对一个匿名多接收者签密方案的安全性分析与改进

李慧贤,巨龙飞
(西北工业大学计算机学院,陕西西安 710072)

摘 要: 2011 年,庞等人利用拉格朗日插值多项式方法构造了一个新的基于身份的多接收者匿名签密方案,并声称在其方案中任何攻击者或合法接收者都无法获取其他合法接收者的身份信息,从而能够保护接收者隐私.本文对庞等人的多接收者签密方案进行安全性分析,发现其方案中任何接收者对于其他接收者都无法实现匿名.同时,本文在其方案基础上进行改进,提出了一种改进方案,以弥补其安全缺陷.最后在随机预言模型下,对改进方案的正确性和接收者匿名性进行了证明.

关键词: 多接收者签密; 匿名性; 基于身份的签密; 拉格朗日插值
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2015)11-2187-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.11.008

Security Analysis and Improvement of an Anonymous Multi-Receiver Signcryption Scheme

LI Hui-xian, JU Long-fei
(*School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an, Shaanxi* 710072, *China*)

Abstract: In 2011, Pang et al proposed a new multi-receiver ID-based anonymous signcryption scheme by using Lagrange interpolating polynomial. They announced that their scheme makes it impossible for an attacker or any other message receivers to derive the identity of a message receiver such that the privacy of each receiver can be guaranteed. In this work, we studied the security of Pang et al's anonymous multi-receiver signcryption scheme. It is regretful that we found a receiver is not really anonymous to any other receivers in Pang et al's scheme. In order to solve this security defect, an improved scheme was proposed. Finally, the improved scheme was proved to satisfy the correctness and receiver anonymity in the random oracle model.

Key words: multi-receiver signcryption; anonymity; identity-based signcryption; Lagrange interpolating

1 引言

多接收者签密能够仅通过一次签密操作完成对多个接收者安全地发送同一消息,比传统的一对一方式更有效、更实用,特别适合网络安全广播和安全组播等业务.目前,多接收者签密已成为信息安全领域的一个研究热点.2006 年,Duan 等人[1]首次提出了一个基于身份的多接收者签密方案.随后一些优秀的多接收者签密方案被提出[2~6].2009 年,Lal 等人[7]提出了第一个签密者匿名的基于身份的多接收者签密方案,并给出了方案的一个应用实例.同年,Elkamchouchi 等人[8]提出了一个可公开验证的基于身份的多接收者签密方案.2010 年,Zhang 等人[9]给出一种签密者匿名的新方案.2012 年,Wang 等人[10]通过分析发现文献[7]和文献[9]提出的方案无法满足语义安全,并给出了证明,同时,Wang 等人在原方案基础上提出了改进的方案.

随着社会的发展,用户对于个人隐私逐渐重视.对于某些特殊的电信服务,比如付费电视、流式音频、视频业务等,用户不希望其他人知道他订阅了哪些业务,此时如何确保接收者的匿名性就显得尤为重要.现有大多数多接收者签密方案[2,3,6~10]的密文信息暴露了接收者身份,因为在这些方案中,所有授权用户的身份信息及其关联顺序是密文的一部分.2011 年,庞等人[11]提出一种新的基于身份的多接收者匿名签密方案.该方案不包

收稿日期:2013-12-31;修回日期:2015-04-27;责任编辑:马兰英
基金项目:国家自然科学基金(No.61103178);中央高校基本科研业务费专项资金(No.3102015JSJ0003);陕西省自然科学基础研究计划资助项目(No.2015JM6294)

含接收者身份列表信息,从而解决了接收者的隐私问题.此外,该方案还满足接收者公平性.但遗憾的是,本文通过对该方案进行安全性分析,发现其中任何接收者对于其他接收者都无法真正地实现匿名.分析其失败原因后,本文在其方案基础上进行改进,并完善了安全模型.

2 庞等人方案及其安全性分析

2.1 庞等人的方案

庞等人的方案[11]主要包含 KeyGen,Extract,Signcrypt 和 De-signcrypt 4 个算法.根据本文分析需求,这里简要介绍其方案解签密算法 De-signcrypt,具体描述如下.

De-signcrypt 算法由解签密者(即消息接收者)执行.输入密文 $C=\langle U,V,W,T,R,L\rangle$, *params*,接收者身份 ID'_j 及其私钥 d'_j,解签密者对 C 进行如下解密:

Verify:

(1)计算 $K=\sum_{i=1}^{m}(R_i+h_iQ_i)$,这里 $h_i=H_3(W,R_i)$, $i\in\{1,2,\cdots,m\}$.

(2)判断 $e(V,P)=e(K,P_{\text{pub}})$是否成立.如果成立,则发送者是集合 L 中的成员之一,否则退出.

Judge:

(1)判断 $V\cdot Q'_j=K\cdot d'_j$ 是否成立.如果成立,则 ID'_j 是授权的接收者,否则退出.

Decrypt:

(1)计算 $\delta_j=T_1+x_jT_2+\cdots+(x_j^{n-1}\bmod q)T_n$,其中 $x_j=H_4(ID'_j)$.

(2)计算 $\sigma'=e(P_{\text{pub}},\delta_j)\cdot e(U,d'_j)^{-1}$ 和 $M=H_2(\sigma')\oplus W$,M 则为解密后的消息.

2.2 庞等人方案的匿名性分析

庞等人[11]声称其方案中每个接收者对于攻击者以及其他接收者都是匿名的,每个接收者可以判断自身是否为授权用户,但是无法判断其他用户是否为授权用户.下面我们将证明其方案无法实现接收者匿名性.

引理 1 假设接收者身份列表为 S_n,对于 $\forall ID'_j\in S_n$,有 $\delta_j=\alpha(P_0+Q'_j)$;$\forall ID'_a\notin S_n$,无法获得 $\delta_a=\alpha(P_0+Q'_a)$.

证明 给定密文 $C=\langle U,V,W,T,R,L\rangle$,接收者身份 $ID'_j\in S_n$ 及其私钥 d'_j,ID'_j 能够获得 $x_j=H_4(ID'_j)$,然后计算

$$\begin{aligned}\delta_j&=T_1+x_jT_2+\cdots+x_j^{j-1}T_j+\cdots+x_j^{n-1}T_n\\&=(a_{1,1}\alpha(P_0+Q'_1)+\cdots+a_{n,1}\alpha(P_0+Q'_n))\\&\quad+(x_ja_{1,2}\alpha(P_0+Q'_1)+\cdots+x_ja_{n,2}\alpha(P_0+Q'_n))+\cdots\\&\quad+(x_j^{j-1}a_{1,j}\alpha(P_0+Q'_1)+\cdots+x_j^{j-1}a_{n,j}\alpha(P_0+Q'_n))+\cdots\\&\quad+(x_j^{n-1}a_{1,n}\alpha(P_0+Q'_1)+\cdots+x_j^{n-1}a_{n,n}\alpha(P_0+Q'_n))\\&=(a_{1,1}+a_{1,2}x_j+\cdots+a_{1,n}x_j^{n-1})\alpha(P_0+Q'_1)\\&\quad+(a_{2,1}+a_{2,2}x_j+\cdots+a_{2,n}x_j^{n-1})\alpha(P_0+Q'_2)+\cdots\\&\quad+(a_{j,1}+a_{j,2}x_j+\cdots+a_{j,n}x_j^{n-1})\alpha(P_0+Q'_j)+\cdots\\&\quad+(a_{n,1}+a_{n,2}x_j+\cdots+a_{n,n}x_j^{n-1})\alpha(P_0+Q'_n)\\&=\alpha(P_0+Q'_j)\end{aligned}\tag{1}$$

同时,任何不属于 S_n 的 ID'_a 无法通过上述计算得到 $\alpha(P_0+Q'_a)$.

$$\begin{aligned}\delta_a&=T_1+x_aT_2+\cdots+x_a^{j-1}T_j+\cdots+x_j^{n-1}T_n\\&=(a_{1,1}\alpha(P_0+Q'_1)+\cdots+a_{n,1}\alpha(P_0+Q'_n))+\cdots\\&\quad+(x_a^{n-1}a_{1,n}\alpha(P_0+Q'_1)+\cdots+x_a^{n-1}a_{n,n}\alpha(P_0+Q'_n))\\&=(a_{1,1}+a_{1,2}x_a+\cdots+a_{1,n}x_a^{n-1})\alpha(P_0+Q'_1)+\cdots\\&\quad+(a_{n,1}+a_{n,2}x_a+\cdots+a_{n,n}x_a^{n-1})\alpha(P_0+Q'_n)\end{aligned}\tag{2}$$

通过上述计算可知,我们无法获知 δ_a 与 Q'_a 的关联关系,另外 $\alpha(P_0+Q'_a)$是一个随机值,因此得到 $\delta_a=\alpha(P_0+Q'_a)$的概率可以忽略.

定理 1 假设现有合法接收者 $ID'_k\in S_n$,输入 ID'_l,计算 δ_l. ID'_k 判断 $e(\delta_k-\delta_l,P)=e(Q'_k-Q'_l,U)$是否成立,如成立,则有 $ID'_l\in S_n$,即 ID'_l 为合法接收者;否则 ID'_l 不是合法接收者.

证明 如果 $ID'_l\in S_n$,即 ID'_l 为合法接收者,由引理 1 可知,有 $\delta_l=\alpha(P_0+Q'_l)$,则

$$\begin{aligned}e(\delta_k-\delta_l,P)&=e(\alpha(P_0+Q'_k)-\alpha(P_0+Q'_l),P)\\&=e(\alpha(Q'_k-Q'_l),P)\\&=e((Q'_k-Q'_l),\alpha P)\\&=e((Q'_k-Q'_l),U)\end{aligned}\tag{3}$$

即,$e((\delta_k-\delta_l),P)=e((Q'_k-Q'_l),U)$成立.

如果 $ID'_l\notin S_n$,即 ID'_l 不是合法接收者,由引理 1 可知,无法获得 $\delta_l=\alpha(P_0+Q'_l)$,所以 ID'_k 无法使得等式 $e((\delta_k-\delta_l),P)=e((Q'_k-Q'_l),U)$成立.

综上可知,由于每个接收者 ID'_j 正确解密所用的秘密参数 δ_j 依赖于同一参数 α,导致攻击者可以利用双线性映射的双线性性,从接收到的密文中得出接收者之间的关联关系(即如果 ID'_l 和 ID'_k 均为合法接收者,则等式 $e((\delta_k-\delta_l),P)=e((Q'_k-Q'_l),U)$成立).任何合法接收者可获知其他用户是否为合法接收者,因此庞等人的方案无法真正实现接收者匿名性.

3 改进的方案

新方案在庞等人方案的基础上进行改进,同样包含 KeyGen,Extract,Anony-signcrypt 和 De-signcrypt 四个算法.下面对改进的方案进行详细描述.

参数生成算法(KeyGen)

该算法由密钥生成中心 PKG 执行,具体如下:

(1)设 G_1 和 G_2 分别是阶为 $q\geqslant 2^k$(k 为长整数)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 $e: G_1 \times G_2 \to G_2$.

(2)定义 4 个单向 Hash 函数:$H_1: \{0,1\}^* \to G_1$;$H_2: G_2 \to \{0,1\}^\lambda$;$H_3: \{0,1\}^\lambda \times G_1 \to Z_q^*$;$H_4: \{0,1\}^* \to Z_q^*$,其中 λ 表示明文的长度,即 $\lambda = |M|$.

(3)选择一个随机数 $s_0 \in Z_q^*$ 为主密钥,设置 $P_{pub} = s_0 P \in G_1$ 为系统的公钥.随机选择 $P_0 \in G_1$,并计算 $g = e(P_{pub}, P_0)$.

(4)公开系统参数 $params = \langle G_1, G_2, q, e, P, P_{pub}, P_0, g, H_1, H_2, H_3, H_4 \rangle$,并秘密保存主密钥 s_0.

私钥提取算法(Extract)

该算法由 PKG 执行.输入参数 $params$、s_0 和身份 $ID \in \{0,1\}^*$,私钥提取过程如下:

(1)计算 ID 的公钥 $Q_{ID} = H_1(ID)$.

(2)设置 ID 的私钥 $d_{ID} = s_0 Q_{ID}$.

签密算法(Anony-signcrypt)

该算法由签密者执行.输入参数 $params$ 和消息 M,设 ID_S 是真正的发送者,$L' = \{ID'_1, ID'_2, \cdots, ID'_n\}$ 是发送者选择的 n 个接收者,ID_S 的签密过程如下:

(1)选择一个用户集 $L = \{ID_1, ID_2, \cdots, ID_m\}$,且 $ID_S \in L$,$L \cap L' = \varnothing$.

(2)随机选择整数 $u_i \in Z_q^*$,$i \in \{1,2,\cdots,m\} \setminus \{S\}$,并计算 $R_i = u_i P$,随机选择整数 $u_S \in Z_q^*$.

(3)随机选择整数 $\alpha_j \in Z_q^*$,$j \in \{1,2,\cdots,n\}$,并计算 $\alpha = \sum_{j=1}^{n} \alpha_j$,$U = \alpha P$,$\sigma = g^\alpha$ 和 $W = H_2(\sigma) \oplus M$.

(4)计算 $h_i = H_3(W, R_i)$,$i \in \{1,2,\cdots,m\} \setminus \{S\}$.令 $R_S = u_S Q_S - \sum_{i=1, i\neq S}^{m} (R_i + h_i Q_i)$,其中 Q_s 是 ID_S 的公钥.令 $R = \{R_1, R_2, \cdots, R_m\}$.

(5)计算 $V = (u_S + h_S) \cdot d_S$,其中 $h_S = H_3(W, R_S)$,d_s 是 ID_S 的私钥.

(6)令 $x_j = H_4(ID'_j)$,$y_j = \alpha(P_0 + Q'_j)$,$j = 1,2,\cdots,n$,得到 n 对数 $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$,构造拉格朗日函数 $F_j(x)$ 满足 x_j 是 $F_j(x) = y_j$ 的解,其中 Q'_j 是 ID'_j 的公钥.

(7)对于 $j = 1,2,\cdots,n$,计算

$$f_j(x) = \prod_{1\leqslant j\neq j'\leqslant n} \frac{x - x_{j'}}{x_j - x_{j'}} = a_{j,1} + a_{j,2}x + \cdots + a_{j,n}x^{n-1},$$

其中 $a_{j,1}, a_{j,2}, \cdots, a_{j,n} \in Z_q$.

(8)对于 $j = 1,2,\cdots,n$,

计算 $T_j = \sum_{j'=1}^{n} a_{j',j} y_{j'}$,$J'_j = \sum_{j'=1}^{n} a_{j',j} J_j$,

其中 $J_j = \alpha \alpha_j^{-1} P_{pub}$.令 $T = \{T_1, T_2, \cdots, T_n\}$,$J = \{J'_1, J'_2, \cdots, J'_n\}$.

(9)密文为:$C = \langle U, V, W, T, R, L, J \rangle$.

解签密算法(De-signcrypt)

该算法由解签密者执行.输入密文 C、$params$、接收者身份 ID'_j 及其私钥 d'_j,对 C 进行如下解密:

Verify:

(1)计算 $K = \sum_{i=1}^{m} (R_i + h_i Q_i)$,这里 $h_i = H_3(W, R_i)$,$i \in \{1,2,\cdots,m\}$.

(2)非注册用户判断 $e(V, P) = e(K, P_{pub})$ 是否成立.若成立,说明发送者是集合 L 中成员之一,且密文有效.

(3)注册用户判断 $e(V, Q'_j) = e(K, d'_j)$ 是否成立.若成立,说明发送者是集合 L 中成员之一,且密文有效,ID'_j 可以继续执行下面的算法对消息进行解密,否则退出.

Decrypt:

(1)计算 $\delta_j = T_1 + x_j T_2 + \cdots + (x_j^{n-1} \bmod q) T_n$,$v_j = J'_j + x_j J'_2 + \cdots + (x_j^{n-1} \bmod q) J'_n$.

(2)计算 $\sigma' = \dfrac{e(v_j, \delta_j)}{e(U, d'_j)}$,$M = H_2(\sigma') \oplus W$,$M$ 则为解密后所得到的消息.

4　分析与证明

4.1　正确性分析

定理 2　Decrypt 算法正确性.解密算法(Decrypt)的解密过程是正确的.

证明　对于每一个 ID'_j,$j \in \{1,2,\cdots,n\}$,计算 δ_j 如下:

$$\begin{aligned}
\delta_j &= T_1 + x_j T_2 + \cdots + x_j^{j-1} T_j + \cdots + x_j^{n-1} T_n \\
&= (a_{1,1}\alpha_1(P_0 + Q'_1) + \cdots + a_{n,1}\alpha_n(P_0 + Q'_n)) \\
&\quad + (x_j a_{1,2}\alpha_1(P_0 + Q'_1) + \cdots + x_j a_{n,2}\alpha_n(P_0 + Q'_n)) + \cdots \\
&\quad + (x_j^{j-1} a_{1,j}\alpha_1(P_0 + Q'_1) + \cdots + x_j^{j-1} a_{n,j}\alpha_n(P_0 + Q'_n)) + \cdots \\
&\quad + (x_j^{n-1} a_{1,n}\alpha_1(P_0 + Q'_1) + \cdots + x_j^{n-1} a_{n,n}\alpha_n(P_0 + Q'_n)) \\
&= (a_{1,1} + a_{1,2}x_j + \cdots + a_{1,n}x_j^{n-1})\alpha_1(P_0 + Q'_1) \\
&\quad + (a_{2,1} + a_{2,2}x_j + \cdots + a_{2,n}x_j^{n-1})\alpha_2(P_0 + Q'_2) + \cdots \\
&\quad + (a_{j,1} + a_{j,2}x_j + \cdots + a_{j,n}x_j^{n-1})\alpha_j(P_0 + Q'_j) + \cdots \\
&\quad + (a_{n,1} + a_{n,2}x_j + \cdots + a_{n,n}x_j^{n-1})\alpha_n(P_0 + Q'_n) \\
&= \alpha_j(P_0 + Q'_j) \qquad (4)
\end{aligned}$$

$$\begin{aligned}
v_j &= J'_1 + x_j J'_2 + \cdots + x_j^{j-1} J'_j + \cdots + x_j^{n-1} J'_n \\
&= (a_{1,1}J_1 + \cdots + a_{n,1}J_n) \\
&\quad + (x_j a_{1,2}J_1 + \cdots + x_j a_{n,2}J_n) + \cdots \\
&\quad + (x_j^{j-1} a_{1,j}J_1 + \cdots + x_j^{j-1} a_{n,j}J_n) + \cdots \\
&\quad + (x_j^{n-1} a_{1,n}J_1 + \cdots + x_j^{n-1} a_{n,n}J_n) \\
&= (a_{1,1} + a_{1,2}x_j + \cdots + a_{1,n}x_j^{n-1})J_1 \\
&\quad + (a_{2,1} + a_{2,2}x_j + \cdots + a_{2,n}x_j^{n-1})J_2 + \cdots
\end{aligned}$$

$$+(a_{j,1}+a_{j,2}x_j+\cdots+a_{j,n}x_j^{n-1})J_i+\cdots$$
$$+(a_{n,1}+a_{n,2}x_j+\cdots+a_{n,n}x_j^{n-1})J_n$$
$$=J_j \tag{5}$$

因此,我们可以得到 $\sigma'=\dfrac{e(v_j,\delta_j)}{e(U,d'_j)}$,具体过程如下:

$$\sigma'=\frac{e(v_j,\delta_j)}{e(U,d'_j)}=\frac{e(J_j,\alpha_j(P_0+Q'_j))}{e(\alpha P,s_0Q'_j)}$$
$$=\frac{e(\alpha\alpha_j^{-1}P_{\text{pub}},\alpha_j(P_0+Q'_j))}{e(\alpha P,s_0Q'_j)}$$
$$=\frac{e(P_{\text{pub}},\alpha P_0)\cdot e(P_{\text{pub}},\alpha Q'_j)}{e(s_0P,\alpha Q'_j)}$$
$$=e(P_{\text{pub}},P_0)^{\alpha}=g^{\alpha}=\sigma \tag{6}$$

所以有 $M=H_2(\sigma')\oplus W$.

4.2 安全性证明

本方案的安全需求包括消息保密性、不可否认性以及接收者匿名性.其中前两个性质与庞等人方案类似,这里不再赘述.下面我们对改进方案的接收者匿名性给出随机预言模型下的安全证明.

4.2.1 安全模型

本文完善了庞等人方案[11]的安全模型,增加了 Anonymous indistinguishability of signcryptions under selective-ID, chosen ciphertext attracts (ANON-sID-CCA)模型和 Anonymous indistinguishability of signcryptions under selective multi-ID, chosen ciphertext attracts (ANON-sMID-CCA)模型.

定义 1 ANON-sID-CCA 假设.假设 A 是一个攻击者(Attacker),定义 Π 是一个基于身份的多接收者匿名签密方案.考虑 A 与一个挑战者(Challenger) B 进行以下互动:

Setup: B 运行该算法,生成主密钥 s_0 以及系统参数 *params*,将 *params* 发送给 A,并秘密保存主密钥 s_0.

Phase 1: A 输出目标接收者身份(ID'_1, ID'_2), B 收到后选择随机数$\beta\in\{1,2\}$.

Phase 2: A 向 B 进行私钥提取询问. B 接收到攻击者的私钥提取询问后,执行私钥提取算法获取私钥 d_j = Extract(*params*, s_0, ID'_j).此处,$ID'_j\neq ID'_i(i=1,2)$.

Phase 3: A 向目标身份进行解签密询问. A 生成发送者身份信息集合 $L=\{ID_1,ID_2,\cdots,ID_m\}$和一个密文 C^*.当接收到一个针对(C^*, ID'_i), $i\in\{1,2\}$的解签密询问后, B 产生 ID'_i 相应的私钥 d'_i,并将 M = De-signcrypt(C^*, *params*, L, ID'_i, d'_i)返回给 A.

Challenge: A 输出一个目标明文. B 产生一个相应的目标密文 C = Anony-signcrypt(*params*, L, ID'_β, *M*),并将该密文返回给 A.

Phase 4: A 执行阶段 2 中的私钥提取询问以及阶段 3 的解签密询问,在解签密询问中,我们限定 $C^*\neq C$.

Guess:最后 A 输出猜测的$\beta'\in\{1,2\}$,如果 $\beta=\beta'$,那么 A 就赢得该交互游戏.

这样的 A 我们称为 ANON-sID-CCA 攻击者,A 猜测成功的优势定义为:

$$\text{Adv}_{\Pi}^{\text{ANON-sID-CCA}}(A)=\left|Pr[\beta=\beta']-\frac{1}{2}\right|.$$

在多项式时间内,如果任何 ANON-sID-CCA 攻击者猜测成功的优势 $\text{Adv}_{\Pi}^{\text{ANON-sID-CCA}}(A)<\varepsilon$ 恒成立,则我们称方案 Π 是(t,ε)-ANON-sID-CCA 安全的.

定义 2 ANON-sMID-CCA 假设.假设 A 是一个攻击者(Attacker),定义 Π 是一个基于身份的多接收者匿名签密方案.考虑 A 与一个挑战者(Challenger) B 进行以下互动:

Setup: B 运行该算法,生成主密钥 s_0 以及系统参数 *params*,将 *params* 发给 A,并秘密保存主密钥 s_0.

Phase 1: A 输出目标接收者身份(ID'_1, ID'_2), B 收到后选择随机数$\beta\in\{1,2\}$.

Phase 2: A 向 B 进行私钥提取询问. B 接收到攻击者的私钥提取询问后,执行私钥提取算法获取私钥 d_j = Extract(*params*, s_0, ID'_j).此处,$ID'_j\neq ID'_i(i=1,2)$.

Phase 3: A 向目标身份进行解签密询问. A 生成发送者身份信息集合 $L=\{ID_1,ID_2,\cdots,ID_m\}$和一个密文 C^*.当接收到一个针对(C^*, ID'_i), $i\in\{1,2\}$的解签密询问后, B 产生 ID'_i 相应的私钥 d'_i,并将 M = De-signcrypt(C^*, *params*, L, ID'_i, d'_i)返回给 A.

Challenge: A 输出目标消息 M 和身份列表$\{ID'_3, ID'_4,\cdots, ID'_n\}(n\geqslant 3)$. B 产生一个相应的目标密文 C = Anony-signcrypt(*params*, M, L, $\{ID'_\beta, ID'_3, ID'_4, \cdots, ID'_n\}$),并将该密文返回给 A.

Phase 4: A 像 Phase 2、3 中一样进行多次询问,注意私钥提取询问时不可以询问 L 中的身份信息,解密询问时不可以询问 C,此处,$C\neq C^*$.

Guess:最终,A 输出其猜测$\beta'\in\{1,2\}$,如果 $\beta=\beta'$,则 A 赢得这场游戏.

如上所述的 A 被称为 ANON-sMID-CCA 攻击者,其优势定义为:

$$\text{Adv}_{\Pi}^{\text{ANON-sMID-CCA}}(A)=\left|Pr[\beta\in\beta']-\frac{1}{2}\right|.$$

在多项式时间内,如果任何 ANON-sMID-CCA 攻击者猜测成功的优势 $\text{Adv}_{\Pi}^{\text{ANON-sMID-CCA}}(A)<\varepsilon$ 恒成立,则我们称方案 Π 是(t,ε)-ANON-sMID-CCA 安全的.

4.2.2 接收者匿名性分析

定理 3 假设存在一个 ANON-sID-CCA 攻击者 A 能够在时间 t 内,以 ε 的优势赢得定义 1 中的游戏(他最多能进行 q_{ex}次密钥提取询问, q_d 次解签密询问和 q_{H_i}次对随机预言 $H_i(i=1,2,3,4)$的询问),那么存在一个算

法 B 能够在时间 $t' \leqslant t + 4q_dO(t_1)$ 内,以优势 $\varepsilon' \geqslant \varepsilon$ 解决 DBDH 问题(其中 t_1 是双线性对运算 e 的运算时间).

证明　下面利用攻击者 A 构造一个解决 DBDH 问题的算法 B.假设 B 得到一个 DBDH 问题随机实例$\langle P, aP, bP, cP, Z\rangle$,$B$ 的目标是判断 $Z = e(P,P)^{abc}$.在接收者匿名性游戏中,B 扮演 A 的挑战者.A 可以向 B 查询 $H_i(i=1,2,3,4)$预言、私钥提取预言、签密预言和解签密预言,这些回答都是随机的.为了保证答案的一致性以避免冲突,B 维护 $L_i(i=1,2,3,4)$列表,分别存储 H_i $(i=1,2,3,4)$的随机预言值.

Phase 1:A 输出 2 个目标身份(ID'_1, ID'_2).

Setup:B 随机选择 $\beta \in \{1,2\}$,设定 $P_0 = bP$, $P_{\text{pub}} = cP$,那么 $g = e(P_0, P_{\text{pub}}) = e(bP, cP) = e(P,P)^{bc}$,将 $params = (G_1, G_2, q, e, P, P_{\text{pub}}, P_0, g, H_1, H_2, H_3, H_4)$作为系统参数发送给 A.

其中 H_1, H_2, H_3 和 H_4 由 B 控制如下.

H_1-query:对于一个询问 $H_1(ID'_j)$,$j \in \{1,2,\cdots, q_{H_1}\}$,如果 L_1 中存在$(ID'_j, t_j, Q'_j, \alpha_j)$,则将 Q'_j 作为询问应答返回.否则,进行以下步骤.

(1)随机选择 $t_j \in Z_q^*$, $\alpha_j \in Z_q^*$.

(2)如果 $ID'_j = ID'_\beta$,那么计算 $Q'_j = bP$.

(3)如果 $ID'_j \neq (ID'_\beta$,且 $ID'_j \neq ID'_i, i(\{1,2\}$,那么计算 $Q'_j = t_jP(P_0$.

(4)如果 $ID'_j \neq ID'_\beta$,且 $ID'_j = ID'_i, i(\{1,2\}$,那么计算 $Q'_j = t_jP$.

(5)将$(ID'_j, t_j, Q'_j, \alpha_j)$存入 L_1,并返回 Q_j.

H_2 询问:对于询问 $H_2(\omega_j)$,$j \in \{1,2,\cdots, q_{H_2}\}$,如果 L_2 中存在(ω_j, h_{2j}),则返回 h_{2j}.否则,B 选择一个随机整数 $h_{2j} \in \{0,1\}^l$,将(ω_j, h_{2j})存入 L_2,并返回 h_{2j}.

H_3 询问:对于询问 $H_3(W_j, R_{ij})$,$i \in \{1,2,\cdots, m\}$,$j \in \{1,2,\cdots, q_{H_3}\}$,如果 L_3 中存在(W_j, R_{ij}, h_{3j}),则返回 h_{3j}.否则 B 选择一个随机整数 $h_{3j} \in Z_q^*$,将(W_j, R_{ij}, h_{3j})存入 L_3,并返回 h_{3j}.

H_4 询问:对于询问 $H_4(ID'_j)$,$j \in \{1,2,\cdots, q_{H_4}\}$,如果 L_4 中存在(ID'_j, h_{4j}),则返回 h_{4j}.否则,B 选择一个随机字符串 $h_{4j} \in Z_q^*$,将(ID'_j, h_{4j})存入 L_4,并返回 h_{4j}.

Phase 2:当 B 接收到 A 关于身份 ID_j 的私钥询问时,查找 L_1 中元组$(ID'_j, t_j, Q'_j, \alpha_j)$,返回 t_j,计算 $d'_j = t_jP_{\text{pub}} = ct_jP$,并将其返回给 A.注意 A 询问的身份满足 $ID'_j \neq ID'_i, i \in \{1,2\}$.假定 A 对身份 ID'_j 进行任何询问前都已进行过 H_1 询问.

Phase 3:当收到 A 提交的关于(C, ID'_i)的解签密询问(其中 $ID'_i, i \in \{1,2\}$,密文 $C = \langle U, V, W, T, R, L, J\rangle$),$B$ 执行如下计算:

查找 L_3,计算 $K = \sum_{i=1}^{m}(R_i + h_iQ_i)$,这里 $h_i = H_3(W_j, R_{ij})$,$i \in \{1,2,\cdots, m\}$,检查在 L_3 中是否存在这样的三元组(W_j, R_{ij}, h_{3j}),使得 $e(V,P) = e(K, P_{\text{pub}})$成立.如果不存在这样的元组,那么 B 拒绝这个解签密询问,并将$\perp$(返回给 A.如果存在,则 B 通过 L_1 得到 ID'_j 的私钥 d'_j,再计算出 δ_j 和 v_j.计算 $\sigma' = \dfrac{e(v_j, \delta_j)}{e(U, d'_j)}$, $M = H_2(\sigma') \oplus W$,返回 M 给 A.

Challenge:A 选择一个明文消息 M,并将其发送给 B.B 令 $U^* = aP, \sigma = Z$,查找 L_1 获得与 $ID_j^{'*}$,$i \in \{1,2,\cdots, n\}$ 相对应的 t_j^* 和 α_j^*,计算出 $y_j^* = \alpha_j^* U^*$, $J_j^* = \alpha_j^{*-1} t_j^* P_{\text{pub}}$,$j \in \{1,2,\cdots, n\}$,继而得到 T_j^*,$j \in \{1,2,\cdots, n\}$.B 最终生成一个目标密文 $C^* = \langle U^*, V^*, W^*, T^*, R^*, L^*, J^*\rangle$并发送给 ID'_β,并将 C^* 返回给 A.

Phase 4:A 执行第 2 阶段中的私钥提取询问,对目标身份 ID'_β 执行第 3 阶段中的解签密询问,注意不能对 ID'_β 进行私钥提取询问,也不能对挑战密文 C^* 进行解签密询问.

Guess:游戏结束时,A 输出其猜测 $\beta' \in \{1,2\}$,如果 $\beta' = \beta$,B 输出 DBDH 问题的解.因为

$$\begin{aligned} Z &= \frac{e(J_j^*, y_j^*)}{e(U^*, d_j^{'*})} = \frac{e(\alpha_j^{*-1} t_j^* P_{\text{pub}}, \alpha_j^* U^*)}{e(U^*, d_j^{'*})} \\ &= \frac{e(cP, t_j^* U^*)}{e(aP, t_j^* cP - cbP)} = \frac{e(cP, t_j^* aP)}{e(aP, t_j^* cP)\, e(aP, -cbP)} \\ &= e(P,P)^{abc} \end{aligned} \tag{7}$$

根据上面的分析,B 完美的模拟了阶段 2 的随机预言 $H_i(i=1,2,3,4)$,阶段 3 的私钥提取询问和阶段 4 的解签密询问.因此,我们可得,

$Pr[B(P, aP, bP, cP, e(P,P)^{abc}) = 1] = Pr[\beta' = \beta]$,

此处, $|Pr[\beta' = \beta] - 1/2| \geqslant \varepsilon$,

同时又知,$Pr[B(P, aP, bP, cP, Z) = 1] = Pr[\beta' = \beta] = 1/2$,其中 Z 是从 G_1 中选择的随机数.因而,我们可得,$Pr[B(P, aP, bP, cP, e(P,P)^{abc}) = 1] - Pr[B(P, aP, bP, cP, Z) = 1] \geqslant |(1/2 \pm \varepsilon) - 1/2| = \varepsilon$,因此,$\varepsilon' \geqslant \varepsilon$, $t' \leqslant t + 4q_dO(t_1)$,其中,$t_1$ 表示线性对 e 运算的时间.

定理 4　从接收到的密文中得出接收者之间的关联关系在计算上是不可行的.

证明　假设密文为 $C = \langle U, V, W, T, R, L, J\rangle$,则有

$$\begin{aligned} \delta(x) &= T_1 + xT_2 + \cdots + x^{n-1} T_n \\ &= f_1(x)\alpha_1(P_0 + Q'_1) + f_2(x)\alpha_2(P_0 + Q'_2) + \cdots \\ &\quad + f_n(x)\alpha_n(P_0 + Q'_n) \\ v(x) &= J'_1 + xJ'_2 + \cdots + x^{n-1} J'_n \\ &= f_1(x) J_1 + f_2(x) J_2 + \cdots + f_n(x) J_n \end{aligned}$$

$$= f_1(x)\alpha_1^{-1}\alpha P_{pub} + f_2(x)\alpha_2^{-1}\alpha P_{pub} + \cdots + f_n(x)\alpha_n^{-1}\alpha P_{pub}$$

对于多项式 $f_i(x)$,满足

$$f_i(x) = \begin{cases} 1, & x = x_i \\ 0, & x \in \{x_1, x_2, \cdots, x_n\} - \{x_i\} \end{cases}$$

(1)当 $x \in \{x_1, \cdots, x_n\}$时,$\delta(x)$包含变量$\{\alpha_1(P_0 + Q'_1), \alpha_2(P_0 + Q'_2), \cdots, \alpha_n(P_0 + Q'_n)\}$,$v(x)$包含变量$\{\alpha_1^{-1}\alpha P_{pub}, \alpha_2^{-1}\alpha P_{pub}, \cdots, \alpha_n^{-1}\alpha P_{pub}\}$.由于 $\alpha_i \in Z_q^*$,$i \in \{1,2,\cdots,n\}$为随机选择整数,所以变量$\{\alpha_1(P_0 + Q'_1), \alpha_2(P_0 + Q'_2), \cdots, \alpha_n(P_0 + Q'_n)\}$和$\{\alpha_1^{-1}\alpha P_{pub}, \alpha_2^{-1}\alpha P_{pub}, \cdots, \alpha_n^{-1}\alpha P_{pub}\}$均互相独立.

(2)当 $x \notin \{x_1, \cdots, x_n\}$时,攻击者可以获取$(P, P_{pub}, \{ID_1, \cdots, ID_t\}, U, v(x), \delta(x))$($t$ 表示合法用户数).由 *xyz*-DDH(*xyz*-Decisional Diffie-Hellman)[12]问题可知,攻击者无法获知哪 n 个用户满足关系 $\delta(x) = f_1(x)\alpha_1(P_0 + Q'_1) + f_2(x)\alpha_2(P_0 + Q'_2) + \cdots + f_n(x)\alpha_n(P_0 + Q'_n)$.

另外,由于 U, V, W 均为随机预言模型下的随机数,因此无法帮助攻击者获取接收者之间的关联关系.

综上可知,从接收到的密文中得出接收者之间的关联关系在计算上是不可行的.

定理 5 本方案在 DBDH 假设和 *xyz*-DDH 假设下是 ANON-sMID-CCA 安全的.

证明 攻击者只有通过以下两种方法获知用户是否为合法接收者:

(1)从接收到的密文中得出接收者之间的关联关系.

(2)通过解签密询问和私钥提取询问获知用户是否为合法接收者.

由定理 3 和定理 4 可知,以上两种方法均不可行,因此改进的方案在 DBDH 假设和 *xyz*-DDH 假设下是(t, ε)-ANON-sMID-CCA 安全的.

5 性能分析和比较

改进方案中 $f_i(x)$和 T_i 是用于隐藏接收者的身份信息,保护接收者的隐私,且使得解密具有公平性. J_i 用于破坏$f_i(x)$和$(P_0 + Q'_i)$之间的关联关系,进而防止攻击者利用拉格朗日插值相关性质获取接收者隐私.

计算 $f_i(x)$、T_i 和 J_i 需要一定的计算代价,但是只要选定了接收者,就可以提前对算 $f_i(x)$、T_i 和 J_i 进行计算以减少签密时的计算开销.如果预先计算 $f_i(x)$、T_i 和 J_i,则不统计这三步的计算量,改进的方案仅需 1 次指数计算,$3m-2$ 次加运算和 $2m+1$ 次乘运算(m 表示发送者隐藏集合的成员人数),无需双线性对运算,因此计算量与庞等人方案相同.

在密文长度上,庞等人方案为$(m + n + 2)|G_1| + |M| + m|ID|$,改进方案为$(m + 2n + 2)|G_1| + |M| + m|ID|$($n$ 表示授权接收者的人数,$|G_1|$表示 G_1 中元素的长度,$|M|$表示明文消息 M 的长度,$|ID|$表示身份信息 ID 的长度),密文长度较文献[11]会稍有增加,但是原方案并没有实现接收者匿名性这一功能,而改进方案在其基础上使得功能更完善,在真正意义上实现了接收者匿名性.总之,与现有的匿名方案相比,改进方案在签密效率及方案功能性方面有很大优势.

6 总结

本文首先指出庞等人的方案无法实现接收者匿名性,并运用拉格朗日插值函数及双线性对性质,给出了攻击方法.由匿名性分析可以看出,庞等人方案中任意接收者对于其他合法接收者无法实现匿名,因此,其方案是不安全的.改进的方案在满足庞等人方案安全属性的基础上,实现了接收者匿名性.文章最后给出了随机预言模型下改进方案的安全性证明.

参考文献

[1] Duan S S, Cao Z F. Efficient and provably secure multi receiver identity based signcryption[A]. 2006 11th Australasian Conference on Information Security and Privacy (ACISP'06)[C]. Berlin: Springer, 2006. 195 – 206.

[2] Yu Y, Yang B, Huang X Y, et al. Efficient identity-based signcryption scheme for multiple receivers[A]. 20017 4th International Conference on Autonomic and Trusted Computing (ATC'07)[C]. Berlin: Springer, 2007. 13 – 21.

[3] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and provably secure certi? cateless multi-receiver signcryption[A]. 2008 2nd International Conference on Provable Security [C]. Berlin: Springer, 2008. 52 – 67.

[4] Selvi S S D, Vivek S S, Srinivasan R, et al. An efficient identity-based signcryption scheme for multiple receivers[A]. 2009 4th International Workshop on Security (IWSEC'09)[C]. Berlin: Springer, 2009. 71 – 88.

[5] Pang L J, Gao L, Pei Q Q, et al. A new ID-based multi-recipient public-key encryption scheme[J]. Chinese Journal of Electronics, 2013, 22(1): 89 – 92.

[6] Zhang J H, Mao J. A novel identity-based multi-signcryption scheme[J]. Computer Communications, 2009, 32(1): 14 – 18.

[7] Lal S, Kushwah P. Anonymous ID based signcryption scheme for multiple receivers[DB/OL]. Cryptology ePrint Archive, Report 2009/345, http://eprint.iacr.org/2009/345.

[8] Elkamchouchi H, Abouelseoud Y. MIDSCYK: An efficient provably secure multirecipient identity-based signcryption scheme[A]. 2009 International Conference on Networking and

Media Convergence[C]. Piscataway: IEEE Press, 2009. 70 – 75.

[9] Zhang B, Xu Q. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model[A]. 2010 2nd Int Conf on Adv Sci and Technol/4th Int Conf on Informat Security and Assurance/2nd Int Conf on Adv Commun and Networking/Int Conf on Ubiquitous Computing and Multimedia [C]. Berlin: Springer, 2010. 15 – 27.

[10] Wang H, Zhang Y, Qin B. Analysis and improvements of two identity based anonymous signcryption schemes for multiple receivers[A]. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications [C]. Los Alamitos, CA, USA: IEEE computer Society, 2012. 1057 – 1062.

[11] 庞辽军,崔静静,李慧贤,等. 新的基于身份的多接收者匿名签密方案[J]. 计算机学报. 2011, 34(11): 2104 – 2113.
Pang Liaojun, Cui Jingjing, Li Huixian et al. A new multi-receiver ID-based anonymous signcryption[J]. Journal of Computers, 2011, 34(11): 2104 – 2113. (in Chinese)

[12] Laguillaumie F, Vergnaud D. Time-selective convertible undeniable signatures[A]. 2005 the Cryptographers' Track at the RSA Conference[C]. Berlin: Springer, 2005. 154 – 171.

作者简介

李慧贤(通信作者)　女,1977 年生于内蒙古乌兰浩特市. 现为西北工业大学计算机学院副教授,硕士生导师. 研究方向为网络与信息安全、安全协议分析与设计、多接收者加密/签密.
E-mail: lihuixian@nwpu.edu.cn

巨龙飞　男,1989 年生于河北邢台市. 现为西北工业大学计算机学院硕士生. 研究方向为安全协议分析与设计、多接收者签密.
E-mail: julongfei0@gmail.com