辨别密文，挑战者 F 可以利用该敌手解决一个特定的 CDHP。

证明 敌手 A_II 可以进行类似于定理 1 中的散列询问，公开密钥询问，秘密值询问部分私钥询问，签密询问，解签密询问，与 A_I 的区别在于 A_II 不能进行公钥替换询问，但是能获知系统主密钥。

挑战阶段：A_II 经过一系列询问后，A_II 输出签密用户身份 ID_u 和 2 个长度相等的明文(p_0,p_1)。F 随机选取 s^*,h^*，$l\in Z_q^*$，$\theta\in\{0,1\}$，令 $T^*=s^*(U_\mathrm{u}+h^*(D_\mathrm{u}+h_\mathrm{u}P_\mathrm{sys}))-U_\mathrm{u}$，并计算 R^*=lP，$C^*=H_2(R^*)\oplus(p_\theta\|ID_\mathrm{u}\|s^*)$，在 L-H_3 中找到与 ID_j^* 对应的 x_j^*，计算 $Y_j^*=l(U_j^*+D_j^*+h_j^*P_\mathrm{sys})$，并得到 V_i^*，最后，将(V_1^*,V_2^*,L ,V_k^*,T^*,C^*)返回给 A_II。

A_II 经过执行散列询问，公开密钥询问，秘密值询问，部分私钥询问，签密询问及解签密询问后（但不能询问 $L^*=(ID_1^*,ID_2^*,\mathrm{L}\ ,ID_k^*)$ 的私钥，也不能对(V_1^*,V_2^*,L ,V_k^*,T^*,C^*)进行解签密询问），输出 θ' 作为对 θ 的猜测，如果猜测与实际吻合，则以极大的概率对 R^*进行了 H_2-散列询问，F 可以从 L-H_2 中查找到(R^*,ξ^*)，并输出 $(W_j^*-h_j^*v)R^*=d_j^*lP$，从而 F 利用敌手 A_II 对密文的辨别解决了一个特定 CDHP。

定理 3 A_I 敌手攻击下的不可伪造性。假设 A_I 为针对无证书签密的第一类型敌手，如果在随机预言机模型下，经过有限次询问 A_I 能以不可忽略的概率伪造出合法签密，则利用该伪造过程挑战者 F 能够给出一个 ECDLP 问题的解。

给定{P,vP}，ECDLP 挑战者 F 希望利用敌手 A_I 伪造一个合法签密的过程计算出 v。首先，F 按照自己的需求将系统参数设置为：P_sys=vP 及 (G,q,P,P_sys, H_0,H_1,H_2,H_3)。

接下来，F 把预先设置好的系统参数发送给 A_I。A_I 收到系统参数后，分别执行 H_0，H_1，H_3 散列询问、部分私钥询问、秘密值询问、公钥代替询问、签密和解签密询问（询问过程与定理 1 中类似，不再赘述）后，进而通过以下步骤伪造 ID_u 的签密：随机选取 r_1^*,s^*， $r_2^*\in Z_q^*$，计算

$$T^*=r_1^*P,\ h^*=H_1(T^*+U_\mathrm{u},ID_\mathrm{u},m,D_\mathrm{u})$$

$$h_\mathrm{u}^*=H_0(ID_\mathrm{u},D_\mathrm{u},U_\mathrm{u}),R^*=r_2^*P$$

$$C^*=H_2(R^*)\oplus(m\|ID_\mathrm{u}\|s^*)$$

在 L-H_3 中找到与 ID_j^* 对应的 x_j^*，计算 $Y_j^*=r_2^*(U_j^*+D_j^*+h_j^*P_\mathrm{sys})$，并得到 V_i^*，最后输出(V_1^*,V_2^*,L ,V_k^*,T^*,C^*)。若该签密能顺利通过验证，则 F 利用敌手 A_I 的上述伪造签密过程输出

$$v=\frac{(r_1^*+u_\mathrm{u}-s^*(u_\mathrm{u}+h^*d_\mathrm{u}))}{s^*h^*h_\mathrm{u}^*}$$

作为 ECDLP 的解。因此，只要敌手 A_I 能伪造出可以通过验证的合法签密，F 就可以通过 A_I 的伪造过程求出一个特定 ECDLP 的解。

定理 4 A_II 敌手攻击下的不可伪造性。假设 A_II 为针对无证书签密的第一类型敌手，如果在随机预言机模型下，经过有限次询问 A_II 能以不可忽略的概率伪造出合法签密，则利用该伪造过程挑战者 F 能够给出一个 ECDLP 问题的解。

给定{P,vP}，ECDLP 挑战者 F 希望利用敌手

A_{II} 伪造一个合法签密的过程计算出 v。首先，F 按照自己的需求将系统参数设置为 $P_{sys}=vP$ 及 $(G,q,P,P_{sys},H_0,H_1,H_2,H_3)$，并将系统参数发送给 A_{II}，按照安全模型的定义 A_{II} 还可以获得系统主密钥 v。A_{II} 依次执行类似于定理 2 中的各项询问，随机选取整数 $r_1^*,s^*,r_2^*\in Z_q^*$，并计算

$$T^*=r_1^*P,\ h^*=H_1(T^*+U_u,ID_u,m,D_u)$$

$$h_u^*=H_0(ID_u,D_u,U_u),R^*=r_2^*P$$

$$C^*=H_2(R^*)\oplus(m\|ID_u\|s^*)$$

在 L-H_3 中找到与 ID_j^* 对应的 x_j^*，计算 $Y_j^*=r_2^*(U_j^*+D_j^*+h_j^*P_{sys})$ 并得到 V_i^*，最后输出伪造的签密 $(V_1^*,V_2^*,\mathrm{L},V_k^*,T^*,C^*)$。

如果该签密能通过验证，则 F 利用敌手 A_{II} 的伪造过程输出

$$d_u=\frac{(r_1^*+u_u-s^*(u_u+vh^*h_u^*))}{s^*h^*}$$

因此，只要敌手 A_{II} 能伪造出可以通过验证的合法签密，F 就可以通过 A_{II} 的伪造过程求出一个特定 ECDLP 的解。

6　性能分析

本节给出所提无证书多接收者签密方案与同类方案在计算效率及安全性方面的比较分析。为了对比本文方案与同类方案的运算效率，用记号 SM 代表椭圆曲线上的点乘运算，用记号 E 代表乘法群上的指数运算，记号 BP 代表双线性对运算（参数规模为 512 bit 的 BP 耗费的时间约为模数大小为 1 024 bit 的 E 耗费时间的 10 倍以上[16]），而 BP 所花费的运算时间是 SM 的 20 倍左右[17]）。由于其他运算（散列运算、点加运算）消耗的时间远少于 SM 和 E，因此不列入效率比较的范围。另外，本文方案签密算法步骤②中计算 $h_i=H_0(ID_i,D_i,U_i)$，选择随机数 $r_2\in Z_q^*$ 及计算 $R=r_2P$ 均未使用对消息 m 签名时使用的一次性随机数 r_1，故可进行预计算；步骤③中计算 $x_i=H_3(ID_i)$，$f_i(x)$ 可以预计算；步骤④中计算 Y_i，V_i 使用了随机数 r_2，可以与步骤②中的运算一起进行预计算，因此本文方案中的步骤③、④可以不列入最终的运算量。对比过程中其他方案按照同样标准计算运算量，即与用于对消息 m 签名的一次性随机数有关的运算不可预计算。

表 1 给出了本文方案与已有的基于身份的多接收者签密方案[3~6]的运算效率对比，可以看出本文方案在签密阶段和解签密阶段均不需要进行双线性对运算，与文献[3~5]相比具有明显的运算优势，文献[6]中的方案 2 在签密和解签密阶段的运算量虽然与接收者人数 k 无关，但却无法确保接收者的匿名性，且系统构造及安全性存在较大问题[7]。而本文解签密阶段的运算量与 k 有关，是因为在签密阶段签密者利用拉格朗日差值多项式将各个接收者的身份信息 $ID_1,ID_2,\cdots,ID_k$ 隐藏在 $(V_1,V_2,\cdots,V_k)$ 中，签密接收者在对签密密文 $\sigma=(V_1,V_2,\cdots,V_k,T,C)$ 进行验证时需要计算

$$Y_i'=V_1+x_iV_2+\mathrm{L}\ x_i^{k-1}(\mathrm{mod}\,q)V_k$$

其中，包含 k–1 次点乘运算。

表 1　　效率比较

签密方案	签密阶段	解签密阶段
文献[3]方案	1BP+(4+k^2)SM	4BP+kSM
文献[4]方案	1E+(k+1)SM	(k+1)E+2BP
文献[5]方案	(3+k)E	5BP
文献[6]方案 2	3E	2BP+3E
本文方案	SM	(k+3)SM

表 2 给出了本文方案与文献[3~6]中方案的安全性比较，综合起来考虑，本文方案基于无证书公钥密码体制设计，避免了基于身份公钥密码存在的密钥托管问题，在确保签密安全性及签密者与接收者匿名性的同时保持了较高的运算效率。

表 2　　安全性比较

签密方案	密钥托管问题	签密者匿名性	接收者匿名性	方案正确性	安全模型
文献[3]方案	存在	满足	满足	签密及验证算法存在错误	随机预言机
文献[4]方案	存在	不满足	不满足	正确	随机预言机
文献[5]方案	存在	不满足	不满足	验证等式中未使用签密者身份信息	标准模型
文献[6]方案 2	存在	不满足	不满足	签密及解签密中使用了主密钥	随机预言机（存在签密伪造）
本文方案	不存在	满足	满足	正确	随机预言机

7 结束语

本文构造了无证书多接收者签密的安全模型，在此基础上利用椭圆曲线密码设计了一种无证书多接收者签密方案，并在随机预言机模型下证明该方案的安全性建立在计算 Diffie-Hellman 问题及椭圆曲线离散对数问题的困难性上。该方案克服了基于身份的多接收者签密存在的私钥托管问题，在签密阶段和解签密阶段均不含双线性对运算，与同类方案相比具有较高的运算效率，且可同时实现对发送者和接收者身份信息的隐藏，因此可以方便地应用于网络环境中需要进行广播签密的场合。

参考文献：

[1] ZHENG Y.Digital signcryption or how to achieve(signature & encryption)<<cost(signature)+cost(encryption) [C]//The Crypto'97. c1997: 291-312.

[2] DUAN S, CAO Z. Efficient and provably secure multi receiver identity based signcryption[C]//The 11th Australasian Conf on Information Security and Privacy (ACISP 2006). LNCS 4058, Heidelberg: Springer-Verlag, c2006: 195-206.

[3] 庞辽军, 李慧贤, 崔静静, 等. 公平的基于身份的多接收者匿名签密设计与分析[J]. 软件学报, 2014, 25(10): 2409-2420.
PANG L J,LI H X,CUI J J, et al. Design and analysis of a fair ID based multi-receiver anonymous signcryption[J]. Journal of Software, 2014, 25(10): 2409-2420.

[4] ZHANG M W, YANG B, TSUYOSHI T. Reconciling and improving of multi-receiver signcryption protocols with threshold decryption[J]. Security and Communication Networks ,2012, 5: 1430-1440.

[5] MING Y, ZHAO X M, WANG Y M. Multi-receiver identity-based signcryption scheme in the standard model[C]//ICICA 2011, LNCS 7030, Springer-Verlag. Berlin Heidelberg, c2011: 487-494.

[6] INTAE K, SEONG O H. Efficient identity-based broadcast signcryption schemes[J]. Security and Communication Networks, 2014, 7(1): 914-925.

[7] ZHANG J, TANG W. On the security of Kim et al. two ID-based broadcast signcryption schemes[J]. Security and Communication Networks, 2015, 8(8): 1509-1514.

[8] ZHANG B, XU QL. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model[C]//The AST/UCMA/ISA/ACN 2010 Conf. on Advances in Computer Science and Information Technology(AST/UCMA/ISA/ACN2010).LNCS 6059. Heidelberg: Springer-Verlag, c2010: 15-27.

[9] NAKANO R, SHIKATA J J. Constructions of signcryption in the multi-user setting from identity-based encryption[C]//IMACC 2013, LNCS 8308. c2013: 324-343.

[10] AHMED F, MASOOD D A, KAUSAR F. An efficient multi recipient signcryption scheme offering non repudiation[C]//2010 10th IEEE International Conference on Computer and Information Technology. C2010: 1577-1581.

[11] ALRIYAMI S, PATERSON K. Certificateless public key cryptography[C]//ASIACRYPT 2003. c2003: 452-473.

[12] 李慧贤, 陈绪宝, 庞辽军, 等. 基于多变量公钥密码体制的无证书多接收者签密体制[J]. 计算机学报, 2012, 35(9): 1881-1889.
LI H X, CHEN X B, PANG L J, et al. Certificateless multi receiver signcryption scheme based on multivariate public key cryptography[J].Chinese Journal of Computers, 2012, 35 (9):1881-1889.

[13] 朱辉, 李晖, 王育民. 不使用双线性对的无证书签密方案[J].计算机研究与发展, 2010, 47(9): 1587-1594.
ZHU H, LI H, WANG Y M. Certificateless signcryption scheme without pairing[J].Journal of Computer Research and Development,2010，47(9):1587-1594.

[14] 刘文浩, 许春香. 无双线性配对的无证书签密机制[J]. 软件学报, 2011, 22(8): 1918-1926.
LIU W H, XU C X. Certificateless signcryption scheme without bilinear pairing[J]. Journal of Software, 2011, 22(8): 1918-1926.

[15] 何德彪. 无证书签密机制的安全性分析[J]. 软件学报, 2013, 24(3): 618-622.
HE D B. Security analysis of a certificateless signcryption scheme[J]. Journal of Software, 2013, 24(3): 618-622.

[16] MIRACL.Multiprecision integer and rational arithmetic C/C++library[EB/OL].http://indigo.ie/mscott/,2004.

[17] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. Int'l Journal of Information Security, 2007, 6(4): 213-241.

作者简介：

秦艳琳（1980-），女，河南安阳人，博士，海军工程大学讲师，主要研究方向为密码学及网络安全。

吴晓平（1961-），男，山西新绛人，海军工程大学教授、博士生导师，主要研究方向为信息安全及系统工程。

胡卫（1979-），男，湖北宜城人，海军工程大学副教授，主要研究方向为网络与信息安全。