令 $er_0,er_1,...,er_{l_A},ex_2,ex_3,...,ex_{n_A}$ 是 A 的临时私钥,A 计算:

$$X=g^{s_A},(U_i=g^{a\lambda_i}h_{\rho_A(i)}^{-r_i},D_i=g^{r_i}),1\leqslant i\leqslant l_A(\text{令集合}\{U,D\}=\{(U_i,D_i),1\leqslant i\leqslant l_A\}).$$

A 发送消息 $EPK_A=(X,\{U,D\},M_A,\rho_A)$给 B.

Step 2. B 接收到 A 发送的消息 EPK_A 后,判断自己的属性集合 S_B 是否满足访问结构(M_A,ρ_A):若不满足,协议终止;若 S_B 满足访问结构(M_A,ρ_A),B 选取访问结构 AS_B,AS_B 对应的 LSSS 矩阵记为 M_B,M_B 的规模是 $l_B\times n_B$,M_B 的行向量与属性之间的一一对应关系记为ρ_B.

B 随机选取 $er_0',er_1',...,er_{l_B}',ex_2',ex_3',...,ex_{n_B}'\in Z_p$,计算:

$$s_B=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},er_0'),$$
$$r_i'=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},er_i'),1\leqslant i\leqslant l_B,$$
$$x_k'=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},ex_k'),2\leqslant k\leqslant n_B.$$

令 $v'=(s_B,x_2',x_3',...,x_{n_B}')\in(Z_p)^{n_B}$,计算 $\lambda_i'=v'\cdot M_B(i)$,其中,$M_B(i)$是矩阵 M_B 的第 i 行,i=1,…,l_B.

令 $er_0',er_1',...,er_{l_B}',ex_2',ex_3',...,ex_{n_B}'$ 是 B 的临时私钥,B 计算:

$$Y=g^{s_B},(V_i=g^{a\lambda_i'}h_{\rho_B(i)}^{-r_i'},E_i=g^{r_i'}),1\leqslant i\leqslant l_B(\text{令集合}\{V,E\}=\{(V_i,E_i),1\leqslant i\leqslant l_B\}).$$

B 发送消息 $EPK_B=(Y,\{V,E\},M_B,\rho_B)$给 A.

Step 3. A 接收到EPK_B后,判定属性集合 S_A 是否满足访问结构(M_B,ρ_B),若不满足,协议终止;否则,按照以下方式计算共享密钥:

令 $I_A=\{i:\rho_B(i)\in S_A\}$,计算 $\{w_A(i)\in Z_p\}_{i\in I_A}$,使得 $\sum_{i=1}^{l_B}w_A(i)\cdot M_B(i)=(1,0,0,...,0)$, $M_B(i)$是矩阵 M_B 的第 i 行,i=1,…,l_B.

计算:

$$\sigma_1=(g_T^{\alpha})^{s_A},$$
$$\sigma_2=e(Y,K_A)\Big/\left(\left(\prod_{i\in I_A}e(V_i,L_A)e(E_i,K_{A,\rho_B(i)})\right)^{w_A(i)}\right),$$
$$\sigma_3=Y^{s_A}.$$

最后,计算出共享密钥 $K_{AB}=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$.

B 收到 EPK_A,并且在 Step 2 中已经判断出自己的属性集合 S_B 满足访问结构(M_A,ρ_A),则 B 按如下方式计算共享密钥.

令 $I_B=\{i:\rho_A(i)\in S_B\}$,计算 $\{w_B(i)\in Z_p\}_{i\in I_B}$,使得 $\sum_{i=1}^{l_A}w_B(i)\cdot M_A(i)=(1,0,0,...,0)$, $M_A(i)$是矩阵 M_A 的第 i 行,i=1,…,l_A.

计算:

$$\sigma_1=e(X,K_B)\Big/\left(\prod_{i\in I_B}(e(U_i,L_B)e(D_i,K_{B,\rho_A(i)}))^{w_B(i)}\right),$$
$$\sigma_2=(g_T^{\alpha})^{s_B},$$
$$\sigma_3=X^{s_B}.$$

最后,计算出共享密钥 $K_{BA}=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$.

4.2 协议的正确性

根据双线性对的性质,A 计算:

$$\sigma_1=(g_T^{\alpha})^{s_A},$$

$$\sigma_2=e(Y,K_A)\Big/\left(\prod_{i\in I_A}(e(V_i,L_A)e(E_i,K_{A,\rho_B(i)}))^{w_A(i)}\right)$$

$$=e(g^{s_B},g^{\alpha})e(g^{s_B},g^{at_A})\Big/\left(\prod_{i\in I_A}e(g^{a\lambda_i'},g^{t_A})^{w_A(i)}e(h_{\rho_B(i)}^{-r_i'},g^{t_A})^{w_A(i)}e(g^{r_i'},h_{\rho_B(i)}^{t_A})^{w_A(i)}\right)$$

$$=e(g^{s_B},g^{\alpha})e(g^{s_B},g^{at_A})\Big/e(g^{a},g^{t_A})^{\sum_{i\in I_A}\lambda_i'w_A(i)}$$

$$=e(g^{s_B},g^{\alpha})e(g^{s_B},g^{at_A})/e(g^{a},g^{t_A})^{s_B}$$

$$=e(g,g)^{\alpha s_B}$$

$$=(g_T^{\alpha})^{s_B},$$

$$\sigma_3=Y^{s_A}=g^{s_As_B}.$$

$$K_{AB}=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)=H((g_T^{\alpha})^{s_A},(g_T^{\alpha})^{s_B},g^{s_As_B},EPK_A,EPK_B) \quad (1)$$

同理,B 计算:

$$\sigma_1=e(X,K_B)\Big/\left(\prod_{i\in I_B}(e(U_i,L_B)e(D_i,K_{B,\rho_A(i)}))^{w_B(i)}\right)$$

$$=e(g^{s_A},g^{\alpha}g^{at_B})\Big/\left(\prod_{i\in I_B}(e(g^{a\lambda_i}h_{\rho_A(i)}^{-r_i},g^{t_B})e(g^{r_i},h_{\rho_A(i)}^{t_B}))^{w_B(i)}\right)$$

$$=e(g^{s_A},g^{\alpha})e(g^{s_A},g^{at_B})\Big/\left(\prod_{i\in I_B}e(g^{a\lambda_i},g^{t_B})^{w_B(i)}e(h_{\rho_A(i)}^{-r_i},g^{t_B})^{w_B(i)}e(g^{r_i},h_{\rho_A(i)}^{t_B})^{w_B(i)}\right)$$

$$=e(g^{s_A},g^{\alpha})e(g^{s_A},g^{at_B})\Big/e(g^{a},g^{t_B})^{\sum_{i\in I_B}\lambda_iw_B(i)}$$

$$=e(g^{s_A},g^{\alpha})e(g^{s_A},g^{at_B})/e(g^{a},g^{t_B})^{s_A}$$

$$=(g_T^{\alpha})^{s_A},$$

$$\sigma_2=(g_T^{\alpha})^{s_B},$$

$$\sigma_3=X^{s_B}=g^{s_As_B}.$$

$$K_{BA}=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)=H((g_T^{\alpha})^{s_A},(g_T^{\alpha})^{s_B},g^{s_As_B},EPK_A,EPK_B) \quad (2)$$

由公式(1)和公式(2)可知,K_{AB}=K_{BA}.

4.3 协议的安全性

定理 1. 若 GCPBDHE 假设和 CDH 假设同时成立,并且 H,H_1 是随机预言机,则本文提出的 ABAKE 协议在 ABeCK 模型下具有选择安全性.

协议的安全性证明过程见附录.

4.4 协议对比

本节将已有的 ABAKE 协议与本文的协议进行对比,对比结果见表 1.

Table 1 Comparison of protocols

表 1 协议的对比

方案	消息长度	计算复杂性	安全模型
文献[4]	(|S|+2)个 G 上的点	(|S|+2)P+(|S|+2)E_1+1E_2	BR&标准模型
文献[7]	(|S|+1)个 G 上的点和 1 个 G_T 上的点	(|S|)P+(|S|+3)E_1+(|S|)E_2	CK&标准模型
文献[8]	(l×$n_{\max}$+1)个 G 上的点	($n_{\max}$+|S|+1)P+(l×($n_{\max}$+n)+2|S|)E_1+2E_2+(l×$n_{\max}$+1)H	eCK&RO 模型
本文协议	(2l+1)个 G 上的点	(2|S|+1)P+(3l+1+2|S|)E_1+2E_2+(l×n+1)H	eCK&RO 模型
文献[11]	(2l+4)个 G 上的点	(2|S|+2)P+(3l+5)E_1+2E_2+H+3Ext	CK+&标准模型

其中,$n_{\max}$表示系统中 LSSS 矩阵的列的最大规模;$l\times n$ 表示 LSSS 矩阵的规模;$|S|$表示用户属性集的规模;P 表示双线性映射;E_1 表示 G 上的指数运算;E_2 表示 G_T 上的指数运算;H 表示 Hash 运算,需要指出的是,若协议中采取了不同的 Hash 运算,例如 t_1 次 H_1 运算和 t_2 次 H 运算,这里简记为(t_1+t_2)次 H 运算;Ext 表示随机提取器的计算复杂度.

一般情况下,$n_{\max}>2$.因此,由表 1 可以看出:与文献[8]相比,同样在 AbeCK&RO 模型下,本文提出的协议降低了消息长度;同时,在 $n_{\max}\geqslant|S|$的情况下,也降低了计算复杂度.

5 结束语

本文对 GCDH 假设进行了扩展,提出了 GCPBDHE 假设,提出了基于属性的认证密钥协商协议.在 GCPBDHE 假设和 CDH 假设成立的条件下,证明了该协议在 ABeCK 模型下是安全的.如何设计安全强度和效率更高的 ABAKE 协议,是下一步要解决的问题.

致谢 审稿专家和编辑老师为本文提出了宝贵的修改建议,在此表示衷心的感谢.

References:

[1] Shamir. Identity-Based cryptosystems and signature schemes. In: Proc. of the CRYPTO'84. Santa Barbara: Springer-Verlag, 1984. 47−53. [doi: 10.1007/3-540-39568-7_5]

[2] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proc. of the EUROCRYPT 2005. Aarhus: Springer Press, 2005. 457−473. [doi: 10.1007/11426639_27]

[3] Wang H, Xu QL, Ban T. A provably secure two-party attribute-based key agreement protocol. In: Proc. of the 5th Int'l Conf. on Intelligent Information Hiding and Multimedia Signal Processing. IEEE Press, 2009. 1042−1045. [doi: 10.1109/IIH-MSP.2009.92]

[4] Wang H, Xu QL. Revocable attribute-based key agreement protocol without random oracles. Journal of Networks, 2009,4(8): 787−794. [doi: 10.4304/jnw.4.8.787-794]

[5] Wang H, Xu QL. Two-Party attribute-based key agreement protocol in the standard model. In: Proc. of the 2009 Int'l Symp. on Information Processing (ISIP 2009). Huangshan: Springer-Verlag, 2009. 325−328.

[6] Gorantla MC, Boyd C, Nieto JMG. Attribute-Based authenticated key exchange. In: Proc. of the 15th Australasian Conf. on Information Security and Privacy (ACISP 2010). Sydney: Springer-Verlag, 2010. 300−317. [doi: 10.1007/978-3-642-14081-5_19]

[7] Ren YJ, Wang JD, Zhuang Y, Tan CH, Fang LM. Attribute-Based authenticated key agreement protocol. Journal of LanZhou University (Nature Sciences), 2010,46(2):103−110 (in Chinese with English abstract).

[8] Yoneyama K. Strongly secure two-pass attribute-based authenticated key exchange. In: Proc. of the Pairing-Based Cryptography. Yamanaka Hot Spring: Springer-Verlag, 2010. 147−166. [doi: 10.1007/978-3-642-17455-1_10]

[9] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Proc. of the 14th Int'l Conf. on Practice and Theory in Public Key Cryptography (PKC2011). Taormina: Springer-Verlag, 2011. 53−70. [doi: 10.1007/978-3-642-19379-8_4]

[10] Wei JH, Hu XX, Liu WF. Attribute-Based authenticated key exchange protocol in multiple attribute authorities environment. Journal of Electronics & Information Technology, 2012,34(2):451−456 (in Chinese with English abstract). [doi: 10.3724/SP.J.1146.2011.00701]

[11] Li Q, Feng DG, Zhang LW, Gao ZG. Enhanced attribute-based authenticated key agreement protocol in the standard model. Chinese Journal of Computers, 2013,36(10):2156−2167 (in Chinese with English abstract).

[12] Okamoto T, Pointcheval D. The gap-problems: A new class of problems for the security of cryptographic schemes. In: Proc. of the 4th Int'l Conf. on Practice and Theory in Public Key Cryptography (PKC 2001). Taormina: Springer-Verlag, 2011. 104−118. [doi: 10.1007/3-540-44586-2_8]

[13] Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Israel Institute of Technology, Technion, Haifa, Israel, 1996.

附中文参考文献:

[7] 任勇军,王建东,庄毅,谭沧海,方黎明.基于属性的认证密钥协商协议.兰州大学学报(自然科学版),2010,46(2):103−110.

[10] 魏江宏,胡学先,刘文芬.多属性机构环境下的属性基认证密钥协商协议.电子与信息学报,2012,34(2):451−456. [doi: 10.3724/SP.J.1146.2011.00701]

[11] 李强,冯登国,张立武,高志刚.标准模型下增强的基于属性的认证密钥协商协议.计算机学报,2013,36(10):2156−2167.

附录: 定理 1 的证明

证明:令 A 是 ABAKE 协议的攻击者,S 是该协议的模拟者,S 的目的是利用 A 解决 CDH 问题或 GCPBDHE 问题.证明该定理的思路是:针对本文设计的 ABAKE 协议,若 A 在多项式时间内能以一个不可忽略的优势区分出测试会话 sid^*的会话密钥和随机选取的会话密钥,则 S 就能在多项式时间内以不可忽略的优势解决 CDH 问题或 GCPBDHE 问题.

令 $\Pr[Suc]$表示 A 攻击成功的概率,即,对 sid^*的会话密钥给出正确判决的概率.

令:

- $AskH$ 表示事件: A 对 sid^*对应的$(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$进行 H 函数查询;
- $\overline{AskH}$ 表示事件: A 未对 sid^*的$(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$进行 H 函数查询.

由于 $\Pr[Suc\wedge\overline{AskH}]=1/2$,因此得到公式(3)成立:

$$\Pr[Suc]=\Pr[Suc\wedge AskH]+\Pr[Suc\wedge\overline{AskH}]=\Pr[Suc\wedge AskH]+1/2 \tag{3}$$

令:

- $AskS$ 表示事件: A 在进行 $StaticReveal$ 查询或 $MasterReveal$ 查询之前,对 $SK_P=(K_P,L_P,\{K_{P,j},\forall j\in S_P\})$进行 H_1 查询;
- $\overline{AskS}$ 表示 $AskS$ 的补事件.

由公式(3)可得:

$$\begin{aligned}\Pr[Suc]&=\Pr[Suc\wedge AskH]+1/2\\&=\Pr[Suc\wedge AskH\wedge AskS]+\Pr[Suc\wedge AskH\wedge\overline{AskS}]+1/2.\end{aligned}$$

由于测试会话一定是一个新鲜会话,并且根据攻击者 A 的攻击行为,我们定义以下事件:

(1) 事件 E_1:测试会话 sid^*没有匹配会话 $\overline{sid^*}$,攻击者对满足访问结构 AS_A 的属性集合 S 进行了 $StaticReveal(S)$查询;

(2) 事件 E_2:测试会话 sid^*没有匹配会话 $\overline{sid^*}$,攻击者对测试会话 sid^*进行了 $EphemeralReveal(sid^*)$查询;

(3) 事件 E_3:测试会话 sid^*存在匹配会话 $\overline{sid^*}$,攻击者对满足访问结构 AS_A 的属性集合 S 进行了 $StaticReveal(S)$查询,并且对满足访问结构 AS_B的属性集合 S 进行了 $StaticReveal(S)$查询;或者进行了 $MasterReveal$ 查询;

(4) 事件 E_4:测试会话 sid^*存在匹配会话 $\overline{sid^*}$,攻击者进行了 $EphemeralReveal(sid^*)$和 $EphemeralReveal(\overline{sid^*})$ 查询;

(5) 事件 E_5:测试会话 sid^*存在匹配会话 $\overline{sid^*}$,攻击者对满足访问结构 AS_B 的属性集合 S 进行了 $StaticReveal(S)$查询;并且进行了 $EphemeralReveal(\overline{sid^*})$ 查询;

(6) 事件 E_6:测试会话 sid^*存在匹配会话 $\overline{sid^*}$,攻击者对满足访问结构 AS_A 的属性集合 S 进行了 $StaticReveal(S)$查询;并且进行了 $EphemeralReveal(sid^*)$查询.

根据 E_1~E_6 定义可知:

$$Suc \wedge AskH \wedge \overline{AskS} = \bigcup_{i=1}^{6}(Suc \wedge AskH \wedge \overline{AskS} \wedge E_i) \tag{4}$$

由公式(3)和公式(4)得到:

$$\begin{aligned}\Pr[Suc] &= \Pr[Suc \wedge AskH \wedge AskS] + \Pr[Suc \wedge AskH \wedge \overline{AskS}] + 1/2\\ &= \Pr[Suc \wedge AskH \wedge AskS] + \Pr\left[\bigcup_{i=1}^{6}(Suc \wedge AskH \wedge \overline{AskS} \wedge E_i)\right] + 1/2\\ &\leqslant \Pr[Suc \wedge AskH \wedge AskS] + \sum_{i=1}^{6}\Pr[(Suc \wedge AskH \wedge \overline{AskS} \wedge E_i)] + 1/2.\end{aligned}$$

令:

$$\begin{aligned}p_0 &= \Pr[Suc \wedge AskH \wedge AskS],\\ p_i &= \Pr[Suc \wedge AskH \wedge \overline{AskS} \wedge E_i], 1 \leqslant i \leqslant 6,\end{aligned}$$

则有:

$$\Pr[Suc] \leqslant \sum_{i=0}^{6} p_i + 1/2 \tag{5}$$

首先假设执行该密钥协商协议的系统用户个数是 N,每个用户至多进行 L 次密钥协商.下面分析 p_i,i=0, 1,…,6 与 S 解决 GCPBDHE 困难问题和 CDH 困难问题的成功率之间的关系.

(1) 事件 $Suc \wedge AskH \wedge AskS$

模拟者 S 随机选择两个用户 A 和 B,并且以 $1/(N^2L)$的概率猜测 A 的第 $i_A \in [1,L]$次会话是攻击者 A 选取的测试会话,将该测试会话记为 sid^*.在事件 $AskS$ 中,允许攻击者 A 在进行 *StaticReveal* 查询或 *MasterReveal* 查询之前执行 SK_A 的 H_1 查询,这说明攻击者在进行 *StaticReveal* 查询或 *MasterReveal* 查询之前已经得到了 A 的长期私钥 SK_A.

模拟者 S 在系统设置中随机选取$\alpha' \in Z_p$,令 $g_T^{\alpha} = e(g^a, g^{a^q})e(g,g)^{\alpha'}$,即$\alpha=\alpha'+a^{q+1}$,则模拟者 S 在接收到攻击者申请的 SK_A 的 H_1 查询请求时,模拟者 S 得到了 $SK_A=(K_A,L_A,\{K_{A,j},\forall j \in S_A\})$.

由于 $K_A / L_A^{a'} = g^{\alpha} = g^{\alpha'+a^{q+1}}$, 因此,$S$ 利用 $e((K_A / L_A^{a'}), g^s) / e(g^{\alpha'}, g^s)$ 可以计算出 $e(g,g)^{a^{q+1}s}$.

因此:

$$\Pr[S \text{ 解决 GCPBDHE 困难问题}] \geqslant p_0/(N^2L).$$

(2) 事件 $Suc \wedge AskH \wedge \overline{AskS} \wedge E_1$

在事件 $Suc \wedge AskH \wedge \overline{AskS} \wedge E_1$,模拟者 S 已知:

$$\begin{aligned}&g, g^s, g^a, ..., g^{(a^q)}, g^{(a^{q+2})}, ..., g^{(a^{2q})}, \forall j \in \{1,2,...,q\},\\ &g^{s \cdot b_j}, g^{a/b_j}, ..., g^{(a^q/b_j)}, g^{(a^{q+2}/b_j)}, ..., g^{(a^{2q}/b_j)}, \forall j,k \in \{1,2,...,q, k \neq j\},\\ &g^{(a \cdot s \cdot b_k / b_j)}, g^{(a^2 \cdot s \cdot b_k / b_j)}, ..., g^{(a^q \cdot s \cdot b_k / b_j)}),\end{aligned}$$

并且接收到攻击者 A 给出的挑战访问结构 (M_A^*, ρ_A^*) 和 (M_B^*, ρ_B^*),其中, M_A^* 是 $l_A^* \times n_A^*$ 规模的矩阵, M_B^* 是 $l_B^* \times n_B^*$ 规模的矩阵.S 对方案进行如下模拟:

- 系统建立

S 随机选取$\alpha' \in Z_p$,令 $g_T^{\alpha} = e(g^a, g^{a^q})e(g,g)^{\alpha'}$, 则$\alpha=\alpha'+a^{q+1}$.该系统用户最多有 U 个属性,对属性集合中的每个属性 x,随机选取 $z_x \in Z_p$.令集合 $\Lambda_x = \{i : \rho_A^*(i) = x, 1 \leqslant i \leqslant l_A^*\}$, 模拟者 S 定义 h_x:

$$h_x = g^{z_x} \prod_{i \in \Lambda_x} g^{aM_{A_i,1}^*/b_i} \cdot g^{a^2 M_{A_i,2}^*/b_i} \cdot \ldots \cdot g^{a^{n_A^*} M_{A_i,n_A^*}^*/b_i},$$

其中, $M_{A_{i,j}}^*$ 是 M_A^* 矩阵的第 i 行 j 列的元素.需要说明的是:若集合 Λ_x 是空集,则 $h_x = g^{z_x}$.

假设系统中有 N 个用户,每个用户最多进行 L 次密钥协商.模拟者 S 随机选择用户 A,B,并且以 $1/N^2L$ 猜测 A 的第 $i_A \in [1,L]$次密钥协商是攻击者攻击的测试会话,将该测试会话记为 sid^*.S按以下方式模拟 A 的第 i_A 次

会话发送的消息 EPK_A:

令 $X=g^s$, S 随机选择 $r_1,r_2,...,r_{l_A^*},x_2,x_3,...,x_{n_A^*}\in Z_p$,则分享的秘密向量为

$$v=(s,sa+x_2,sa^2+x_3,\ldots,sa^{n-1}+x_{n_A^*})\in(Z_p)^{n_A^*}.$$

对于任意的 $i\in\{1,...,n_A^*\}$,定义 $R_i=\{k:\rho_A^*(k)=\rho_A^*(i),k=1,2,...,l_A^*,且k\neq i\}$,计算:

$$U_i=h_{\rho_A^*(i)}^{r_i}\left(\prod_{j=2,...,n_A^*}(g^a)^{M_{A_{i,j}^*}^* x_j}\right)(g^{b_i s})^{-z_{\rho_A^*(i)}^*}\left(\prod_{k\in R_i}\prod_{j=1,...,n_A^*}(g^{a^j\cdot s\cdot(b_i/b_k)})^{M_{A_{k,j}^*}^*}\right),$$

$$D_i=g^{-r_i}g^{-sb_i},$$

其中,$M_{A_{i,j}^*}^*$ 是 M_A^* 矩阵的第 i 行 j 列的元素.

$EPK_A=(X,\{U,D\},M_A^*,\rho_A^*)$ 是用户 A 在会话 sid^* 中发出的消息.

- 模拟过程

为了回答攻击者对 H_1,H 的查询,S 建立两个列表 L_{H_1} 和 L_H;为了回答攻击者对 *SessionReveal* 的查询,$\mathcal{S}$建立列表$\mathcal{L}_K$.

① $H_1(K_P,L_P,\{K_{P,j},\forall j\in S_P\},x)$:如果存在 $(K_P,L_P,\{K_{P,j},\forall j\in S_P\},*)\in\mathcal{L}_{H_1}$, $\mathcal{S}$返回相应查询值;否则,$\mathcal{S}$随机选取 $x'\in Z_p$,将 x'返回给攻击者,并在 L_{H_1} 中记录$(K_P,L_P,\{K_{P,j},\forall j\in S_P\},x')$.

② $H(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}})$:

(a) 如果存在 $(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}},*)\in L_H$, $\mathcal{S}$返回相应查询值;

(b) 如果不存在 $(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}},*)\in L_H$, $\mathcal{S}$判断 P 是否是 A、$\bar{P}$ 是否是 B、该会话是否为 A 的第 i_A 次会话,若都成立,接着调用 DBDH 随机预言机,若:

$$DBDH(X,g^a,g^{a^q},\sigma_1/e(X,g^{\alpha'}))=1,$$
$$DBDH(Y,g^a,g^{a^q},\sigma_2/e(Y,g^{\alpha'}))=1,$$
$$e(X,Y)=e(g,\sigma_3)$$

都成立,则$\mathcal{S}$终止,并且输出$\sigma_1/e(X,g^{\alpha'})$(此时, $\sigma_1/e(X,g^{\alpha'})=e(g,g)^{a^{q+1}s}$, $s_A=s$);

(c) 如果不存在 $(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}},*)\in L_H$, 调用 DBDH 随机预言机,若:

$$DBDH(X,g^a,g^{a^q},\sigma_1/e(X,g^{\alpha'}))=1(即\sigma_1/e(X,g^{\alpha'})=e(g,g)^{a^{q+1}s_P}),$$
$$DBDH(Y,g^a,g^{a^q},\sigma_2/e(Y,g^{\alpha'}))=1(即\sigma_1/e(X,g^{\alpha'})=e(g,g)^{a^{q+1}s_{\bar{P}}}),$$
$$e(X,Y)=e(g,\sigma_3)$$

都成立,则生成一个随机数 $K\in\{0,1\}^k$ 返回给攻击者,并在 L_H 中记录:

$$(\sigma_1,\sigma_2,\sigma_3,EPK_P,EPK_{\bar{P}},K).$$

③ $Send(I,S_P,S_{\bar{P}})$: 若 $P=A$,并且该会话是 A 的第 i_A 次会话,$\mathcal{S}$将 EPK_A 返回给攻击者;否则,$\mathcal{S}$按照协议执行过程生成 EPK_P 返回给用户,并记录 $(S_P,S_{\bar{P}},EPK_P)$.

④ *SessionReveal*(*sid*):模拟者查询 L_K,若攻击者申请 sid^*的会话密钥,则 S 失败终止;若 *sid* 在 L_K 列表中,则 S 将列表中的会话密钥 K 返回给攻击者;若 *sid* 不在 L_K 列表中,查询 L_H,将 H 中 *sid* 对应的 K 返回给用户,并将(*sid*,K)记录在列表 L_K 中.

⑤ *EphemeralReveal*(*sid*):若攻击者申请 sid^*的临时私钥,则 S 失败终止;否则, S 返回给攻击者 $er_0,er_1,\ldots,er_l$, $ex_2,ex_3,\ldots,ex_n\in Z_p$,其中,$l,n$ 分别是访问结构对应的矩阵 M 的行和列数.

⑥ *StaticReveal*(S_P):在事件 E_1 中,用户属性集合 S_P 不满足访问结构 M_A^*,因此,模拟者可以找到向量:

$$w=(w_1,...,w_{n_A^*})\in(Z_p)^{n_A^*},$$

其中,$w_1=-1$;并且对于任意满足条件 $\rho_A^*(i)\in S_P$ 的行标识 i,满足条件 $w\cdot M_A^*(i)=0$. 模拟者选取一个随机数 $r\in Z_p$,

模拟者令 $t=r+w_1a^q+w_2a^{q-1}+...+w_{n_A^*}a^{q-n_A^*+1}$.

利用已知的 $g^a,...,g^{(a^q)}$, 计算出 $L_P=g^r\prod_{i=1,...,n_A^*}(g^{a^{q+1-i}})^{w_i}=g^t, K_P=g^{\alpha'}g^{ar}\prod_{i=2,...,n_A^*}(g^{a^{q+1-i}})^{w_i}=g^{\alpha'}g^{at}$.

$\forall x\in\mathcal{S}_P$,令集合 $\Lambda_x=\{i:\rho_A^*(i)=x,i=1,2,...,l_A^*\}$, 模拟者计算 $K_{P,x}$:

$$K_{P,x}=L_P^{z_x}\prod_{i\in\Lambda_x}\prod_{j=1,...,n_A^*}\left(g^{(a^j/b_i)r}\prod_{\substack{k=1,...,n_A^*\\k\neq j}}(g^{a^{q+1+j-k}/b_i})^{w_k}\right)^{M_{i,j}^*}.$$

若 Λ_x 是空集,则模拟者令 $K_{P,x}=L_P^{z_x}$.

⑦ *MasterReveal*:$\mathcal{S}$失败终止.

⑧ *Test*(*sid*):若测试会话不是 sid^*,S 失败终止;否则,S 随机生成$\xi\in\{0,1\}^k$,将ξ返回给攻击者.

在事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_1$ 中,若攻击者$\mathcal{A}$攻击成功,则攻击者必然查询了 $H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$.因此,根据步骤②中情况(b)的分析,攻击者利用$\sigma_1/e(X,g^{\alpha'})$可以计算出 $e(g,g)^{a^{q+1}s}$. 因此,

$$\Pr[S\text{ 解决 GCPBDHE 问题}]\geqslant p_1/(N^2L).$$

(3) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_2$

在事件 E_2 中,测试会话 sid^*不存在匹配会话 $\overline{sid^*}$,A 可以查询 *EphemeralReveal*(sid^*),但不能查询满足访问结构(M_B,ρ_B)的长期私钥和满足访问结构(M_A,ρ_A)的长期私钥,或者不能查询系统主私钥.由于 H_1 是随机预言机,并且 H_1 的输入包括属性集对应的长期私钥,故$\mathcal{A}$以一个可以忽略的概率得到正确的 $s_A,r_1,r_2,...,r_{l_A^*},x_2,x_3,...,x_{n_A^*}$. 因此与 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_1$ 事件中 S 的模拟过程相似,同样得到模拟者$\mathcal{S}$的成功率:

$$\Pr[S\text{ 解决 GCPBDHE 问题}]\geqslant p_2/(N^2L).$$

(4) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$

在事件 E_3 中,测试会话 sid^*存在匹配会话 $\overline{sid^*}$,A 可以查询 *MasterReveal*,或者可以同时查询满足访问结构(M_B,ρ_B)的长期私钥和满足访问结构(M_A,ρ_A)的长期私钥,但是不允许查询 *EphemeralReveal*(sid^*)和 *Ephemeral Reveal* ($\overline{sid^*}$) .模拟者 S 以 $1/(N^2L)$的概率猜测测试会话是 sid^*,即:会话双方是 A,B,并且是 A 的第 i_A 次会话.模拟者 S 的目的是解决 CDH 问题,即:模拟者已知(g^b,g^c),求解 g^{bc}. S 模拟的方案在系统建立和私钥生成阶段与真实方案相同, S 在生成 EPK_A 和 EPK_B 的过程中嵌入 g^b,g^c,具体方法如下:

A 随机选择 $er_1,...,er_{l_A},ex_2,ex_3,...,ex_{n_A}\in Z_p$, 计算:

$$r_i=H_1(K_A,L_A,\{K_{A,j},\forall j\in S_A\},er_i),1\leqslant i\leqslant l_A,$$
$$x_k=H_1(K_A,L_A,\{K_{A,j},\forall j\in S_A\},ex_k),2\leqslant k\leqslant n_A.$$

令秘密向量 $v=(b,x_2,x_3,...,x_{n_A})\in(Z_p)^{n_A}$, 则有:

$$\lambda_i=v\cdot M_A(i)=bM_{A_{i,1}}+x_2M_{A_{i,2}}+...+x_{n_A}M_{A_{i,n_A}},$$

其中,$M_A(i)$是 M_A 的第 i 行,i=1,…,l_A.令:

$$X=g^b,\left(U_i=(g^b)^{aM_{A_{i,1}}}\left(\prod_{j=2}^{n_A}(g^a)^{x_2M_{A_{i,j}}}\right)h_{\rho_A(i)}^{-r_i},D_i=g^{r_i}\right),1\leqslant i\leqslant l_A(\text{令集合}\{U,D\}=\{(U_i,D_i),1\leqslant i\leqslant l_A\}).$$

A 发送消息 EPK_A=(X,{U,D},M_A,ρ_A)给 B.

B 随机选取 $er_1',...,er_{l_B}',ex_2',ex_3',...,ex_{n_B}'\in Z_p$, 计算:

$$r_i'=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},er_i'),1\leqslant i\leqslant l_B,$$
$$x_k'=H_1(K_B,L_B,\{K_{B,j},\forall j\in S_B\},ex_k'),2\leqslant k\leqslant n_B.$$

令秘密向量 $v'=(c,x_2',x_3',...,x_{n_B}')$, 计算:

$$\lambda_i'=v'\cdot M_B(i),$$

其中,$M_B(i)$是矩阵 M_B 的第 i 行,i=1,…,l_B.B 计算:

$$Y=g^c,\left(V_i=(g^c)^{aM_{B_{i,1}}}\left(\prod_{j=2}^{n_B}(g^a)^{x_2M_{B_{i,j}}}\right)h_{\rho_B(i)}^{-r_i'},E_i=g^{r_i'}\right),1\leqslant i\leqslant l_B(\text{令集合}\{V,E\}=\{(V_i,E_i),1\leqslant i\leqslant l_B\}).$$

B 发送消息 $EPK_B=(Y,\{V,E\},M_B,\rho_B)$给 A.

在事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$ 中,攻击者必然输入正确的$\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B$ 查询 H 预言机,因此,攻击者可以求解出 $g^{bc}=\sigma_3$,得到:

$$\Pr[S\text{ 解决 CDH 问题}]\geqslant p_3/(N^2L).$$

(5) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_4$

在事件 E_4 中,测试会话 sid^*存在匹配会话 $\overline{sid^*}$,A 查询 $EphemeralReveal(sid^*)$和 $EphemeralReveal(\overline{sid^*})$, 但不允许查询满足访问结构$(M_B,\rho_B)$的长期私钥和满足访问结构$(M_A,\rho_A)$的长期私钥,也不允许查询系统主私钥.

由于 H_1 是随机预言机,因此,A 只能以可以忽略的概率得到正确的$\{s_A,r_i,x_j(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)\}$和$\{s_B,r_i',x_j'(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)\}$.与 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$ 事件中$\mathcal{S}$的模拟过程相似,得到模拟者$\mathcal{S}$的成功率:

$$\Pr[S\text{ 解决 CDH 问题}]\geqslant p_4/(N^2L).$$

(6) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_5$

在事件 E_5 中,测试会话 sid^*存在匹配会话 $\overline{sid^*}$,A 查询满足访问结构(M_B,ρ_B)的属性集对应的长期私钥和 $EphemeralReveal(\overline{sid^*})$, 不允许查询满足访问结构$(M_A,\rho_A)$的属性集对应的长期私钥和 $EphemeralReveal(sid^*)$,也不允许查询 $MasterReveal$.由于 H_1 是随机预言机,因此, A 只能以可以忽略的概率得到正确的$\{s_A,r_i,x_j(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)\}$和 $s_B,r_i',x_j'(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)$. 与 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$ 事件中$\mathcal{S}$的模拟过程相似,得到模拟者$\mathcal{S}$的成功率:

$$\Pr[S\text{ 解决 CDH 问题}]\geqslant p_5/(N^2L).$$

(7) 事件 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_6$

在事件 E_6 中,测试会话 sid^*存在匹配会话 $\overline{sid^*}$,A 查询 $EphemeralReveal(sid^*)$和满足访问结构(M_A,ρ_A)的属性集对应的长期私钥,不查询满足访问结构(M_B,ρ_B)的属性集对应的长期私钥和 $EphemeralReveal(\overline{sid^*})$, 不查询 $MasterReveal$.由于 H_1 是随机预言机,因此, A 只能以可以忽略的概率得到正确的$\{s_A,r_i,x_j(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)\}$和 $s_B,r_i',x_j'(1\leqslant i\leqslant l_A,2\leqslant j\leqslant n_A)$. 与 $Suc\wedge AskH\wedge\overline{AskS}\wedge E_3$ 事件中 S 的模拟过程相似,模拟者 S 的成功率:

$$\Pr[S\text{ 解决 CDH 问题}]\geqslant p_6/(N^2L).$$

针对上述 7 个事件的分析结果,得到以下两个结论.

结论 1. $\Pr[S\text{ 解决 GCPBDHE 困难问题}]\geqslant\max\{p_0,p_1,p_2\}/(N^2L)$.

结论 2. $\Pr[S\text{ 解决 CDH 困难问题}]\geqslant\max\{p_3,p_4,p_5,p_6\}/(N^2L)$.

假设攻击者 A 攻击成功,则下面不等式成立:

$$\Pr[Suc]\geqslant 1/2+\varepsilon \tag{6}$$

由公式(5)和公式(6)得到: $\sum_{i=0}^{6}p_i\geqslant\varepsilon$.

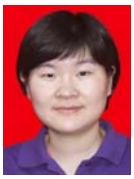
又由于 $7*\max\{p_i,i=0,1,...,6\}\geqslant\sum_{i=0}^{6}p_i$, 因此得到:$\max\{p_i,i=0,1,\ldots,6\}\geqslant\varepsilon/7$.

由于 $\Pr[S\text{ 解决 GCPBDHE 困难问题}]\geqslant\max\{p_0,p_1,p_2\}/(N^2L)$,若 $\max\{p_i,i=0,1,\ldots,6\}\in\{p_0,p_1,p_2\}$,则 $\Pr[S\text{ 解决 GCPBDHE 困难问题}]\geqslant\varepsilon/(7N^2L)$,这与 GCPBDHE 假设是矛盾的;

由于 $\Pr[S\text{ 解决 CDH 困难问题}]\geqslant\max\{p_3,p_4,p_5,p_6\}/(N^2L)$,若 $\max\{p_i,i=0,1,\ldots,6\}\in\{p_3,p_4,p_5,p_6\}$,则 $\Pr[S\text{ 解决 CDH 困难问题}]\geqslant\varepsilon/(7N^2L)$,这与 CDH 假设是矛盾的.

根据上述分析,若 GCPBDHE 假设和 CDH 假设同时成立,并且 H_1,H 是随机预言机,本文提出的 ABAKE 协议在 ABeCK 模型下具有选择安全性.

下面粗略分析模拟者 S 的计算复杂度.为了描述方便,记调用一次 H_1 预言机的计算复杂度为 T_{H_1},DBDH 预言机的计算复杂度为 T_{DBDH},消息 EPK 的计算复杂度为 T_{EPK},对运算的计算复杂度为 T_e,用户长期私钥的计算复杂度为 T_{SK},用户临时私钥以及系统主私钥的计算复杂度相对较小,忽略不计.由于每个事件中 S 的计算复杂度的具体表达式都非常复杂,因此,我们这里只给出了一个粗略的上界,即:事件(1)中, S 的计算复杂度小于 $N^2L(T_{H_1}+2T_{DBDH})+4T_e$;在事件(2)~事件(7)中, S 的计算复杂度都小于 $N^2L(T_{H_1}+2T_{DBDH}+T_{EPK})+N\cdot T_{SK}$,在假设 T_{H_1},T_{DBDH},T_{EPK},T_e 和 T_{SK} 都是多项式时间的条件下, S 的计算复杂度也是多项式时间的.



高海英(1978－),女,河南沈丘人,博士,副教授,主要研究领域为密码理论.