给 $\mathcal{A}_{\mathrm{I}}^1$;若 c_{ID}=1,则$\mathcal{C}$选取随机数 $x_{ID}, y_{ID} \in Z_q^*$,并返回 SK_{ID}=〈x_{ID},y_{ID}〉给 $\mathcal{A}_{\mathrm{I}}^1$,并添加相应的元组〈$ID$,$x_{ID}$,$y_{ID}$〉到 L_{SK}中,确保$\mathcal{C}$对 $\mathcal{A}_{\mathrm{I}}^1$关于同一身份私钥生成询问的应答是一致的.

混合签密询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$对元组〈$ID_S$,$ID_R$,$m$〉($\mathcal{A}_{\mathrm{I}}^1$已完成对 ID_S 和 ID_R 的公钥生成询问)的混合签密询问时,$\mathcal{C}$对 ID_S 进行私钥生成询问、对 ID_R 进行公钥生成询问,获知相应的私钥 $SK_{ID_S}=(x_{ID_S}, y_{ID_S})$ 以及公钥 $PK_{ID_R}=(X_{ID_R}, Y_{ID_R})$,运行混合签密算法 $Sign_{hybrid}$生成相应的密文σ,并将σ返回给 $\mathcal{A}_{\mathrm{I}}^1$.

泄露询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$关于身份 ID 对应私钥 SK_{ID}的泄露询问 f_i()时,检测 $\mathcal{A}_{\mathrm{I}}^1$对 SK_{ID}的所有泄露询问的输出 $f_i(SK_{ID})$总和 $\sum_{k=1}^{i} f_k(SK_{ID})$是否超出系统设定的泄露参数$\lambda$:若 $\sum_{k=1}^{i} f_k(SK_{ID}) > \lambda$,则$\mathcal{C}$忽略 $\mathcal{A}_{\mathrm{I}}^1$的泄露询问;否则,返回相应的泄露信息 $f_i(SK_{ID})$给 $\mathcal{A}_{\mathrm{I}}^1$.

解混合签密询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$对元组〈$ID_S$,$ID_R$,$\sigma$〉(假设 $\mathcal{A}_{\mathrm{I}}^1$对 ID_S和 ID_R已进行了公钥生成询问)的解混合签密询问时,$\mathcal{C}$在 L_{PK}中查询 ID_R所对应的元组 $\langle ID_R, X_{ID_R}, Y_{ID_R}, c_{ID_R}\rangle$,并进行下述操作.

① 若 $\langle ID_R, X_{ID_R}, Y_{ID_R}, c_{ID_R}\rangle \in L_{PK}$ 且 $c_{ID_R}=0$, 则$\mathcal{C}$以 ID_R 和 ID_S 为索引查询 L_{SK} 与 L_{PK},分别获知 SK_{ID_R} 和 PK_{ID_S},并运行解混合签密算法 $UnSign_{hybrid}$,返回相应的结果 M给 $\mathcal{A}_{\mathrm{I}}^1$,若输入的密文无效,则$\mathcal{C}$返回特殊符号⊥.

② 若 $\langle ID_R, X_{ID_R}, Y_{ID_R}, c_{ID_R}\rangle \in L_{PK}$ 且 $c_{ID_R}=1$,$\mathcal{C}$以 ID_R 为索引在 L_1 中查询 $\langle ID_S, X_{ID_R}, Y_{ID_R}, h_1^{ID_R}\rangle \in L_1$,并计算 $U'=T(X_{ID_R}+Y_{ID_R}+h_1^{ID_R}P_{Pub})$,以 ID_S 为索引,在 L_2 中查询〈ID_S,C,U',T,S,h_2〉$\in L_2$:

- 若等式 $Verify_I^{h_2}(\pi,(PK_{ID_S}, Params))=1$ 成立,则随机选择 $M\in\{0,1\}^m$,并返回给 $\mathcal{A}_{\mathrm{I}}^1$;
- 否则,$\mathcal{C}$返回特殊符号⊥.

③ 若 $\langle ID_R, X_{ID_R}, Y_{ID_R}, c_{ID_R}\rangle \notin L_{PK}$ (即,公钥被替换),$\mathcal{C}$以 ID_R为索引在 L_{PK},L_1查询 $\langle ID_R, X'_{ID_R}, Y'_{ID_R}, c_{ID_R}\rangle \in L_{PK}$ 和 $\langle ID_R, X'_{ID_R}, Y'_{ID_R}, h_1^{ID_R}\rangle \in L_1$,并计算 $U'=T(X'_{ID_R}+Y'_{ID_R}+h_1^{ID_R}P_{Pub})$:当 $c_{ID_R}=0$ 时,$\mathcal{C}$以 ID_R和 ID_S为索引查询列表 L_{SK}与 L_{PK},分别获知 SK_{ID_R} 和 PK_{ID_S},并运行算法 $UnSign_{hybrid}$返回 M 给 $\mathcal{A}_{\mathrm{I}}^1$;当 $c_{ID_R}=1$时,$\mathcal{C}$以 ID_S为索引在 L_2 中查询〈ID_S,C,U',T,S,h_2〉$\in L_2$,若等式 $Verify_I^{h_2}(\pi,(PK_{ID_S}, Params))=1$ 成立,则随机选择 $M\in\{0,1\}^m$,并返 L_2回给 $\mathcal{A}_{\mathrm{I}}^1$;否则,$\mathcal{C}$返回特殊符号⊥.

挑战: $\mathcal{A}_{\mathrm{I}}^1$输出两个身份($ID_S$,$ID_R$)和两个等长的明文($M_0$,$M_1$),其中,$ID_R$ 是挑战身份.收到 $\mathcal{A}_{\mathrm{I}}^1$发送的挑战信息后,$\mathcal{C}$对 ID_S和 ID_R进行公钥生成询问后进行下述操作:

① 若 $c_{ID_R}=0$,则$\mathcal{C}$结束,并终止模拟.

② 否则,令 U=aP,$\mathcal{C}$选取满足 $U=T(X_S+Y_S+h_1^S P_{Pub})$ (其中, $h_1^S=H_1(ID_S, X_S, Y_S)$)的随机数 $T\in Z_q^*$,随机选取 $W\in G$,$S\in\{0,1\}^t$和 $f\leftarrow\{0,1\}$,分别计算 K=Ext(W,S)和 C=Enc(K,M_f);计算:

$$\pi = Prove_I^{\alpha}(SK_{ID_S}, (PK_{ID_S}, Params)).$$

其中,α=H_3(ID_S,C,U,T,S);令σ=(π,T,C,S)是$\mathcal{C}$对 M_f的混合签密密文,发送 ID_S,ID_R和σ给 $\mathcal{A}_{\mathrm{I}}^1$.

输出:收到挑战密文之后,经过多项式次数的上述询问(除了泄露询问)后, $\mathcal{A}_{\mathrm{I}}^1$输出对随机数 f 的猜测 $f'\leftarrow\{0,1\}$,但 $\mathcal{A}_{\mathrm{I}}^1$不能对 ID_R 进行私钥生成询问;对公钥被替换的任何身份都不能进行私钥提取询问;也不能对 ID_S,ID_R和σ进行解混合签密询问.

若 f'=f,$\mathcal{C}$输出 $abP=(h_1^{ID_R})^{-1}[W-(r_{know}^1+r_{know}^2)U]$ (其中, $W=(r_{know}^1+r_{know}^2+bh_1^{ID_R})U$)作为 CDH 困难问题的有效解;否则,$\mathcal{C}$没有解决 CDH 困难问题.

若敌手 $\mathcal{A}_{\mathrm{I}}^1$在多项式时间内赢得游戏 1,分两种情况讨论:

① 敌手 $\mathcal{A}_{\mathrm{I}}^1$能够以不可忽略的优势攻破本文机制;

② 任何敌手都无法攻破本文机制,但在泄露信息的协助下,敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 能够赢得游戏 1.

声称 1. 若 PPT 敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 能够以不可忽略的优势ε攻破本文机制,则算法$\mathcal{C}$能够以如下优势解决 CDH 问题:

$$Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1}}^{CDH}(k)=\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{1}{q(q_{S}+1)}$$

令事件$\mathcal{E}_1$表示询问阶段 $\mathcal{A}_{\mathrm{I}}^{1}$ 对挑战身份 ID_R 未进行私钥生成询问,即 $\Pr[\mathcal{E}_1]=1-\frac{q_{SK}}{2^{k}}$;事件$\mathcal{E}_2$表示询问阶段对 ID_R 未进行混合签密询问,即 $\Pr[\mathcal{E}_2]=1-\frac{q_{S}}{2^{k}}$;事件$\mathcal{E}_3$表示挑战阶段$\mathcal{C}$未终止,即 $\Pr[\mathcal{E}_3]=\frac{1}{q_{S}+1}$;事件$\mathcal{E}_4$表示挑战阶段$\mathcal{C}$输出一个有效的挑战密文,即 $\Pr[\mathcal{E}_4]=\frac{1}{q}$.于是,整个模拟过程中$\mathcal{C}$不终止的概率为

$$\Pr[\mathcal{E}_1\wedge\mathcal{E}_2\wedge\mathcal{E}_3\wedge\mathcal{E}_4]=\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{1}{q(q_{S}+1)}.$$

综上所述,忽略信息的泄露,若敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 能够以不可忽略的优势ε攻破本文混合签密机制,则有算法$\mathcal{C}$能够以不可忽略的优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1}}^{CDH}(k)=\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{\varepsilon}{q(q_{S}+1)}$ 输出 CDH 问题的有效解.

声称 2. 若任意的 PPT 敌手都无法以不可忽略的优势攻破本文混合签密机制,但在相关泄露信息的协助下,敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 能够在游戏 1 中获胜,则算法$\mathcal{C}$能够以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1},Leakage}^{CDH}(k)\leqslant\frac{2^{\frac{m+\lambda}{2}-1}}{\sqrt{q}}$ 解决 CDH 问题.

作为敌手,$\mathcal{A}_{\mathrm{I}}^{1}$ 能够从挑战密文、公钥和λ-比特的泄露信息中获知关于私钥的相关信息.令 $Leak_{SK}$ 表示 $\mathcal{A}_{\mathrm{I}}^{1}$ 获得的关于挑战身份 ID_R 私钥 SK_{ID_R} 所有泄露函数 $f_i()(i\geqslant 1)$的输出,则 $Leak_{SK}$ 最多有 2^{λ}个值.有下述关系成立:

$$\begin{aligned}\tilde{H}_{\infty}(U(x_{ID_R}+y_{ID_R})\mid PK_{ID_R},\sigma,Params,Leak_{SK})&=\tilde{H}_{\infty}(U(x_{ID_R}+y_{ID_R})\mid PK_{ID_R},Leak_{SK})\\&=\tilde{H}_{\infty}(x_{ID_R},y_{ID_R}\mid PK_{ID_R},Leak_{SK})\\&\geqslant\tilde{H}_{\infty}(x_{ID_R},y_{ID_R}\mid PK_{ID_R})-\lambda\\&\geqslant\log q-\lambda.\end{aligned}$$

在上述公式中,σ和 $Params$ 与私钥 SK_{ID_R} 无关,并且 $U(x_{ID_R}+y_{ID_R})$ 是关于 SK_{ID_R} 的单向映射.由引理 1 可知,$\mathcal{A}_{\mathrm{I}}^{1}$ 获知 SK_{ID_R} 的概率至多为 $2^{-\tilde{H}_{\infty}(U(x_{ID_R}+y_{ID_R})\mid PK_{ID_R},\sigma,Params,Leak_{SK})}\leqslant\frac{2^{\lambda}}{q}$,则 $\mathcal{A}_{\mathrm{I}}^{1}$ 输出 $K=Ext(U(x_{ID_R}+y_{ID_R}),S)$ 的最大概率为 $\frac{1}{2}\sqrt{2^{l_2}\frac{2^{\lambda}}{q}}=\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}$.因此,在相关泄露信息的协助下,$\mathcal{A}_{\mathrm{I}}^{1}$ 输出 $f'=f$ 的概率为 $\Pr[f'=f]_{Under}\leqslant\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}$;若未得到泄露信息的协助,则 $\mathcal{A}_{\mathrm{I}}^{1}$ 输出 $f'=f$ 的概率为 $\Pr[f'=f]_{\mathrm{Without}}=\frac{1}{2}$.于是,$\mathcal{C}$解决 CDH 问题的概率为

$$\Pr[f'=f]\leqslant\frac{1}{2}+\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}.$$

因此$\mathcal{C}$解决 CDH 问题的优势为 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1},Leakage}^{CDH}(k)=\Pr[f'=f]-\frac{1}{2}\leqslant\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}$,其中,$\lambda\leqslant\log q-l_2-\omega\log(k)$.

由声称 1 和声称 2 可知,引理 5 得证. □

引理 6. 若存在敌手 $\mathcal{A}_{\mathrm{II}}^{1}$ 能够在多项式时间内赢得游戏 2,则存在算法$\mathcal{C}$,能够在多项式时间内以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{II}}^{1},Leakage}^{IND\text{-}KL\text{-}CCA2}(k,\lambda)\in\left[\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{\varepsilon}{q(q_{S}+1)},\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{\varepsilon}{q(q_{S}+1)}+\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}\right]$ 解决 CDH 问题.

证明过程与引理 5 相似,本文不再赘述.

定理 1. 若 CDH 假设成立,则本文混合签密机制Π=(*Setup*,*KeyGen*,$Sign_{hybrid}$,$UnSign_{hybrid}$)在随机谕言机模型下是语义安全的抵抗 IND-KL-CCA2.

由引理 5 和引理 6 可知,定理 1 得证.

3.2 不可伪造性

引理 7. 若存在敌手 $\mathcal{A}_{\mathrm{I}}^2$ 能够在多项式时间内赢得游戏 3,则存在算法$\mathcal{C}$,能够在多项式时间内以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^2,Leakage}^{EUF\text{-}KL\text{-}CMA}(k,\lambda)\in\left[\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)},\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)}+\frac{2^{\lambda}}{q-q_d+1}\right]$ 解决 DL 困难问题.其中,泄露参数$\lambda\leqslant\log q-l_2-\omega\log(k)$,$q_S$($q_S<q$)为混合签密询问的次数,$q_{SK}$($q_{SK}<q$)为私钥生成询问的次数,$q_d$($q_d<q$)为解混合签密询问的次数,$\varepsilon$是敌手 $\mathcal{A}_{\mathrm{I}}^2$ 攻破本文混合签密机制的优势.

证明:算法$\mathcal{C}$是一个 DL 问题的解决者,输入为$\langle P,bP\rangle$,其中,$b\in Z_q^*$ 且未知,目标是计算 b.$\mathcal{C}$以 $\mathcal{A}_{\mathrm{I}}^2$ 为子程序并充当游戏的挑战者.$\mathcal{C}$运行 Setup 算法,并发送 *Params* 给 $\mathcal{A}_{\mathrm{I}}^2$,令 $P_{Pub}=bP$,并秘密保存主密钥 S_{MSK};维持列表 L_1,L_2,L_{SK},L_{PK} 分别用于跟踪 $\mathcal{A}_{\mathrm{I}}^2$ 对谕言机 H_1,H_2,私钥生成和公钥生成的询问.初始时,各列表为空.

询问:敌手 $\mathcal{A}_{\mathrm{I}}^2$ 执行多项式有界次的 H_1 询问、H_2 询问、私钥提取、公钥提取、公钥替换、混合签密、泄露询问和解混合签密询问,$\mathcal{C}$按引理 5 中的应答方式对相关询问进行应答.但在该游戏中,挑战身份是 ID_S 而不是 ID_R.

伪造: $\mathcal{A}_{\mathrm{I}}^2$ 选择 $u\in Z_q^*$,并计算 $U=uP$,选取满足 $U=T(X_S+Y_S+h_1^S P_{Pub})$ (其中, $h_1^S=H_1(ID_S,X_S,Y_S)$)的随机数 $T\in Z_q^*$,随机选取 $S\in\{0,1\}^t$,并计算 $K=Ext(u(X_{ID_R}+Y_{ID_R}+h_1^{ID_R}P_{Pub}),S)$ 和 $C=Enc(K,M)$,选取随机数 $\pi\in Z_q^*$,则 $\sigma=(\pi,T,C,S)$是 $\mathcal{A}_{\mathrm{I}}^2$ 伪造的关于 ID_S,ID_R 和 M 的混合签密密文,其中,对 M 未进行混合签密询问. $\mathcal{A}_{\mathrm{I}}^2$ 发送 ID_S,ID_R 和σ给$\mathcal{C}$.伪造阶段, $\mathcal{A}_{\mathrm{I}}^2$ 可进行概率多项式时间次数的上述询问,但 $\mathcal{A}_{\mathrm{I}}^2$ 不能对 ID_S 进行私钥生成询问,对公钥被替换的任何身份都不能进行私钥生成询问.

当$\mathcal{C}$接收到 $\mathcal{A}_{\mathrm{I}}^2$ 所发送的伪造信息后,以 ID_S 为索引查询 L_{PK},获知相应的元组$\langle ID_S,X_{ID_S},Y_{ID_S},c_{ID_S}\rangle$并进行下述操作:

① 若 $c_{ID_S}=0$,则$\mathcal{C}$结束,并终止模拟.

② 否则,$\mathcal{C}$输出 $b=(Th_1^{ID_S})^{-1}[u-T(r_{know}^1+r_{know}^2)]$ (其中, $T=u(r_{know}^1+r_{know}^2+bh_1^{ID_S})^{-1}$)作为 DL 问题的有效解.

声称 3. 若 PPT 敌手 $\mathcal{A}_{\mathrm{I}}^2$ 能够以不可忽略的优势ε伪造合法的混合签密密文,则算法$\mathcal{C}$能够以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^2}^{DL}(k)=\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q_S+1}$ 解决 DL 问题.

令事件$\mathcal{E}_1$表示询问阶段 $\mathcal{A}_{\mathrm{I}}^2$ 对挑战身份 ID_S 未进行私钥生成询问,即 $\Pr[\mathcal{E}_1]=1-\frac{q_{SK}}{2^k}$;事件$\mathcal{E}_2$表示询问阶段 $\mathcal{A}_{\mathrm{I}}^2$ 对挑战身份 ID_S 未进行混合签密询问,即 $\Pr[\mathcal{E}_2]=1-\frac{q_S}{2^k}$;事件$\mathcal{E}_3$表示挑战阶段$\mathcal{C}$未终止,即 $\Pr[\mathcal{E}_3]=\frac{1}{q_S+1}$;事件$\mathcal{E}_4$表示敌手 $\mathcal{A}_{\mathrm{I}}^2$ 输出了有效的伪造信息,即 $\Pr[\mathcal{E}_4]=\frac{1}{q}$.于是,整个模拟过程中$\mathcal{C}$不终止的概率为

$$\Pr[\mathcal{E}_1\wedge\mathcal{E}_2\wedge\mathcal{E}_3\wedge\mathcal{E}_4]=\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{1}{q(q_S+1)}.$$

综上所述,忽略信息的泄露,若 $\mathcal{A}_{\mathrm{I}}^2$ 能够以不可忽略的优势ε攻破本文机制,则算法$\mathcal{C}$能够以不可忽略的优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^2}^{DL}(k)=\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)}$ 输出 DL 问题的有效解.

声称 4. 若任意的 PPT 敌手都无法以不可忽略的优势攻破本文机制的不可伪造性,但在相关泄露信息的协助下,敌手 $\mathcal{A}_{\mathrm{I}}^{2}$ 能够在游戏 3 中获胜,即 $\mathcal{A}_{\mathrm{I}}^{2}$ 输出了有效的伪造签名,则算法 $\mathcal{C}$ 能够以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{2},Leakage}^{DL}(k)\leqslant\frac{2^{\lambda}}{q-q_d+1}$ 解决 DL 问题.

令 $Leak'_{SK}$ 表示 $\mathcal{A}_{\mathrm{I}}^{2}$ 选择的所有关于身份 ID_S 私钥 SK_{ID_S} 的泄露信息,则 $Leak'_{SK}$ 最多有 2^{λ} 个值.有关系 $\tilde{H}_{\infty}(SK_{ID_S}\mid PK_{ID_S},\sigma,Params,Leak'_{SK})\geqslant\tilde{H}_{\infty}(SK_{ID_S}\mid PK_{ID_S})-\lambda\geqslant\log q-\lambda$ 成立,式中,σ 和 $Params$ 与私钥 SK_{ID_S} 无关.根据引理 1 可知,$\mathcal{A}_{\mathrm{I}}^{2}$ 获知 SK_{ID_S} 的概率最多为 $2^{-\tilde{H}_{\infty}(SK_{ID_S}\mid PK_{ID_S},\sigma,Leak'_{SK})}\leqslant\frac{2^{\lambda}}{q}$.

如果混合签密密文 $\sigma=(\pi,T,C,S)$ 满足等式 $Verify_T^{\alpha}(\pi,(PK_{ID_S},Params))=1$ (其中,$\alpha=H_3(ID_a,C,U,T,S)$ 和 $U=T(X_{ID_S}+Y_{ID_S}+h_1^{ID_S}P_{Pub})$),则称密文 σ 为有效密文;否则,称 σ 为无效密文.伪造攻击过程中,$\mathcal{A}_{\mathrm{I}}^{2}$ 可至多向解混合签密谕言机 $UnSign_{hybrid}^{\mathcal{O}}()$ 提出 q_d 次询问.在上述询问应答的帮助下,$\mathcal{A}_{\mathrm{I}}^{2}$ 输出最终的伪造密文.

令 σ' 是 $\mathcal{A}_{\mathrm{I}}^{2}$ 向 $UnSign_{hybrid}^{\mathcal{O}}()$ 询问的第 1 个密文,则 $UnSign_{hybrid}^{\mathcal{O}}()$ 接收 σ' 的优势至多是 $\frac{2^{\lambda}}{q}$;若 $UnSign_{hybrid}^{\mathcal{O}}()$ 拒绝了该密文 σ',则 $\mathcal{A}_{\mathrm{I}}^{2}$ 可获知关于私钥的相关信息,此时,$\mathcal{A}_{\mathrm{I}}^{2}$ 生成有效密文的优势至多是 $\frac{2^{\lambda}}{q-1}$.综合考虑所有的 q_d 次解混合签密询问,可知 $\mathcal{A}_{\mathrm{I}}^{2}$ 伪造有效密文的优势至多是 $\frac{2^{\lambda}}{q-q_d+1}$.于是,算法 $\mathcal{C}$ 解决 DL 问题的优势为

$$Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1},Leakage}^{CDH}(k)\leqslant\frac{2^{\lambda}}{q-q_d+1}.$$

其中,$\lambda\leqslant\log q-l_2-\omega\log(k)$.

由声称 3 和声称 4 证明可知,引理 7 得证. □

引理 8. 若存在敌手 $\mathcal{A}_{\mathrm{II}}^{2}$ 能够在多项式时间内赢得游戏 4,则存在算法 $\mathcal{C}$,能在多项式时间内,以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{II}}^{2},Leakage}^{EUF\text{-}KL\text{-}CMA}(k,\lambda)\in\left[\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)},\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)}+\frac{2^{\lambda}}{q-q_d+1}\right]$ 解决 DL 问题.

证明过程与引理 7 类似,本文不再赘述.

定理 2. 若 DL 假设成立,则本文混合签密机制 $\Pi=(Setup,KeyGen,Sign_{hybrid},UnSign_{hybrid})$ 在随机谕言机模型下是存在性不可伪造的抵抗 EUF-KL-CMA.

由引理 7 和引理 8 可知,定理 2 得证.

3.3 公开验证性

本文方案中,当发送者和接收者关于密文的有效性发生争执,需要公开验证发送者身份时,第三方无需收发双方的任何私有信息,只需验证等式 $Verify_T^{\alpha}(\pi,(PK_{ID_S},Params))=1$ (其中,参数 α 均可由相关公开信息计算得到)是否成立即可,因此,本文方案具有公开验证性.

3.4 不可否认性

本文方案中,密文消息是不可伪造的.因此,若发送者确实生成了签密密文,该发送者就不能否认;同时,由公开验证性可知,任何第三方均可公开验证密文发送者的身份,因此,本文方案具有不可否认性.

3.5 前/后向安全性

本文方案中,即使在某次签密密文的收发过程中,攻击者获得签密发送者或密文接收者的相关参数,由于密文生成参数是随机选取的,具有较强的新鲜性,因此,攻击者无法获知先前的密文及相关参数,则攻击者无法获得先前的明文消息.同时,攻击者也无法猜测发送者即将发送的签密密文及其相关参数,所以也无法获知即将要

发送的明文消息.因此,本文方案具有完美的前/后向安全性.

4 性能分析

与现有的混合签密方案[7−11]进行比较时,计算开销主要取决于混合签密和签密验证算法的计算量,且计算量主要统计双线性映射及群上点乘运算和指数运算的执行次数,但未统计可提前准备的相关计算及混合签密中必须进行的对称加解密运算;通信开销主要通过密文的长度来衡量;而安全属性主要讨论方案的不可伪造性、机密性和抗泄露性等.

表 1 中相关符号的含义如下:$\mathcal{O}_M$表示群上的点乘运算,$\mathcal{O}_E$表示群上的指数运算,$\mathcal{O}_B$表示双线性映射运算,$\mathcal{O}_{Ext}$表示随机提取器运算,$\mathcal{O}_P$表示 tSE-NIZK 论证的 Prove 运算,$\mathcal{O}_V$表示 tSE-NIZK 论证的 Verify 运算,$|M|$表示明文消息 M 的长度,$|G|$表示群 G 上相应元素的长度,$|Z|$表示 Z_q^* 上相应元素的长度,$|\{0,1\}^n|$表示字符串$\{0,1\}^n$的长度.

Table 1 Comparison of computational efficiency

表 1 效率比较结果

混合签密机制	计算效率		通信开销	安全属性				
	混合签密	解混合签密	密文长度	不可伪造性	机密性	公开验证性	不可否认性	抗泄露性
文献[7]	$2\mathcal{O}_M+\mathcal{O}_B$	$5\mathcal{O}_B$	$2\|G\|+\|M\|$	√	√	√	√	×
文献[8]	$2\mathcal{O}_M$	$\mathcal{O}_M+3\mathcal{O}_B$	$\|\{0,1\}^n\|+2\|G\|+\|M\|$	√	√	√	√	×
文献[9]	$\mathcal{O}_M+\mathcal{O}_B$	$\mathcal{O}_M+\mathcal{O}_B$	$\|Z\|+\|M\|$	√	√	×	×	×
文献[11]	$\mathcal{O}_M+2\mathcal{O}_E+2\mathcal{O}_B$	$\mathcal{O}_M+\mathcal{O}_E+6\mathcal{O}_B$	$\|Z\|+\|G\|+\|M\|$	√	√	×	√	×
本文方案	$\mathcal{O}_M+\mathcal{O}_{Ext}+\mathcal{O}_P$	$\mathcal{O}_M+\mathcal{O}_{Ext}+\mathcal{O}_V$	$2\|Z\|+\|M\|$	√	√	√	√	√

√表示方案具有该属性,×表示方案不具有该属性

如表 1 所示,在计算效率方面,由于运行一次双线性对运算的时间较大,因此相对于现有的使用双线性映射的混合签密机制[7−11]而言,不使用双线性映射的混合签密机制具有更大的效率优势,即本文方案在效率方面有明显的优势;在安全性方面,文献[7–9,11]的方案不具有抗泄露性,在信息可泄露的环境中,上述机制[7−11]无法满足其所声称的安全性,而本文机制依然保持其原有的安全性;文献[9,11]中方案不满足公开验证性;文献[9]的方案不具有不可否认性.综上所述,现有的混合签密机制[7−11]在计算效率或安全性方面存在一定的不足.相对于上述机制,本文机制的计算和通信效率及安全性更优.

5 结束语

签密作为一种较为理想的数据信息安全传输方法,其安全性和计算开销对其实际应用有着至关重要的作用.本文针对传统混合签密方案[7−11]无抗泄露的能力和存在计算效率低的不足,在不使用双线性映射的基础上提出了安全、高效的抗泄露无证书混合签密机制,并在随机谕言机模型下基于 CDH 和 DL 问题对本文机制的机密性和不可伪造性进行了证明;同时,分析了本文方案的公开验证性、前/后向安全性和不可否认性等安全属性.与现有的无证书混合签密机制[7−11]相比,本文机制不仅具有更优的计算效率和安全性,而且在信息可泄露的环境中依然保持其所声称的安全性,即本文方案具有抵抗秘密信息泄露的能力.

由于随机提取器的运算必须有随机种子的参与,在一定程度上会增加密文的传输负载.下一阶段,本文将构造不使用随机提取器的抗泄露无证书混合签密机制.

References:

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption). In: Proc. of the Advances in Cryptology—CRYPTO'97. Berlin, Heidelberg: Springer-Verlag, 1997. 165–179. [doi: 10.1007/BFb0052234]

[2] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proc. of the Advances in Cryptology—ASIACRYPT 2003. Berlin, Heidelberg: Springer-Verlag, 2003. 452–473. [doi: 10.1007/978-3-540-40061-5_29]

[3] Shamir A. Identity-Based cryptosystems and signature schemes. In: Proc. of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, 1985. 47−53. [doi: 10.1007/3-540-39568-7_5]
[4] Dent AW. Hybrid signcryption schemes with outsider security. In: Proc. of the Information Security. Berlin, Heidelberg: Springer-Verlag, 2005. 203−217. [doi: 10.1007/11556992_15]
[5] Dent AW. Hybrid signcryption schemes with insider security. In: Proc. of the Information Security and Privacy. Berlin, Heidelberg: Springer-Verlag, 2005. 253−266. [doi: 10.1007/11506157_22]
[6] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 2003,33(1):167−226. [doi: 10.1137/S0097539702403773]
[7] Li F, Shirase M, Takagi T. Certificateless hybrid signcryption. In: Proc. of the Information Security Practice and Experience. Berlin, Heidelberg: Springer-Verlag, 2009. 112−123. [doi: 10.1007/978-3-642-00843-6_11]
[8] Li F, Shirase M, Takagi T. Identity-Based hybrid signcryption. In: Proc. of the Int'l Conf. on Availability, Reliability and Security (ARES 2009). IEEE, 2009. 534−539. [doi: 10.1109/ARES.2009.44]
[9] Sun YX, Li H. Efficient certificateless hybrid signcryption. Ruan Jian Xue Bao/Journal of Software, 2011,22(7):1690−1698 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3825.htm [doi: 10.3724/SP.J.1001.2011.03825]
[10] Selvi SSD, Vivek SS, Pandu Rangan C. Breaking and re-building a certificateless hybrid signcryption scheme. Lecture Notes in Computer Science, 2010:294−307. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=F4BD72725754665BBCB2010D8E30910B?doi=10.1.1.215.5905&rep=rep1&type=pdf
[11] Yu HF, Yang B. Provably secure certificateless hybrid signcryption. Chinese Journal of Computers, 2015,38(4):804−813 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2015.00804]
[12] Kocher PC. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Proc. of the Advances in Cryptology—CRYPTO'96. Berlin, Heidelberg: Springer-Verlag, 1996. 104−113. [doi: 10.1007/3-540-68697-5_9]
[13] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems. In: Proc. of the Advances in Cryptology—CRYPTO'97. Berlin, Heidelberg: Springer-Verlag, 1997. 513−525. [doi: 10.1007/BFb0052259]
[14] Kocher P, Jaffe J, Jun B. Differential power analysis. In: Proc. of the Advances in Cryptology—CRYPTO'99. Berlin, Heidelberg: Springer-Verlag, 1999. 388−397. [doi: 10.1007/3-540-48405-1_25]
[15] Halderman JA, Schoen SD, Heninger N, Clarkson W, Paul W, Calandrino JA, Feldman AJ, Appelbaum J, Felten EW. Lest we remember: Cold-Boot attacks on encryption keys. Communications of the ACM, 2009,52(5):91−98. [doi: 10.1145/1506409.1506429]
[16] Dodis Y, Haralambiev K, López-Alt A, Wichs D. Efficient public-key cryptography in the presence of key leakage. In: Proc. of the Advances in Cryptology—ASIACRYPT 2010. Berlin, Heidelberg: Springer-Verlag, 2010. 613−631. [doi: 10.1007/978-3-642-17373-8_35]
[17] Li SJ, Zhang FT, Sun YX, Shen LM. Efficient leakage-resilient public key encryption from DDH assumption. Cluster Computing, 2013,16(4):797−806. [doi: 10.1007/s10586-013-0253-z]
[18] Liu SL, Weng J, Zhao YL. Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks. In: Proc. of the Topics in Cryptology—CT-RSA 2013. Berlin, Heidelberg: Springer-Verlag, 2013. 84−100. [doi: 10.1007/978-3-642-36095-4_6]
[19] Naor M, Segev G. Public-Key cryptosystems resilient to key leakage. SIAM Journal on Computing, 2012,41(4):772−814. [doi: 10.1137/100813464]

附中文参考文献:

[9] 孙银霞,李晖.高效无证书混合签密.软件学报,2011,22(7):1690−1698. http://www.jos.org.cn/1000-9825/3825.htm [doi: 10.3724/SP.J.1001.2011.03825]
[11] 俞惠芳,杨波.可证安全的无证书混合签密.计算机学报,2015,38(4):804−813. [doi: 10.3724/SP.J.1016.2015.00804]

周彦伟(1986－),男,甘肃通渭人,博士生,工程师,主要研究领域为密码学,匿名通信技术,可信计算.

王青龙(1970－),男,博士,副教授,主要研究领域为密码学及其应用.

杨波(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.