标准模型下可托管的基于身份认证密钥协商

陈 明
(宜春学院数学与计算机科学学院,江西宜春 336000)

摘 要: 现有会话密钥可托管的 ID-AKA(IDentity-based Authenticated Key Agreement)协议要么存在已知安全缺陷,要么是在随机预言模型下可证明安全.基于 Boneh 等人定义的安全陷门函数,提出一种会话密钥可托管的 ID-AKA 协议.在 ID-BJM 模型基础上,扩展定义了 ID-AKA 协议分析的标准安全模型.扩展模型将安全游戏划分为两个阶段,去除了随机预言机,能完备地模拟不同类型敌手的行为.在扩展模型下,新协议的安全性被规约为多项式时间敌手求解判定性 BDH(Bilinear Diffie-Hellman)难题和判定性 BDHI(Bilinear Diffie-Hellman Inversion)难题,具有可证明安全性.

关键词: 认证密钥协商; 基于身份密码体制; 双线性映射; 标准模型; 密钥托管
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2015)10-1954-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.10.012

Escrowable Identity-Based Authenticated Key Agreement in the Standard Model

CHEN Ming
(*School of Mathematics and Computer Science, Yichun University, Yichun, Jiangxi* 336000, *China*)

Abstract: In recent years, a few escrowable ID-AKA protocols have been proposed, but none of them are provably secure in the standard model while simultaneously having strong security. The main issue is how a simulator is able to deal with reveal-queries without the help of random oracles. In this paper, we presented a method incorporating a built-in security trapdoor function in an escrowable ID-AKA protocol. The security of our protocol relied on the hardness of the decisional Bilinear Diffie-Hellman Inversion problem. Meanwhile, we extended the security game of ID-AKA protocols to resist stronger adversarial powers, which allowed our security game to capture additional security properties such as perfect forward secrecy, ephemeral secrets reveal resistance and so on. Assuming that no adversary can obtain the master secret key and each party in the protocol has at least one uncompromised secret, our scheme is secure.

Key words: authenticated key agreement; identity-based cryptography; bilinear pairing; standard model; key escrow

1 引言

认证密钥协商(Authenticated Key Agreement, AKA)协议是一类重要的安全协议,广泛应用于开放网络环境下,网络实体之间确认彼此身份、协商共享的会话密钥,从而建立起安全信道,为通信提供机密性、认证性和完整性保障.

近年来,基于身份的认证密钥协商协议成为本领域研究的新热点.基于公钥基础设施(Public-Key Infrastructure, PKI)密码体制存在公钥证书管理的负担.基于身份密码体制(Identity-Based Cryptography, IBC)能规避 PKI 体制中的公钥证书管理问题.IBC 是一种将用户身份标识(ID)作为用户公钥的非对称密码体制.自 Boneh 等人[1]基于双线性对理论提出基于身份加密方案以来,IBC 体制得到广泛深入的研究[2~18],许多研究者相继提出 ID-AKA 协议[5~18].

ID-AKA 协议主要分为会话密钥托管和无会话密钥托管两类.会话密钥托管是指 KGC(Key Generation Center)可利用主密钥和特定会话的公开消息恢复出该会话的密钥.在移动自组织网络、无线传感网络,或者需要访问控制、审计和安全追踪等安全需求的场合,会话密钥可托管的 ID-AKA 协议具有重要的研究和应用价值.

Chen 等学者[6]定义了 ID-AKA 协议安全模型(记为 ID-BJM 模型).但是,该模型没有考虑会话临时秘密泄

收稿日期:2014-11-15;修回日期:2015-06-15;责任编辑:孙瑶
基金项目:江西省自然科学基金(No.2014ZBAB207022)

露攻击.随后,Huang 等人[9]将 eCK 模型[19]拓展到 ID-AKA 协议分析领域,提出 ID-eCK 模型.Ni 等人[12]建立了会话密钥托管模式下 ID-AKA 协议 eCK 模型(记为 eID-eCK 模型).上述模型将哈希函数模拟为随机预言机,但是,这样的随机预言机在现实世界中无法实现.而标准模型去除了随机预言机,具有更强的安全规约.王圣宝[13]和高志刚[14]等学者将 ID-BJM 模型扩展应用于标准模型下的 ID-AKA 协议分析(记为 ID-wsBJM 模型).与 ID-BJM 模型相同,ID-wsBJM 模型不能模拟会话临时秘密泄露攻击.并且,ID-BJM 模型采用一个独立的游戏模拟 ID-AKA 协议的完美(KGC)前向安全性(见文献[6]的定理 2),而王圣宝和高志刚等学者却忽略了该游戏.陈明[17]扩展了 ID-wsBJM 模型,能模拟 ID-AKA 协议的完美前向安全性,但仍然不能模拟会话临时秘密泄露攻击.可见,具有 ID-eCK 安全的标准模型需要进一步研究.

早期的 ID-AKA 方案采用较弱的安全模型,不满足完美前向安全性和(或)抗临时秘密泄露等安全属性.Huang 等人[9]提出一种在 ID-eCK 模型下可证明安全的 ID-AKA 方案(记为 Huang 协议).随后,Fujioka 等人[10]也提出一种 ID-eCK 安全的 ID-AKA 方案(记为 Fujioka 协议).Huang 协议和 Fujioka 协议不支持会话密钥托管.最近,Pandit 等人[11]提出一组 ID-AKA 协议,包括会话密钥可托管和无托管方案.Ni 等人[12]提出会话密钥可托管的 ID-AKA 协议(记为 Ni 协议),并在 eID-eCK 模型下可证明安全.上述协议在随机预言模型下可证明安全,而另外一些学者则关注标准模型下的 ID-AKA 协议.王圣宝等人[13]首先提出标准模型下会话密钥可托管的 ID-AKA 协议.但是,汪小芬[15]等学者指出该协议不满足完美前向安全,并提出一种改进方案.高志刚等人[14]采用更弱的安全假设,提出标准模型下的 ID-AKA 协议(记为 Gao 协议).但是,上述协议[13~15]采用弱安全模型,不能抵抗临时秘密泄漏攻击.高海英[16]提出可抵抗临时秘密泄漏攻击的 ID-AKA 协议(记为 Ghy 协议).然而,Ghy 协议不能抵抗密钥泄漏伪装攻击[17].任勇军等[18]提出标准模型下增强的 ID-AKA 协议,在 eCK 模型[19]下可证明安全,但任勇军协议不能工作于会话密钥托管模式.因此,标准模型下具有强安全性且会话密钥可托管的 ID-AKA 协议仍然需要进一步研究.

本文研究了会话密钥可托管的 ID-AKA 协议及其标准安全模型,主要贡献体现在以下两个方面.第一,建立具有 eID-eCK 安全的标准安全模型.首先,建立标准安全模型需要去除 eID-eCK 模型中的随机预言机.本文采用了 Boneh 和 Boyen[20]定义的安全陷门函数,并将 ID-AKA 协议的模拟过程分为两个阶段,以去除随机预言机.其次,形式化定义敌手的能力,完备模拟 eID-eCK 安全属性.相对传统模型中定义的单一“新鲜预言机(fresh oracle)”,本文扩展定义了三种类型的新鲜预言机,能更清晰地模拟不同类型敌手的行为.第二,提出一种会话密钥可托管的 ID-AKA 协议,充分考虑了用户长期私钥泄漏和会话临时秘密泄漏等安全需求,具有强安全性.

2　背景知识

2.1　双线性映射及困难问题与假设

这里简要描述与本文相关的基本理论,详细内容请参考文献[1,6,20].

双线性映射:给定大素数 p,阶为 p 的循环群 $\boldsymbol{G}$ 和 $\boldsymbol{G}_T$,g 是 $\boldsymbol{G}$ 的一个生成元,如果 $e:\boldsymbol{G}\times\boldsymbol{G}\rightarrow\boldsymbol{G}_T$ 是从 $\boldsymbol{G}$ 到 $\boldsymbol{G}_T$ 的一个有效的双线性映射,那么满足:

①双线性:给定 $u,v\in\boldsymbol{G}$ 和任意 $a,b\in\mathbb{Z}_p$,满足 $e(u^a,v^b)=e(u,v)^{ab}$.

②非退化性:$e(g,g)\neq 1$.

③可计算性:任意的 $u,v\in\boldsymbol{G}$,存在多项式时间算法能成功计算 $e(u,v)$.

BDH 问题:给定 $g,g^a,g^b,g^c\in\boldsymbol{G}$ 作为输入,输出 $e(g,g)^{abc}$.

Decisional BDH 问题(DBDH):给定一个 BDH 问题实例和一个随机的 $T\in\boldsymbol{G}_T$,如果存在算法 B 使得:$|\Pr[B(g,g^a,g^b,g^c,e(g,g)^{abc})=0]-\Pr[B(g,g^a,g^b,g^c,T)=0]|\geqslant\varepsilon$,称算法 B 以优势 ε 解决 DBDH 问题.

(t,ε)-DBDH 假设:若不存在 t 时间算法以不可忽略的优势 ε 解决 DBDH 问题,那么称 (t,ε)-DBDH 假设在群 $\boldsymbol{G}$ 和 $\boldsymbol{G}_T$ 上成立.

***q*-BDHI 问题:**给定一个随机的 $\alpha\in\mathbb{Z}_p$ 和一个含 $q+1$ 个元素的向量 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})\in\boldsymbol{G}^{q+1}$ 作为输入,输出 $e(g,g)^{1/\alpha}$.

Decisional *q*-BDHI 问题(*q*-DBDHI):给定一个 q-BDHI 问题实例和一个随机的 $T\in\boldsymbol{G}_T$,如果存在算法 B 使得:$|\Pr[B(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},e(g,g)^{1/\alpha})=0]-\Pr[B(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},T)=0]|\geqslant\varepsilon$,那么称算法 B 以优势 ε 解决 q-DBDHI 问题.

(t,ε,q)-DBDHI 假设:若不存在 t 时间算法以不可忽略的优势 ε 解决 q-DBDHI 问题,那么我们称 (t,ε,q)-DBDHI 假设在群 $\boldsymbol{G}$ 和 $\boldsymbol{G}_T$ 上成立.

2.2　目标抗碰撞散列函数

TCR(Target Collision Resistant Hash Function)函数:令 $\boldsymbol{M}$ 和 $\{0,1\}^k$ 为有限集,k 为密钥长度,那么 $\{\mathrm{TCR}:\boldsymbol{M}\rightarrow\{0,1\}^k\}$ 表示目标抗碰撞散列函数族.

$(t,\varepsilon_{\mathrm{TCR}})$-TCR 假设:给定一个消息 $M\in\boldsymbol{M}$ 和一个 TCR 函数 H,如果不存在 t 时间算法以不可忽略的优势

ε_{TCR}找到消息 $M' \in \boldsymbol{M}$ 使得：$M' \neq M \wedge H(M') = H(M)$ 成立，那么称 H 满足(t, ε_{TCR})-TCR 假设.

2.3 ID-AKA 协议安全模型

综合现有研究成果[5~17]，ID-AKA 协议应满足以下安全属性：已知会话密钥安全、无密钥控制、抗未知密钥共享、抗密钥泄露伪装(Key-Compromise Impersonation resilience, KCI)、完美前向安全(Perfect Forward Secrecy, PFS)、KGC 前向安全、抗临时秘密泄露安全(Ephemeral Secrets Reveal Resistance, ESR).

本文重点研究会话密钥可托管的 ID-AKA 协议，这类协议要求 KGC 可利用主密钥和特定会话的公开消息恢复出该会话的会话密钥，不考虑 KGC 前向安全.研究表明[6,11,13,14]，在密钥协商阶段嵌入未经任何加工的 Diffie-Hellman 密钥交换，会话密钥可托管的 ID-AKA 协议可转换为无会话密钥托管的 ID-AKA 协议.

本文将 ID-AKA 协议分为部分协议 π_0和完整协议 π_1.π_0输入系统参数、用户身份(ID_i, ID_j)及其私钥，输出会话秘密值 $K_{i,j} \in \boldsymbol{G}_T$.这里，$K_{i,j}$不是最终的会话密钥，而是产生会话密钥的秘密参数.完整协议 π_1包含 π_0，并根据 π_0输出的秘密参数 $K_{i,j}$，使用 TCR 函数导出最终的会话密钥.因此，与现有模型不同，本文安全模型分为两个阶段，第一阶段使用扩展的 ID-BJM 模型$(Game_0)$分析 π_0的安全性，第二阶段讨论协议 π_0转换到 π_1的安全性$(Game_1)$.除了引入 TCR 函数 H 用于计算会话密钥外，$Game_1$与 $Game_0$的游戏过程相同.下面定义 $Game_0$.

协议 π_0被模拟为挑战者 B 与敌手 A 之间的游戏 $Game_0$.预言机 $\Pi^s_{i,j}$定义为实体 i 与 j 的第 s 个会话实例.A 被允许执行以下询问，询问分为两个阶段，并且询问是无序和自适应的.面对 A 的询问，B 模拟 π_0的相应算法分别做出应答.询问包括：Send$(\Pi^s_{i,j}, M)$ 询问、Ephemeral-secret$(\Pi^s_{i,j})$询问、Corrupt(ID_i)询问和 Reveal$(\Pi^s_{i,j})$询问.上述询问参考 ID-BJM 模型和 eCK 模型，具体内容见本文 4.2 节.

定义 1(匹配预言机) 如果预言机 $\Pi^s_{i,j}$和 $\Pi^t_{j,i}$具有相同的会话 ID(会话 ID 由用户标识和会话临时参数连接而成)，称 $\Pi^s_{i,j}$和 $\Pi^t_{j,i}$互为匹配预言机.

定义 2(fresh-oracle-I) $\Pi^s_{i,j}$是类型 I 新鲜预言机，那么：$\Pi^s_{i,j}$已成功完成(处于 Accepted 状态)；A 从未提交 Corrupt(ID_j)询问；A 从未提交 Reveal$(\Pi^s_{i,j})$询问和 Reveal$(\Pi^t_{j,i})$询问；A 从未提交 Ephemeral-secret$(\Pi^s_{i,j})$询问.(其中，$\Pi^s_{i,j}$与 $\Pi^t_{j,i}$互为匹配预言机，以下同)

定义 3(fresh-oracle-II) $\Pi^s_{i,j}$是类型 II 新鲜预言机，那么：$\Pi^s_{i,j}$已完成；A 从未提交 Reveal$(\Pi^s_{i,j})$询问和 Reveal$(\Pi^t_{j,i})$询问；A 从未提交 Ephemeral-secret$(\Pi^s_{i,j})$询问和 Ephemeral-secret$(\Pi^t_{j,i})$询问.

定义 4(fresh-oracle-III) $\Pi^s_{i,j}$是类型 III 新鲜预言机，那么：$\Pi^s_{i,j}$已完成；A 从未提交 Reveal$(\Pi^s_{i,j})$询问和 Reveal$(\Pi^t_{j,i})$询问；A 从未提交 Corrupt(ID_i)询问和 Corrupt(ID_j)询问.

第一阶段询问结束后，A 选择新鲜预言机 $\Pi^u_{I,J}$请求 Test$(\Pi^u_{I,J})$询问.Test 询问以后，A 可以继续执行除 Test 外的询问，但要求 A 不能破坏挑战预言机 $\Pi^u_{I,J}$的新鲜性.最后，A 输出对 Test 询问中 b 的猜测 b'，如果 $b' = b$，那么 A 赢得游戏 $Game_0$.A 赢得 $Game_0$的优势定义为：$\mathrm{Adv}_A^{Game_0}(k) = |\Pr[b' = b] - 1/2|$.

定义 5 如果协议 π_0满足如下要求，被认为满足部分 ID-AKA 安全：①在 $\Pi^u_{I,J}$和 $\Pi^v_{J,I}$之间存在良性(benign)[6]攻击者 A 的情况下，总能协商相同的会话秘密 K，且 K 在 $\boldsymbol{G}_T$上随机均匀分布；②$\mathrm{Adv}_A^{Game_0}(k)$是可忽略的.($\Pi^u_{I,J}$与 $\Pi^v_{J,I}$互为匹配预言机).

定义 6 如果(t, ε_{TCR})-TCR 假设成立，且协议 π_0满足部分 ID-AKA 安全，则 π_1满足 ID-AKA 安全.

3 可托管的 ID-AKA 协议

基于文献[20]定义的安全陷门函数，提出一种会话密钥可托管的 ID-AKA 协议.给定素阶为 p 且满足双线性映射 $e: \boldsymbol{G} \times \boldsymbol{G} \to \boldsymbol{G}_T$的循环群$(\boldsymbol{G}, \boldsymbol{G}_T)$.

系统建立：输入安全参数 κ，输出系统参数 params $= (g, u, v, h, H)$.g 为 $\boldsymbol{G}$ 的生成元，KGC 随机选择 α，$\beta, \gamma \in \mathbb{Z}_p$，计算 $u = g^{\alpha}, v = g^{\beta}$ 和 $h = g^{\gamma}$.其中(α, β)为系统主密钥，γ 为会话密钥恢复秘密参数，(u, v, h)为 KGC 公钥.$H: \{0,1\}^* \to \{0,1\}^k$为密钥导出函数.KGC 公布系统参数 params $= (g, u, v, h, H)$.

密钥产生：提交用户身份 $ID_i \in \mathbb{Z}_p$，KGC 随机选取 $r_i \in \mathbb{Z}_p$，如果 $ID_i + \alpha r_i + \beta = 0 \pmod p$，则重新选取 r_i，计算用户私钥 $d_i = (r_i, h_i)$.其中 $h_i = h^{1/(ID_i + \beta + \alpha r_i)}$.通过安全信道发送 d_i给 ID_i.

密钥协商：

①用户 A 随机选择 $x \in \mathbb{Z}_p$，计算 $T_{A_1} = (vg^{ID_B})^{x + r_A}$，$T_{A_2} = u^{x + r_A}$，并发送 $T_{A_1} \| T_{A_2}$给 B.

②用户 B 随机选择 $y \in \mathbb{Z}_p$，计算 $T_{B_1} = (vg^{ID_A})^{y + r_B}$，$T_{B_2} = u^{y + r_B}$，并发送 $T_{B_1} \| T_{B_2}$给 A.

③收到 $T_{B_1} \| T_{B_2}$，A 计算 $K_{AB} = e(T_{B_2}^{r_A} \cdot T_{B_1}, h_A)^{x + r_A}$.

④收到 $T_{A_1} \| T_{A_2}$，B 计算 $K_{BA} = e(T_{A_2}^{r_B} \cdot T_{A_1}, h_B)^{y + r_B}$.

⑤A 和 B 分别计算会话密钥 $SK_{AB} = H(ID_A \| ID_B \| T_{A_1} \| T_{A_2} \| T_{B_1} \| T_{B_2} \| K_{AB})$和 $SK_{BA} = H(ID_A \| ID_B \| T_{A_1} \|$

$T_{A_2} \| T_{B_1} \| T_{B_2} \| K_{BA})$.

会话密钥托管:KGC 记录会话状态($\mathrm{ID}_A \| \mathrm{ID}_B \| T_{A_1} \| T_{A_2} \| T_{B_1} \| T_{B_2}$),当需要恢复该轮会话密钥,KGC 计算 $K = e(T_{A_2}^{1/\alpha}, T_{B_2}^{1/\alpha})^{\gamma}$ 和会话密钥 $\mathrm{SK} = H(\mathrm{ID}_A \| \mathrm{ID}_B \| T_{A_1} \| T_{A_2} \| T_{B_1} \| T_{B_2} \| K)$.

根据 2.3 节的定义,部分协议 π_0 输出 K_{AB} 和 K_{BA},由密钥协商步骤① ~ ④组成,完整协议 π_1 输出 SK_{AB} 和 SK_{BA},由密钥协商步骤① ~ ⑤组成.

4 分析与比较

4.1 协议正确性分析

协议的正确性通过下列等式证明:

$$\begin{aligned} K_{AB} &= e(T_{B_2}^{r_A} \cdot T_{B_1}, h_A)^{x+r_A} \\ &= e((u^{y+r_B})^{r_A}(vg^{\mathrm{ID}_A})^{y+r_B}, h^{1/(\mathrm{ID}_A+\beta+\alpha r_A)})^{x+r_A} \\ &= e(g^{\mathrm{ID}_A+\beta+\alpha r_A}, h^{1/(\mathrm{ID}_A+\beta+\alpha r_A)})^{(x+r_A)(y+r_B)} \\ &= e(g,h)^{(x+r_A)(y+r_B)} \end{aligned} \tag{1}$$

$$\begin{aligned} K_{BA} &= e(T_{A_2}^{r_B} \cdot T_{A_1}, h_B)^{y+r_B} \\ &= e((u^{r_B}vg^{\mathrm{ID}_B})^{x+r_A}, h^{1/(\mathrm{ID}_B+\beta+\alpha r_B)})^{y+r_B} \\ &= e(g^{\mathrm{ID}_B+\beta+\alpha r_B}, h^{1/(\mathrm{ID}_B+\beta+\alpha r_B)})^{(x+r_A)(y+r_B)} \\ &= e(g,h)^{(x+r_A)(y+r_B)} \end{aligned} \tag{2}$$

$$\begin{aligned} K &= e(T_{A_2}^{1/\alpha}, T_{B_2}^{1/\alpha})^{\gamma} \\ &= e((u^{x+r_A})^{1/\alpha}, (u^{y+r_B})^{1/\alpha})^{\gamma} \\ &= e(g^{x+r_A}, g^{y+r_B})^{\gamma} \\ &= e(g,g^{\gamma})^{(x+r_A)(y+r_B)} \\ &= e(g,h)^{(x+r_A)(y+r_B)} \end{aligned} \tag{3}$$

由式(1) ~ (3)可得 $K = K_{AB} = K_{BA}$,从而可以计算相同的会话密钥 $\mathrm{SK} = \mathrm{SK}_{AB} = \mathrm{SK}_{BA}$.

4.2 协议安全性分析

定理 1　假设在相互匹配的预言机 $\Pi_{i,j}^s$ 和 $\Pi_{j,i}^u$ 之间仅存在良性攻击者,那么 $\Pi_{i,j}^s$ 与 $\Pi_{j,i}^u$ 总能协商相同的会话秘密 K,且 K 在 $\boldsymbol{G}_T$ 上随机均匀分布.

证明　假设 A 是一个良性攻击者,能够如实地传递预言机发出的消息,那么相互匹配的预言机 $\Pi_{i,j}^s$ 和 $\Pi_{j,i}^u$ 都能正确接收彼此发送的会话消息.根据 4.1 节的结论,$\Pi_{i,j}^s$ 和 $\Pi_{j,i}^u$ 总能计算得到相同的会话秘密 K_{ij} 或 K_{ji}.且由于 x 和 y 分别是 ID_i 和 ID_j 随机选择的临时秘密参数,那么会话秘密值 K_{ij} 或 K_{ji} 可看成是随机生成,在 $\boldsymbol{G}_T$ 上均匀分布.证毕.

定理 2　假设 A 最多发起了 q_s 次会话,创建了 q_i 个用户和 q_o 个预言机,如果 (t,ε,q)-DBDHI 假设成立,那么协议 π_0 满足类型 I$(t',\varepsilon',q_s,q_i,q_o)$-ID-AKA 安全.这里,$\varepsilon' \geq \dfrac{\varepsilon}{q_i \cdot q_o}$,$t' = t + O(q\theta + q_i\varphi + q_o(\theta+\varphi+\tau+\xi))$,$\xi$、$\theta$、$\varphi$ 和 τ 分别表示对运算、$\boldsymbol{G}$ 上的乘法运算、$\boldsymbol{G}$ 上的指数运算和 $\boldsymbol{G}_T$ 上的指数运算时间.

证明　假设存在敌手$(t,\varepsilon,q_s,q_i,q_o)$-A 赢得 Game_0,则可以构造一个算法 B 利用 A 解决 q-DBDHI 问题.给定 q-DBDHI 挑战$(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},T)$,B 的任务是区分 T 等于 $e(g,g)^{1/\alpha}$ 或者是 $\boldsymbol{G}_T$ 的一个随机成员.

B 随机选择 $w_1,w_2,\cdots,w_{q-1} \in \mathbb{Z}_p$ 和 $\tau \in \mathbb{Z}_p$;令多项式 $f(z) = \tau \prod_{i=1}^{q-1}(z+w_i)$,展开可得 $f(z) = \sum_{i=0}^{q-1} c_i z^i$,其中,$c_0$ 为非零常数;B 计算 $h = \prod_{i=0}^{q-1}(g^{\alpha^i})^{c_i} = g^{f(\alpha)}$,这里要求 $w_j \neq -\alpha$,$j \in \{1,\cdots,q-1\}$;针对每个身份 ID_i($i \in \{1,\cdots,q-1\}$),B 构造$(w_i, g^{f_i(z)} = h^{1/(\alpha+w_i)})_{i=1}^{q-1}$,令 $f_i(z) = f(z)/(z+w_i) = \sum_{j=0}^{q-2} d_j z^j$,代入公式可得 $h^{1/(\alpha+w_i)} = g^{f_i(z)} = \prod_{j=0}^{q-2}(g^{(\alpha)^j})^{d_j}$;设置 $u = g^{\alpha}$.B 计算 $T_h = T^{v_0} \cdot T_0$,其中,$T_0 = \prod_{j=1}^{q-1} e(g, g^{c_j\alpha^{j-1}})$,显然有 $(T_0)^{\alpha} = \prod_{j=1}^{q-1} e(g, g^{c_j\alpha^j}) = e(g, g^{f(\alpha)-c_0})$.若 $T = e(g,g)^{1/\alpha}$,那么 $T_h = e(g, g^{f(\alpha)})^{1/\alpha} = e(g,h)^{1/\alpha}$.B 随机选择 $a,b \in \mathbb{Z}_p$,使得 $ab = \mathrm{ID}^* \in \mathbb{Z}_p$,设置 $v = u^{-a}g^{-ab} = g^{-a(\alpha+b)}$,发布公开参数 $\mathrm{params} = \{g,u,v,h\}$.由于 $\alpha,a,b \in \mathbb{Z}_p$ 独立于 A 的视角,且随机分布,所以公开参数独立于 A 的视角,在空间上随机均匀分布.

假设 q_s 是发起的最大会话数,A 创建了 q_i($q_i < q$)个用户和 q_o 个预言机.B 设定 $\mathrm{ID}_J = \mathrm{ID}^*$,$J \in [1,q_i]$,随机选择 $X \in [1,q_o]$,并按下列方式回答 A 的询问.

Corrupt(ID_i):B 维护初始为空的列表 $\boldsymbol{L}_{\mathrm{ID}}$,格式为$(\mathrm{ID}_i, r_i, h_i)$.收到该询问,如果 $\mathrm{ID}_i = \mathrm{ID}_J$,B 终止游戏(Event1);否则,如果元组$(\mathrm{ID}_i, r_i, h_i)$存在,B 输出$(r_i, h_i)$;否则,B 构造参数 $r_i = a + \dfrac{\mathrm{ID}_i - ab}{w_i}$,使得等式$(r_i - a)(\alpha + w_i) = \mathrm{ID}_i + \beta + r_i\alpha$ 成立,然后计算 $h_i = (g^{f_i(\alpha)})^{1/(r_i-a)} = h^{1/(r_i-a)(\alpha+w_i)} = h^{1/(\mathrm{ID}_i+\beta+r_i\alpha)}$,设置 ID_i 的私钥为(r_i, h_i),更新 $\boldsymbol{L}_{\mathrm{ID}}$,输出$(r_i, h_i)$.由于 $\alpha,\beta,w_i \in \mathbb{Z}_p$ 随机均匀分布,且独立于 A 的视角,因此这一私钥有效且在密钥空间上随机均匀分布.

Send$(\Pi_{i,j}^s, M)$:B 维护初始为空的列表 $\boldsymbol{L}_{\mathrm{S}}$,列表格式为$(\Pi_{i,j}^s, \mathrm{trans}_{i,j}^s, K_{i,j}^s, f_{i,j}^s)$.这里,$\mathrm{trans}_{i,j}^s = (\mathrm{ID}_i^s, \mathrm{ID}_j^s, t_i^s, M_i^s, M_j^s)$记录预言机的会话状态;$K_{i,j}^s$ 为会话秘密;$f_{i,j}^s \in (0,1)$是预言机是否完成的标志,初值为 0($f_{i,j}^s = 1$ 表示 $\Pi_{i,j}^s$ 处于 Accepted 状态).

①如果 $\Pi_{i,j}^s$ 已存在,且 $\Pi_{i,j}^s$ 为发起者预言机,B 设置 $M_j^s = M$,$f_{i,j}^s = 1$.

②如果 $M = \lambda$,创建 $\Pi_{i,j}^s$ 为发起者预言机;否则 M

$\neq\lambda$,创建 $\Pi^s_{i,j}$为响应者预言机.

③如果 $s=X$,此时 $\Pi^s_{i,j}$为类型 I 新鲜预言机,如果 $j\neq J$,B 终止游戏(Event 2);否则,B 随机选择 $\rho\in\mathbb{Z}_p$,按如下方式计算响应消息:

$$T_{i_1}=g^{-a\rho}({}^{v}g^{\mathrm{ID}_J})^{r_i}=(vg^{\mathrm{ID}_J})^{r_i+(\rho/\alpha)}$$

$$T_{i_2}=g^{\rho}\cdot u^{r_i}=u^{r_i+(\rho/\alpha)}$$

这里,如果 $\Pi^s_{i,j}$为发起者预言机,令 $x=\rho/\alpha$,则 $T_{i_1}=(vg^{\mathrm{ID}_J})^{r_i+x}$,$T_{i_2}=u^{r_i+x}$,B 设置 $t^s_i=\perp$,$M^s_i=T_{i_1}\parallel T_{i_2}$,否则,令 $y=\rho/\alpha$,则 $T_{i_1}=(vg^{\mathrm{ID}_J})^{r_i+y}$,$T_{i_2}=u^{r_i+y}$,B 设置 $t^s_i=\perp$,$M^s_i=T_{i_1}\parallel T_{i_2}$,$M^s_j=M$,$f^s_{i,j}=1$.

④否则,如果 $s\neq X$,且 $i=J$,B 随机选择 $x\in\mathbb{Z}_p$,计算 $T_{i_1}=(vg^{\mathrm{ID}_j})^{x+a}$,$T_{i_2}=u^{x+a}$,若 $\Pi^s_{i,j}$为发起者预言机,B 设置 $t^s_i=x$,$M^s_i=T_{i_1}\parallel T_{i_2}$,否则设置 $t^s_i=x$,$M^s_i=T_{i_1}\parallel T_{i_2}$,$M^s_j=M$,$f^s_{i,j}=1$($\Pi^s_{i,j}$为响应者预言机).

⑤否则,$s\neq X$ 且 $i\neq J$,B 询问 Corrupt(ID_i)取得 ID_i 的私钥,随机选择 $x\in\mathbb{Z}_p$,按照协议计算(T_{i_1},T_{i_2}),若 $\Pi^s_{i,j}$为发起者预言机,设置 $M^s_i=T_{i_1}\parallel T_{i_2}$,$t^s_i=x$,否则设置 $t^s_i=x$,$M^s_i=T_{i_1}\parallel T_{i_2}$,$M^s_j=M$,$f^s_{i,j}=1$.

⑥最后将会话状态写入$\mathrm{trans}^s_{i,j}$,输出 M^s_i.

Ephemeral-secret($\Pi^s_{i,j}$):收到该询问,如果 $s=X$,B 终止游戏(Event3);否则 B 输出 $\Pi^s_{i,j}$的临时秘密.

Reveal($\Pi^s_{i,j}$):如果 $\Pi^s_{i,j}$是 fresh-oracle-I 或者与 fresh-oracle-I 相匹配,B 终止游戏(Event4);否则,如果 $f^s_{i,j}=0$,B 返回$\perp$;否则 B 查询列表 $\boldsymbol{L}_S$,如果 $K^s_{i,j}\neq\perp$则返回 $K^s_{i,j}$;否则在列表 $\boldsymbol{L}_S$中查找 $\Pi^b_{j,i}$满足 $\Pi^b_{j,i}$与 $\Pi^s_{i,j}$匹配,B 读取 $\Pi^b_{j,i}$的临时秘密 t^b_j.

①如果 $i\neq J$,B 取得 ID_i的私钥(r_i,h_i),令 $M^s_j=T_{j_1}\parallel T_{j_2}$,计算 $K^s_{i,j}=e(T^{r_i}_{j_2}\cdot T_{j_1},h_i)^{t^s_i+r_i}$.

②如果 $j\neq J$,B 取得 ID_j的私钥(r_j,h_j),令 $M^s_i=T_{i_1}\parallel T_{i_2}$,计算 $K^s_{i,j}=e(T^{r_j}_{i_2}\cdot T_{i_1},h_j)^{t^b_j+r_j}$.

③B 输出 $K^s_{i,j}$,用 $K^s_{i,j}$更新 $\boldsymbol{L}_S$的相应表项.

Test($\Pi^s_{i,j}$):第一阶段询问结束以后,A 请求 fresh-oracle-I 的 Test 询问.如果 $s\neq X$,或者存在已攻破的预言机 $\Pi^w_{j,i}$与 $\Pi^s_{i,j}$相匹配,那么 B 终止游戏(Event 5);否则,B 在 $\boldsymbol{L}_S$中查询 $\Pi^s_{i,j}$的匹配预言机$\Pi^w_{j,i}$,B 读取临时秘密 t^w_j,令 $M^s_i=T_{i_1}\parallel T_{i_2}$,计算并输出 $K^s_{i,j}=((T_h)^{\rho}e(g,h)^{r_i})^{t^w_j+a}$.

Test 询问结束以后,A 可以继续执行 Test 以外的询问,但不能破坏 fresh-oracle-I 的新鲜性.最后,A 返回其猜测位 $b'\in\{0,1\}$.B 直接输出 b'作为对 q-DBDHI 挑战的应答.

如果 B 未终止游戏,则事件 1/2/3/4/5 未发生,敌手 A 选择了 fresh-oracle-I 进行挑战应答(Event 6).那么 Event 6 发生的概率为:

$$\begin{aligned}&\Pr[\text{Event 6}]\\&=\Pr[\overline{\text{Event1}\vee\text{Event2}\vee\text{Event3}\vee\text{Event4}\vee\text{Event5}}]\\&\geqslant\frac{1}{q_i\cdot q_o}\end{aligned}$$

A 赢得游戏的概率为:

$$\Pr[\text{A wins}\mid\text{Event 6}]\geqslant\frac{\varepsilon}{q_i\cdot q_o}$$

如果 $T=e(g,g)^{1/\alpha}$,那么 $K^s_{i,j}=((T_h)^{\rho}e(g,h)^{r_i})^{t^w_j+a}=(e(g,h)^{\rho/\alpha}e(g,h)^{r_i})^{t^w_j+a}=(e(g,h)^{r_i+(\rho/\alpha)})^{t^w_j+a}$,此时有:

$$\begin{aligned}&|\Pr[\mathrm{B}(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},e(g,g)^{1/\alpha})=0]|\\&=1/2+\Pr[\text{A wins}\mid\text{Event6}]\geqslant 1/2+\frac{\varepsilon}{q_i\cdot q_o}\end{aligned}$$

如果 $T\neq e(g,g)^{1/\alpha}$,那么 $T_h\in\boldsymbol{G}_T$在 $\boldsymbol{G}_T$上随机均匀分布,有:$|\Pr[\mathrm{B}(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},T)=0]|=1/2$.

那么 B 利用 A 成功解决 q-DBDHI 问题的优势:

$$\begin{aligned}&|\Pr[\mathrm{B}(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},e(g,g)^{1/\alpha})=0]\\&-\Pr[\mathrm{B}(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},T)=0]|\\&\geqslant\frac{\varepsilon}{q_i\cdot q_o}\end{aligned}$$

从算法的时间复杂度来看,在系统参数构造阶段执行了 $O(q)$次 $\boldsymbol{G}$ 上的乘法运算、在询问阶段执行了 $O(q_o)$次 $\boldsymbol{G}$ 上的乘法运算、$O(q_i+q_o)$次 $\boldsymbol{G}$ 上的指数运算、$O(q_o)$次 $\boldsymbol{G}_T$上的指数运算以及 $O(q_o)$次双线性对运算.算法的时间复杂度为:$t'=t+O(q\theta+q_i\varphi+q_o(\theta+\varphi+\tau+\xi))$.证毕.

定理 3 假设 A 最多发起了 q_s次协议会话,创建了 q_i个用户和 q_o个预言机,如果(t,ε)-DBDH 假设成立,那么协议 π_0满足类型 II$(t',\varepsilon',q_s,q_i,q_o)$-ID-AKA 安全.这里,$\varepsilon'\geqslant\frac{\varepsilon}{q_o}(1-\frac{2}{q_o})^2$,$t'=t+O(q_i\varphi+q_o(\theta+\varphi+\tau+\xi))$.($\theta$,$\varphi$,$\tau$ 和ξ 定义同定理 2)

定理 4 假设 A 最多发起了 q_s次协议会话,创建了 q_i个用户和 q_o个预言机,如果(t,ε)-DBDH 假设成立,那么协议 π_0满足类型 III$(t',\varepsilon',q_s,q_i,q_o)$-ID-AKA 安全.这里,$\varepsilon'=(1-\frac{2}{q_i})(1-\frac{2}{q_o})\frac{\varepsilon}{q_o}$,$t'=t+O(q_i\varphi+q_o(\theta+\varphi+\tau+\xi))$.

证明 假设存在敌手$(t,\varepsilon,q_s,q_i,q_o)$-A 赢得 Game_0,那么可以构造一个算法 B 利用 A 解决 DBDH 问题.给定 DBDH 挑战(g,g^a,g^b,g^c,T),B 的任务是区分 $T=e(g,g)^{abc}$或者是 $\boldsymbol{G}_T$中的一个随机成员.

B 随机选取生成元 $g\in \boldsymbol{G}$ 及 $\alpha,\beta\in\mathbb{Z}_p$,计算 $u=g^{\alpha}$ 和 $v=g^{\beta}$,设定 $h=g^{a}$,将 params=(g,u,v,h)发送给 A.

B 随机选择 $X\in[1,q_o]$,$I\in[1,q_i]$,$J\in[1,q_i]$,$I\neq J$,并维护初始为空的列表 $\boldsymbol{L}_{\mathrm{ID}}$和 $\boldsymbol{L}_{\mathrm{S}}$,按下列方式回答 A 的询问.其中 $q_s,q_i,q_o,\boldsymbol{L}_{\mathrm{ID}},\boldsymbol{L}_{\mathrm{S}}$的定义同定理 2.

Corrupt(ID_i):收到该询问

①对于 fresh-oracle-II,如果 $\boldsymbol{L}_{\mathrm{ID}}$中存在元组$(\mathrm{ID}_i,r_i,h_i)$,B 输出$(r_i,h_i)$;否则,B 随机选择 $r_i\in\mathbb{Z}_p$,按密钥产生算法计算 ID_i的私钥$(r_i,h_i=h^{1/(\mathrm{ID}_i+\beta+r_i\alpha)})$,更新 $\boldsymbol{L}_{\mathrm{ID}}$,并输出$(r_i,h_i)$.

②对于 fresh-oracle-III,如果 $\mathrm{ID}_i=\mathrm{ID}_I$或 $\mathrm{ID}_i=\mathrm{ID}_J$,B 终止游戏(Event1);否则,与①相同.

Send($\Pi_{i,j}^{s}$,M):收到该询问

①如果 $\Pi_{i,j}^{s}$已存在,且为发起者预言机,B 设置 $M_j^s=M$,$f_{i,j}^{s}=1$.

②否则如果 $M=\lambda$,创建 $\Pi_{i,j}^{s}$为发起者预言机;否则,$M\neq\lambda$,创建 $\Pi_{i,j}^{s}$为响应者预言机.

③对于 fresh-oracle-II,B 询问 Corrupt(ID_i),取得 ID_i的密钥(r_i,h_i).

(a)如果 $s=X$,B 随机选择 $l_i\in\mathbb{Z}_p$,令 $t_b=(g^b)^{l_i}$,计算:$T_{i_1}=(t_b)^{(\beta+\mathrm{ID}_j)/\alpha}\cdot(vg^{\mathrm{ID}_j})^{r_i}=(vg^{\mathrm{ID}_j})^{r_i+l_ib/\alpha}$,$T_{i_2}=t_b\cdot u^{r_i}=u^{r_i+l_ib/\alpha}$;否则,$\Pi_{i,j}^{s}$与 $\Pi_{j,i}^{X}$相匹配,令 $t_c=(g^c)^{l_i}$,计算:$T_{i_1}=(t_c)^{(\beta+\mathrm{ID}_j)/\alpha}\cdot(vg^{\mathrm{ID}_j})^{r_i}=(vg^{\mathrm{ID}_j})^{r_i+l_ic/\alpha}$,$T_{i_2}=t_c\cdot u^{r_i}=u^{r_i+l_ic/\alpha}$;如果 $\Pi_{i,j}^{s}$为发起者预言机,B 设置 $t_i^s=l_i$,$M_i^s=T_{i_1}\parallel T_{i_2}$,否则 B 设置 $t_i^s=l_i$,$M_i^s=T_{i_1}\parallel T_{i_2}$,$f_{i,j}^{s}=1$,$M_j^s=M$.

(b)否则,$s\neq X$ 且 $\Pi_{i,j}^{s}$不是与 $\Pi_{u,v}^{X}$相匹配的预言机,B 随机选择 $x\in\mathbb{Z}_p$,按照协议计算(T_{i_1},T_{i_2}),若 $\Pi_{i,j}^{s}$为发起者预言机,设置 $t_i^s=x$,$M_i^s=T_{i_1}\parallel T_{i_2}$,否则设置 $t_i^s=x$,$M_i^s=T_{i_1}\parallel T_{i_2}$,$M_j^s=M$,$f_{i,j}^{s}=1$.

④对于 fresh-oracle-III,B 随机选择 $x,\rho_I,\rho_J\in\mathbb{Z}_p$,并记录$(\rho_I,\rho_J)$作为 ID_I、ID_J的秘密参数.

(a)如果 $i=I$,计算:$T_{i_1}=(g^b)^{\rho_I(\beta+\mathrm{ID}_j)}(vg^{\mathrm{ID}_j})^{x}=(vg^{\mathrm{ID}_j})^{x+\rho_Ib}$,$T_{i_2}=(g^b)^{\rho_I}\cdot u^{x}=u^{x+\rho_Ib}$;如果 $i=J$,计算:$T_{i_1}=(g^c)^{\rho_J(\beta+\mathrm{ID}_j)}(vg^{\mathrm{ID}_j})^{x}=(vg^{\mathrm{ID}_j})^{x+\rho_Jc}$,$T_{i_2}=(g^c)^{\rho_J}\cdot u^{x}=u^{x+\rho_Jc}$.

(b)如果 $i\neq I\wedge i\neq J$,B 询问 Corrupt(ID_i),取得ID_i^s的密钥(r_i,h_i),计算 $T_{i_1}=(vg^{\mathrm{ID}_j})^{x+r_i}$,$T_{i_2}=u^{x+r_i}$.

(c)如果 $\Pi_{i,j}^{s}$为发起者预言机,设置 $t_i^s=x$,$M_i^s=T_{i_1}\parallel T_{i_2}$,否则设置 $t_i^s=x$,$M_i^s=T_{i_1}\parallel T_{i_2}$,$M_j^s=M$,$f_{i,j}^{s}=1$.

⑤最后输出 M_i^s.

Ephemeral-secret($\Pi_{i,j}^{s}$):收到该询问,如果 $\Pi_{i,j}^{s}$是 fresh-oracle-II,或者是与 fresh-oracle-II 相匹配的预言机,B 终止游戏(Event2);如果 $\Pi_{i,j}^{s}$在 $\boldsymbol{L}_{\mathrm{S}}$中不存在则输出$\perp$,否则输出 $\Pi_{i,j}^{s}$的临时秘密 t_i^s.

Reveal($\Pi_{i,j}^{s}$):收到该询问

①如果 $\Pi_{i,j}^{s}$是 fresh-oracle-II 或与 fresh-oracle-II 相匹配,B 终止游戏(Event3);如果 $f_{i,j}^{s}=0$,B 输出$\perp$;否则,B 查询列表 $\boldsymbol{L}_{\mathrm{S}}$,如果 $K_{i,j}^{s}\neq\perp$则返回 $K_{i,j}^{s}$;否则,B 询问 Corrupt(ID_i)计算 $K_{i,j}^{s}=e(T_{j_2}^{r_i}\cdot T_{j_1},h_i)^{t_i^s+r_i}$.

②若 $\Pi_{i,j}^{s}$是 fresh-oracle-III 或与 fresh-oracle-III 相匹配,B 终止游戏(Event4);如果 $f_{i,j}^{s}=0$,B 输出$\perp$;否则,B 查询列表 $\boldsymbol{L}_{\mathrm{S}}$,如果 $K_{i,j}^{s}\neq\perp$则返回 $K_{i,j}^{s}$,否则存在 $\Pi_{j,i}^{b}$与 $\Pi_{i,j}^{s}$相匹配,读取临时秘密 t_j^b.

(a)如果 $i=I\wedge j=J$,B 计算

$$K_{i,j}^{s}=T^{\rho_I\rho_J}e((g^b)^{\rho_I},h)^{t_j^b}e((g^c)^{\rho_J},h)^{t_i^s}e(g,h)^{t_i^st_j^b}.$$

(b)如果 $i=J\wedge j=I$,B 计算

$$K_{i,j}^{s}=T^{\rho_I\rho_J}e((g^c)^{\rho_J},h)^{t_j^b}e((g^b)^{\rho_I},h)^{t_i^s}e(g,h)^{t_i^st_j^b}.$$

(c)如果 $i\neq I\wedge i\neq J$,B 询问 Corrupt(ID_i^s),取得ID_i^s的密钥(r_i,h_i),计算 $K_{i,j}^{s}=e(T_{j_2}^{r_i}\cdot T_{j_1},h_i)^{r_i+t_i^s}$.

(d)如果 $j\neq J\wedge j\neq I$,B 询问 Corrupt(ID_j^s),取得ID_j^s的密钥(r_j,h_j),计算 $K_{i,j}^{s}=e(T_{i_2}^{r_j}\cdot T_{i_1},h_j)^{r_j+t_j^b}$.

③用 $K_{i,j}^{s}$更新 $\boldsymbol{L}_{\mathrm{S}}$的相应表项,最后输出 $K_{i,j}^{s}$.

Test($\Pi_{i,j}^{s}$):第一阶段询问结束以后

①A 请求 fresh-oracle-II Test 询问.如果 $s\neq X$,或存在已攻破的预言机 $\Pi_{j,i}^{w}$与 $\Pi_{i,j}^{s}$相匹配,则终止游戏(Event5);否则 B 查询列表 $\boldsymbol{L}_{\mathrm{ID}}$和 $\boldsymbol{L}_{\mathrm{S}}$,计算并输出 $K_{i,j}^{X}=T^{t_i^st_j^{w}/\alpha^2}e((g^b)^{t_i^s/\alpha},h)^{r_j}e((g^c)^{t_j^w/\alpha},h)^{r_i}e(g,h)^{r_ir_j}$.

②A 请求 fresh-oracle-III Test 询问.若 $s\neq X\vee i\neq I\vee j\neq J$,或存在已攻破的预言机 $\Pi_{j,i}^{w}$与 $\Pi_{i,j}^{s}$相匹配,终止游戏(Event6);否则 B 查询列表 $\boldsymbol{L}_{\mathrm{S}}$,计算并输出 $K_{I,J}^{X}=T^{\rho_I\rho_J}e((g^b)^{\rho_I},h)^{t_j^w}e((g^c)^{\rho_J},h)^{t_i^X}e(g,h)^{t_i^Xt_j^w}$.

Test 询问结束以后,A 可以继续执行 Test 以外的询问,但不能破坏 fresh-oracle-II 和 fresh-oracle-III 的新鲜性.最后,A 返回其猜测位 $b'\in\{0,1\}$.B 输出 b'作为对 DBDH 挑战的应答.

如果 B 未终止游戏,下面从两个方面分析 B 利用 A 求解 DBDH 问题的概率:

①敌手 A 选择了 fresh-oracle-II 进行挑战应答(Event7),那么 Event7 发生的概率为

$$\Pr[\mathrm{Event7}]=\Pr[\overline{\mathrm{Event2}\vee\mathrm{Event3}\vee\mathrm{Event5}}].$$

从模拟过程可以看出事件 2/3/5 相互独立,则

$$\Pr[\mathrm{Event7}]=\Pr[\overline{\mathrm{Event2}}]\wedge\Pr[\overline{\mathrm{Event3}}]\wedge\Pr[\overline{\mathrm{Event5}}]$$

$$\geq\frac{1}{q_o}(1-\frac{2}{q_o})^2$$

A 赢得游戏的概率为:

$$\Pr[\text{A wins}|\text{Event7}]\geqslant\frac{\varepsilon}{q_o}(1-\frac{2}{q_o})^2.$$

如果 $T=e(g,g)^{abc}$,此时有

$$K_{i,j}^{s}=T^{t_i^s t_j^w/\alpha^2}e((g^b)^{t_i^s/\alpha},h)^{r_i}e((g^c)^{t_j^w/\alpha},h)^{r_i}e(g,h)^{r_i r_j}$$
$$=e(g,h)^{(r_i+l_i b/\alpha)(r_j+l_j c/\alpha)}$$

则

$$|\Pr[\mathrm{B}(g,g^a,g^b,g^c,e(g,g)^{abc})=0]|$$
$$=1/2+\Pr[\text{A wins}|\text{Event7}]$$
$$\geqslant 1/2+\frac{\varepsilon}{q_o}(1-\frac{2}{q_o})^2.$$

如果 $T\neq e(g,g)^{abc}$,在 $\boldsymbol{G}_T$上随机分布,则

$$|\Pr[\mathrm{B}(g,g^a,g^b,g^c,T)=0]|=1/2.$$

那么 B 利用 A 成功解决 DBDH 问题的优势为

$$|\Pr[\mathrm{B}(g,g^a,g^b,g^c,e(g,g)^{abc})=0]$$
$$-\Pr[\mathrm{B}(g,g^a,g^b,g^c,T)=0]|$$
$$\geqslant\varepsilon(1-\frac{2}{q_o})^2.$$

②A 选择了 fresh-oracle-III 进行挑战应答(Event8),那么 Event8 发生的概率为

$$\Pr[\text{Event8}]=\Pr[\overline{\text{Event1}\vee\text{Event4}\vee\text{Event6}}].$$

从模拟过程可以看出事件 1/4/6 相互独立,则

$$\Pr[\text{Event8}]=\Pr[\overline{\text{Event1}}]\wedge\Pr[\overline{\text{Event4}}]\wedge\Pr[\overline{\text{Event6}}]$$
$$\geqslant(1-\frac{2}{q_i})(1-\frac{2}{q_o})\frac{1}{q_o}.$$

A 赢得游戏的概率为

$$\Pr[\text{A wins}|\text{Event8}]\geqslant(1-\frac{2}{q_i})(1-\frac{2}{q_o})\frac{\varepsilon}{q_o}.$$

如果 $T=e(g,g)^{abc}$,有

$$K_{I,J}^{X}=T^{\rho_I\rho_J}e((g^b)^{\rho_I},h)^{t_j^w}e((g^c)^{\rho_J},h)^{t_i^X}e(g,h)^{t_i^X t_j^w}$$
$$=e(g,h)^{(t_i^X+\rho_I b)(t_j^w+\rho_J c)}$$

则

$$|\Pr[\mathrm{B}(g,g^a,g^b,g^c,e(g,g)^{abc})=0]|$$
$$=1/2+\Pr[\text{A wins}|\text{Event8}]$$
$$\geqslant 1/2+(1-\frac{2}{q_i})(1-\frac{2}{q_o})\frac{\varepsilon}{q_o}.$$

如果 $T\neq e(g,g)^{abc}$在 $\boldsymbol{G}_T$上随机均匀分布,则

$$|\Pr[\mathrm{B}(g,g^a,g^b,g^c,T)=0]|=1/2.$$

那么 B 利用 A 成功解决 DBDH 问题的优势为

$$|\Pr[\mathrm{B}(g,g^a,g^b,g^c,e(g,g)^{abc})=0]$$
$$-\Pr[\mathrm{B}(g,g^a,g^b,g^c,T)=0]|$$
$$\geqslant(1-\frac{2}{q_i})(1-\frac{2}{q_o})\frac{\varepsilon}{q_o}.$$

在询问阶段执行了 $O(q_o)$次 $\boldsymbol{G}$ 上的乘法运算、$O(q_i+q_o)$次 $\boldsymbol{G}$ 上的指数运算、$O(q_o)$次 G_T上的指数运算以及 $O(q_o)$次双线性对运算,那么算法的时间复杂度为:$t'=t+O(q_i\varphi+q_o(\theta+\varphi+\tau+\xi))$.证毕.

定理 5 如果$(t,\varepsilon_{\mathrm{TCR}})$-TCR 假设成立,且 π_0满足$(t',\varepsilon',q_s,q_i,q_o)$-ID-AKA 安全,则 π_1满足(t^*,ε^*)-ID-AKA 安全.这里,$\varepsilon^*\geqslant\varepsilon'(1-\varepsilon_{\mathrm{TCR}})$,$t^*=t'+O(q_o\eta)$.

证明 除引入 TCR 函数 $H(*)$用于计算会话密钥外,Game_1与 Game_0的游戏过程相同.如果 Hash 碰撞事件发生,那么 B 终止游戏 Game_1.这里定义 Hash 碰撞事件发生的概率为 $\Pr[\text{Hash Abort}]$.

如果$(t,\varepsilon_{\mathrm{TCR}})$-TCR 假设成立,则

$$\Pr[\text{Hash Abort}]\leqslant\varepsilon_{\mathrm{TCR}}$$
$$\Rightarrow\Pr[\overline{\text{HashAbort}}]\geqslant(1-\varepsilon_{\mathrm{TCR}}).$$

A 赢得游戏 Game_1的概率为:

$$\Pr[\text{A wins Game}_1]=\Pr[\text{A wins Game}_0\wedge\overline{\text{HashAbort}}].$$

由于 A 赢得游戏 Game_0与 Hash 碰撞事件相互独立,那么

$$\Pr[\text{A wins Game}_1]$$
$$=\Pr[\text{A wins Game}_0]\Pr[\overline{\text{HashAbort}}]$$
$$\geqslant\varepsilon'(1-\varepsilon_{\mathrm{TCR}}).$$

因此,$\varepsilon^*\geqslant\varepsilon'(1-\varepsilon_{\mathrm{TCR}})$.

Game_1比 Game_0增加了 $O(q_o)$次 Hash 运算.令 η 表示 Hash 运算时间,那么,$t^*=t'+O(q_o\eta)$.

4.3 分析与比较

表 1 对最近提出的几种 ID-AKA 协议进行了比较.计算性能方面主要列举了 $\boldsymbol{G}$ 上的乘法运算(M)、$\boldsymbol{G}$ 和 $\boldsymbol{G}_T$上的指数运算(E,E_T)以及双线性对运算(P).安全性方面主要列举了密钥泄露伪装(KCI)、完美前向安全(FPS)和抗临时秘密泄露(ESR)三个安全属性(这三个安全属性包含了主要的 AKA 协议缺陷).通信开销方面,列出了单个用户发送和接收的数据量,其中,1G(G_T)表示群 $\boldsymbol{G}$($\boldsymbol{G}_T$)上的 1 个元素,1H 表示一个哈希值.

从安全模型来看,目前主要存在随机预言模型和标准模型(无随机预言)两类.Huang 等人[9]提出 ID-eCK 模型,能模拟完美前向安全性和抗临时秘密泄露安全性,较 ID-mBJM 模型[8]更完备.而王圣宝[13]和高志刚[14]等人则定义了无随机预言的 ID-BJM 模型,但是他们都忽略了 ID-BJM 模型对前向安全性的模拟.因此,他们的模型比 ID-BJM 模型更弱,我们用 ID-wsBJM 表示.本文模型(记为 ID-esBJM)在 ID-wsBJM 模型基础上扩展模拟完美前向安全性和抗临时秘密泄露安全性.

在计算开销和通信开销方面.本文方案仅使用了 1 次双线性对运算,具有更低的计算开销.通信开销相比 Wang[8]、Ni[12]和 Huang[9]等方案多了 1 个群 $\boldsymbol{G}$ 上的元素.根据系统参数构造所选择的安全级别和循环群类型,群 $\boldsymbol{G}$ 上的 1 个元素通常为几十字节到几百字节不

等,2 个群 $\boldsymbol{G}$ 上的元素可以封装在 1 个 IP 分组中,不需要增加 IP 分组数量.因此,相对而言,本文方案的总体性能更优.

此外,为了去除随机预言机,标准模型需要构造特殊的安全陷门函数,因此,标准模型下的安全协议往往采用非标准的困难数学问题及假设.虽然 Gao 协议[14]采用了较弱的安全假设(DBDH 假设),但是该方案没有考虑抗临时秘密泄露安全性,安全性较弱.本文采用的 q-BDHI 问题及其判定性假设,衍生自 DHI 假设.文献[20]讨论了 DHI 假设与标准安全假设(Generalized DH assumption)的关系,表明 q-DHI 假设蕴含 $(q+1)$-Generalized DH 假设.

表 1　ID-AKA 协议比较

协议	计算开销	主要安全属性			通信开销	困难数学问题及假设	是否会话密钥托管	安全模型
		K-CI	FPS	ESR				
Wang 协议[8]	$1M+2E_T+2P$	√	√	×	1G	GBDH	是	随机预言模型(ID-mBJM)
Huang 协议[9]	$3M+2P$	√	√	√	1G	BDH	否	随机预言模型(ID-eCK)
Fujioka 协议[10]	$4E+4P$	√	√	√	1G	BDH	否	随机预言模型(ID-eCK)
Pandit(Π_2)协议[11]	$1M+2E_T+2P$	√	√	√	1G+1H	GBDH	是	随机预言模型(ID-eCK)
Pandit(Π_6)协议[11]	$3M+1E_T+4P$	√	√	√	2G+1H	GBDH	否	随机预言模型(ID-eCK)
Ni 协议[12]	$3M+2P$	√	√	√	1G	CBDH	是	随机预言模型(eID-eCK)
Gao 协议[14]	$5E+2P$	√	√	×	2G	BDH	是	标准模型(ID-wsBJM)
Ghy 协议[16]	$2E+6E_T+1P$	×	√	√	$1G+2G_T$	q-ABDHE	否	标准模型(ID-wsBJM)
Chen 协议[17]	$2E+3E_T+1P$	√	√	√	2G	q-ABDHE	否	标准模型(ID-sBJM)
本文协议	$4E+1E_T+1P$	√	√	√	2G	BDH/q-BDHI	是	标准模型(ID-esBJM)

5　结束语

本文研究了可托管的基于身份认证密钥协商协议及其安全模型.提出的 ID-AKA 协议基于双线性映射理论和判定性 q-BDHI 假设,采用隐式认证方式,仅需 1 轮信息交互.KGC 可通过监控公开信道收集相关参数,恢复特定会话的会话密钥,实现会话密钥托管.基于 ID-BJM 模型,本文将协议模拟分为无散列函数的部分游戏 $Game_0$和完整游戏 $Game_1$两个阶段,扩展定义新鲜预言机,实现了对主要安全属性的形式化模拟.在扩展模型下,本文协议被证明具有强安全性.

参考文献

[1] Boneh D, Franklin M. Identity-based encryption from the weil pairing[A]. Proceedings of the CRYPTO (LNCS 2139)[C]. Berlin: Springer, 2001. 213 – 229.

[2] 钟欢,许春香.基于身份的多方认证组密钥协商协议[J].电子学报,2008,36(10):1869 – 1872.
Zong Huan, Xu Chun-xiang. ID-basedmulti-party authenticated key agreement protocols using multilinear forms[J]. Acta Electronica Sinica, 2008, 36(10): 1869 – 1872. (in Chinese)

[3] 王竹,戴一奇,叶顶锋.普适安全的基于身份的签名机制[J].电子学报,2011,39(7):1613 – 1617.
Wang Zhu, Dai Yi-qi, Ye Ding-feng. Universally composable identity-based signature[J]. Acta Electronica Sinica, 2011, 39(7): 1613 – 1617. (in Chinese)

[4] 明洋,王育民.标准模型下可证安全的通配符基于身份加密方案[J].电子学报,2013,41(10):2082 – 2086.
Ming Yang, Wang Yu-min. Provably secure identity-based encryption scheme with wildcard in the standard model[J]. Acta Electronica Sinica, 2013, 41(10): 2082 – 2086. (in Chinese)

[5] Shim K. Efficient ID-based authenticated key agreement protocol based on the Weil pairing[J]. Electronics Letters, 2003, 39(8): 653 – 654.

[6] Chen L, Cheng Z, Smart N. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security, 2007, 6(4): 213 – 241.

[7] Chow S, Choo K-KR. Strongly-secure identity-based key agreement and anonymous extension[A]. Proceedings of the ISC (LNCS 4779)[C]. Berlin: Springer, 2007. 203 – 220.

[8] Wang SB, Cao ZF, Cheng ZH, Choo K-KR. Perfect forward secure identity-based authenticated key agreement protocol in the escrow mode[J]. Science in China Series F: Information Sciences, 2009, 52(8): 1358 – 1370.

[9] Huang H, Cao Z. An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem[A]. Proceedings of the ACM ASIACCS[C]. New York: ACM, 2009. 333 – 342.

[10] Fujioka A, Hoshino F, Kobayashi T, et al. Id-eCK secure ID-based authenticated key exchange on symmetric and asymmetric pairing[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, 96(6): 1139 – 1155.

[11] Pandit T, Barua R, Tripathy S. ECK secure single round ID-based authenticated key exchange protocols with master perfect forward secrecy[A]. Proceedings of the 8th International Conference on Network and System Security (LNCS 8792)[C]. Berlin: Springer, 2014. 435 – 447.

[12] Ni L, Chen GL, Li JH. Escrowable identity-based authenticated key agreement protocol with strong security[J]. Computers & Mathematics with Applications, 2013, 65(9): 1339 – 1349.

[13] 王圣宝,曹珍富,董晓蕾.标准模型下可证安全的身份基认证密钥协商协议[J].计算机学报,2007,30(10):1842 – 1852.
Wang Sheng-Bao, Cao Zhen-Fu, Dong Xiao-Lei. Provably secure identity-based authenticated key agreement protocols in the standard model[J]. Chinese Journal of Computers, 2007, 30(10): 1842 – 1854. (in Chinese)

[14] 高志刚,冯登国.高效的标准模型下基于身份认证密钥协商协议[J].软件学报,2011,22(5):1031 – 1040.
Gao Zhi-Gang, Feng Deng-Guo. Efficientidentity-based authenticated key agreement protocol in the standard model[J]. Journal of Software, 2011, 22(5): 1031 – 1040. (in Chinese)

[15] 汪小芬,陈原,肖国镇.基于身份的认证密钥协商协议的安全分析与改进[J].通信学报,2008,29(12):16 – 21.
Wang Xiao-Fen, Chen Yuan, Xiao Guo-Zhen. Analysis and improvement of an ID-based authenticated key agreement protocol[J]. Journal on Communications, 2008, 29(12): 16 – 21. (in Chinese)

[16] 高海英.可证明安全的基于身份的认证密钥协商协议[J].计算机研究与发展,2012,49(8):1685 – 1689.
Gao Hai-ying. Provable secure ID-based authenticated key agreement protocol[J]. Journal of Computer Research and Development, 2012, 49(8): 1685 – 1689. (in Chinese)

[17] 陈明.标准模型下增强的身份基认证密钥协商[J].计算机应用研究,2014,31(6):1869 – 1873.
Chen Ming. Extended identity-based authenticated key agreement in standard model[J]. Application Research of Computers, 2014, 31(6): 1869 – 1873. (in Chinese)

[18] 任勇军,王建东,王箭,徐大专,庄毅.标准模型下基于身份的认证密钥协商协议[J].计算机研究与发展,2010,47(9):1604 – 1610.
Ren Yong-jun, Wang Jian-dong, Wang Jian, Xu Da-zhuan, Zhuang Yi. Identity-based authenticated key agreement protocol in the standard model[J]. Journal of Computer Research and Development, 2010, 47(9): 1604 – 1610. (in Chinese)

[19] LaMacchia BA, Lauter K, Mityagin A. Stronger security of authenticated key exchange[A]. Proceedings of the 1st International Conference on Provable Security (LNCS 4784)[C]. Berlin: Springer, 2007. 1 – 16.

[20] Boneh D, Boyen X. Efficient selective identity-based encryption without random oracles[J]. Journal of Cryptology, 2011, 24(4): 659 – 693.

作者简介

陈 明 男,1978 年 5 月出生,重庆北碚人.2003 年、2007 年和 2011 年在重庆大学分别获工学学士、工学硕士和工学博士学位.现为宜春学院数学与计算机科学学院教师,从事信息安全、安全协议分析与设计等方面的研究工作.
E-mail: chenming9824@aliyun.com