第27卷 第8期
2017年8月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol. 27 No. 8
Aug. 2017

无双线性对的无证书聚合签密方案

王梦殊,祁正华
(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:无证书聚合签密是把多个用户对不同消息产生的不同签密聚合成一个签密,不仅保证信息传输的机密性和认证性,而且降低了信息传输的功耗,因此应用于大规模分布式通信中的多对一模式。聚合签密方案大多需要进行双线性对运算,效率不高。为此,提出了一种高效的无线性对的无证书聚合签密方案。该方案在随机预言模型下应用离散对数,对原有的无双线性对聚合签名算法进行了改进,形成了更为安全、高效的聚合签密方案。基于所提出的聚合签密方案安全模型,分析研究了随机预言模型下提出方案的不可伪造性和机密性,并对其有效性和可行性进行了验证。理论分析表明,所提出的方案在多个签密者存在的条件下,不仅具有机密性、不可伪造性,还具有更高的计算效率。

关键词:无证书聚合签密;随机预言模型;无双线性对;离散对数问题

中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2017)08-0115-06

doi:10.3969/j.issn.1673-629X.2017.08.024

A Certificateless Aggregate Signcryption Scheme without Bilinear Pairing

WANG Meng-shu,QI Zheng-hua
(School of Computer Science and Technology,Nanjing University of Posts and Telecommunications,
Nanjing 210003,China)

Abstract:Certificateless aggregate signcryption scheme can aggregate different signcryptions generated by multi-users corresponding to various information into one signcryption,which can not only ensure the confidentiality and certification in information transmission but also reduce power dissipation. Therefore,it is applied in the multiple-to-single mode in large-scale distributed communication. Most aggregate signcryption schemes need computation of bilinear pairing with poor efficiency. For that,an efficient certificateless aggregate signcryption schemes without bilinear pairing is proposed,where disperse logarithm is employed in random oracle model to improve the original aggregate signature algorithm without bilinear pairing for safer and more effective one. Based on the proposed aggregate signcryption security model,investigation and analysis on the presented scheme with random oracle model is performed and validation on its effectiveness and feasibility also conducted. Theoretical analysis shows that in the presence of multiple signcrypter it owns not only the confidentiality and unforgeability but also higher computational efficiency.

Key words:certificateless aggregate signcryption;random oracle model;without bilinear pairing;discrete logarithm problem

0 引 言

签密[1]在合理逻辑步骤里同时完成信息的签名与伽马。2009年,Selvi等[2]提出了基于身份的签密方案,并证明了其安全性。祁正华[3]进行了基于身份的签密方案研究;于刚[4]进行了若干签密研究。聚合签密能将多个密文进行聚合且提供批量验证,极大降低了信息传输的功耗,大幅提升了签密验证的效率,适用在大规模分布式通信的多对一模式下。Ren等[5]提出了一种可证明安全的聚合签密方案;苏爱东等[6]提出了一种密文长度固定的聚合签密方案,但未给出形式化的安全性证明。

无证书密码体制于2003年由Al-Riyami等[7]提出,解决了公钥证书管理及验证问题和密钥托管问题。Barbosa等[8]提出了无证书签密方案并给出了安全模型。陆海军[9]和Eslami等[10]在随机预言模型下分别提出了可证明安全的无证书聚合签密方案;Qi等[11]提出了无证书环签密方案,但是上述签密方案中用了较多双线性对运算,因此效率较低。Qi等[12]对基于身份的聚合签密进行了安全性分析,但使用了双线性对。周彦伟等[13]提出的无证书聚合签名方案运算量

收稿日期:2016-09-01 **修回日期**:2016-12-07 **网络出版时间**:2017-07-05

基金项目:国家自然科学基金资助项目(61073188)

作者简介:王梦殊(1993-),女,硕士研究生,研究方向为网络与信息安全;祁正华,副教授,博士研究生,研究方向为网络与信息安全。

网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20170705.1651.048.html

小,无需进行双线性运算,因此参考其无双线性对的特点,提出了无双线性对的无证书聚合签密方案并进行了理论分析。

1 相关基础

1.1 离散对数问题

离散对数问题(Discrete Logarithm Problem,DLP):设 G 是 q 阶循环群, q 为素数。给定两个元素 $P,Q \in G$,找到使 $Q = nP$ 成立的整数 n 。

1.2 聚合签密方案的安全模型

文献[4]定义的安全模型,无证书聚合签密方案将面临 A_1 和 A_2 两类敌手的攻击。

A_1 类敌手不知道系统的主密钥,但可以进行公钥替换操作,或利用所有用户的公钥来对系统主密钥进行攻击,因此 A_1 类敌手为恶意用户。A_2 类敌手已知系统主密钥,具有计算所有用户部分公钥私钥的能力,但不可以替换用户公钥,因此 A_2 类敌手为恶意的 KGC。

选择密文攻击下的机密性和适应性,选择消息攻击下的不可伪造性。方案机密性证明中,U_1 是 A_1 类敌手的挑战者,U_2 是 A_2 类敌手的挑战者,不可伪造性证明中,T_1 是 A_1 类敌手的挑战者,T_2 是 A_2 类敌手的挑战者。文献[14]详细介绍了无证书聚合签密方案在 A_1 和 A_2 两类敌手适应性选择消息攻击下不可伪造性的定义及相应游戏,不再叙述。

定义 1:类型 A_1 攻击下的密文机密性。类型 A_1 的攻击者不能在多项式时间内,以不可忽略的优势赢得以下博弈,则该签密方案在选择密文攻击下具有不可区分性。

SETUP:挑战者 U_1 将生成的系统公共参数发送给敌手 A_1 并保存系统主密钥。

第一阶段:敌手能够多项式次执行的询问如下:

部分密钥生成问询:A_1 输入(ID_i,X_i)进行问询,就可得到(y_i,Y_i)。

私钥生成问询:A_1 输入 ID_i 问询,得到 $SK_i = (x_i, y_i)$ 。

公钥替换询问:A_1 输入 ID_i 和公钥 $PK_i = (X_i,Y_i)$ 问询,选择新的公钥 $PK_i' = (X_i',Y_i')$ 替换 PK_i 。

签密问询:A_1 输入(ID_i,m_i,ID_B)问询,得到:

$\delta_i = (V,V_i,S_i,W_i) = \text{Signcryption}(ID_i,m_i,ID_B)$

解签密问询:A_1 输入签密 δ_i 和身份(ID_i,ID_B)问询,U_1 可进行解签密,将解签密结果返回 A_1。

挑战阶段:A_1 选择要挑战的两个明文 $m_i(i \in \{0,1\})$ 和两个身份 ID_i,ID_B ,不能在第一阶段询问 ID_B 的私钥。U_1 选择一个随机的比特 b ,计算 $\delta^* = \text{Signcryption}(m_b,ID_i,ID_B)$,将 δ^* 发送 A_1。

第二阶段:类似于第一阶段,A_1 能够多项式次执行询问,并且不能询问用户 ID_B 私钥或对 δ^* 进行解签密询问。

猜测阶段:最后 A_1 提交一个比特 b' ,若 $b' = b$,那么 A_1 在此游戏中获胜。游戏中敌手的优势为 $Adv[A_1] = | Pr[b' - b] - 0.5 |$ 。

定义 2:类型 A_2 攻击下的密文机密性。类型 A_2 的攻击者不能在多项式时间内,以不可忽略的优势赢得以下博弈,则该签密方案在选择密文攻击下具有不可区分性[15]。

SETUP:挑战者 U_2 将生成的系统公共参数发送给敌手 A_2 并保存系统主密钥。

第一阶段:敌手可适应性地进行以下多项式数量级的询问:部分密钥生成问询、私钥生成问询、签密问询、解签密问询与定义 1 的问询一样,由 A_1 问询变成 A_2 问询,但不进行公钥替换询问。

第二阶段:类似于第一阶段,A_2 能够多项式次执行询问,并且不能询问用户 ID_B 的私钥或对 δ^* 进行解签密询问。

猜测阶段与定义 1 中类似,最终 A_2 获胜。

2 基于离散对数问题的聚合签密方案

无证书聚合签密由 7 个算法组成,分别是系统初始化、用户密钥设置、部分私钥提取、签密、聚合签密和聚合解签密。

系统初始化:定义阶为素数 q ($q > 2^k$)的循环群 G,P 为群 G 的一个生成元,定义抗碰撞的安全哈希函数:$H_1:\{0,1\}^{L_1} \times G \times G \to Z_q^*$,$H_2:\{0,1\}^{L_2} \times G \times G \to Z_q^*$, $H_3:G \times \{0,1\}^{L_1} \times G \times G \to Z_q^*$,L_1 为用户身份标识的比特长度, L_2 为明文消息的比特长度。随机选取主密钥 s 计算系统公钥 $P_{pub} = sP$,公开参数 $<q,P,G,P_{pub},H_1,H_2,H_3>$,秘密保存主密钥 s 。

用户密钥设置:用户 u_i 随机选取秘密值 x_i ,计算公开参数 $X_i = x_iP$ 。

部分私钥提取:u_i 发送{ ID_i,X_i }给 KGC,KGC 随机选取 $r_i \in Z_q^*$,$Y_i = r_iP$,$h_{i1} = H_1(ID_i,X_i,Y_i)$,$y_i = r_i + sh_{i1}$,用户私钥由(x_i,y_i)组成,公钥由(X_i,Y_i)组成。

签密:用户 u_i 对发送给 ID_B 的消息 m_i 签密如下:

(1)随机选择 $a_i \in z_q^*$,计算 $V_i = a_iP$;将 V_i 发送给其他 $n - 1$ 个用户,当 u_i 收到其他 $n - 1$ 个用户的共享信息 m_i 后,计算 $V = \sum_{i=1}^{n} V_i$,$Z_i = a_i(Y_B + P_{pub}h_{i1})$;

(2)计算 $h_{i2} = H_2(ID_i \parallel m_i,V,Z_i)$;

(3)计算 $T_i = H_3(V_i,ID_B,V,a_iX_B)$;

(4)计算 $W_i = T_i \oplus (m_i \parallel ID_i)$,$S_i = a_i + (x_i + y_i)h_{i2}$ 。这样 $\delta_i = (V,V_i,S_i,W_i)$ 为 u_i 对 ID_B 消息 m_i 的

签密。

聚合签密:在接收到 n 个签密:$\delta_i = (V, V_i, S_i, W_i)$ 后,计算 $V' = \sum_{i=1}^{n} V_i$,若 $V' = V$,计算 $S = \sum_{i=1}^{n} S_i$,聚合签密为 $\delta = < \{V_i, W_i\}_{i=1}^{n}, S, V >$ 。

解签密:ID_B 对 u_i 发送的签密 $\delta_i = (V, V_i, S_i, W_i)$ 的解签密步骤如下:

(1)计算 $T_i = H_3(V_i, ID_B, V, x_B V_i)$,$ID_i \parallel m_i = W_i \oplus T_i$;

(2)计算 $Z_i = a_i(Y_B + P_{pub} h_{i1}) = y_B V_i$,$h_{i1} = H_1(ID_i, X_i, Y_i)$,$h_{i2} = H_2(ID_i \parallel m_i, V, Z_i)$;

(3)根据等式 $S_i P = V_i + (X_i + Y_i + P_{pub} h_{i1}) h_{i2}$ 进行检测,若正确输出对应消息 $m_i \parallel ID_i$,否则验证失败。

聚合解签密:接收者 ID_B 通过如下步骤对聚合签密 $\delta = < \{V_i, W_i\}_{i=1}^{n}, S, V >$ 进行解签密。

(1)计算 $T_i = H_3(V_i, ID_B, V, x_B V_i)$,$ID_i \parallel m_i = W_i \oplus T_i$;

(2)计算 $Z_i = a_i(Y_B + P_{pub} h_{i1}) = y_B V_i$;

(3)计算 $h_{i1} = H_1(ID_i, X_i, Y_i)$,$h_{i2} = H_2(ID_i \parallel m_i, V, Z_i)$,通过等式 $SP = V + \sum_{i=1}^{n} h_{i2}(X_i + Y_i + P_{pub} h_{i1})$ 进行验证,正确即输出对应的 $m_i \parallel ID_i (i = 1, 2, \cdots, n)$,否则认为聚合签密无效。

3　安全性分析

3.1　正确性

方案的正确性证明如下:

通过 $S_i P = V_i + (X_i + Y_i + P_{pub} h_{i1}) h_{i2}$ 对签密进行验证:

$$
\begin{aligned}
S_i P &= [a_i + (x_i + y_i) h_{i2}] P = \\
&a_i P + (x_i P + y_i P) h_{i2} = \\
&V_i + (X_i + Y_i + P_{pub} h_{i1}) h_{i2}
\end{aligned}
$$

通过 $SP = V + \sum_{i=1}^{n} h_{i2}(X_i + Y_i + P_{pub} h_{i1})$ 对聚合签密进行验证:

$$
\begin{aligned}
SP &= (\sum_{i=1}^{n} S_i) P = \sum_{i=1}^{n} [a_i + (x_i + y_i) h_{i2}] P = \\
&\sum_{i=1}^{n} [V_i + (X_i + Y_i + P_{pub} h_{i1}) h_{i2}] = \\
&V + \sum_{i=1}^{n} h_{i2}(X_i + Y_i + P_{pub} h_{i1})
\end{aligned}
$$

3.2　安全性

引理 1:在随机预言模型下,若存在 A_1 类敌手能在多项式时间内以不可忽略的优势 ε 赢得以下博弈,则称该签密方案具有不可伪造性(其中,A_1 最多进行 q_s 次签密询问,q_k 次部分密钥生成询问和 q_{sk} 次私钥生成询问),且存在算法 T_1,能在多项式时间以不可忽略的优势($Adv(T_1) \geqslant (1 - \frac{q_k}{2^k})(1 - \frac{q_{sk}}{2^k}) \frac{\varepsilon}{ne(q_s + n)}$)成功解决离散对数问题。

证明:假设算法 T_1 作为离散对数问题的 solver,输入的元组(P, bP)中 $b \in Z_q^*$ 是未知的,目的是得到 b ,T_1 以 A_1 充当挑战者,运行 SETUP 算法,生成公开参数 PParam=< $q, P, G, P_{pub}, H_1, H_2, H_3$ >,令 $P_{pub} = bP$,将 PParam 给 A_1,同时 T_1 维护列表 $L_1, L_2, L_3, L_k, L_{sk}, L_{pk}, L_{rp}, L_s, L_{as}$,这些列表作用是分别用于跟踪 A_1 对预言机 H_1, H_2, H_3,部分密钥生成,私钥生成,公钥生成,公钥替换,签密和解签密的询问。起初列表都是空的。T_1 选择身份 ID_j 作为其猜测的挑战者身份,则 T_1 选择身份 ID_j 的概率为 $\chi \in [\frac{1}{q_s + n}, \frac{1}{q_s + 1}]$ 。

询问阶段:敌手 A_1 进行下述询问:

H_1 查询:当 A_1 向预言机 H_1 询问 $H_1(ID_i, X_i, Y_i)$ 时,T_1 进行下述操作:

①如果列表 L_1 中存在相应的元组 < ID_i, X_i, Y_i, h_{i1} >, 则 T_1 返回 h_{i1} 给 A_1;

②否则,T_1 随机选取 $h_{i1} \in Z_q^*$,使 L_1 中不存在相应的元组< ID_i, X_i, Y_i, h_{i1} >,并添加< *, *, *, h_{i1} >到 L_1,同时返回 h_{i1} 给 A_1。

H_2 查询:当 A_1 向预言机 H_2 询问 $H_2(ID_i \parallel m_i, V, Z_i)$ 时,T_1 进行下述操作:

①如果列表 L_2 中存在相应元组< $ID_i, m_i, Z_i, V, h_{i2}$ >, 则 T_1 返回给 A_1;

②否则,T_1 随机选取 $x_i \in Z_q^*$,计算 $X_i = x_i P$,通过对 ID_i 和 X_i 进行部分密钥生成询问获知相应的元组 < ID_i, y_i, Y_i >,添加元组< ID_i, x_i, y_i >到 L_{sk} ,返回 $SK_i = (x_i, y_i)$ 给 A_1,同时添加元组< ID_i, X_i, Y_i >到列表 L_{pk} 。

H_3 查询:当 A_1 向预言机 H_3 询问 $H_3(V_i, ID_B, V, a_i X_B)$ 时,T_1 进行下述操作:

①如果列表 L_3 中存在相应的元组< $V_i, ID_B, V, a_i X_B, T_i$ >,则 T_1 返回给 A_1;

②否则,T_1 随机选取 $T_i \in Z_q^*$,使得 L_3 中不存在相应的元组< *, *, *, *, T_i >,并添加相应元组< $V_i, ID_B, V, a_i X_B, T_i$ >到 L_3,同时返回 T_i 给 A_1。

部分密钥生成询问:当 A_1 要对 ID_i 和公开参数 X_i 进行部分密钥生成询问时,T_1 进行如下操作:

①若 L_k 中存在相应元组< ID_i, y_i, Y_i >,则 T_1 返回相应的值(y_i, Y_i)给 A_1;

②否则,如果 $ID_i \neq ID_j$,T_1 随机选取 $y_i, h_{i1} \in Z_q^*$,计算 $Y_i = y_i P - P_{pub} h_{i1}$,添加元组< ID_i, y_i, Y_i >到 L_k ,返回(y_i, Y_i)给 A_1,如果列表 L_1 中不存在相应元组,则添加元组< ID_i, X_i, Y_i, h_{i1} >到 L_1 中;如果 $ID_i = ID_j$,T_1 随机选取 $y_i, h_{i1} \in Z_q^*$,令 $Y_j = r_{know} P$ ($r_{know} \in Z_q^*$ 是已知

的随机数)，添加元组< ID_j, y_j, Y_j >到列表 L_k，返回(y_j, Y_j)给 A_1，如果列表 L_1 中不存在相应元组，则添加元组< ID_i, X_i, Y_i >到 L_1。

私钥生成询问：当 A_1 要对 ID_i 的私钥生成执行问询时，T_1 进行如下操作：

①如果列表 L_{sk} 中存在元组< ID_i, x_i, y_i >，则返回相应的值 $\mathrm{SK}_i = (x_i, y_i)$ 给 A_1；

②否则，T_1 随机选取 $x_i \in Z_q^*$，计算 $X_i = x_i P$，通过对 ID_i 和 X_i 进行部分密钥生成询问，获知相应的元组< ID_i, y_i, Y_i >，添加元组< ID_i, x_i, y_i >到 L_{sk}，返回 $\mathrm{SK}_i = (x_i, y_i)$ 给 A_1。

公钥生成询问：当 A_1 要对身份 ID_i 的公钥生成执行询问时，T_1 进行下述操作：

①如果 L_{pk} 中存在元组< ID_i, X_i, Y_i >，则返回 $\mathrm{PK}_i = (X_i, Y_i)$ 给 A_1；

②否则，T_1 随机选取 $x_i \in Z_q^*$，计算 $X_i = x_i P$，通过对 ID_i 和 X_i 进行部分密钥生成询问获知相应的元组< ID_i, y_i, Y_i >，添加元组< ID_i, X_i, Y_i >到 L_{pk}，返回 $\mathrm{PK}_i = (X_i, Y_i)$ 给 A_1，同时添加元组< ID_i, x_i, y_i >到列表 L_{sk}。

公钥替换询问：A_1 选择一个新的公钥 $\mathrm{PK}_i' = (X_i', Y_i')$ 代替任何合法用户的原始公钥 PK_i。

签密询问：当 T_1 收到 A_1 关于发送方身份、消息、接收方身份< $\mathrm{ID}_i, m_i, \mathrm{ID}_\mathrm{B}$ >签密询问时，执行操作如下：

①如果 $\mathrm{ID}_i = \mathrm{ID}_j$，则 T_1 放弃，终止模拟；

②否则，T_1 随机选取 $a_i \in z_q^*$，计算 $V_i = a_i P$，按照签密算法进行签密，生成签密 $\delta_i = (V, V_i, S_i, W_i)$ 返回给 A_1。

聚合签密询问：当 T_1 收到 A_1 关于发送方身份、消息、接收方身份< $\mathrm{ID}_i, m_i, \mathrm{ID}_\mathrm{B}$ >的签密询问时，执行如下步骤：

①如果对于全部的 ID_i，$\mathrm{ID}_i \neq \mathrm{ID}_j$，则 T_1 根据签密问询得到的 $\delta_i = (V, V_i, S_i, W_i)$，计算 $S = \sum_{i=1}^{n} S_i$，生成聚合签密 $\delta = <\{V_i, W_i\}_{i=1}^{n}, S, V>$，返回给 A_1。

②否则 T_1 弃权，停止模拟。

解签密问询：当 T_1 收到 A_1 关于发送者身份、接收者身份、签密< $\mathrm{ID}_i, \mathrm{ID}_\mathrm{B}, \delta_i$ >的解签密询问时，T_1 查询 L_1，判断其中是否存在 ID_i 对应的元组：

①倘若 L_1 中存在 ID_i 所对应的元组且 $\mathrm{ID}_i \neq \mathrm{ID}_j$，按照解签密算法进行解密，并验证 $S_i P = V_i + (X_i + Y_i + P_{\mathrm{pub}} h_{i1}) h_{i2}$ 是否成立，若成立 T_1 返回 1 给 A_1，否则返回 0；

②如果 L_1 中存在 ID_i 所对应的元组且 $\mathrm{ID}_i = \mathrm{ID}_j$，则当 L_2 中存在 ID_i 相对应的元组< $\mathrm{ID}_i, m_i, Z_i, V, h_{i2}$ >时，T_1 返回 1 给 A_1，否则返回 0；

③如果 L_1 中不存在 ID_i 所对应的元组，则当 L_2 中存在 ID_i 对应的元组< $\mathrm{ID}_i, m_i, Z_i, V, h_{i2}$ >时，T_1 返回 1 给 A_1，否则返回 0。

伪造：进行多项式有界次上述问询后，A_1 输出对发送者身份、消息、接收者身份< $\mathrm{ID}_i, m_i, \mathrm{ID}_\mathrm{B}$ > $(1 \leqslant i \leqslant n)$ 的聚合签密 $\delta = <\{V_i, W_i\}_{i=1}^{n}, S, V>$，其中至少有一个 ID_i 未进行部分密钥生成询问和私钥生成询问，同时至少有一个 m_i 未进行签密询问。

①如果对于所有的 $\mathrm{ID}_i (1 \leqslant i \leqslant n)$，都有 $\mathrm{ID}_i \neq \mathrm{ID}_j$，就将模拟中止。

②否则(至少存在一个 $\mathrm{ID}_i (1 \leqslant i \leqslant n)$ 与 ID_j 相等)，T_1 在列表 $L_1, L_2, L_3, L_{\mathrm{sk}}, L_{\mathrm{pk}}$ 中查找身份 ID_i $(1 \leqslant i \leqslant n)$ 对应的记录值，并检验等式 $\mathrm{SP} = V + \sum_{i=1}^{n} h_{i2} (X_i + Y_i + P_{\mathrm{pub}} h_{i1})$ 是否成立：

①如果成立，则 T_1 输出

$$b = (h_{i1} h_{i2})^{-1} \cdot \{S - \sum_{i=1, i \neq j}^{n} [a_i + h_{i2}(x_i + y_i)] - a_j - h_{j2}(x_j + r_{\mathrm{know}})\}$$

作为离散对数问题的有效解；

②否则，T_1 没有解决离散对数问题。

如果 A_1 在询问阶段对 ID_i $(1 \leqslant i \leqslant n)$ 执行了部分密钥生成询问和私钥生成询问，T_1 中止模拟，事件 ε_1 表明至少存在一个 ID_f ($f \in [1, n]$)未进行部分密钥生成询问和私钥生成询问，事件 ε_2 表明 T_1 在签密询问时未终止，那么：$\Pr[\varepsilon_1] \geqslant \frac{1}{n}(1 - \frac{q_k}{2^k})(1 - \frac{q_{\mathrm{sk}}}{2^k})$，$\Pr[\varepsilon_2 | \varepsilon_1] = (1 - \gamma)^{q_s}$，因此 T_1 在询问阶段不终止的概率为：

$$\Pr[\varepsilon_1 \wedge \varepsilon_2] = \Pr[\varepsilon_1 | \varepsilon_2]\Pr[\varepsilon_1] \geqslant \frac{1}{n}(1 - \frac{q_k}{2^k})(1 - \frac{q_{\mathrm{sk}}}{2^k})(1 - \gamma)^{q_s}$$

事件 ε_3 表示 T_1 在挑战阶段未中止，也就是 A_1 在挑战阶段伪造的聚合签密中包含身份 ID_j，T_1 在挑战阶段不终止概率为 $\Pr[\varepsilon_3] = \chi$。在整个模拟过程中，$\mathrm{T}_1$ 不中止概率至少为 $\frac{1}{n}(1 - \frac{q_k}{2^k})(1 - \frac{q_{\mathrm{sk}}}{2^k})(1 - \gamma)^{q_s}\chi$。由于 $\chi \in [\frac{1}{q_s + n}, \frac{1}{q_s + 1}]$，则当 q_s 足够大时，$(1 - \gamma)^{q_s}$ 趋向于 e^{-1}，因此模拟过程中 T_1 不终止的概率至少为 $(1 - \frac{q_k}{2^k})(1 - \frac{q_{\mathrm{sk}}}{2^k})\frac{1}{ne(q_s + n)}$。

由以上说明可知，倘若 T_1 在模拟过程中未中止，A_1 以不可忽略优势 ε 攻破了方案的不可伪造性，则 T_1 能以不可忽略优势($\mathrm{Adv}(\mathrm{T}_1) \geqslant (1 - \frac{q_k}{2^k})(1 - \frac{q_{\mathrm{sk}}}{2^k})$

$\frac{\varepsilon}{ne(q_s+n)}$）成功解决离散对数问题。

引理 2：在随机预言模型下，若存在 A_2类敌手能在多项式时间内，以不可忽略的优势 ε 赢得以下博弈，则称该签密方案具有不可伪造性（其中 A_2至多进行的签密询问次数与引理 1 中 A_1一样），且存在算法 T_2，能在多项式时间内以不可忽略优势（ $\mathrm{Adv}(T_2) \geqslant (1-\frac{q_k}{2^k})(1-\frac{q_{sk}}{2^k})\frac{\varepsilon}{ne(q_s+n)}$ ）成功解决离散对数问题。

证明：假设算法 T_2是个离散对数问题的 solver，输入的元组（ P,bP ）中 $b \in Z_q^*$ 是未知的，目的是得到 b 。A_2以 T_2充当挑战者，T_2执行 SETUP 算法，将生成的公开参数 PParam 发送给 A_2，保存主密钥，T_2维护列表与 T_1维护列表类似，除了不维护公钥替换。起初各列表都是空的。T_2选择身份 ID_j 作为其猜测的挑战者身份，概率为 $\chi \in [\frac{1}{q_s+n},\frac{1}{q_s+1}]$ 。

询问：敌手 A_2对预言机 H_1,H_2,H_3，私钥生成，公钥生成，签密和解签密的询问过程与引理 1 相同。

部分密钥生成询问：当 A_2执行对 ID_i 和公开参数 X_i 的部分密钥生成询问时，T_1进行如下操作：

①如果列表 L_k 中存在相应元组 $<\mathrm{ID}_i,y_i,Y_i>$，则 T_1返回相应值（ y_i,Y_i ）给 A_1；

②否则如果 $\mathrm{ID}_i \neq \mathrm{ID}_j$ ，T_2随机选取 $y_i,h_{i1} \in Z_q^*$ ，计算 $Y_i = y_iP - P_{\mathrm{pub}}h_{i1}$ ，添加元组 $<\mathrm{ID}_i,y_i,Y_i>$到 L_k 中，返回（ y_i,Y_i ）给 A_2，同时添加元组 $<\mathrm{ID}_i,X_i,Y_i,h_{i1}>$到 L_1 中；如果 $\mathrm{ID}_i = \mathrm{ID}_j$ ，T_1随机选取 $y_i,h_{i1} \in Z_q^*$ ，令 $Y_j = bP$ ，添加元组 $<\mathrm{ID}_j,y_j,Y_j>$到 L_k 中，返回（ y_j,Y_j ）给 A_2，同时添加元组 $<\mathrm{ID}_i,X_i,Y_i,y_j>$到 L_1 中。

解签密问询：当 T_2收到 A_2关于发送者身份，接收者身份，签密 $<\mathrm{ID}_i,\mathrm{ID}_B,\delta_i>(1 \leqslant i \leqslant n)$ 的解签密询问时，T_2查询 L_1 中是否存在 ID_i 对应的元组：

①若 L_1 中存在 ID_i 对应的元组且 $\mathrm{ID}_i \neq \mathrm{ID}_j$ ，则按解签密算法进行解密，并验证 $S_iP = V_i + (X_i + Y_i + P_{\mathrm{pub}}h_{i1})h_{i2}$ 是否成立，如果成立，则 T_2返回 1 给 A_2，否则返回 0。

②如果 L_1 中存在 ID_i 所对应的元组且 $\mathrm{ID}_i = \mathrm{ID}_j$ ，则当 L_2 中存在 ID_i 相对应的元组 $<\mathrm{ID}_i,m_i,Z_i,V,h_{i2}>$ 时，T_2返回 1 给 A_2，否则返回 0。

伪造：进行多项式有界次上述询问后，A_2输出对发送者身份，消息，接收者身份 $<\mathrm{ID}_i,m_i,\mathrm{ID}_B>(1 \leqslant i \leqslant n)$ 的聚合签密 $\delta = <\{V_i,W_i\}_{i=1}^n,S,V>$ ，其中至少有一个 ID_i 未进行部分密钥生成询问和私钥生成询问，同时至少有一个 m_i 未进行签密询问。

①如果对所有 ID_i 都有 $\mathrm{ID}_i \neq \mathrm{ID}_j$ ，终止模拟。

②否则如果 ID_i 与 ID_j 相等，则 T_1在列表 $L_1,L_2,L_3,L_{sk},L_{pk}$ 中查询 ID_i 对应的记录值，并验证等式 $SP = V + \sum_{i=1}^{n} h_{i2}(X_i + Y_i + P_{\mathrm{pub}}h_{i1})$ 是否成立：

如果等式成立，则 T_2输出：

$$b = (h_{i2})^{-1} \cdot \{S - \sum_{i=1,i\neq j}^{n}[a_i + h_{i2}(x_i + y_i)] - a_j - h_{j2}(x_j + sh_{i1})\}$$

作为离散对数问题的有效解；否则，T_2没有解决离散对数问题。

由引理 1 证明可知：在整个模拟过程中，T_2不终止的概率至少为 $(1-\frac{q_k}{2^k})(1-\frac{q_{sk}}{2^k})\frac{1}{ne(q_s+n)}$ ，因此如果 T_2在模拟过程中未中止，且 A_2以不可忽略优势攻破方案的不可伪造性，那么 T_2能以不可忽略的优势（ $\mathrm{Adv}(T_2) \geqslant (1-\frac{q_k}{2^k})(1-\frac{q_{sk}}{2^k})\frac{\varepsilon}{ne(q_s+n)}$ ）成功解决离散对数问题。

引理 3：在随机预言模型下，若不存在任何多项式数量级的敌手 A_1在下面的游戏中能以不可忽略优势获胜，那么称该方案具有机密性。

证明：假设算法 U_1是离散对数问题的 solver，输入的元组（ P,bP ）中 $b \in Z_q^*$ 是未知的，目的是得到 b 。A_1将 U_1作为挑战者，U_1运行 SETUP 算法，将生成的公开参数 Params 发送给 A_1，令 $P_{\mathrm{pub}} = bP$ ，同时 U_1维护列表 $L_1,L_2,L_3,L_k,L_{sk},L_{pk},L_{rp},L_s,L_{as}$ 分别用于跟踪 A_1对预言机 H_1,H_2,H_3，部分密钥生成，私钥生成，公钥生成，公钥替换，签密和解签密的询问。起初各列表都是空的。U_1选择身份 ID_j 作为其猜测的挑战者身份。

询问：敌手 A_1询问过程与引理 1 相似。

第一阶段，A_1或许产生两个长度相等的消息 m_{i0}，m_{i1} 来接受挑战。随机选择并通过执行签密算法获得 u_i 对发送给 ID_B 的关于消息 m_{ib} 的签密和聚合签密 $\{\delta_i,\delta\}$，返回 δ^* 给敌手 A_1。

第二阶段与第一阶段的模拟类似，不同的是 A_1不能对 $\delta^* = <\{V_i,W_i\}_{i=1}^n,S,V>$ 进行解签密询问，也不许对 ID_B 进行 H_1 问询和私钥询问[16]。

结束时，猜想 A_1被返回，若等式成立，则输出 1；否则，输出 0。由于敌手 A_1不能进行解签密询问，应用 $<\mathrm{ID}_i,m_i,Z_i,V,h_{i2}>$进行 H_2 问询。这里 $Z_i = y_BV_i$，y_B 是接收者的部分密钥，并且 $y_B = r_{\mathrm{know}} + bh_{i1}$，$Y_B = r_{\mathrm{know}}P$，$Z_i = a_i(Y_B + P_{\mathrm{pub}}h_{i1}) = y_BV_i$，$b = (h_{i1})^{-1}((V_i)^{-1}[a_i(Y_B + P_{\mathrm{pub}}h_{i1})] - r_{\mathrm{know}})$，由于离散对数问题中计算 n 是困难的，因此已知 Z_i 和 V_i 求取 b 也是困难的。

引理 4：在随机预言模型下，若不存在任何多项式数量级的敌手 A_2在下面的游戏中能以不可忽略优势获胜，那么称该方案具有机密性。

证明:假设算法 U_2 是离散对数问题的 solver,输入的元组(P,bP)中 $b \in Z_q^*$ 未知,目的是得到 b ,A_2 将 U_2 作为挑战者,U_2 执行 SETUP 算法,将生成的公开参数 PParam 发送给 A_2,保存主密钥,同时 U_2 维护列表 $L_1,L_2,L_3,L_k,L_{sk},L_{pk},L_s,L_{as}$ 分别用于跟踪 A_1 对预言机 H_1,H_2,H_3,部分密钥生成,私钥生成,公钥生成,签密和解签密的询问。起初各列表都是空的。U_2 选择身份 ID_j 作为其猜测的挑战者身份。

询问:敌手 A_2 询问过程与引理 2 相似。

在第一阶段和第二阶段与引理 3 模拟类似,不同的是这里 $Z_i = y_B V_i$,y_B 是接收者的部分密钥,并且 $y_B = b + sh_{i1}$,$Y_B = bP$,$Z_i = a_i(Y_B + P_{pub}h_{i1}) = y_B V_i$,则有 $b = (V_i)^{-1}a_i(Y_B + P_{pub}h_{i1}) - sh_{i1}$ 。由于离散对数问题中计算 n 是困难的,因此已知 Z_i 和 V_i 求取 b 也是困难的。

3.3 效率分析

表 1 是上述方案与文献[6,9,17-18]的签密方案进行性能比较的结果。耗时比较大的计算主要有双线性对运算、幂运算和数乘运算,d 表示双线性运算,h 表示指数运算,t 代表 G 上的点乘运(由于其他方案都使用了双线性运算,因此将群 G 记为 G_1,G_2,G_2 为 G_1 的双线性映射)。

表 1 签密方案运算量比较

方案	签密	解签密	运算总量
文献[6]	$3nh$	$(n+1)d+(3n-3)t$	$3nh+(n+1)d+(3n-3)t$
文献[9]	nd	$(3n+2)d$	$(4n+2)d$
文献[17]	$3nh+nd+nt$	$nd+nt$	$2nd+3nh+2nt$
文献[18]	$n(d+2t)$	$(n+3)d$	$(2n+3)d+2nt$
文中方案	$2nt$	$3nt+t$	$(5n+1)t$

表 1 分析了 5 种聚合签密方案的运算量,点乘运算对比对运算和指数运算耗时少许多。文中方案签密者只需 2 次点乘运算,而文献[9,17-18]都需要进行双线性对运算,文献[9]在签密时运算量较小,但解签密时高于文中方案。文献[6]的指数运算较大,且其在解签密阶段比文中方案多了许多双线性运算和指数运算。因此文中方案较为高效。

4 结束语

为提高无证书聚合签名和无证书签密方案的有效性和安全性,在随机预言模型具有可证安全性的基础上,提出了无双线性对的聚合签密方案。该方案基于离散对数难题,避免了双线性对运算。由于离散对数难题至今未能解决,因此该方案更为安全可靠。在签密者人数不止一个的情况下,提高了签密和解签密的计算效率。

参考文献:

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption) [C]//Annual international cryptology conference. Berlin: Springer,1997:165-179.

[2] Selvi S S,Vivek S S,Shriram J,et al. Identity based aggregate signcryption schemes[C]//International conference on progress in cryptology-indocrypt. [s. l.]:[s. n.],2009:378-397.

[3] 祁正华. 基于身份的签密方案研究[D]. 南京:南京邮电大学,2012.

[4] 于 刚. 若干签密方案研究[D]. 郑州:解放军信息工程大学,2012.

[5] Ren Xunyi,Qi Zhenghua,Yang Geng. Provably secure aggregate signcryption scheme[J]. ETRI Journal,2012,34(3):421-428.

[6] 苏爱东,张永翼. 密文长度固定的全聚合签密方案[J]. 计算机应用研究,2015,32(9):2820-2822.

[7] Riyami S A,Paterson K. Certificatless public key cryptography [C]//Proceedings of the ASIACRYPT. Berlin:Springer-Verlag,2003:452-473.

[8] Barbosa M,Farshim P. Certificateless signcryption[C]//Proceedings of ASIACCS. Tokyo,Japan:ACM Press,2008:369-372.

[9] 陆海军. 聚合签名与聚合签密研究[D]. 杭州:杭州师范大学,2012.

[10] Eslami Z,Nasrollah P. Certificateless aggregate signcryption: security model and a concrete construction secure in the random oracle model[J]. Journal of King Saud University Computer and Information Sciences,2014,26(3):276-286.

[11] Qi Zhenghua,Yang Geng,Ren Xunyi. Provably secure certificateless ring signcryption scheme[J]. China Communications,2011,8(3):99-106.

[12] QI Zhenghua,Ren Xunyi,Yang Geng. Provably secure general aggregate signcryption scheme in the random oracle model [J]. China Communications,2012,9(11):107-116.

[13] 周彦伟,杨 波,张文政. 高效可证安全的无证书聚合签名方案[J]. 软件学报,2015,26(12):3204-3214.

[14] Zhang L,Qin B,Wu Q H,et al. Efficient many-to-one authentication with certificate-less aggregate signatures[J]. Computer Networks,2010,54(14):2482-2491.

[15] 高键鑫,吴晓平,秦艳琳,等. 无双线性对的无证书安全签密方案[J]. 计算机应用研究,2014,31(4):1195-1198.

[16] 王大星,腾济凯. 可证明安全的基于身份的聚合签密方案[J]. 计算机应用,2015,35(2):412-415.

[17] Han Yiliang,Chen Fei. The multilinear mapsbased certificateless aggregate signcryption scheme[C]//International conference on cyber-enabled distributed computing and knowledge discovery. [s. l.]:[s. n.],2015:92-99.

[18] Liu Jianhua,Zhao Changxiao,Mao Kefei. Efficient certificateless aggregate signcryption scheme based on XOR[J]. Computer Engineering and Applications,2016,26(3):176-186.