匿名的无证书多接收者签密机制

周彦伟[1,2,3],杨 波[1,2,3],张文政[2]
(1. 陕西师范大学计算机科学学院,陕西西安 710062;2. 保密通信重点实验室,四川成都 610041;
3. 中国科学院信息工程研究所信息安全国家重点实验室,北京 100093)

摘 要: 为了满足广播通信环境下发送者的多消息发送需求,本文提出可证安全的无证书多接收者多消息签密机制,密文中不再包含接收者身份列表,实现对接收者身份等隐私信息的保护;同时发送者可在一次签密操作中完成多消息发送任务. 相较与现有方案而言,除具有保密性和不可伪造性之外,本文机制具有较强的匿名性和较高的计算效率,满足广播通信环境中多消息的匿名发送需求.

关键词: 无证书签密; 多接收者; 多消息; 匿名性; 保密性; 不可伪造性
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2016)08-1784-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.08.002

Anonymous Certificateless Signcryption Scheme with Multi-receiver

ZHOU Yan-wei[1,2,3], YANG Bo[1,2,3], ZHANG Wen-zheng[2]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *Science and Technology on Communication Security Laboratory, Chengdu, Sichuan* 610041, *China*;
3. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: To satisfy the senders' needs of sending multi-message in the broadcast communication environment, a certificateless signcryption scheme with multi-receiver and multi-message was proposed. The ciphertext no longer contains receivers' identity list to protect receivers' privacy. And, as well, the senders can fulfill sending multi-message in a single operation. Compared with the present scheme, apart from confidentiality and unforgery, this scheme is better in anonymity and has a higher computational efficiency, satisfy the needs of sending multi-message in broadcast communication environment.

Key words: certificateless signcryption; multi-receiver; multi-message; anonymity; confidentiality; unforgeability

1 引言

广播环境下用户个人信息的保护需求,推进了多接收者签密机制的研究. 国内外研究者相继提出了多接收者签密机制[1~15],然而多数机制[1~10,12,13,15]的密文信息易暴露接收者身份,因为在这些机制中接收者的身份列表或密文标记列表是其密文的一部分;多数机制[3,5,8,10~15]以基于身份的密码系统为基础,存在密钥托管的问题;多数机制[1~14]仅具有单消息发送能力,发送者仅能发送单个消息给多位不同的接收者,无法满足发送者的多消息发送需求.

由于传统公钥密码系统需要昂贵而又繁琐的证书管理机制,而基于身份的密码系统存在密钥托管的不足. 为弥补上述不足,文献[16]提出了无证书公钥密码系统,私钥由用户和密钥生成中心 KGC (Key Generator Center)共同生成,该系统中 KGC 无法获知任何用户的私钥.

针对现有机制存在的不足,本文提出无证书的多接收者多消息签密机制,该机制解决了接收者的隐私保护问题,仅有授权的接收者才能正确解密;同时能向多个接收者发送多个消息,满足发送者的多消息发送需求;并在随机谕言机模型下,基于计算性 Diffie-Hell-

收稿日期:2014-12-22;修回日期:2015-08-20;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61572303, No. 61272436, No. 61402275);中国科学院信息工程研究所信息国家重点实验室基金(No. 2015-MS-10);保密通信重点实验室基金(No. 9140C110206140C11050);中央高校基本科研业务费专项资金(No. GK201504016);陕西师范大学优秀博士论文基金(No. X2014YB01)

man (Computational Diffie-Hellman,CDH) 问题和离散对数(Discrete Logarithm,DL)问题证明了本文机制的保密性和不可伪造性.

2 基础知识

2.1 双线性映射

设 G_1,G_2 为阶是大素数 q 的循环群,P 是 G_1 的一个生成元. 当 $\tilde{e}:G_1\times G_1\to G_2$ 满足下列性质时,称 $\tilde{e}$ 是一个双线性映射.

①双线性:$\tilde{e}(aP,bQ)=\tilde{e}(P,Q)^{ab}$,对所有的 $P,Q\in G_1,a,b\in Z_q^*$ 均成立.

②非退化性:存在 $P,Q\in G_1$,使得 $\tilde{e}(P,Q)\neq I_{G_2}$,其中 I_{G_2} 为群 G_2 的单位元.

③可计算性:对于 $P,Q\in G_1$,可在多项式时间内完成 $\tilde{e}(P,Q)$ 的计算.

2.2 困难性问题及假设

设 G 为阶是大素数 q 的循环群,P 是群 G 的一个生成元;已知 $P,aP\in G$,DL 问题的目标是计算未知的 $a\in Z_q^*$.

在概率多项式时间内算法 A 成功解决 DL 问题的概率为 $Adv^{\mathrm{DL}}(A)=\Pr[A(P,aP)=a]$. 其中,概率来源于 a 的随机选取及 A 的随机选择.

DL 假设. 对于任意的概率多项式时间算法 A,概率 $Adv^{\mathrm{DL}}(A)$ 是可忽略的.

设 G 为阶是大素数 q 的循环群,P 是群 G 的一个生成元;已知 $P,aP,bP\in G$,CDH 问题的目标是计算 abP.

在概率多项式时间内算法 A 成功解决 CDH 问题的概率为 $Adv^{\mathrm{CDH}}(A)=\Pr[A(P,aP,bP)=abP]$. 其中,概率来源于 a,b 的随机选取及 A 的随机选择.

CDH 假设. 对于任意的概率多项式时间算法 A,概率 $Adv^{\mathrm{CDH}}(A)$ 是可忽略的.

2.3 安全模型

具体安全模型的定义详见文献[6],由文献[6]可知本文机制将面临 A_I 和 A_{II} 两类敌手的攻击,其中 A_I 类敌手 $A_I^i(i=1,2)$ 无法掌握系统主密钥,但具有替换用户公钥的能力. A_{II} 类敌手 $A_I^i(i=1,2)$ 可掌握系统主密钥,但不具有替换用户公钥的能力.

3 本文无证书多接收者多消息签密机制

3.1 系统初始化

系统初始化时,KGC 执行下述操作:

①定义双线性映射 $\tilde{e}:G_1\times G_1\to G_2$,其中 G_1,G_2 为阶是大素数 q 的加法循环群和乘法循环群,P 是群 G_1 的一个生成元;

②定义抗碰撞单向哈希函数:$H_1:\{0,1\}^{L_1}\times G_1\times G_1\to Z_q^*$,$H_2:\{0,1\}^{L_1}\times G_1\to\{0,1\}^{L_2}\times G_1$,$H_3:\{0,1\}^{L_1}\times\{0,1\}^{L_2}\times G_1\to G_1$,其中 L_1 为用户身份标识的长度,L_2 为明文消息的长度.

③定义索引函数 $f_{index}:Z_q^*\times\{0,1\}^{L_1}\to Z_q^*$,$f_{index}(n,ID)\in\{1,\cdots,n\}$ 中 n 表示索引区间的尺寸,ID 为用户身份标识,即 f_{index} 能方便接收者从密文集合中准确定位自己的密文.

④选取系统主密钥 $S_{msk}\in Z_q^*$,计算系统公钥为 $P_{Pub}=S_{msk}P$,KGC 公开系统参数 $Params=\{q,G_1,G_2,e,P,P_{Pub},H_1,H_2,H_3,f_{index},\oplus\}$(其中⊕为异或运算),秘密保存主密钥 S_{msk}.

3.2 用户密钥生成

①首先用户 ID_i 随机选择秘密值 $x_{ID_i}\in Z_q^*$,计算公开参数 $X_{ID_i}=x_{ID_i}P$,发送 ID_i 和 X_{ID_i} 给 KGC.

②给定身份 ID_i 和 X_{ID_i},KGC 随机选取秘密数 $r_{ID_i}\in Z_q^*$,计算 $y_{ID_i}=r_{ID_i}+S_{msk}H_1(ID_i,X_{ID_i},Y_{ID_i})$ 和 $Y_{ID_i}=r_{ID_i}P$,通过安全信道将部分私钥 y_{ID_i} 和部分公钥 Y_{ID_i} 返回给.

③通过等式 $y_{ID_i}P=Y_{ID_i}+P_{Pub}H_1(ID_i,X_{ID_i},Y_{ID_i})$ 用户 ID_i 可实现对 y_{ID_i} 和 Y_{ID_i} 的合法性验证,则 ID_i 的公私钥对为 $<SK_{ID_i}=(x_{ID_i},y_{ID_i}),PK_{ID_i}=(X_{ID_i},Y_{ID_i})>$.

3.3 多消息签密(MultiSign)

多消息签密算法的输入为签密者身份、消息集合 $M=\{m_1,\cdots,m_n\}$ 和授权接收者身份集合 $ID_R=\{ID_{R_1},\cdots,ID_{R_n}\}$. 签密者 Alice(身份标识为 ID_A)的具体签密步骤如下:

①随机选取秘密数 $t_A\in Z_q^*$,计算 $T_A=t_AP$.

②对每一位接收者 $R_i(i=\{1,\cdots,n\})$,首先计算索引标号 $J_{R_i}=f_{index}(n,ID_{R_i})$;然后计算 $(EK'_{J_{R_i}},EK''_{J_{R_i}})=H_2(ID_{R_i},t_A(X_{R_i}+Y_{R_i}+P_{Pub}h_{R_i}^1))$(其中 $EK'_{J_{R_i}}\in\{0,1\}^{L_2}$,$EK''_{J_{R_i}}\in G_1$ 和 $h_{R_i}^1=H_1(ID_{R_i},X_{R_i},Y_{R_i})$)、$C'_{J_{R_i}}=m_{J_{R_i}}\oplus WK'_{J_{R_i}}$ $V_{J_{R_i}}=(t_A+x_A+y_A)U_{J_{R_i}}$(其中 $U_{J_{R_i}}=H_3(ID_A,c_{J_{R_i}},T_A)$)和 $C''_{J_{R_i}}=V_{J_{R_i}}+EK''_{J_{R_i}}$,令 $C_{J_{R_i}}=<C'_{J_{R_i}},C''_{J_{R_i}}>$

③计算 $v_A=t_A(x_A+y_A)^{-1}$ 后,将密文 $\sigma=<v_A,C=\{C_1,\cdots,C_n\}>$ 以广播的形式发送给每一位接收者 $R_i(i=\{1,\cdots,n\})$.

3.4 解签密(UnSign)

接收者 $R_i(i\in[1,n])$ 收到密文 $\sigma=<v_A,C=\{C_1,\cdots,C_n\}>$ 后,根据索引号 $J_{R_i}=f_{Index}(n,ID_R)$ 从集合 $C=\{C_1,\cdots,C_n\}$ 中准确定位密文 $C_{J_{R_i}}=<c'_{J_{R_i}},c''_{J_{R_i}}>$. 该算法的具体过程如下:

(1)密文解密

①计算 $T'_A=v_A(X_A+Y_A+P_{Pub}h_A)$(其中 $h_A=H_1(ID_A,X_A,Y_A)$,$<X_A,Y_A>$ 为 Alice 的公钥).

②计算 $(DK'_{J_{R_i}},DK''_{J_{R_i}})=H_2(ID_{R_i},(x_{R_i}+y_{R_i})T'_A)$.

③计算 $m'_{J_{R_i}}=c'_{J_{R_i}}\oplus DK'_{J_{R_i}}$ 和 $V'_{J_{R_i}}=c''_{J_{R_i}}-DK''_{J_{R_i}}$.

(2)合法性验证

①计算 $U'_{J_R}=H_3(ID_A,c'_{J_R},T'_A)$.

②验证 $\tilde{e}(P,V'_{J_R})=\tilde{e}(U'_{J_R},T'_A+X_A+Y_A+P_{Pub}h_A)$ 是否成立,若成立则接收 m'_{J_R},否则返回符号 $\perp$.

3.5 正确性

3.5.1 解密的正确性

因为:$T'_A=v_A(X_A+Y_A+P_{Pub}h_A)$

$=t_A(x_A+y_A)^{-1}(x_A+r_A+S_{msk}h_A)P=t_AP=T_A$.

其中,$y_A=r_A+S_{msk}h_A$,$h_A=H_1(ID_A,X_A,Y_A)$.

$(DK'_{J_R},DK''_{J_R})=H_2(ID_{R_i},(x_{R_i}+y_{R_i})T'_A)$

$=H_2(ID_{R_i},t_A(x_{R_i}+r_{R_i}+S_{msk}h^1_{R_i})P)$

$=H_2(ID_{R_i},t_A(X_{R_i}+Y_{R_i}+P_{Pub}h^1_{R_i}))$

$=(EK'_{J_R},EK''_{J_R})$.

其中,$y_{R_i}=r_{R_i}+S_{msk}h^1_{R_i}$,$h^1_{R_i}=H_1(ID_{R_i},X_{R_i},Y_{R_i})$.

则 $EK'_{J_R}=DK'_{J_R}$ 和 $EK''_{J_R}=DK''_{J_R}$.

因此 $m'_{J_R}=c'_{J_R}\oplus DK'_{J_R}=m_{J_R}\oplus EK'_{J_R}\oplus DK'_{J_R}=m_{J_R}$ 和 $V'_{J_R}=c''_{J_R}\oplus DK''_{J_R}=V_{J_R}+EK''_{J_R}-DK''_{J_R}=V_{J_R}$ 成立.

3.5.2 签名的正确性

因为:$V'_{J_R}=V_{J_R}$ 和 $U'_{J_R}=H_3(ID_A,c'_{J_R},T'_A)$

$=H_3(ID_A,c_{J_R},T_A)=U_{J_R}$

因此 $\tilde{e}(P,V'_{J_R})=\tilde{e}(P,V_{J_R})=\tilde{e}(P,(t_A+x_A+y_A)U_{J_R})$

$=\tilde{e}(U_{J_R},T_A+X_A+Y_A+P_{Pub}h_A)$

$=\tilde{e}(U'_{J_R},T'_A+X_A+Y_A+P_{Pub}h_A)$

4 安全性证明

安全性证明过程中所涉及的相关游戏均在文献[6]中给出了具体定义,本文不再赘述.

4.1 保密性证明

定理 1(A_I 类敌手的保密性) 若有 A_I 类敌手 A^1_I 在多项式时间内能以不可忽略的优势 ε 赢得文献[6]中的相关游戏(A^1_I 最多进行 q_{SK} 次私钥生成询问,q_S 次签密询问和 q_R 次公钥替换询问),则存在算法 β 在多项式时间内至少以不可忽略的优势 $(1-\frac{q_{SK}}{2^k})(1-\frac{q_R}{2^k})\frac{\varepsilon}{e(q_S+1)}$($e$ 为自然对数底数)解决 CDH 问题.

证明 以敌手 A^1_I 为子程序构造 CDH 问题的解决算法 β. 对于 β 而言,输入为元组 (P,aP,bP),目标是计算 abP. β 运行 *Setup* 生成相应的系统参数 *Params* 和主密钥 S_{msk},并发送 *Params* 给 A^1_I;同时维护列表 $L_1,L_2,L_3,L_{SK},L_{PK}$ 分别用于跟踪对谕言机 H_1、H_2、H_3 的询问及私钥生成和公钥生成询问,开始时各列表均为空. β 猜测身份 ID_J($J\in[1,q_S+1]$)是敌手选取的挑战身份.

H_2 询问:收到 A^1_I 的询问 $H_2(ID_i,g_i)$ 后,若存在 $<ID_i,g_i,h_2>\in L_2$,则 β 返回 h_2 给 A^1_I;否则,β 选取满足条件 $<*,*,h_2>\notin L_2$ 的随机值 $h_2=<h'_2,h''_2>$(其中 $h'_2\in\{0,1\}^{L_2}$,$h''_2\in G_1$),添加 $<ID_i,g_i,h_2>$ 到 L_2 中,并返回相应的 h_2 给 A^1_I.

H_3 询问:收到 A^1_I 的询问 $H_3(ID_i,c_i,T_i)$ 后,当存在 $<ID_i,c_i,T_i,h_3>\in L_3$,则 β 返回相应的 h_3 给 A^1_I;否则,若 $ID_i=ID_J$,β 令 $h_3=aP$;若 $ID_i\neq ID_J$,则 β 选取满足条件 $<*,*,*,h_3>\notin L_3$ 的随机值 $h_3\in G_1$;添加 $<ID_i,c_i,T_i,h_3>$ 到 L_3 中,并返回相应的 h_3 给 A^1_I.

公钥生成询问:当 A^1_I 对 ID_i 进行公钥生成询问时,若存在 $<ID_i,X_i,Y_i>\in L_{PK}$,则 β 返回相应的 $PK_i=<X_i,Y_i>$ 给 A^1_I;否则,β 随机选取 $x_i,y_i,h_1\in Z^*_q$,计算 $Y_i=y_iP-P_{Pub}h_1$ 和 $X_i=x_iP$,添加 $<ID_i,X_i,Y_i>$ 到 L_{PK} 中,添加 $<ID_i,x_i,y_i>$ 到 L_{SK} 中,添加 $<ID_i,X_i,Y_i,h_1>$ 到 L_1 中,并返回 $PK_i=<X_i,Y_i>$ 给 A^1_I.

H_1 询问:收到 A^1_I 的询问 $H_1(ID_i,X_i,Y_i)$ 后,β 检索 L_1 中 ID_i 相对应的元组 $<ID_i,X_i,Y_i,h_1>$,并返回 h_1 给 A^1_I. 特别的,对 ID_i 进行 H_1 询问之前,已完成对 ID_i 的公钥生成询问.

公钥替换询问:A^1_I 能用随机的公钥 PK'_i 替换任意用户 ID_i 的合法公钥 PK_i.

私钥生成询问:当 A^1_I 对 ID_i 进行私钥生成询问时,若存在 $<ID_i,x_i,y_i>\in L_{SK}$,则 β 返回相应的 $SK_i=<x_i,y_i>$ 给 A^1_I;否则,β 对 ID_i 进行公钥生成询问(在该询问中将生成 ID_i 对应的私钥)后,查询 L_{SK} 并返回相应的 $SK_i=<x_i,y_i>$ 给 A^1_I.

签密询问:当收到 A^1_I 关于 ID_S 和 $ID_R=\{ID_{R_1},\cdots,ID_{R_n}\}$ 及 $M=\{m_1,\cdots,m_n\}$ 的多消息签密询问时,β 进行下述操作:

(1)若 $ID_S\neq ID_J$,β 对 $ID_{R_j}(j=1,2,\cdots,n)$ 和 ID_S 分别进行公钥生成和私钥生成询问后,运行签密算法 $MultiSign(M,ID_S,SK_S,ID_R,PK_R)$ 生成相应的密文 $\sigma=<v_S,C=\{C_1,C_2,\cdots,C_n\}>$,并返回 σ 给 A^1_I.

(2)若 $ID_S=ID_J$,则 β 停止模拟,并退出.

解签密询问 当收到 A^1_I 关于 ID_S、ID_{R_j} 和 $\sigma_{J_R}=<v_S,C_{J_R}=<c'_{J_R},c''_{J_R}>>$ 的解签密询问时,β 针对 ID_S 查询 L_{PK}(假设 A^1_I 对 ID_S 已进行了公钥生成询问),并进行下述操作:

(1)若 $<ID_S,X_S,Y_S>\in L_{PK}$ 且 $ID_S\neq ID_J$,β 分别对 ID_{R_j} 和 ID_S 进行私钥生成和公钥生成询问后,运行解签密算法 $UnSign(\sigma_{J_R},ID_S,PK_S,ID_{R_j},SK_{R_j})$ 对密文 σ_{J_R} 进行解密,并返回相应的结果给 A^1_I.

(2)若 $<ID_S,X_S,Y_S>\in L_{PK}$ 且 $ID_S=ID_J$,β 按下述步骤进行解签密:

①若 L_1、L_2 和 L_3 中分别存在相应的元组 $<ID_S,X_S,Y_S,h_1>G_{L_1}$、$<ID_{R_j},g_{R_j},h_2=<h'_2,h''_2>>G_{L_2}$ 和 $<ID_S,c_{J_R},T_S,h_3>G_{L_3}$,$\beta$ 计算 $m_{J_R}=c'_{J_R}\oplus h'_2$ 和 $V_{J_R}=c''_{J_R}\oplus h''_2$,

当验证等式 $\tilde{e}(P,V_{J_k})=\tilde{e}(h_3,T_S+X_S+Y_S+P_{Pub}h_1)$ 成立时,β 返回消息 m_{J_k} 给 A_I^1;

②否则,β 停止模拟,拒绝密文并退出.

(3)若 L_{PK} 中不存在相应的元组(公钥被替换),β 按下述步骤进行解签密:

①若 L_1、L_2 和 L_3 中分别存在相应的元组 $<ID_S,X'_S,Y'_S,h_1>\in L_1$、$<ID_{R_j},g_{R_j},h_2=<h'_2,h''_2>>\in L_2$ 和 $<ID_S,c_{J_k},T_S,h_3>\in L_3$,$\beta$ 计算 $m_{J_k}=c'_{J_k}\oplus h'_2$ 和 $V_{J_k}=c''_{J_k}\oplus h''_2$,当验证等式 $\tilde{e}(P,V_{J_k})=\tilde{e}(h_3,T_S+X'_S+Y'_S+P_{Pub}h_1)$ 成立时,β 返回消息 m_{J_k} 给 A_I^1;

②否则,β 停止模拟,拒绝密文并退出.

挑战:在第一阶段的结尾,A_I^1 生成挑战消息 $M_0=\{m_0^1,\cdots,m_0^n\}$ 和 $M_1=\{m_1^1,\cdots,m_1^n\}$ 且($|m_0^i|=|m_1^i|$),ID_S 和 $ID_R=\{ID_{R_1},\cdots,ID_{R_n}\}$,$\beta$ 进行下述操作:

①若 $ID_S\neq ID_J$,β 失败,并停止模拟.

②若 $ID_S=ID_J$,β 随机选取 $b\leftarrow\{0,1\}$,并按下述步骤生成 $M_b=\{m_b^1,\cdots,m_b^n\}$ 的签密密文:令 $T_S=bP$;对每一位接收者 R_i 计算索引标号 $J_{R_i}=f_{Index}(n,ID_{R_i})$($i=\{1,2,\cdots,n\}$);选取满足条件 $(EK'_{J_{R_i}},EK''_{J_{R_i}})=H_2(ID_{R_i},(x_{R_i}+y_{R_i})T_S)$ 的随机值 $EK'_{J_{R_i}}\in\{0,1\}^{L_2}$ 和 $EK''_{J_{R_i}}\in G_1$,并计算 $C'_{J_{R_i}}=m_{J_{R_i}}+EK'_{J_{R_i}}$,向谕言机 H_3 询问 $H_3(ID_S,c_{J_{R_i}},T_S)$ 获得对应的 h_3(即 $U_{J_{R_i}}=h_3$);选取满足条件 $\tilde{e}(P,V_{J_{R_i}})=\tilde{e}(U_{J_{R_i}},T_S+X_S+Y_S+P_{Pub}h_S)$ 的随机值 $V_{J_{R_i}}\in G_1$;$C''_{J_{R_i}}V_{J_{R_i}}+EK''_{J_{R_i}}$,令 $C_{J_{R_i}}=<c'_{J_{R_i}},c''_{J_{R_i}}>$;选取满足条件 $T_S=v_S(X_S+Y_S+P_{Pub}h_1)$ 的随机数 $v_S\in Z_q^*$ 后,将密文 $\sigma=<v_S,C=\{C_1,C_2,\cdots,C_n\}>$ 返回给 A_I^1.

模拟最后 A_I^1 输出对随机数的猜测 b',若 $b=b'$ 且 ID_S 所对应的公钥未被替换,那么 β 输出 $abP=V_{J_{R_i}}-(x_S+y_S)h_3$ 作为 CDH 问题的有效解;否则,β 终止退出,即未解决 CDH 问题.

β 为 A_I^1 模拟了真实的攻击环境,若 β 在模拟过程中未终止,且 A_I^1 以不可忽略的优势 ε 攻破本文机制的保密性,则 β 可解决 CDH 问题.

设 δ 表示上述游戏中 $ID_S=ID_J$ 的概率,则有 $\delta=\Pr[ID_S=ID_J]=\frac{1}{q_S+1}$(下文中 δ 的含义与此相同,下文不再赘述).

询问阶段当 A_I^1 对 ID_S 进行了私钥生成,则 β 会终止,定义事件 E_1 表示 A_I^1 对 ID_S 未进行私钥生成;事件 E_2 表示签密询问过程 β 未终止;则 $\Pr[E_1]=(1-\frac{q_{SK}}{2^k})$,$\Pr[E_2]=(1-\delta)^{q_S}$,即询问阶段 β 不终止的概率为 $(1-\frac{q_{SK}}{2^k})(1-\delta)^{q_S}$;挑战阶段 A_I^1 选取的挑战身份 ID_S 是 ID_J 且对 ID_S 未进行公钥替换询问,则挑战阶段 β 不终止的概率为 $(1-\frac{q_R}{2^k})\delta$.

在整个模拟过程中 β 不终止的概率为 $(1-\frac{q_{SK}}{2^k})(1-\frac{q_R}{2^k})(1-\delta)^{q_S}\delta$. 由于 $\delta=\frac{1}{q_S+1}$,则当 q_S 足够大时,$(1-\delta)^{q_S}=(\frac{q_S}{q_S+1})^{q_S}$ 趋向于 e^{-1},则模拟过程中 β 不终止的概率至少为 $(1-\frac{q_{SK}}{2^k})(1-\frac{q_R}{2^k})\frac{1}{e(q_S+1)}$.

综上所述,若 A_I^1 能以不可忽略的优势 ε 攻破本文机制的保密性,则 β 至少能以不可忽略的优势 $(1-\frac{q_{SK}}{2^k})(1-\frac{q_R}{2^k})\frac{\varepsilon}{e(q_S+1)}$ 解决 CDH 问题.

定理 2(A_{II} 类敌手的保密性) 若有 A_{II} 类敌手 A_{II}^1 在多项式时间内能以不可忽略的优势赢得文献[6]中的相关游戏(A_{II}^1 最多进行 q_{SK} 次私钥生成询问和 q_S 次签密询问),则存在算法 β 在多项式时间内至少以不可忽略的优势 $(1-\frac{q_{SK}}{2^k})\frac{\varepsilon}{e(q_S+1)}$($e$ 为自然对数底数)解决 CDH 问题.

证明思路与定理 1 类似,此处不再赘述.

4.2 不可伪造性证明

定理 3(A_I 类敌手的不可伪造性) 若有 A_I 类敌手 A_I^2 在多项式时间内能以不可忽略的优势赢得文献[6]中的相关游戏(A_I^2 最多进行 q_{SK} 次私钥生成询问和 q_S 次签密询问),则存在算法 β 在多项式时间内至少以不可忽略的优势 $(1-\frac{q_{SK}}{2^k})\frac{\varepsilon}{e(q_S+1)}$($e$ 为自然对数底数)解决 DL 问题.

证明 以敌手 A_I^2 为子程序构造解决 DL 问题的算法 β. 对于 β 而言,输入为元组 (P,aP),目标是计算 a. β 运行 *Setup* 生成相应的系统参数 *Params* 和主密钥 S_{msk},并发送 *Params* 给 A_I^2,其中令 $P_{Pub}=aP$(即有 $S_{msk}=a$);维护列表 L_1,L_2,L_3,L_{SK},L_{PK} 分别用于跟踪对谕言机 H_1,H_2、H_3 的询问及私钥生成和公钥生成询问,开始时各列表均为空. β 猜测 ID_J($J\in[1,q_S+1]$)是 A_I^2 选取的挑战身份.

询问:A_I^2 执行定理 1 中对谕言机 H_1、H_2 的询问、私钥生成询问和公钥替换询问.

***H_3* 询问:**当收到询问 $H_3(ID_i,m_i,T_i)$ 时,若 $<ID_i,m_i,T_i,h_3>\in L_3$,则 β 返回相应的 h_3 给 A_I^2;否则,β 选取满足条件 $<*,*,*,h_3>\notin L_3$ 的随机值 $h_3\in G_1$,添加 $<ID_i,m_i,T_i,h_3>$ 到 L_3 中,并返回 h_3 给 A_I^2.

公钥生成询问:当 A_I^2 对 ID_i 进行公钥生成询问时,算法 β 进行下述操作:

①若 $<ID_i, X_i, Y_i> \in L_{PK}$,则 β 返回相应的 $PK_i = <X_i, Y_i>$ 给 A_I^2.

②否则,β 随机选取 $x_i, y_i, h_1 \in Z_q^*$,若 $ID_i \neq ID_J$,则计算 $Y_i = y_i P - P_{Pub} h_1$ 和 $X_i = x_i P$,添加元组 $<ID_i, x_i, y_i>$ 到 L_{SK} 中;若 $ID_i = ID_J$,令 $Y_i = n_{Know} P$(其中 n_{Know} 为 β 已知的数),计算 $X_i = x_i P$,添加元组 $<ID_i, x_i, \perp>$ 到 L_{SK} 中;添加 $<ID_i, X_i, Y_i>$ 到 L_{PK} 中,添加 $<ID_i, X_i, Y_i, h_1>$ 到 L_1 中,并返回 $PK_i = <X_i, Y_i>$ 给 A_I^2.

签名询问:当收到 A_I^2 进行关于 ID_S 和 $M = \{m_1, m_2, \cdots, m_n\}$ 的签名询问时,β 进行下述操作:

① 如果 $ID_S \neq ID_J$,β 对 ID_S 进行私钥生成询问后,运行 $Sign(M, ID_S, SK_S)$ 生成相应的签名 $\sigma = <v_S, V = \{V_1, V_2, \cdots, V_2\}>$ 返回给 A_I^2.

②如果 $ID_S = ID_J$,则 β 停止模拟,并退出.

签名验证询问:当收到 A_I^2 关于 ID_S、m_{J_R}($J_R \in [1, n]$)和 $\sigma_{J_R} = <v_S, V_{J_R}>$ 的签名验证询问时,β 针对 ID_S 查询 L_{PK}(假设 A_I^2 对 ID_S 已进行了公钥生成询问)后,进行下述操作:

(1)若存在 $<ID_S, X_S, Y_S> \in L_{PK}$ 且 $ID_S \neq ID_J$,β 运行 $UnSign(\sigma, ID_S, PK_S)$,并返回结果给 A_I^2.

(2)若存在 $<ID_S, X_S, Y_S> \in L_{PK}$ 且 $ID_S = ID_J$,β 按下述步骤进行签名验证:

①若 L_1 和 L_3 中分别存在相应的元组 $<ID_S, X_S, Y_S, h_1> G_{L_1}$ 和 $<ID_S, m_{J_R}, T_S, h_3> G_{L_3}$,当验证等式 $\tilde{e}(P, V_{J_R}) = \tilde{e}(h_3, T_S + X_S + Y_S + P_{Pub} h_1)$ 成立时,β 返回 *True* 给 A_I^2;

②否则,β 停止模拟,并退出.

(3)若列表 L_{PK} 中不存在相应的元组(公钥被替换),β 按下述步骤进行签名验证:

①若 L_1 和 L_3 中分别存在相应的元组 $<ID_S, X'_S, Y'_S, h_1> G_{L_1}$ 和 $<ID_S, m_{J_R}, T_S, h_3> G_{L_3}$,当验证等式 $\tilde{e}(P, V_{J_R}) = \tilde{e}(h_3, T_S + X'_S + Y'_S + P_{Pub} h_1)$ 成立时,β 返回 *True* 给 A_I^2;

②否则,β 停止模拟,并退出.

伪造:经过多项式有界次上述询问后,A_I^2 伪造 ID_S 关于 $M = \{m_1, m_2, \cdots, m_n\}$ 的签名:选取随机数 $t_S \in Z_q^*$,计算 $T_S = t_S P$;向谕言机 H_3 询问 $H_3(ID_S, m_{J_R}, T_S)$ 获得对应的 h_3(其中,$J_{R_i} \in \{1, 2, \cdots, n\}$,则 $U_{J_R} = h_3$);选取满足条件 $\tilde{e}(P, V_{J_R}) = \tilde{e}(U_{J_R}, T_S + X_S + Y_S + P_{Pub} h_S)$ 的随机值 $V_{J_R} \in G_1$;选取满足条件 $T_S = v_S(X_S + Y_S + P_{Pub} h_S)$ 的随机数 $v_S \in Z_q^*$ 后,输出伪造签名 $\sigma = <v_S, V = \{V_1, V_2, \cdots, V_n\}>$.

若 A_I^2 伪造了合法签名且 $ID_S = ID_J$,则 β 选取满足等式 $av_S h_1 P = T_S - v_S(X_S + Y_S)$ 的随机数 $a \in Z_q^*$(其中 $h_1 = H_1(ID_S, X_S, Y_S)$)作为 DL 问题的有效解;否则,$\beta$ 终止退出,即 β 未解决 DL 问题.

询问阶段当 A_I^2 对 ID_S 进行了私钥生成询问,则 β 会终止. 定义事件 E_1 表示 A_I^2 对 ID_S 未进行私钥生成询问;事件 E_2 表示签名询问过程中 β 未终止;则 $\Pr[E_1] = 1 - \frac{q_{SK}}{2^k}$,$\Pr[E_2] = (1-\delta)^{q_s}$,即询问阶段 β 不终止的概率为 $(1 - \frac{q_{SK}}{2^k})(1-\delta)^{q_s}$,挑战阶段 β 不终止的概率为 δ.

在整个模拟过程中 β 不终止的概率为 $(1 - \frac{q_{SK}}{2^k})(1-\delta)^{q_s}\delta$. 由定理 1 可知 $\delta = \frac{1}{q_S + 1}$,则当 q_S 足够大时,$(1-\delta)^{q_s} = (\frac{q_S}{q_S + 1})^{q_s}$ 趋向于 e^{-1},因此,在模拟过程中 β 不终止的概率至少为 $(1 - \frac{q_{SK}}{2^k})\frac{1}{e(q_S + 1)}$.

若 A_I^2 能以不可忽略的优势 ε 攻破本文机制的不可伪造性,则 β 至少以不可忽略的优势 $(1 - \frac{q_{SK}}{2^k})\frac{\varepsilon}{e(q_S + 1)}$ 解决 *DL* 问题.

定理 4(A_{II} 类敌手的不可伪造性) 若有 A_{II} 类敌手 A_{II}^2 在多项式时间内能以不可忽略的优势赢得文献[6]中的相关游戏(A_{II}^2 最多进行 q_{SK} 次私钥生成询问和 q_S 次签密询问),则存在算法 β 在多项式时间内至少以不可忽略的优势 $(1 - \frac{q_{SK}}{2^k})\frac{\varepsilon}{e(q_S + 1)}$($e$ 为自然对数底数)解决 DL 问题.

证明思路与定理 3 类似,此处不再赘述

5 性能分析

本节将本文机制的匿名性、安全性等性质与相关机制[3~15]进行比较,并给出具体如表 1 所示的比较结果. 表 1 中 UnAnon 表示相应的参与者不具有匿名性;Anon 表示相应的参与者具有匿名性;UnSec 表示机制不具有相应的安全属性;Sec 表示机制具有相应的安全属性.

表 1　本文机制与现有机制的性能比较结果

机制	匿名性		安全性		消息数量	不足
	接收者	发送者	保密性	不可伪造性		
文献[3]	UnAnon	Anon	Unsec	Unsec	单消息	存在密钥托管问题,接收者不具有匿名性
文献[4]	UnAnon	Anon	Unsec	Sec	单消息	接收者不具有匿名性
文献[6,8,9]	UnAnon	Anon	Sec	Sec	单消息	接收者不具有匿名性
文献[7]	UnAnon	Anon	Unsec	Unsec	单消息	接收者不具有匿名性
文献[10]	UnAnon	Anon	Sec	Unsec(KGC)	单消息	存在密钥托管问题,不具有公开验证性,接收者不具有匿名性
文献[11]	Anon	Anon	Sec	Unsec(KGC)	单消息	存在密钥托管问题
文献[12]	UnAnon	Anon	Sec	Sec	单消息	接收者不具有匿名性
文献[13]	UnAnon	Anon	Sec	Unsec	单消息	存在密钥托管问题,接收者不具有匿名性
文献[14]	Anon	Anon	Sec	Unsec(KGC)	单消息	存在密钥托管问题,不具有公开验证性
文献[15]	UnAnon	Anon	Sec	Unsec(KGC)	多消息	存在密钥托管问题,接收者不具有匿名性
本文机制	Anon	Anon	Sec	Sec	多消息	与现有机制[5-15]比较尚无

注:表 1 中 Unsec(KGC)表示由于密钥托管问题造成的恶意 KGC 伪造攻击

6　效率分析

本节将从计算效率和通信开销两个方面将本文机制与相关机制[6,9-15]进行比较,并给出具体如表 2 所示的比较结果. 表 2 中 B_e 表示双线性映射运算;B_E 表示指数运算. $|Z_q^*|$ 表示 Z_q^* 中元素的长度;$|G|$ 表示 G 中元素的长度;$|M|$ 表示明文消息的长度;$|ID|$ 表示用户身份标识的长度. m 表示发送者伪装列表的成员数;n 表示接收者列表的成员数.

在计算效率方面,由于双线性映射和指数运算是影响机制性能的主要因素,因此表 1 主要对双线性映射和指数运算的次数进行了统计,对哈希及异或等计算量较少的运算并未统计. 在传输效率方面,由于本文机制进行多消息签密,导致密文的长度较长;若进行单消息通信,则本文机制具有较短的密文长度.

相较与现有机制而言,本文机制在完成多消息签密的同时,具有较高的计算和通信效率;并且本文机制具有更优的安全性能.

表 2　本文机制与现有机制的效率比较结果

机制	签密效率	解签密效率	密文长度
文献[6]	$2nB_E$	$3B_e$	$2n\|G\|+(n+1)\|Z_q^*\|+\|M\|+n\|ID\|$
文献[9]	nB_e+nB_E	$3B_e$	$2\|G\|+n\|M\|$
文献[10]	$1B_E$	$4B_e$	$(m+n+2)\|G\|+\|M\|+(m+n)\|ID\|$
文献[11]	$2B_e+3B_E$	$(n+4)B_e$	$(n+2)\|G\|+\|M\|$
文献[12]	$2nB_E$	$2B_e+3B_E$	$(2n+1)\|G\|+\|M\|+n\|ID\|$
文献[13]	$1B_E$	$2B_e+1B_E$	$(n+1)\|G\|+\|M\|+n\|ID\|$
文献[14]	$1B_e$	$(n+3)B_e$	$(m+n+2)\|G\|+2n\|M\|+m\|ID\|$
文献[15]	$1B_e$	$1B_E$	$2\|Z_q^*\|+2n\|M\|$
本文机制	0	$2B_e$	$n\|G\|+\|Z_q^*\|+n\|M\|$

7　结束语

本文为满足接收者的匿名性和发送者的多消息发送需求,提出无证书的多接收者多消息签密机制,签密密文中不再包含接收者的身份列表,实现对接收者隐私信息的保护;同时公用的信息集合确保密文解密的独立性. 相关分析表明除具有保密性和不可伪造性之外,本文机制功能更加完善,因此本文机制是安全有效的无证书多接收者多消息签密机制.

由于双线性映射的运算量较大,下一步将在本文的基础上研究不使用双线性映射的无证书多接收者多消息签密机制.

参考文献

[1] Duan S, Cao Z. Efficient and Provably Secure Multi-receiver Identity-Based Signcryption[A]. 11th Australasian Conference on Information Security and Privacy[C]. Berlin Heidelberg: Springer, 2006. 195 – 206.

[2] Lal S, Kushwah P. Anonymous ID based signcryption scheme for multiple receivers[EB/OL]. https:. eprint. iacr. org/2009/345. pdf.

[3] Yu Y, Yang B, Huang X, et al. Efficient Identity-Based Signcryption Scheme for Multiple Receivers[A]. 4th International Conference on Autonomic and Trusted Computing, Berlin Heidelberg: Springer, 2007. 13 – 21.

[4] Fagen Li, Yupu Hu, Shuanggen Liu: Efficient and provably secure multi-recipient signcryption from bilinear pairings [J]. Wuhan University Journal of Natural Sciences, 2007, 12(1): 17 – 20.

[5] Selvi S S D, Vivek S S, Gopalakrishnan R, et al. On the Provable Security of Multi-Receiver Signcryption Schemes [EB/OL]. https:. eprint. iacr. org/2008/238. pdf.

[5] Selvi S S D, Vivek S S, Rangan C P. A note on the Certificateless Multi-receiver Signcryption Scheme[EB/OL]. https:. eprint. iacr. org/2009/308. pdf.

[7] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and provably secure certificateless multi-receiver signcryption[A]. Second International Conference on Provable Security[C]. Springer Berlin Heidelberg, 2008. 52 – 67.

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

[9] Wu Lei. An ID-based multi-receiver signcryption scheme in MANET[J]. Journal of Theoretical & Applied Information Technology, 2012, 46(1), 120 – 124.

[10] Lal S, Kushwah P. Anonymous ID Based Signcryption Scheme for Multiple Receivers[EB/OL]. https:. eprint. iacr. org/2009/345. pdf.

[11] Bo Zhang, Qiuliang Xu. Identity-based multi-signcryption scheme without random oracles[J]. Chinese Journal of Computer. 2010, 33(1), 2104 – 2112.

[12] Miao S, Zhang F, Zhang L. Cryptanalysis of a certificateless multi-receiver signcryption scheme[A]. International Conference on Multimedia Information Networking and Security[C]. New York: IEEE, 2010. 593 – 597.

[13] Li F, Xiong H, Nie X. A new multi-receiver ID-based signcryption scheme for group communications[A]. International Conference on Communications, Circuits and Systems[C]. New York: IEEE, 2009. 296 – 300.

[14] Bo Zhang, Qiuliang Xu. An ID-based anonymous signcryption scheme for multiple receivers secure[J]. International Journal of Advanced Science and Technology, 2010, 20(7): 9 – 24.

[15] Qiu Jing, Bai Jun, Song Xin-chuan, et al. Secure and efficient multi-message and multi-receiver ID-based signcryption for rekeying in ad hoc networks[J]. Journal of Chongqing University, 2013, 12(2): 91 – 96.

[16] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[A]. International Conference on the Theory and Application of Cryptology and Information Security [C]. Berlin Heidelberg: Springer, 2003. 452 – 473.

作者简介

周彦伟 男,1986 年生于甘肃通渭. 陕西师范大学计算机科学学院博士生. 研究方向为无线通信技术、匿名通信技术、密码学.
E-mail: zhouyanwei1986@163. com

杨 波(通信作者) 男,1963 年生于陕西富平. 教授,博士生导师,陕西省"百人计划"特聘教授. 研究方向为密码学、信息安全.
E-mail: byang@snnu. edu. cn