

一种增强的移动互联网身份基认证密钥协商协议

孙海燕, 李玲玲, 张 玲, 张建伟, 黄万伟

(郑州轻工业大学 软件学院, 郑州 450002)

摘 要: 针对双线性对运算耗时较多和 PKI 证书管理负担重的问题, 王真等人提出基于身份的移动互联网高效认证密钥协商协议(通信学报, 2017 年第 8 期), 但该协议不能抵抗临时私钥泄露攻击, 不具备 eCK 安全性。为此, 提出一种不使用双线性对运算的身份基认证密钥协商协议, 并在 GDH 假设和随机预言机模型下, 证明其具备 eCK 安全性。分析结果表明, 该协议密钥协商阶段仅需 4 个椭圆曲线点乘运算, 与 CKD-10、XW-12、WML-17 等协议相比效率较高, 单轮通信次数和计算代价较少, 适用于移动互联网环境。

关键词: 双线性对; 攻击; eCK 模型; 基于身份的密码学; 认证密钥协商

开放科学(资源服务)标志码(OSID):



中文引用格式: 孙海燕, 李玲玲, 张玲, 等. 一种增强的移动互联网身份基认证密钥协商协议[J]. 计算机工程, 2019, 45(9): 153-160, 182.

英文引用格式: SUN Haiyan, LI Lingling, ZHANG Ling, et al. An enhanced identity-based authentication key agreement protocol for mobile Internet[J]. Computer Engineering, 2019, 45(9): 153-160, 182.

An Enhanced Identity-based Authentication Key Agreement Protocol for Mobile Internet

SUN Haiyan, LI Lingling, ZHANG Ling, ZHANG Jianwei, HUANG Wanwei

(Software Engineering College, Zhengzhou University of Light Industry, Zhengzhou 450002, China)

[Abstract] To address the problems of time-consuming bilinear pairings and the heavy burden of PKI certificate management, WANG Z, et al. proposed an identity-based efficient Authentication Key Agreement (AKA) protocol for mobile Internet (Journal of Communications, 2017, No. 8), but this protocol cannot resist the attack of temporary private key leakage and does not have eCK security. For this reason, an identity-based authentication AKA protocol without bilinear pairings operation is proposed, whose eCK security is proved under the GDH assumption and random oracle model. Analysis results show that this protocol only needs four elliptic curve point multiplication in the key agreement stage, which is more efficient than CKD-10, XW-12, WML-17 and other protocols. Meanwhile, its single round communication times and computational cost are less, which is suitable for mobile Internet environment.

[Key words] bilinear pairings; attack; eCK model; identity-based cryptography; Authentication Key Agreement (AKA)

DOI: 10.19678/j.issn.1000-3428.0053945

0 概述

认证密钥协商 (Authentication Key Agreement, AKA) 机制允许隐式认证的两个或多个参与方能够在公开网络下协商出一个只有他们自己知道的共享会话密钥, 以确保后续会话消息的机密性、认证性和完整性。基于身份的 AKA (ID-AKA) 协议^[1] 由于不存在基于 PKI 的 AKA 协议中严重的证书管理问题, 因此受到研究者广泛的关注。

自使用双线性对运算的 ID-AKA 协议^[2] 被提出以来, 大量类似协议相继出现^[3-5]。由文献[3, 6]可知, 在同样安全等级下, 一个双线性对的操作代价是一个椭圆曲线点乘操作代价的 3 倍~20 倍。在移动互联网中, 对于传感器节点等资源受限的节点而言, 基于双线性对运算的协议执行效率较低, 而不使用双线性对运算的 ID-AKA 协议能更好地适应资源受限的设备。

文献[7]构建了一种适用于 AKA 协议的形式化

基金项目: 国家自然科学基金(61502436, 61672471); 河南省科技攻关项目(172102210060); 郑州轻工业大学博士基金(2014BSJJ081)。

作者简介: 孙海燕(1983—), 女, 讲师、博士, 主研方向为密码协议; 李玲玲, 硕士研究生; 张 玲、张建伟、黄万伟, 博士。

收稿日期: 2019-02-19 **修回日期:** 2019-04-12 **E-mail:** sunhaiyan2520@163.com

安全模型——BR (Bellare-Rogaway) 模型, 此后, mBR 模型、CK (Canetti-Krawczyk) 模型^[8]和 eCK 模型^[9]等相继被提出。上述安全模型都试图捕捉尽可能多的安全属性^[4], 其中, eCK 安全模型捕捉的安全属性最多, CK 模型捕捉的安全性属性次之, mBR 模型捕捉的安全属性最少。在现有不使用双线性对的 ID-AKA 协议中, 文献[10]协议在 CK 模型下进行安全性证明, 文献[11-13]协议基于 mBR 模型, 文献[14-15]协议基于 CK 模型, 只有文献[16-19]协议基于 eCK 模型, 其中: 文献[17]提出一种需要 6 个椭圆曲线点乘运算的不使用双线性对的 ID-AKA 协议; 文献[18]提出一种需要 5 个椭圆曲线点乘运算的协议; 文献[19]提出一种只需要 4 个点乘运算的协议 WML-17, 协议效率较高。

本文指出 WML-17 协议在 eCK 模型下存在不安全性, 进而提出一个 eCK 安全且不使用双线性对的 ID-AKA 协议。针对 WML-17 协议不能抵抗临时私钥泄露攻击的问题, 分析形式化下敌手的攻击方式, 指出文献[19]安全性证明中的缺陷。在此基础上, 提出一个增强性方案, 并证明其在 GDH 困难问题假设下能够达到 eCK 安全。

1 预备知识

1.1 复杂性假设

令 G 表示素数 q 阶循环加法群, 并令 P 为 G 的一个生成元。 G 上的 Diffie-Hellman 假设^[17]描述如下:

1) 计算性 Diffie-Hellman (CDH) 假设: 对于未知的 $a, b \in \mathbb{Z}_q^*$, 给定 P, aP, bP , 在多项式时间算法内计算 abP 是无法实现的。

2) 判定性 Diffie-Hellman (DDH) 假设: 对于未知的 $a, b, c \in \mathbb{Z}_q^*$, 给定 P, aP, bP, cP , 在多项式时间算法内无法判定 $c = ab \bmod q$ 是否成立。

3) 间隙性 Diffie-Hellman (GDH) 假设: 对于未知的 $a, b \in \mathbb{Z}_q^*$, 给定 P, aP, bP , 在多项式时间算法内借助 DDH 预言机计算 abP 是无法实现的。

1.2 eCK 安全模型

适合 ID-AKA 协议的 eCK 安全模型, 事实上是原始 eCK 安全模型^[9]从 PKI 环境下到基于身份密码学环境下的转换。

1) 协议参与者: 协议参与者被模拟为一组参与方, 其中每一个参与者被模拟为概率多项式时间 (Probability Polynomial Time, PPT) 图灵机。任意两方可以参与协议的一次执行。每一个参与方至多执行多项式次会话。令 $\Pi_{i,j}^m$ 表示 ID_i 拥有的与意定同伴 ID_j 的第 m 次会话。如果 ID_i 能够计算 $\Pi_{i,j}^m$ 的会话密钥 $SK_{i,j}^m$, 则称 $\Pi_{i,j}^m$ 被接受。

2) 攻击者模型: 敌手 \mathcal{A} 同样被模拟为一个 PPT 图灵机, 其控制整个通信链路, 可以根据自己意愿随

意地窃听、拦截、暂停、重放、修改和插入消息。敌手 \mathcal{A} 可以执行以下询问:

(1) $EphemeralKeyReveal(\Pi_{i,j}^m)$: 敌手访问会话 $\Pi_{i,j}^m$ 的临时私钥。

(2) $SessionKeyReveal(\Pi_{i,j}^m)$: 敌手获取已接受会话 $\Pi_{i,j}^m$ 的会话密钥。

(3) $StaticKeyReveal(ID_i)$: 返回参与方 ID_i 的长期私钥给敌手 \mathcal{A} 。

(4) $KGCStaticKeyReveal$: 敌手得到 KGC 的主私钥。

(5) $Send(\Pi_{i,j}^m, M)$: 敌手代表参与方 ID_j 给会话 $\Pi_{i,j}^m$ 发送消息 M (M 可以为空消息 λ), 并且得到参与方 ID_i 的回答。空消息 λ 意味着 ID_i 为会话发起者。如果消息非空, 需要进一步判断 ID_i 是否是会话发起者。如果 ID_i 为会话发起者, 仅做出决定 (接受或者拒绝); 否则, 返回消息 M' 并做出决定 (接受或者拒绝)。

(6) $Test(\Pi_{i,j}^m)$: $Test$ 询问要求 $\Pi_{i,j}^m$ 是新鲜的 (下文将给出新鲜性的定义), 且只允许敌手执行一次。收到此询问后, 一次公平硬币 $b \in \{0, 1\}$ 会被执行。如果 $b = 0$, 敌手会得到一个会话密钥; 否则, 敌手会得到一个随机串 (其与会话密钥密钥同样本空间)。

3) 游戏: 游戏分为 2 个阶段: 阶段 1 和阶段 2。在阶段 1, 敌手 \mathcal{A} 可以询问任意多项式数量界的除 $Test$ 外的其他 5 个查询。阶段 1 结束, 敌手开始阶段 2。在阶段 2, 敌手 \mathcal{A} 选择测试会话 $\Pi_{i,j}^m$ 来执行唯一的 $Test(\Pi_{i,j}^m)$ 查询, 其中 $\Pi_{i,j}^m$ 必须拥有新鲜性。阶段 2 结束后敌手依旧可以执行除 $Test$ 外的其他 5 个查询, 但要保持 $\Pi_{i,j}^m$ 的新鲜性。一旦敌手给出 b 的猜测 b' , 游戏结束。

4) 分析: 当 $b' = b$ 和 $\Pi_{i,j}^m$ 依然是新鲜的, 敌手 \mathcal{A} 赢得上述游戏。敌手优势被定义为 $Adv_{\mathcal{A}}(k) = |2Pr[\mathcal{A} \text{ 成功}] - 1|$ 。

定义 1 (匹配会话) 设会话 $\Pi_{i,j}^m$ 和 $\Pi_{j,i}^n$ 已经接受, 如果参与方 ID_i 计算 $\Pi_{i,j}^m$ 的会话密钥的消息集 $\{ID_j, ID_j, M_j, M_j\}$ 和参与方 ID_j 计算 $\Pi_{j,i}^n$ 的会话密钥的消息集 $\{ID_j, ID_i, M_j, M_i\}$ 是相同的, 则称 $\Pi_{i,j}^m$ 和 $\Pi_{j,i}^n$ 为匹配会话。

定义 2 (新鲜性) 假定 $\Pi_{i,j}^m$ 是已接受的会话。如果满足下列情况, 则 $\Pi_{i,j}^m$ 是新鲜的:

1) $\Pi_{i,j}^m$ 及其匹配会话 $\Pi_{j,i}^n$ (存在的话) 的会话密钥不能被敌手获取。

2) 当 $\Pi_{i,j}^m$ 持有匹配会话时, 参与方 ID_i 的长期私钥以及在 $\Pi_{i,j}^m$ 中的临时私钥不能同时被敌手获取, 参与方 ID_j 的长期私钥以及在匹配会话 $\Pi_{j,i}^n$ 中的临时私钥不能同时被敌手获取。

3) 当 $\Pi_{j,i}^n$ 没有匹配会话时, 参与方 ID_i 的长期私钥以及在 $\Pi_{i,j}^m$ 中的临时私钥不能同时被敌手获取, 参

与方 ID_j 的长期私钥不能被敌手得到。

定义3 (eCK 安全性) 如果一个 ID-AKA 协议满足如下条件,则称其是安全的:

1) 在良性敌手面前,持有匹配会话的会话总是与其匹配会话持有相同的会话密钥。

2) 没有一个 PPT 敌手能够以不容忽视的优势赢取游戏。

2 WML-17 协议及安全性分析

2.1 协议描述

WML-17 协议^[19]由以下3个阶段构成:

1) 系统建立。给定安全参数 k , 信任机构 KGC 首先构造 $(E/F_p, G, q, P)$, 其中, p 为一个 k 位的大素数, E/F_p 为有限域 F_p 上的一条椭圆曲线, G 为 E/F_p 上的一个生成元 P 生成的素数阶 q 循环加法群。首先, KGC 从群 \mathbb{Z}_q^* 中选取一个随机元素 s 为主私钥, 设置主公钥为 $P_{\text{sys}} = sP$, 然后选择2个 Hash 函数 $H_1: \{0,1\}^* \times G \rightarrow \mathbb{Z}_q^*$ 和 $H_2: \{0,1\}^* \times \{0,1\}^* \times G^4 \rightarrow \{0,1\}^k$ 。最后, KGC 秘密地保存主私钥, 公开 $(E/F_p, G, q, P, P_{\text{sys}}, H_1, H_2)$ 。

2) 用户公钥和私钥生成。假定用户 A 的身份为 ID_A 。KGC 从群 \mathbb{Z}_q^* 中选取一个随机元素 r_A , 计算 $R_A = r_A P$, $h_A = H_1(ID_A, R_A)$ 与 $d_A = r_A + h_A s$, 设置 A 的私钥为 d_A , 并将 d_A 以安全的模式传输给用户 A。此外, KGC 公开 ID_A 与 R_A 。用户 A 计算公钥 $P_A = R_A + h_A P_{\text{sys}}$, 且在 $d_A P = P_A$ 的相等下判定 d_A 是有效的。

3) 认证密钥协商。假定持有唯一身份 ID_A 的用户 A 和持有唯一身份 ID_B 的用户 B 执行此阶段, A 为发起方, 协商过程如下:

(1) A 从群 \mathbb{Z}_q^* 中选取一个随机元素 e_A 作为其临时私钥, 计算其临时公钥 $E_A = e_A P$, 然后发送 $\{R_A, E_A\}$ 给 B。

(2) B 收到 E_A 后, 从群 \mathbb{Z}_q^* 中选取一个随机元素 e_B 作为其临时私钥, 计算其临时公钥 $E_B = e_B P$, 然后发送 $\{R_B, E_B\}$ 给 A。

(3) 此时 A 持有 E_B, R_B 与 ID_B , A 计算 $P_B = R_B + H_1(ID_B, R_B) P_{\text{sys}}$, $K_{AB}^1 = d_A E_B + (d_A + e_A) P_B$, $K_{AB}^2 = e_A E_B$, 以及共享的会话密钥 $SK_{AB} = H_2(ID_A, ID_B, E_A, E_B, K_{AB}^1, K_{AB}^2)$ 。

(4) 此时 B 拥有 E_A, R_A 与 ID_A , B 计算 $P_A = R_A + H_1(ID_A, R_A) P_{\text{sys}}$, $K_{BA}^1 = d_B E_A + (d_B + e_B) P_A$, $K_{BA}^2 = e_B E_A$, 以及共享的会话密钥 $SK_{BA} = H_2(ID_A, ID_B, E_A, E_B, K_{BA}^1, K_{BA}^2)$ 。

2.2 非形式化下敌手的攻击

假定参与方为 A 和 B, A 是发起者, A 持有 ID_A, R_A, d_A , 用户 B 持有 ID_B, d_B, R_B 。假冒 B 的攻击者 $\mathcal{A}(B)$ 实施的临时私钥泄露攻击过程如下:

1) 用户 A 从群 \mathbb{Z}_q^* 中选取一个随机元素 e_A , 计算 $E_A = e_A P$, 发送 $\{R_A, E_A\}$ 给 $\mathcal{A}(B)$ 。

2) $\mathcal{A}(B)$ 收到 E_A 后, 随机选取 $e'_B \in \mathbb{Z}_q^*$, 计算 $P_B = R_B + H_1(ID_B, R_B) P_{\text{sys}}$, $E'_B = e'_B P - P_B$, 发送 $\{R_B, E'_B\}$ 给 A。

3) 用户 A 按照协议规定进行会话密钥计算, 即 $SK_{AB} = H_2(ID_A, ID_B, E_A, E'_B, K_{AB}^1, K_{AB}^2)$, 其中, $K_{AB}^1 = d_A E'_B + (d_A + e_A) P_B$, $K_{AB}^2 = e_A E'_B$, $P_B = R_B + H_1(ID_B, R_B) P_{\text{sys}}$ 。

攻击者 $\mathcal{A}(B)$ 首先获取 A 选取的临时私钥 e_A , 然后计算 $P_A = R_A + H_1(ID_A, R_A) P_{\text{sys}}$, $P_B = R_B + H_1(ID_B, R_B) P_{\text{sys}}$, $K_{BA}^1 = e_A P_B + e'_B P_A$, $K_{BA}^2 = e_A E'_B$, 以及会话密钥 $SK_{BA} = H_2(ID_A, ID_B, E_A, E'_B, K_{BA}^1, K_{BA}^2)$ 。

分析: 因为 $K_{AB}^1 = d_A E'_B + (d_A + e_A) P_B = d_A (e'_B P - P_B) + d_A P_B + e_A P_B = d_A e'_B P + e_A P_B = e'_B P_A + e_A P_B = K_{BA}^1$, $K_{AB}^2 = e_A E'_B = K_{BA}^2$, 所以 $SK_{AB} = SK_{BA}$, 这意味着敌手 $\mathcal{A}(B)$ 和 A 持有的会话密钥相同。因此, WML-17 协议不能满足临时私钥泄露攻击抵抗性。

2.3 形式化下敌手的攻击

本节将指出 WML-17 协议不具备 eCK 安全性, 即证明存在一个攻击者 \mathcal{A} 总能赢得其和模拟器 \mathcal{CH} 间的游戏。假定攻击者 \mathcal{A} 想要攻击目标会话 $\Pi_{A,B}^\ell$, 其中用户 A 持有 ID_A , 用户 B 持有 ID_B 。游戏描述如下:

1) 游戏初始化: 模拟器 \mathcal{CH} 生成系统主密钥 s 和系统参数 $(E/F_p, G, q, P, P_{\text{sys}}, H_1, H_2)$, 然后发送系统参数给攻击者 \mathcal{A} 。模拟器 \mathcal{CH} 利用 s 为用户 A 产生 R_A, d_A , 为用户 B 产生 R_B, d_B 。此处, H_1 和 H_2 是一般的哈希函数。

2) 游戏的第一阶段:

(1) \mathcal{A} 执行 $\text{Send}(\Pi_{A,B}^\ell, \perp)$ 查询后。收到 Send 查询后, 模拟器 \mathcal{CH} 从群 \mathbb{Z}_q^* 中选取一个随机元素 e_A , 计算 $E_A = e_A P$, 回复 $\{R_A, E_A\}$ 给 \mathcal{A} 。

(2) \mathcal{A} 执行 $\text{Send}(\Pi_{B,A}^m, \perp)$ 查询后。收到 Send 查询后, 模拟器 \mathcal{CH} 从群 \mathbb{Z}_q^* 中选取一个随机元素 e_B , 计算 $E_B = e_B P$, 回复 $\{R_B, E_B\}$ 给 \mathcal{A} 。

(3) 获取 R_B 后, 攻击者 \mathcal{A} 随机选择 $e'_B \in \mathbb{Z}_q^*$, 计算 $P_B = R_B + H_1(ID_B, R_B) P_{\text{sys}}$, $E'_B = e'_B P - P_B$ 。然后 \mathcal{A} 执行 $\text{Send}(\Pi_{A,B}^\ell, \{R_B, E'_B\})$ 查询。收到此 Send 查询后, \mathcal{CH} 将该会话的状态设定为已接受。

(4) 攻击者 \mathcal{A} 查询 $\text{EphemeralKeyReveal}(\Pi_{A,B}^\ell)$, 然后获得参与方 A 的临时密钥 e_A 。

3) 游戏的第二阶段: 由新鲜性定义可知会话 $\Pi_{A,B}^\ell$ 是新鲜的。敌手 \mathcal{A} 执行 $\text{Test}(\Pi_{A,B}^\ell)$ 。收到 Test 询问, \mathcal{CH} 公平地抛一次硬币 $b \in \{0,1\}$, 如果 $b=0$, \mathcal{CH} 返回其按照协议具体计算的值 $SK_{A,B}^\ell$, 如果 $b=1$, 返回随机值 $sk' \in \{0,1\}^k$ 。此处 $SK_{A,B}^\ell = H_2(ID_A, ID_B, E_A, E'_B, K_{AB}^1, K_{AB}^2)$, 其中, $K_{AB}^1 = d_A E'_B + (d_A + e_A) P_B$, $K_{AB}^2 = e_A E'_B$, $P_B = R_B + H_1(ID_B, R_B) P_{\text{sys}}$ 。

4) 游戏结束: 攻击者 \mathcal{A} 先计算 $P_A = R_A + H_1(ID_A, R_A)P_{\text{sys}}, P_B = R_B + H_1(ID_B, R_B)P_{\text{sys}}, K_{BA}^1 = e_A P_B + e_B' P_A, K_{BA}^2 = e_A E_B' + e_B' E_A'$, 以及 $SK_{BA} = H_2(ID_A, ID_B, E_A, E_B', K_{BA}^1, K_{BA}^2)$ 。然后根据 $SK_{A,B}^{\ell} = SK_{BA}$ 的结果来给定 b 的结果。如果 $SK_{A,B}^{\ell} = SK_{BA}$, 攻击者 \mathcal{A} 猜测 $b = 0$; 否则, 猜测 $b = 1$ 。

分析: 因为 $SK_{A,B}^{\ell} = SK_{BA}$ (其证明过程类似于等式 $SK_{AB} = SK_{BA}$ 的证明), 所以攻击者 \mathcal{A} 总是正确地猜测 b 的值, 即 $\Pr[\mathcal{A} \text{ 成功}] = 1$, 由此可知, $\text{Adv}_{\mathcal{A}}(k) = 12\Pr[\mathcal{A} \text{ 成功}] - 1 = 1$ 。因此, WML-17 协议不具备 eCK 安全性。

2.4 安全缺陷

2.2 节与 2.3 节的分析展示了 WML-17 协议的安全缺陷, 这使得此 WML-17 协议的安全证明变得无效。通过仔细观察, 笔者发现 WML-17 协议的安全证明中存在不严格的分析。具体来说, 文献[19]中对第 3 类情况“攻击者 \mathcal{A} 只掌握双方临时私钥”的分析是不恰当的。在“攻击者 \mathcal{A} 只掌握双方临时私钥”的情况下, 需要考虑测试会话 $\Pi_{A,B}^{\ell}$ 的匹配会话是否存在。如果 $\Pi_{A,B}^{\ell}$ 无匹配会话, 则 B 的临时密钥 e_B 是由攻击者 \mathcal{A} 选择的, 模拟器是无法获知 e_B 的; 如果 $\Pi_{A,B}^{\ell}$ 有匹配会话, 则 B 的临时密钥 e_B 是由模拟器 \mathcal{CH} 选择的, 此时攻击者 \mathcal{A} 可以通过执行 EphemeralKeyReveal 询问获取临时密钥 e_B 。在 $\Pi_{A,B}^{\ell}$ 没有匹配会话的情况下, 即在模拟器 \mathcal{CH} 无法获取 e_B 的情况下, \mathcal{CH} 无法由 $K_{AB}^1 = e_B(aP) + e_A(bP) + CDH(aP, bP, abP)$ 推导出 $CDH(aP, bP, abP)$ 的。因此, 模拟器 \mathcal{CH} 不能解决 GDH 问题, 进而归约失败。

3 增强性方案

为弥补 WML-17 协议中的安全缺陷, 本文提出一个增强性方案。该方案的系统建立和用户公私钥阶段与 WML-17 协议基本一致。增强性方案的认证密钥协商阶段描述如下:

假定持有唯一身份 ID_A 的用户 A 和持有唯一身份 ID_B 的用户 B 执行此阶段, A 为发起方, 其协商过程如下:

1) A 从群 \mathbb{Z}_q^* 中选取一个随机元素 e_A 作为其临时私钥, 计算其临时公钥 $E_A = e_A P$, 发送 $\{R_A, E_A\}$ 给 B 。

2) B 从群 \mathbb{Z}_q^* 中选取一个随机元素 e_B 作为其临时私钥, 计算其临时公钥 $E_B = e_B P$, 发送 $\{R_B, E_B\}$ 给 A 。

3) 收到 $\{R_B, E_B\}$ 后, A 计算 $P_B = R_B + H_1(ID_B, R_B)P_{\text{sys}}, K_{AB}^1 = (d_A + 2e_A)(P_B + 2E_B), K_{AB}^2 = (d_A + e_A)(P_B + E_B)$, 以及共享的会话密钥 $SK_{AB} = H_2(ID_A, ID_B, E_A, E_B, K_{AB}^1, K_{AB}^2)$ 。

4) 收到 $\{R_A, E_A\}$ 后, B 计算 $P_A = R_A + H_1(ID_A, R_A)P_{\text{sys}}, K_{BA}^1 = (d_B + 2e_B)(P_A + 2E_A), K_{BA}^2 = (d_B + e_B)(P_A + E_A)$, 以及共享的会话密钥 $SK_{BA} = H_2(ID_A, ID_B, E_A, E_B, K_{BA}^1, K_{BA}^2)$ 。

增强性方案的正确性验证如下: 因为 G 为加法循环群且 $d_A P = P_A, d_B P = P_B, E_B = e_B P, E_A = e_A P$, 所以 $K_{AB}^2 = (d_A + 2e_A)(P_B + 2E_B) = d_A P_B + 2d_A E_B + 2e_A P_B + 4e_A E_B = d_A d_B P + 2d_A e_B P + 2e_A d_B P + 4e_A e_B P = d_B P_A + 2d_B E_A + 2e_B P_A + 4e_B E_A = d_B (P_A + 2E_A) + 2e_B (P_A + 2E_A) = K_{BA}^1$, 同理可得 $K_{AB}^1 = K_{BA}^2$, 因此, $SK_{A,B} = SK_{BA}$ 。

4 安全性证明

定理 1 在 GDH 假设以及函数 H_1 和 H_2 被视为随机预言机的情况下, 增强性方案满足第 1.2 节概述的 eCK 安全性。

证明 如果定义 3 展示的 2 个条件成立, 则协议满足 eCK 安全性。第 1 个条件由第 3 节展示的正确性得以保证。下面采取反证法论证第 2 个条件成立, 即假设一个敌手 \mathcal{A} 以不容忽视的机率成功攻破协议, 则能够利用 \mathcal{A} 构造一个能够以不容忽视的机率求解 GDH 问题的模拟器 \mathcal{CH} 。

假定 k 为安全参数, 攻击协议的 PPT 敌手 \mathcal{A} 以不容忽视的优势 $\text{Adv}_{\mathcal{A}}(k)$ 赢得游戏。假定游戏中, 每一方至多从事 $n_s(k)$ 个会话, \mathcal{A} 涉及至多 $n_p(k)$ 个不同的诚实参与方以及执行至多 n_0 次 H_2 查询。由于 H_2 被视为随机预言机, 发起 Test 询问(成功概率为 $1/2$)后, \mathcal{A} 只能通过猜测攻击(直接猜出正确的会话密钥)、密钥复制攻击(敌手建立一个会话, 它和目标会话非匹配, 但会话密钥却相同)以及伪造攻击(某一时刻, 敌手自己计算 $K_{a,b}^1$ 和 $K_{a,b}^2$, 然后执行 $H_2(ID_a, ID_b, E_a, E_b, K_{a,b}^1, K_{a,b}^2)$)赢得游戏(即能够成功区分随机串和目标会话的会话密钥)。

对于猜测攻击而言, 因为会话密钥是 H_2 的输出, \mathcal{A} 直接猜出正确会话密钥的机率为 $O(1/2^k)$ 。显然, 概率是可忽略不计的。对于密钥复制攻击而言, 其概率为 $O(n_s(k)^2/2^k)$, 可忽略不计。

目前只剩下伪造攻击, 伪造攻击采取归约的方式进行分析。如果敌手 \mathcal{A} 以不容忽视的机率通过伪造攻击攻破协议, 则可以利用敌手 \mathcal{A} 来构造以不容忽视的优势解决 GDH 问题的模拟器 \mathcal{CH} 。在这里, \mathcal{CH} 和 \mathcal{A} 一起执行安全模型中描述的游戏, \mathcal{CH} 回答 \mathcal{A} 的所有询问, 令 $\text{Adv}_{\mathcal{CH}}^{\text{GDH}}(k)$ 为 \mathcal{CH} 解决 GDH 的优势。给定 GDH 问题实例 $(U = uP, V = vP)$, 其中 $u, v \in \mathbb{Z}_q^*, P \in G$, \mathcal{CH} 的任务是在 DDH 的帮助下计算 $CDH(U, V) = uvP$ 。当游戏开始时, \mathcal{CH} 以 $1/n_p(k)^2 n_s(k)$ 的概率猜测敌手 \mathcal{A} 选取的测试会话为 $\Pi_{a,b}^n$, 其中 $a, b \in [1, n_p(k)]$ 且 $a = b, n \in [1, n_s(k)]$ 。接下来, 模拟器 \mathcal{CH} 需要猜测敌手的策略选择。根

据定义 2,需要考虑测试会话 $\Pi_{a,b}^n$ 有无匹配会话。如果测试会话 $\Pi_{a,b}^n$ 拥有匹配会话 $\Pi_{b,a}^l$,则敌手 \mathcal{A} 是被动敌手,敌手只能被动转发两参与方之间的消息,进一步说明 $\Pi_{a,b}^n$ 和 $\Pi_{b,a}^l$ 的消息以及临时私钥是由模拟器 \mathcal{CH} 产生的。无匹配会话意味着敌手 \mathcal{A} 是主动敌手,即 ID_a 的消息以及临时私钥是由模拟器 \mathcal{CH} 产生的,而 ID_b 的消息以及临时私钥则是由敌手产生的。基于上述分析和新鲜性定义,模拟器 \mathcal{CH} 必须从如下 4 种情况中猜测敌手的策略选择,其中, ID_a 的临时私钥指 ID_a 持有的目标会话 $\Pi_{a,b}^n$ 的临时私钥, ID_b 的临时私钥指 ID_b 持有的匹配会话 $\Pi_{b,a}^l$ 的临时私钥。

1) 策略 S1: 被动敌手 \mathcal{A} 不知道 ID_a 的长期私钥和 ID_b 的临时私钥。

2) 策略 S2: 被动敌手 \mathcal{A} 不知道 ID_a 和 ID_b 的临时私钥。

3) 策略 S3: 主动或被动敌手 \mathcal{A} 不知道 ID_a 的临时私钥和 ID_b 的长期私钥。

4) 策略 S4: 主动或被动敌手 \mathcal{A} 不知道 ID_a 和 ID_b 的长期私钥。

如果 \mathcal{A} 以不容忽视的机率通过“伪造攻击”攻破协议,则必有一个策略下其概率不容忽视。

4.1 策略 S1 分析

在策略 S1 下对敌手 \mathcal{A} 和模拟器 \mathcal{CH} 间的游戏进行分析,具体如下:

1) 建立阶段: \mathcal{CH} 建立 KGC 的公钥和所有参与方的长期私钥。 \mathcal{CH} 维护列表 Λ_{Setup} , 条目形如 $(ID_i, (d_i, R_i), P_i)$ 且值初始为空。

(1) \mathcal{CH} 选取一随机值 $P_{\text{sys}} \in G$ 作为 KGC 的公钥。

(2) 对于参与方 ID_a 而言, \mathcal{CH} 从 \mathbb{Z}_q^* 中选取一个随机元素 h_a , 计算 $R_a = U - h_a P_{\text{sys}}$, 同时令 $H_1(ID_a, R_a) = h_a$, $d_a = \perp$, 设置 d_a 为 ID_a 的长期私钥。因此, 参与方 ID_a 的长期公钥可以计算为 $P_a = R_a + H_1(ID_a, R_a) P_{\text{sys}} = R_a + h_a P_{\text{sys}} = U$ 。

(3) 对于其他参与方 $ID_i (i \neq a)$, \mathcal{CH} 从 \mathbb{Z}_q^* 中选取 2 个随机元素 h_i, d_i , 计算 $R_i = d_i P - h_i P_{\text{sys}}$, 同时令 $H_1(ID_i, R_i) = h_i$, 并设置 d_i 为 ID_i 的长期私钥。因此, $P_i = R_i + h_i P_{\text{sys}} = d_i P$ 。

(4) 对于任意参与方 $ID_i (i \in [1, n_p(k)])$, \mathcal{CH} 给敌手 \mathcal{A} 传输 (ID_i, R_i) , 并分别在列表 Λ_{Setup} 和 Λ_{H_1} 中插入条目 $(ID_i, (d_i, R_i), P_i)$ 和 (ID_i, R_i, h_i) 。

2) 游戏第一阶段: \mathcal{CH} 维护 4 个列表 Λ_{H_1} 、 Λ_{H_2} 、 Λ_{Send} 和 Λ_{Reveal} , 分别用于处理随机预言机 H_1 、 H_2 、Send 和 SessionKeyReveal 询问。对于如下询问, \mathcal{A} 可以无次序地询问多项式界次数, \mathcal{CH} 回答 \mathcal{A} 的询问如下:

(1) $H_1(ID_i, R_i)$: 如果 Λ_{H_1} 中有与 (ID_i, R_i, h_i) 相匹配的条目存在, \mathcal{CH} 响应 h_i 给 \mathcal{A} 。否则, \mathcal{CH} 从群 \mathbb{Z}_q^* 中选取一个随机元素 h_i , 在列表 Λ_{H_1} 中插入条目

(ID_i, R_i, h_i) , 并回复 h_i 给 \mathcal{A} 。

(2) $\text{StaticKeyReveal}(ID_i)$: 如果 ID_i 是 ID_a , \mathcal{CH} 中止; 否则, \mathcal{CH} 返回 ID_i 的长期私钥 d_i 给 \mathcal{A} 。

(3) $\text{KGCStaticKeyReveal}$: \mathcal{CH} 退出游戏。

(4) $\text{EphemeralKeyReveal}(\Pi_{i,j}^m)$: 如果 $\Pi_{i,j}^m$ 是匹配会话 $\Pi_{b,a}^l$, \mathcal{CH} 退出游戏; 否则, \mathcal{CH} 返回临时私钥 $r_{i,j}^m$ 作为应答。

(5) $\text{Send}(\Pi_{i,j}^m, M)$: \mathcal{CH} 维护的列表 Λ_{Send} 中的条目形如 $(\Pi_{i,j}^m, \text{tran}_{i,j}^m, r_{i,j}^m)$ 且值初始为空, 其中, $\text{tran}_{i,j}^m$ 是到现在 $\Pi_{i,j}^m$ 传输和得到的一切消息集, $r_{i,j}^m$ 是 ID_i 所拥有的会话 $\Pi_{i,j}^m$ 的临时私钥。

如果 M 是 $\text{tran}_{i,j}^m$ 中第 2 个消息, \mathcal{CH} 设置该会话为已接受; 否则, 若 $\Pi_{i,j}^m = \Pi_{b,a}^l$, \mathcal{CH} 令 $r_{i,j}^m = \perp$, 在列表 Λ_{Setup} 中获取 R_b , 给 \mathcal{A} 回应 $\{R_b, E_b = V = vP\}$, 并修改 Λ_{Send} 中 $\Pi_{i,j}^m$ 的条目; 否则, \mathcal{CH} 从 \mathbb{Z}_q^* 中选取一个随机元素 $r_{i,j}^m$, 在列表 Λ_{Setup} 中获取 R_i , 给 \mathcal{A} 回应 $\{R_i, r_{i,j}^m P\}$, 并修改 Λ_{Setup} 中 $\Pi_{i,j}^m$ 的条目。

(6) $\text{SessionKeyReveal}(\Pi_{i,j}^m)$: \mathcal{CH} 维护的列表 Λ_{Reveal} 中的条目形如 $(\Pi_{i,j}^m, ID_{\text{ini}}^m, ID_{\text{resp}}^m, E_{\text{ini}}^m, E_{\text{resp}}^m, SK_{i,j}^m)$ 且值初始为空, 其中下标 ini 代表发起者, 下标 resp 代表响应者。

如果 $\Pi_{i,j}^m$ 尚未接受, \mathcal{CH} 返回 \perp ; 否则, 若 $\Pi_{i,j}^m$ 是测试会话 $\Pi_{a,b}^n$ 或者匹配会话 $\Pi_{b,a}^l$, \mathcal{CH} 结束游戏; 否则, 若 $\Pi_{i,j}^m$ 的会话密钥 $SK_{i,j}^m$ 已存在, \mathcal{CH} 返回 $SK_{i,j}^m$; 否则, 从列表 Λ_{Send} 中获取 $\{R_i, E_i\}$ 和 $\{R_j, E_j\}$, 执行 $H_1(ID_i, R_i)$ 查询获取结果 h_i , 执行 $H_1(ID_j, R_j)$ 查询获取结果 h_j , 计算 $P_i = R_i + h_i P_{\text{sys}}$ 和 $P_j = R_j + h_j P_{\text{sys}}$, 然后以 (ID_i, ID_j, E_i, E_j) (ID_i 为发起者) 或者 (ID_j, ID_i, E_j, E_i) (ID_j 为发起者) 为索引, 查看列表 Λ_{H_2} 中是否有匹配项使得 $\text{DDH}(P_i + 2E_i, P_j + 2E_j, K_{i,j}^1) = 1$ 和 $\text{DDH}(P_i + E_i, P_j + E_j, K_{i,j}^2) = 1$ 。如果存在, 则从列表 Λ_{H_2} 中获取 h_K 并设置其为 $SK_{i,j}^m$; 否则均匀选取随机串 $SK_{i,j}^m \in \{0, 1\}^k$ 。最后 \mathcal{CH} 返回 $SK_{i,j}^m$, 并在列表 Λ_{Reveal} 中插入条目 $(\Pi_{i,j}^m, ID_{\text{ini}}^m, ID_{\text{resp}}^m, E_{\text{ini}}^m, E_{\text{resp}}^m, SK_{i,j}^m)$ 。

(7) $H_2(ID_i, ID_j, E_i, E_j, K_{i,j}^1, K_{i,j}^2)$: \mathcal{CH} 维护的列表 Λ_{H_2} 的条目形如 $(ID_i, ID_j, E_i, E_j, K_{i,j}^1, K_{i,j}^2, h_K)$ 。

如果列表 Λ_{H_2} 中存在匹配条目 $(ID_i, ID_j, E_i, E_j, K_{i,j}^1, K_{i,j}^2)$, \mathcal{CH} 返回 h_K ; 否则, 以 $(*, ID_i, ID_j, E_i, E_j, *)$ 为索引在 Λ_{Reveal} 中查找。如果匹配条目存在, 验证 $\text{DDH}(P_i + 2E_i, P_j + 2E_j, K_{i,j}^1) = 1$ 和 $\text{DDH}(P_i + E_i, P_j + E_j, K_{i,j}^2) = 1$ 是否成立, 其中, $P_i = R_i + h_i P_{\text{sys}}$, $P_j = R_j + h_j P_{\text{sys}}$, $h_i = H_1(ID_i, R_i)$ 。如果 2 个等式均成立, 从 Λ_{Reveal} 中获取相应的 $SK_{i,j}^m$ 并令其为 h_K ; 否则 (没有匹配条目, 或起码有一个等式不成立), 均匀选取随机串 $h_K \in \{0, 1\}^k$ 。最终 \mathcal{CH} 返回 h_K , 并更新列表 Λ_{H_2} 。

3) 游戏第二阶段: \mathcal{A} 仅能查询一次下列询问。

$Test(\Pi_{i,j}^m)$: 若 $\Pi_{i,j}^m$ 非目标会话 $\Pi_{a,b}^n$, \mathcal{CH} 退出游戏; 否则, \mathcal{CH} 从 $\{0,1\}^k$ 中均匀选取随机串 ξ , 并返回 ξ 给 \mathcal{A} 。

分析: 如果 \mathcal{A} 选定策略 S1、目标会话 $\Pi_{a,b}^n$ 及其匹配会话 $\Pi_{b,a}^l$, 则 \mathcal{CH} 不会退出游戏。如果 \mathcal{A} 通过伪造攻击赢得游戏, 则其必定查询了 $H_2(ID_a, ID_b, E_a, V, K_{a,b}^1, K_{a,b}^2)$ 或 $H_2(ID_b, ID_a, V, E_a, K_{a,b}^1, K_{a,b}^2)$, 其中 E_a 和 V 分别是 \mathcal{CH} 选取的 ID_a 和 ID_b 的临时公钥, $K_{a,b}^1 = (DLOG(U) + 2r_{a,b}^n)(P_b + 2V)$, $K_{a,b}^2 = (DLOG(U) + r_{a,b}^n)(P_b + V)$ 。为解决 GDH 问题, \mathcal{CH} 从 Λ_{H_2} 中获取条目, 然后利用自己知道的 $r_{a,b}^n$, 输出 $GDH(U, V) = K_{a,b}^1 - K_{a,b}^2 - r_{a,b}^n(P_b + 3V)$ 。

\mathcal{CH} 解决 GDH 问题的优势为:

$$Adv_{\mathcal{CH}}^{GDH}(k) \geq \frac{Adv_{\mathcal{A}}(k)}{4n_0 n_p^2(k) n_s^2(k)}$$

因此, 如果 $Adv_{\mathcal{A}}(k)$ 是不容忽视的, 则 \mathcal{CH} 的优势是不容忽视的, 这与 GDH 假设矛盾。

4.2 策略 S2 分析

对策略 S2 的分析如下:

1) 建立阶段: \mathcal{CH} 建立 KGC 的公私钥和所有参与方的长期私钥。 \mathcal{CH} 维护初始空列表 Λ_{Setup} , 条目形如 $(ID_i, (d_i, R_i), P_i)$ 。

(1) \mathcal{CH} 从 \mathbb{Z}_q^* 中选取一个随机元素 s 作为 KGC 的主私钥。因此, 此事件可以模拟主私钥前向安全性。

(2) 对于任意参与方 $ID_i (i \in [1, n_p(k)])$, \mathcal{CH} 从 \mathbb{Z}_q^* 中选取 2 个随机元素 h_i, d_i , 计算 $R_i = d_i P - h_i P_{sys}$, 同时令 $H_1(ID_i, R_i) = h_i$, 并设置 d_i 为 ID_i 的长期私钥。因此, $P_i = R_i + h_i P_{sys} = d_i P$ 。

(3) 对于任意参与方 $ID_i (i \in [1, n_p(k)])$, \mathcal{CH} 给敌手 \mathcal{A} 传输 (ID_i, R_i) , 并分别在列表 Λ_{Setup} 和 Λ_{H_1} 中插入条目 $(ID_i, (d_i, R_i), P_i)$ 和 (ID_i, R_i, h_i) 。

2) 游戏第一阶段: \mathcal{CH} 维护 4 个初始空列表 $\Lambda_{H_1}, \Lambda_{H_2}, \Lambda_{Send}$ 和 Λ_{Reveal} , 分别用于处理随机预言机 $H_1, H_2, Send$ 和 $SessionKeyReveal$ 询问。对于如下询问, \mathcal{A} 可以无次序的询问多项式界次数。 \mathcal{CH} 回答 \mathcal{A} 的询问如下:

(1) $H_1(ID_i, R_i), H_2(ID_i, ID_j, R_i, R_j, E_i, E_j, K_{i,j}^1, K_{i,j}^2)$ 和 $SessionKeyReveal(\Pi_{i,j}^m)$: 这 3 个询问的回答同 S1。

(2) $StaticKeyReveal(ID_i)$: \mathcal{CH} 返回 ID_i 的长期私钥 d_i 给 \mathcal{A} 。

(3) $KGCStaticKeyReveal$: \mathcal{CH} 返回 s 给 \mathcal{A} 。

(4) $EphemeralKeyReveal(\Pi_{i,j}^m)$: 若 $\Pi_{i,j}^m = \Pi_{a,b}^n$ 或 $\Pi_{i,j}^m = \Pi_{b,a}^l$, \mathcal{CH} 退出游戏; 否则, \mathcal{CH} 返回临时私钥 $r_{i,j}^m$ 给敌手 \mathcal{A} 。

(5) $Send(\Pi_{i,j}^m, M)$: \mathcal{CH} 维护的列表 Λ_{Send} 中的条目形如 $(\Pi_{i,j}^m, tran_{i,j}^m, r_{i,j}^m)$, 其中 $tran_{i,j}^m$ 是目前 $\Pi_{i,j}^m$ 传输和得到的一切消息集, $r_{i,j}^m$ 是 ID_i 所拥有的会话 $\Pi_{i,j}^m$ 的临时私钥。

如果 M 是 $tran_{i,j}^m$ 中第 2 个消息, \mathcal{CH} 设置该会话为已接受; 否则, 若 $\Pi_{i,j}^m = \Pi_{a,b}^n$, \mathcal{CH} 令 $r_{i,j}^m = \perp$, 在列表 Λ_{Setup} 中获取 R_a , 给 \mathcal{A} 回应 $\{R_a, E_a = U\}$, 并修改 Λ_{Send} 中 $\Pi_{i,j}^m$ 的条目; 否则, 若 $\Pi_{i,j}^m = \Pi_{b,a}^l$, \mathcal{CH} 令 $r_{i,j}^m = \perp$, 在列表 Λ_{Setup} 中获取 R_b , 给 \mathcal{A} 回应 $\{R_b, E_b = V = vP\}$, 并修改 Λ_{Send} 中 $\Pi_{i,j}^m$ 的条目; 否则, \mathcal{CH} 从 \mathbb{Z}_q^* 中选取一个随机元素 $r_{i,j}^m$, 在列表 Λ_{Setup} 中获取 R_i , 给 \mathcal{A} 回应 $\{R_i, r_{i,j}^m P\}$, 并修改 Λ_{Send} 中 $\Pi_{i,j}^m$ 的条目。

3) 游戏第二阶段: \mathcal{A} 仅能查询一次 $Test(\Pi_{i,j}^m)$ 。此询问的回答同 S1。

分析: 如果 \mathcal{A} 选定策略 S2、目标会话 $\Pi_{a,b}^n$ 及其匹配会话 $\Pi_{b,a}^l$, 则 \mathcal{CH} 不会退出游戏。如果 \mathcal{A} 通过伪造攻击赢得游戏, 则其必定查询了 $H_2(ID_a, ID_b, U, V, K_{a,b}^1, K_{a,b}^2)$ 或 $H_2(ID_b, ID_a, V, U, K_{a,b}^1, K_{a,b}^2)$, 其中 U 和 V 分别是 \mathcal{CH} 选取的 ID_a 和 ID_b 的临时公钥, $K_{a,b}^1 = (d_a + 2DLOG(U))(P_b + 2V)$, $K_{a,b}^2 = (d_a + DLOG(U))(P_b + V)$ 。为解决 GDH 问题, \mathcal{CH} 从列表 Λ_{H_2} 中获取条目, 然后利用自己知道的 d_a , 输出

$$GDH(U, V) = \frac{1}{2} K_{a,b}^1 - K_{a,b}^2 + d_a P_b。$$

\mathcal{CH} 解决 GDH 问题的优势为:

$$Adv_{\mathcal{CH}}^{GDH}(k) \geq \frac{Adv_{\mathcal{A}}(k)}{4n_0 n_p^2(k) n_s^2(k)}$$

因此, 如果 $Adv_{\mathcal{A}}(k)$ 是不容忽视的, 则 \mathcal{CH} 的优势是不容忽视的, 这与 GDH 假设矛盾。

4.3 策略 S3 分析

在策略 S3 下, 敌手可能是主动敌手, 因此, ID_b 的消息以及临时私钥可能是敌手产生的。

1) 建立阶段: \mathcal{CH} 建立 KGC 的公钥和所有参与方的长期私钥, \mathcal{CH} 维护列表 Λ_{Setup} , 条目形如 $(ID_i, (d_i, R_i), P_i)$ 。

(1) \mathcal{CH} 选取一随机值 $P_{sys} \in G$ 作为 KGC 的公钥。

(2) 对于参与方 ID_b 来说, \mathcal{CH} 从 \mathbb{Z}_q^* 中选取一个随机元素 h_b , 计算 $R_b = V - h_b P_{sys}$, 同时令 $H_1(ID_b, R_b) = h_b$, $d_b = \perp$, 设置 d_b 为 ID_b 的长期私钥。因此, 参与方 ID_b 的长期公钥可以计算为 $P_b = R_b + H_1(ID_b, R_b) P_{sys} = R_b + h_b P_{sys} = V$ 。

(3) 对于其他参与方 $ID_i (i \neq b)$, \mathcal{CH} 从 \mathbb{Z}_q^* 中选取 2 个随机元素 h_i, d_i , 计算 $R_i = d_i P - h_i P_{sys}$, 同时令 $H_1(ID_i, R_i) = h_i$, 并设置 d_i 为 ID_i 的长期私钥。因此, $P_i = R_i + h_i P_{sys} = d_i P$ 。

(4) 对于任意参与方 $ID_i (i \in [1, n_p(k)])$, CH 给敌手 \mathcal{A} 传输 (ID_i, R_i) , 并分别在列表 Λ_{Setup} 和 Λ_{H_1} 中插入条目 $(ID_i, (d_i, R_i), P_i)$ 和 (ID_i, R_i, h_i) 。

2) 游戏第一阶段: CH 维护 4 个列表 Λ_{H_1} 、 Λ_{H_2} 、 Λ_{Send} 和 Λ_{Reveal} , 分别用于处理随机预言机 H_1 、 H_2 、 $Send$ 和 $SessionKeyReveal$ 询问。对于如下询问, \mathcal{A} 可以无次序的询问多项式界次数。 CH 回答 \mathcal{A} 的询问如下:

(1) $H_1(ID_i, R_i)$ 、 $KGCStaticKeyReveal$ 和 $H_2(ID_i, ID_j, R_i, R_j, E_i, E_j, K_{i,j}^1, K_{i,j}^2)$: 这 3 个询问的回答如同 S1。

(2) $StaticKeyReveal(ID_i)$: 如果 ID_i 是 ID_b , CH 中止; 否则, CH 返回 ID_i 的长期私钥 d_i 给 \mathcal{A} 。

(3) $EphemeralKeyReveal(\Pi_{i,j}^m)$: 如果 $\Pi_{i,j}^m$ 是测试会话 $\Pi_{a,b}^m$, CH 退出游戏; 否则, CH 返回临时私钥 $r_{i,j}^m$ 作为应答。

(4) $Send(\Pi_{i,j}^m, M)$: CH 维护的列表 Λ_{Send} 中的条目形如 $(\Pi_{i,j}^m, tran_{i,j}^m, r_{i,j}^m)$, 其中, $tran_{i,j}^m$ 是 $\Pi_{i,j}^m$ 传输和得到的一切消息集, $r_{i,j}^m$ 是 ID_i 所拥有的会话 $\Pi_{i,j}^m$ 的临时私钥。

如果 M 是 $tran_{i,j}^m$ 中第 2 个消息, CH 设置该会话为已接受; 否则, 如果 $\Pi_{i,j}^m = \Pi_{a,b}^m$, CH 令 $r_{i,j}^m = \perp$, 在列表 Λ_{Setup} 中获取 R_a , 给 \mathcal{A} 回应 $\{R_a, E_a = U\}$, 并修改 Λ_{Send} 中 $\Pi_{i,j}^m$ 的条目; 否则, CH 从 \mathbb{Z}_q^* 中选取一个随机元素 $r_{i,j}^m$, 在列表 Λ_{Setup} 中获取 R_i , 给 \mathcal{A} 回应 $\{R_i, r_{i,j}^m P\}$, 并修改 Λ_{Send} 中 $\Pi_{i,j}^m$ 的条目。

(5) $SessionKeyReveal(\Pi_{i,j}^m)$: 此询问和 S1 的基本一致, 不同之处在于 S1 中匹配会话是必定存在, S3 中匹配会话是有可能存在。

3) 游戏第二阶段: \mathcal{A} 仅能查询一次 $Test(\Pi_{i,j}^m)$ 。此询问的回答同 S1。

分析: 如果 \mathcal{A} 选定策略 S3、目标会话 $\Pi_{a,b}^m$ 及其匹配会话 $\Pi_{b,a}^m$ (如有), 则 CH 不会退出游戏。如果 \mathcal{A} 通过伪造攻击赢得游戏, 则其必定查询了 $H_2(ID_a, ID_b, U, E_b, K_{a,b}^1, K_{a,b}^2)$ 或 $H_2(ID_b, ID_a, E_b, U, K_{a,b}^1, K_{a,b}^2)$, 其中, U 是 CH 返回的临时公钥, E_b 是 CH 选定的 (有匹配会话) 或者敌手选取的 (无匹配会话), $K_{a,b}^1 = (d_a + 2DLOG(U))(V + 2E_b)$, $K_{a,b}^2 = (d_a + DLOG(U))(V + E_b)$ 。为解决 GDH 问题, CH 从列表 Λ_{H_2} 中获取条目, 然后利用自己知道的 d_a , 输出

$$GDH(U, V) = 2K_{a,b}^2 - \frac{1}{2}K_{a,b}^1 - \frac{d_a}{2}(3V + 2E_b)。$$

CH 解决 GDH 问题的优势为:

$$Adv_{CH}^{GDH}(k) \geq \frac{Adv_{\mathcal{A}}(k)}{4n_0^2 n_p^2(k) n_s^2(k)}$$

因此, 如果 $Adv_{\mathcal{A}}(k)$ 是不容忽视的, 则 CH 的优势是不容忽视的, 这与 GDH 假设矛盾。

4.4 策略 S4 分析

对策略 S4 的分析如下:

1) 建立阶段: CH 建立 KGC 的公钥和所有参与方的长期私钥。 CH 维护列表 Λ_{Setup} , 条目形如 $(ID_i, (d_i, R_i), P_i)$ 。

(1) CH 选取一随机值 $P_{sys} \in G$ 作为 KGC 的公钥。

(2) 对于参与方 ID_a 而言, CH 从 \mathbb{Z}_q^* 中选取一个随机元素 h_a , 计算 $R_a = U - h_a P_{sys}$, 同时令 $H_1(ID_a, R_a) = h_a$, $d_a = \perp$, 设置 d_a 为 ID_a 的长期私钥。因此, 参与方 ID_a 的长期公钥可以计算为 $P_a = R_a + H_1(ID_a, R_a) P_{sys} = R_a + h_a P_{sys} = U$ 。

(3) 对于参与方 ID_b 而言, CH 从 \mathbb{Z}_q^* 中选取一个随机元素 h_b , 计算 $R_b = V - h_b P_{sys}$, 同时令 $H_1(ID_b, R_b) = h_b$, $d_b = \perp$, 设置 d_b 为 ID_b 的长期私钥。因此, 参与方 ID_b 的长期公钥可以计算为 $P_b = R_b + H_1(ID_b, R_b) P_{sys} = R_b + h_b P_{sys} = V$ 。

(4) 对于其他参与方 $ID_i (i \neq a, i \neq b)$, CH 从 \mathbb{Z}_q^* 中选取 2 个随机元素 h_i, d_i , 计算 $R_i = d_i P - h_i P_{sys}$, 同时令 $H_1(ID_i, R_i) = h_i$, 并设置 d_i 为 ID_i 的长期私钥。因此, $P_i = R_i + h_i P_{sys} = d_i P$ 。

(5) 对于任意参与方 $ID_i (i \in [1, n_p(k)])$, CH 给敌手 \mathcal{A} 传输 (ID_i, R_i) , 并分别在列表 Λ_{Setup} 和 Λ_{H_1} 中插入条目 $(ID_i, (d_i, R_i), P_i)$ 和 (ID_i, R_i, h_i) 。

2) 游戏第一阶段: CH 维护 4 个列表 Λ_{H_1} 、 Λ_{H_2} 、 Λ_{Send} 和 Λ_{Reveal} , 分别用于处理随机预言机 H_1 、 H_2 、 $Send$ 和 $SessionKeyReveal$ 询问。对于如下询问, \mathcal{A} 可以无次序地询问多项式界次数。 CH 回答 \mathcal{A} 的询问如下:

(1) $SessionKeyReveal(\Pi_{i,j}^m)$ 、 $KGCStaticKeyReveal$ 、 $H_1(ID_i, R_i)$ 、 $H_2(ID_i, ID_j, R_i, R_j, E_i, E_j, K_{i,j}^1, K_{i,j}^2)$: 这 4 个询问的回答同 S3。

(2) $StaticKeyReveal(ID_i)$: 如果 $ID_i = ID_a$ 或 $ID_i = ID_b$, CH 结束游戏; 否则, CH 返回 ID_i 的长期私钥 d_i 给 \mathcal{A} 。

(3) $EphemeralKeyReveal(\Pi_{i,j}^m)$: CH 返回临时私钥 $r_{i,j}^m$ 给敌手 \mathcal{A} 。

(4) $Send(\Pi_{i,j}^m, M)$: CH 维护的列表 Λ_{Send} 中的条目形如 $(\Pi_{i,j}^m, tran_{i,j}^m, r_{i,j}^m)$, 其中, $tran_{i,j}^m$ 是 $\Pi_{i,j}^m$ 传输和得到的所有消息集, $r_{i,j}^m$ 是 ID_i 所拥有的会话 $\Pi_{i,j}^m$ 的临时私钥。

如果 M 是 $tran_{i,j}^m$ 中第 2 个消息, CH 设置该会话为已接受; 否则, CH 从 \mathbb{Z}_q^* 中选取一个随机元素 $r_{i,j}^m$, 在列表 Λ_{Setup} 中获取 R_i , 给 \mathcal{A} 回应 $\{R_i, r_{i,j}^m P\}$, 并修改 Λ_{Send} 中 $\Pi_{i,j}^m$ 的条目。

3) 游戏第二阶段: \mathcal{A} 仅能查询一次 $Test(\Pi_{i,j}^m)$ 。此询问的回答同 S1。

分析:如果 A 选择策略 S4、目标会话 $\Pi_{a,b}^n$ 及其匹配会话 $\Pi_{b,a}^l$ (有的话),则 CH 不会退出游戏。如果 A 通过伪造攻击赢得游戏,则其必定查询了 $H_2(ID_a, ID_b, E_a, E_b, K_{a,b}^1, K_{a,b}^2)$ 或 $H_2(ID_b, ID_a, E_b, E_a, K_{a,b}^1, K_{a,b}^2)$, 其中 $E_a = r_{a,b}^n P$ 是 CH 返回的临时公钥, E_b 是 CH 选定的(有匹配会话)或者敌手选取的(无匹配会话), $K_{a,b}^1 = (DLOG(U) + 2r_{a,b}^n)(V + 2E_b)$, $K_{a,b}^2 = (DLOG(U) + r_{a,b}^n)(V + E_b)$ 。为解决 GDH 问题, CH 从 Λ_{H_2} 中获取条目,然后利用自己知道的 $r_{a,b}^n$, 输出 $GDH(U, V) = 2K_{a,b}^2 - K_{a,b}^1 + 2r_{a,b}^n E_b$ 。

CH 解决 GDH 问题的优势为:

$$Adv_{CH}^{GDH}(k) \geq \frac{Adv_A(k)}{4n_0^2 n_p^2(k) n_s^2(k)}$$

因此,如果 $Adv_A(k)$ 是不容忽视的,则 CH 的优势是不容忽视的,这与 GDH 假设矛盾。

5 协议比较

对本文改进协议和其他无双线性对的 ID-AKA 协议在效率 and 安全性方面进行比较。由于无双线性对的协议往往基于点乘、Hash 运算、点加、点减等运算,因此本文只考虑时间复杂度相对比较大的点乘运算。令 T_{EM} 表示执行一次点乘运算所耗费的时间。为评估方案的安全性,此处考虑协议采取的安全模型以及是否满足 eCK 安全性,比较结果如表 1 所示。

表 1 不同协议的效率与安全性比较

协议	计算 代价	通信代价 (轮数)	安全 模型	eCK 安全性
LI-13 协议 ^[13]	$4T_{EM}$	1	mBR	N
FG-10 协议 ^[14]	$4T_{EM}$	1	CK	N
CKD-10 协议 ^[12]	$5T_{EM}$	1	mBR	N
XW-12 协议 ^[15]	$7T_{EM}$	2	CK	N
WML-17 协议 ^[19]	$5T_{EM}$	1	eCK	N
SWZ-16 协议 ^[16-17]	$6T_{EM}$	1	eCK	Y
NCLH-16 协议 ^[18]	$5T_{EM}$	1	eCK	Y
本文改进协议	$4T_{EM}$	1	eCK	Y

由表 1 可知:与 FG-10 协议^[14] 和 Li-13 协议^[13] 相比,本文改进协议效率相同但拥有较强的安全性;与 CKD-10 协议^[12]、XW-12 协议^[15]、WML-17 协议^[19] 相比,本文改进协议的安全性强且效率高;与 SWZ-16 协议^[16-17] 和 NCLH-16 协议^[18] 相比,本文改进协议与其具有同样的安全性,但效率最高。

综上,与现有无双线性对的 ID-AKA 协议相比,本文改进协议具有最优的安全性,并达到了最优的轮效率和计算效率,因此其更适合应用于移动互联网等实际应用场景。

6 结束语

本文分析文献[19]中无双线性对运算的 ID-AKA 协议,证明该协议无法满足 eCK 安全性,同时给出非形式化和形式化下敌手的攻击方式,指出其安全证明中的缺陷。在此基础上,提出一个增强性方案,并证明该方案具有 eCK 安全性。分析结果表明,本文协议在单轮的情况下仅需要 4 个点乘运算完成密钥协商阶段,计算效率较高,适合用于移动互联网等实际应用场景。由于无双线性对运算的 ID-AKA 协议在 seCK 模型^[20]下不安全,因此下一步将对此进行改进,设计一个 seCK 安全的 ID-AKA 协议。

参考文献

- [1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proceedings of Cryptology-Crypto'84. Berlin, Germany: Springer, 1984:47-53.
- [2] SMART N P. An identity based authenticated key agreement protocol based on the Weil pairing[J]. Electronics Letters, 2002, 38(13): 630-632.
- [3] CHEN Liqun, CHENG Zhaohui, SMART N P. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security, 2007, 6(4): 213-241.
- [4] HUANG Hai, CAO Zhenfu. An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem[C]//Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Berlin, Germany: Springer, 2009: 363-368.
- [5] PANDIT T, BARUA R, TRIPATHY S. eCK secure single round ID-based authenticated key exchange protocols with master perfect forward secrecy[C]//Proceedings of the 8th International Conference on Network and System Security. Berlin, Germany: Springer, 2014: 435-447.
- [6] ARANHAD F, FAZ-HERNÁNDEZ A, LÓPEZ J, et al. Faster implementation of scalar multiplication on Koblitz curves[C]//Proceedings of the 2nd International Conference on Cryptology and Information Security in Latin America. Berlin, Germany: Springer, 2012: 177-193.
- [7] BELLARE M, ROGAWAY P. Entity authentication and key distribution[C]//Proceedings of Cryptology-Crypto'93. Berlin, Germany: Springer, 1993: 232-249.
- [8] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]//Proceedings of Cryptology-Eurocrypt'01. Berlin, Germany: Springer, 2001: 453-474.
- [9] LaMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange[C]//Proceedings of the 1st International Conference on Provable Security. Berlin, Germany: Springer, 2007: 1-16.

(下转第 182 页)

(上接第 160 页)

- [10] ZHUA R W, YANG Guoming, WONG D S. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices [J]. Theoretical Computer Science, 2007, 378(2):198-207.
- [11] 曹雪菲,寇卫东,樊凯,等. 无双线性对的基于身份的认证密钥协商协议[J]. 电子与信息学报, 2009, 31(5):1241-1244.
- [12] CAO Xuefei, KOU Weidong, DU Xiaoni. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges [J]. Information Sciences, 2010, 180(15):2895-2903.
- [13] 李坤. 基于身份的认证密钥协商协议研究[D]. 西安: 西安电子科技大学, 2013.
- [14] FIORE D, GENNARO R. Making the Diffie-Hellman protocol identity-based [C]//Proceedings of Cryptology-CT-RSA'10. Berlin, Germany: Springer, 2010:165-178.
- [15] XIE Min, WANG Libin. One-round identity-based key exchange with perfect forward security [J]. Information Processing Letters, 2012, 112(14/15):587-591.
- [16] 孙海燕. 认证密钥协商协议及其应用[D]. 北京: 北京邮电大学, 2014.
- [17] SUN Haiyan, WEN Qiaoyan, ZHANG Hua, et al. A strongly secure identity-based authenticated key agreement protocol without pairings under the GDH assumption [J]. Security and Communication Networks, 2015, 8(17):3167-3179.
- [18] NI Liang, CHEN Gongliang, LI Jianhua, et al. Strongly secure identity-based authenticated key agreement protocols without bilinear pairings [J]. Information Sciences, 2016, 367-368(1):176-193.
- [19] 王真, 马兆丰, 罗守山. 基于身份的移动互联网高效认证密钥协商协议[J]. 通信学报, 2017, 38(8):19-27.
- [20] SUN Haiyan, WEN Qiaoyan, LI Wenmin. A strongly secure pairing-free certificateless authenticated key agreement protocol under the CDH assumption [J]. SCIENCE CHINA Information Sciences, 2016, 59(3):1-15.

编辑 金胡考