分类号 TP399 学号 22020063

U D C 004.77 密级 公开

工学硕士学位论文

无证书低交互认证密钥协商协议研究

硕 士 生 姓 名 姜晶

学 科 专 业 计算机科学与技术

研 究 方 向 密码应用

指 导 教 师 王小峰 副研究员

协助指导教师 邢倩倩 助理研究员

国防科技大学研究生院

二〇二四年十月

Research on certificateless low-interaction authenticated key exchange protocol

Candidate: Jing Jiang

Supervisor: Prof. Xiaofeng Wang

Associate Supervisor: Assist.Prof. Qianqian Xing

A thesis

Submitted in partial fulfillment of the requirements

for the degree of Master of Engineering

in computer science and technology

Graduate School of National University of Defense Technology

Changsha, Hunan, P. R. China

Oct, 2024

独 创 性 声 明

本人声明所呈交的学位论文是我本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表和撰写过的研究成果，也不包含为获得国防科技大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文题目：无证书低交互认证密钥协商协议研究

学位论文作者签名：_____ 日期： 年 月 日

学位论文版权使用授权书

本人完全了解国防科技大学有关保留、使用学位论文的规定。本人授权国防科技大学可以保留并向国家有关部门或机构送交论文的复印件和电子文档，允许论文被查阅和借阅;可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密学位论文在解密后适用本授权书。）

学位论文题目：无证书低交互认证密钥协商协议研究

学位论文作者签名：_____ 日期： 年 月 日

作者指导教师签名：_____ 日期： 年 月 日

目 录

表 目 录

图 目 录

摘 要

认证密钥交换协议又称为认证密钥协商协议（Authentication Key Exchange, AKE），不仅确保网络通信的机密性、完整性和真实性，还为用户提供了安全的身份认证。当前的 AKE 协议根据公钥验证方式的不同，主要分为基于证书的 AKE，基于标识的 AKE 和基于无证书的 AKE。针对高安全、低延时通信的需求，基于证书的 AKE 具有高昂的证书管理和分发成本，基于标识的 AKE 和基于无证书的 AKE 具有更广阔的应用场景。本文结合实际应用场景，设计了不同需求下的 AKE 协议，本文的主要工作包括:

1、SOK 协议是零交互（无公钥查询、无证书验证、无交互）的唯一方案，但是 SOK 协议并不满足已知密钥安全，一旦会话密钥泄露，将会泄露所有会话密钥。因此，本文首次提出了具有已知密钥安全的零交互认证密钥协商（Identity-Based Zero-Interactive Authenticated Key Exchange，IB-ZIAKE）协议，通过引入每个会话独有的公开的随机因子，通信双方产生唯一的会话密钥，再通过引入单向哈希函数从双线性对计算中生成唯一的会话密钥，确保即使过去的会话密钥泄露，敌手也无法直接从双线性对计算结果获取当前的会话密钥，协议满足已知密钥安全。其次，本文拓展了基于标识的零交互认证密钥协商协议的安全模型，将认证密钥协商协议的安全性从共享密钥的不可区分性（IND-SK）扩展到已知密钥安全。实验结果表明 IB-ZIAKE 协议和 SOK 协议性能无明显差异，但是 IB-ZIAKE 协议能抵抗已知密钥攻击。

2、目前针对基于标识的 AKE 协议大多基于相同体制下，对于通信双方处于不同体制下的研究较少。因此，本文首次提出了基于标识与基于无证书体制下的跨域认证密钥协商协议（Cross-Domain Authenticated key Exchange，CDAKE），即通信一方基于标识密码体制生成用户公私钥，另一方基于无证书公钥密码体制生成用户公私钥，解决了不同体制下用户直接通信的需求。同时本文改进了 Lippold[1] 提出的无证书 eCK 模型，在此安全模型下，基于 CDH 假设和 CBDH 假设, 对该跨域协议提供严格安全证明，证明该协议满足已知密钥安全，前向安全，抗密钥泄漏伪装安全，抗未知密钥共享安全。

关键词: **零交互密钥协商；跨域密钥协商；可证明安全**

ABSTRACT

Authentication Key Exchange (AKE) not only ensures the confidentiality, integrity and authenticity of network communication, but also provides secure authentication for users. The current AKE protocols are mainly divided into certificate-based AKE, identity-based AKE and certificateless AKE according to the different ways of public key authentication. To meet the requirements of high security and low latency communication, certificate-based AKE has high certificate management and distribution costs, while identity-based AKE and certificateless AKE have broader application scenarios. In this paper, we design the AKE protocol under different requirements according to the practical application scenarios. The main work of this paper includes:

1. The SOK protocol is the only scheme with zero interaction (no public key query, no certificate verification, and no interaction). However, the SOK protocol does not satisfy the known key security. Once the session key is leaked, all the session keys will be leaked. Therefore, Identity-Based Zero-Interactive Authenticated Key Exchange (IB-ZIAKE) protocol is firstly proposed in this paper, which is secure with known key. Both sides of the communication generate a unique session key, and then generate a unique session key from the bilinear pairing calculation by introducing a one-way hash function to ensure that even if the past session key is leaked, the adversary cannot directly obtain the current session key from the bilinear pairing calculation result, and the protocol meets the security of the known key. Secondly, this paper extends the security model of identity-based zero-interaction authenticated key agreement protocol, which extends the security of authenticated key agreement protocol from the indistinguishability of shared key (IND-SK) to the security of known key. The experimental results show that there is no significant difference between IB-ZIAKE protocol and SOK protocol, but IB-ZIAKE protocol can resist the known key attack.

2. At present, most of the identity-based AKE protocols are based on the same system, and there is little research on the two sides of the communication in different systems. Therefore, this paper first proposes identity-based and certificateless cross-domain authenticated key agreement protocols (Cross-Domain Domain Authenticated key Exchange, CDAKE), that is, one side of communication generates users' public and private keys based on identity-based cryptosystem. The other party generates the public and pri-

vate keys of the user based on the certificateless public key cryptosystem, thereby meeting the requirement of direct communication of the user under different systems. At the same time, this paper improves the certificateless eCK model proposed by Lippold [1], under this security model, based on CDH assumption and CBDH assumption, provides strict security proof for the cross-domain protocol, proves that the protocol meets the requirements of known key security and forward security. Security against key disclosure and masquerade, security against unknown key sharing.

Key Words: Zero-interactive key exchange; cross-domain key exchange; provable security

符号使用说明

κ	安全参数
ID_A	用户 A 的身份标识
d_A	用户的私钥
r_i	随机因子
x	用户的秘密值
y	用户的部分私钥
X	用户的公钥
Π_{ij}^t	用户 i 与用户 j 发起的第 t 个会话
$\in_R$	从集合中随机选择一个元素
$\Pi_{j,i}^w$	用户 j 与用户 i 发起的第 w 个会话，作为会话 Π_{ij}^t 的匹配会话
sid_j^t	用户 i 执行的第 t 个会话的会话标识符
$sk_{i,j}^t$	用户 i 执行的第 t 个会话的会话密钥
$\mathbb{G}_1$，$\mathbb{G}_2$	群
ψ	同构映射
$\mathbb{F}_q$	阶为 q 的域
$\mathbb{F}_{q^k}$	阶为 q 的域的 k 次扩域
$\varepsilon(n)$	可忽略函数

第一章　绪论

在当今复杂多变的网络环境中，各种在线服务和分布式系统已成为日常生活与商业运营不可或缺的一部分。随着数据交换量的激增及用户隐私保护意识的增强，确保信息传输的安全性与完整性成为了亟待解决的关键问题。在此背景下，认证密钥协商协议（Authentication Key Exchange, AKE）成为构建安全通信基石的核心机制之一, 不仅能够有效验证通信双方的身份真实性，防止中间人攻击和身份伪装，还能在双方之间安全地生成并共享会话密钥，该密钥随后用于加密后续的数据传输，确保信息的机密性和不可篡改性。基于标识的认证密钥协商协议通过用户标识生成用户公钥，能够简化密钥管理的复杂性，降低传统公钥密码体制中高昂的证书管理成本。为了进一步提高协议效率，研究者提出了基于标识的无交互密钥协商协议 SOK 协议[2]。

然而，现有的基于标识的无交互密钥协商协议 SOK[2] 不满足已知密钥安全，一旦某次会话密钥泄露将会泄露所有的会话密钥；另一方面，目前的跨域密钥协商协议中对基于标识的跨域密钥协商的协议研究较少，没有针对基于标识与基于无证书密码体制的跨域密钥协商方案。随着跨域通信需求的日益增长，设计基于标识的高安全无交互的认证密钥协商协议、设计基于标识与基于无证书体制的跨域密钥协商协议成为亟待解决的问题。

本章首先对认证密钥协商协议的研究背景和意义进行介绍，然后详细讨论了当前无交互密钥协商协议和跨域密钥协商协议存在的问题，而后介绍本文的工作，包括设计基于标识的具有已知密钥安全的零交互认证密钥协商协议（Identity-Based Zero-Interactive Authenticated Key Exchange , IB-ZIAKE），拓展了基于标识的密钥协商协议的安全模型，提升了基于标识的无交互密钥协商方案的安全性；设计首个基于标识与基于无证书体制下的跨域认证密钥协商协议（Cross-Domain Authenticated key Exchange, CDAKE），并改进了无证书 eck 模型，实现了通信双方基于标识与基于无证书体制下的跨域密钥协商，最后介绍本文的组织结构。

1.1　研究背景

随着信息技术的迅猛发展和广泛应用，网络安全问题已成为全球关注的焦点。近年来，随着云计算、物联网、大数据等新兴技术的普及，网络环境日益复杂，黑客攻击、信息泄露、数据篡改等安全事件频发，给个人、企业和国家带来了巨大的损失和风险。在这种形势下，密钥协商协议作为网络安全的重要基石，其作用愈发凸显。密钥协商协议的主要目的是在两个或多个参与方之间建立一个共享的、秘密的密钥, 以保护后续的通信。具体来说，通信双方分别利用自己的私钥与对方

的公钥进行计算，协商出一致的会话密钥如图1.1所示。除了通信双方之外，别人无法得知会话密钥，通信双方使用这个会话密钥对通信数据的加密保护，这一机制在防止信息泄露、保障数据完整性、抵抗恶意攻击等方面发挥着至关重要的作用。特别是在无线网络、移动通信等场景中，密钥协商协议成为了确保通信安全的关键所在。

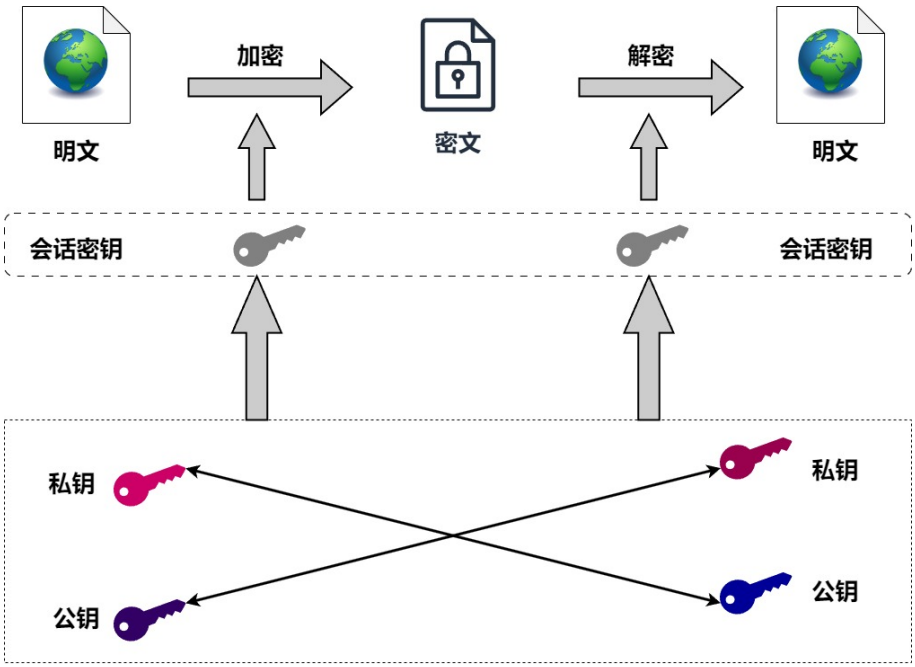

图 1.1　密钥协商协议示意图

密钥协商协议的研究路线如图1.2所示。1976 年，Diffie-Hellman [3] 提出的公钥密码体制使得通信交互的双方可在公开信道上进行密钥协商，开启了密码学的新时代。然而 DH 密钥协商技术由于缺乏身份的认证，极易遭受到中间人攻击，一个简单的解决方案是将密钥协商协议与数字签名方案相结合，获得认证的密钥协商方案。但该解决方案存在最大的问题就是会导致消息的长度远大于 DH 协议中要求的消息长度。对此，Law[4] 等人提出了 MQV 协议，在不增加带宽和消息流数量的情况下实现了身份认证。MQV 协议利用静态的 DH 公私钥对交换一对临时的 DH 公钥，结合临时密钥和静态密钥获得一致的会话密钥，这就将身份认证问题转变为了对静态公钥的认证问题，而对静态公钥的认证则可以通过证书模式来解决。

然而 MQV 协议被 Kaliski 证明易受到未知密钥共享攻击，Krawczyk[5] 提出了 MQV 的哈希变体，即 HMQV 协议，在计算会话密钥时引入了自身 DH 值和对方身份的哈希，将 MQV 的安全目标在随机预言机模型下得到形式化证明。Sarr[6] 指出了两种针对 HMQV 可能存在的攻击，并提出了 FHMQV，进一步提高算法的安全性。然而大量的证书使用会对证书授权 (Certificate Authority，CA) 中心带来较

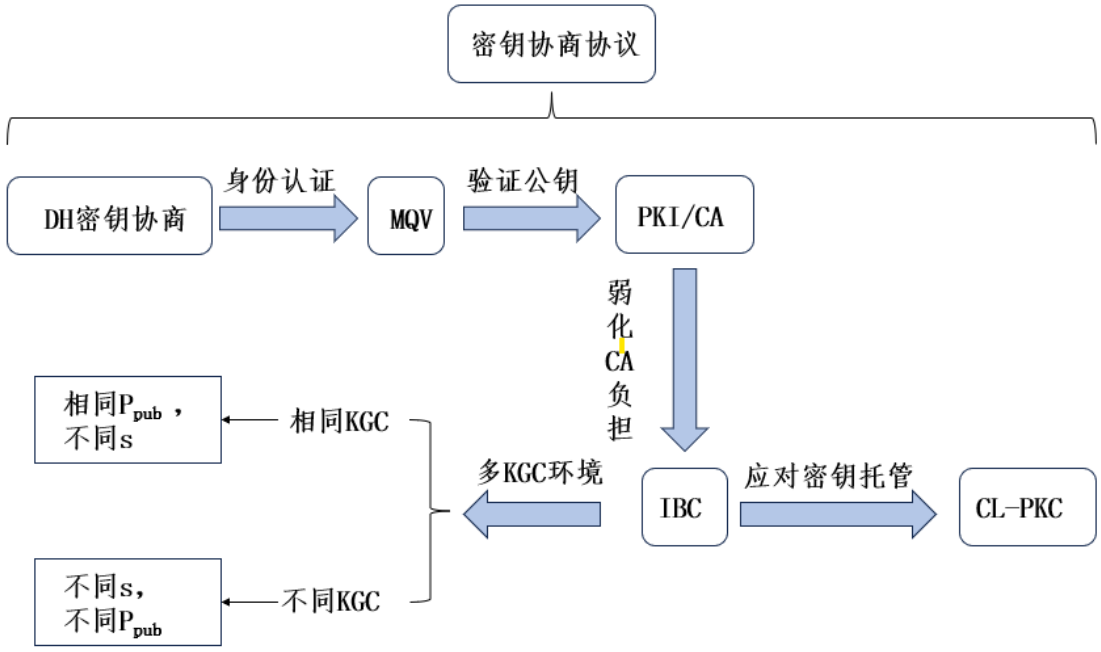

图 1.2　密钥协商协议研究路线

大的负担，对此，研究者提出了基于标识的密码体制[7]，基于标识的密钥协商协议利用标识作为用户公钥，身份信息可以直接作为对公钥的认证，弱化 CA 负担。针对基于标识的密钥协商方案，又可以根据用户所属管理域不同，可以分为相同 KGC 环境下的密钥协商和不同 KGC 环境下的密钥协商[8]。然而，在基于标识的密钥协商协议中，KGC 可以解密任意用户的信息，存在密钥托管问题，因此研究者又提出了无证书密码体制[9]，用户密钥由用户自行选择的秘密值和 KGC 传递的部分私钥组成，无证书体制的密钥协商协议[10–12] 能弱化 CA 负担的同时也避免了密钥托管问题，但协议设计会更加复杂。

认证密钥协商（Authentication Key Exchange, AKE）协议是保障通信安全的主要技术之一。认证密钥协商的主要目的是在两个或多个参与方之间建立一个共享的、秘密的密钥, 以保护后续的通信。认证密钥协商协议的核心在于验证用户的身份, 并在用户身份被确认后, 生成加密通信所需的安全密钥。然而, 在公钥密码体制下, 用户的公钥是公开的, 如何验证用户身份成为了关键问题。当前的认证密钥协商协议依据不同的公钥验证机制可大致分为三类，第一类是传统的基于证书的公钥密码体制（Public Key Cryptography, PKC），第二类是基于标识密码体制（Identity-Based Cryptography, IBC ），第三类是无证书公钥密码体制（Certificateless Public Key Cryptography, CL-PKC），如图1.3所示。

基于证书体制的 AKE 协议是目前应用最广泛的认证密钥协商协议之一。它依赖于公钥基础设施（Public Key Infrastructure, PKI）和数字证书，通过证书颁发

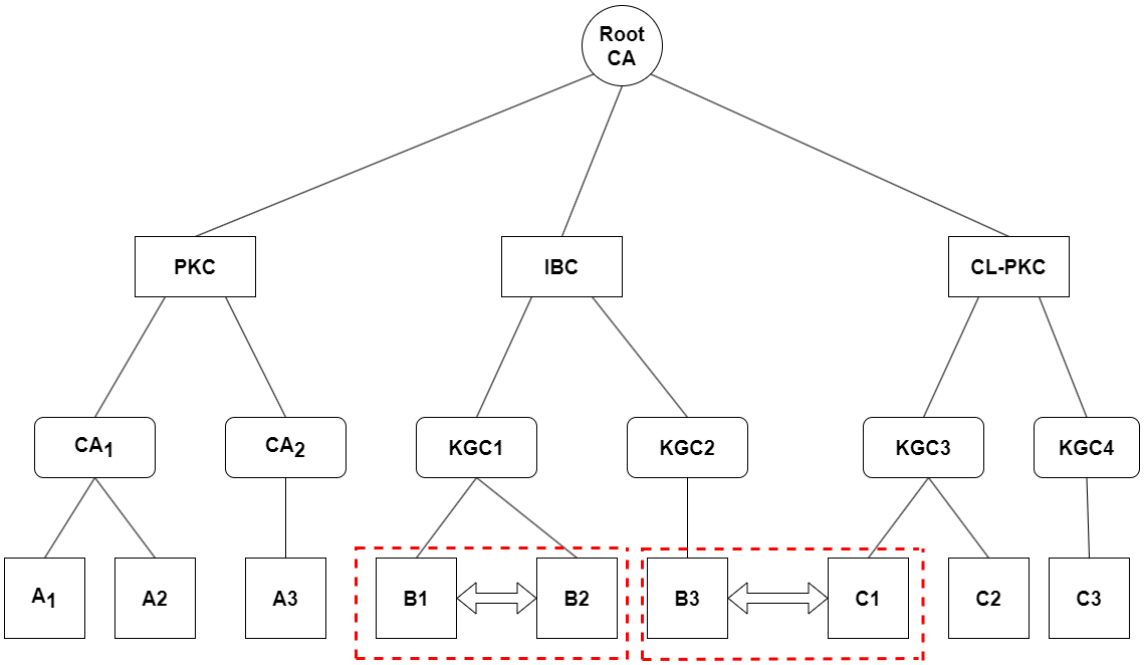

图 1.3　认证密钥协商协议分类

机构（Certificate Authority, CA）验证用户的身份，并使用公钥密码学算法实现认证和密钥协商。这种协议的优点在于安全性高，能够有效防止密钥泄露和身份伪造。然而，其缺点也显而易见：证书的管理和分发成本高昂，特别是在大型网络中，证书的维护和更新成为一大挑战。此外，证书体制的 AKE 协议还存在证书撤销和证书路径验证等复杂问题。基于标识的 AKE 通过用户的唯一标识（如电子邮件地址、电话号码等）直接生成公钥，无需额外的证书验证。这种协议的优点在于简化了密钥管理过程，降低了成本。然而，密钥托管问题也是一大挑战，即用户的私钥可能由密钥生成中心（KGC）托管，存在被滥用的风险。无证书体制的 AKE 协议结合了基于证书体制和基于标识体制的 AKE 的优点，通过引入 KGC 和部分私钥的概念，实现了用户私钥的生成和分发，同时无需额外的证书，同时避免了密钥托管问题。无证书体制 AKE 协议的优点在于提高了安全性，降低了密钥管理的复杂性，并保护了用户的隐私，但是设计一个安全的无证书密钥协商协议需要综合考虑多种安全因素，更为复杂。因此，针对不同应用场景设计安全高效的认证密钥协商协议具有重要的理论价值和实际意义。

针对低延时的通信需求，可以通过减少交互次数降低通信延时，提高通信效率, 研究人员提出了无交互密钥协商（Non-Interactive Key Exchange , NIKE）协议, 这些协议允许两个参与者通过将自己的私钥与另一方的公钥相结合, 独立生成共享密钥, 从而消除了交互式通信的需要。NIKE 协议通常分为三类：基于证书的 NIKE，基于标识的 NIKE 和基于无证书的 NIKE。基于证书的 NIKE 协议[13, 14] 依赖于公钥基础设施（Public Key Infrastructure, PKI）, 用户可以获取并验证对方的

公钥，虽然双方没有直接交互, 但他们需要借助证书查询和验证对方的公钥。基于无证书的 NIKE 协议[15, 16] 虽然双方没有直接交互, 但需要隐式地获取并验证对方的公钥，严格来说, 这些协议并不完全符合零交互密钥协商的要求。

相比之下, 只有基于标识的无交互密钥协商（Identity-Based Non-Interactive Key Exchange, IB-NIKE）协议才能实现真正的零交互密钥协商, 因为它们不需要公钥查询、证书验证或事先交互, 如图1.3中 B_1 与 B_2 的通信。第一个 IB-NIKE 构造被称为 SOK, 由 Sakai、Ohgishi 和 Kasahara [2] 提出。随后, SOK 的改进和证明在 [17–21] 中得到了探讨。然而, 这些协议并不提供已知密钥的安全性。一个会话密钥的泄露会导致所有其他会话密钥的泄露。为了解决这一问题, 本文拟提出具有已知密钥安全的基于标识的零交互认证密钥协商（Identity-Based Zero-Interactive Authenticated Key Exchange, IB-ZIAKE）协议。

传统的网络环境采用“烟囱式”的架构, 各通信设备由所属的认证服务器统一认证, 由此产生了众多的认证域。然而, 随着网络环境日趋复杂，各设备之间的通信不局限于单一域, 而是多个域之间的通信。由于不同域之间的差异性较大, 使用的密码体系和系统参数各不相同。在特定的信任域中，每个域环境都有自己的用户和资源，然而，由于用户可以提出不同类型的需求，而这些需求可能不是由单个域系统提供的，因此，一个域系统不得不请求另一个域系统或多个域系统。因此，多领域协同工作，即跨领域互操作的需求不断上升。随着跨域通信需求的增加, 认证通信的安全性问题也越来越突出, 因此跨域设备间的密钥协商成为了一个亟待解决的问题。

目前存在的跨域认证密钥协商协议, 通信方大多都位于同一密码体制的不同域内通信, 例如通信双方均处于传统公钥密码（PKC）体制[22–24], 或者均处于标识体制[8, 25, 26], 或均处于无证书体制[27, 28]。针对不同体制下的跨域认证密钥协商协议, 文献[29–31] 提到了基于标识密码体制与基于证书体制的跨域认证密钥协商协议, 但目前针对基于标识密码体制与基于无证书体制跨域认证密钥协商协议研究较少, 如图1.3中 B_3 与 C_1 的通信。因此，本文拟提出基于标识与基于无证书体制下的跨域认证密钥协商协议（Cross-domain Authenticated key Exchange，CDAKE），解决了不同体制下用户跨域通信的需求。

1.2 研究贡献

本文主要针对无证书低交互密钥协商协议进行研究, 提出了已知密钥安全的基于标识的零交互认证密钥协商协议 IB-ZIAKE(如图1.4所示）和基于标识与基于无证书体制的跨域认证密钥协商协议 CDAKE（如图1.5），并改进了相关的安全模型，且在对应的安全模型下分别对所提协议进行严格安全证明，最后基于

BLS-12381 曲线实现了所提协议，并进行了性能和安全性分析。具体来说，本文的贡献如下：

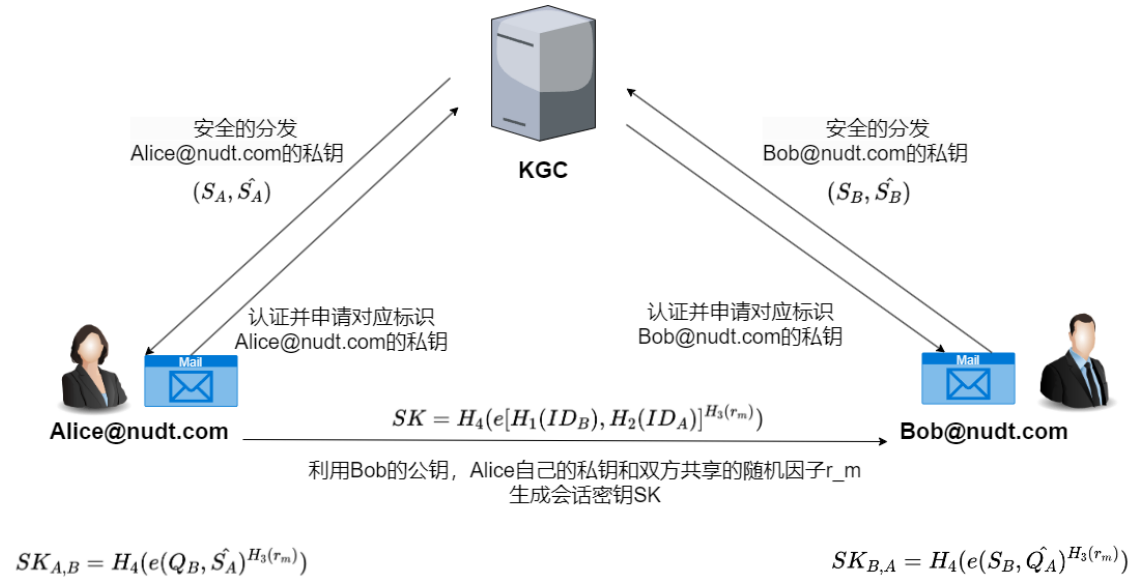

图 1.4　IB-ZIAKE 协议结构

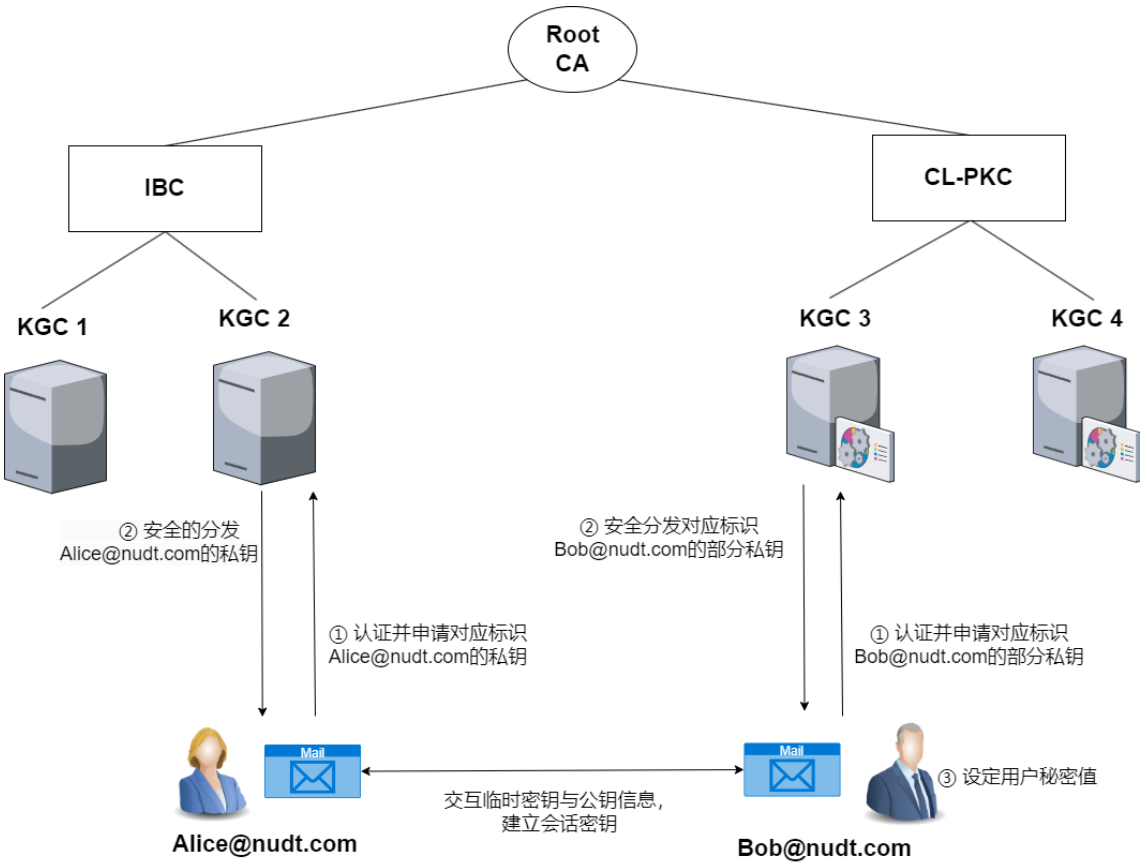

图 1.5　CDAKE 协议结构

(1) 本文定义了基于标识的 AKE 协议的已知密钥安全模型，将密钥协商协议的安全性从共享密钥的不可区分性（IND-SK）扩展到已知密钥安全。与 Kenneth 和 Srinivasan[20] 提出的安全模型相比, 已知密钥安全模型允许对手掌握所有用户过去的会话密钥。其次，本文首次提出了具有已知密钥安全的零交互密钥协商协议（Identity-Based Zero-Interactive Authenticated Key Exchange，IB-ZIAKE），通过引入每个会话独有的共享随机因子，使用单向哈希函数从双线性对计算中生成唯一的会话密钥，无需进行公钥查询、证书验证或事先交互, 能实现首次发送数据时立即开始数据传输, 而无需等待传统的往返时间。随后，基于所提出的已知密钥安全模型给出 IB-ZIAKE 协议的严格证明。最后基于 BLS-12381 曲线对比了 IB-ZIAKE 协议和原始的 SOK 协议，发现协议性能几乎没有变化，但是协议的安全性得到显著提升。

(2) 本文改进了 Lippold[1] 提出的无证书 eCK 模型, 在此安全模型下设计了首个基于标识与基于无证书体制的跨域认证密钥协商协议（Cross-Domain Authenticated key Exchange，CDAKE）。对于通信一方基于标识体制，另一方基于无证书体制，实现了跨域通信的需求。随后，基于 CDH 假设和 CBDH 假设, 对该跨域协议提供严格安全证明，证明该协议满足前向安全，抗密钥泄漏伪装安全，抗未知密钥共享安全。最后，基于 BLS-12381 曲线，在 Ubuntu 系统上实现了 CDAKE 协议。

1.3 论文结构

本文工作主要是研究无证书低交互的密钥协商协议, 通过对原始 SOK 协议的改进, 提出具有已知密钥安全的 IB-ZIAKE 协议, 并将其应用到 T-IP 协议中, 使得协议能够抵抗已知密钥攻击和重放攻击。另一方面, 随着跨域通信需求的增加, 本文提出了基于标识与基于无证书体制的跨域认证密钥协商协议 CDAKE。本文共分为五章, 如图1.6所示，各个章节的具体内容安排如下:

第1章是绪论。首先针对协议设计的初衷，阐述协议设计的研究背景与意义, 分析了当前零交互认证密钥协商协议和跨域认证密钥协商协议的不足，然后给出了本文的贡献和行文结构。

第2章为相关研究综述，首先阐述了目前无交互认证密钥协商协议和跨域认证密钥协商协议的研究现状，重点介绍了基于标识的零交互认证密钥协商协议和基于标识的跨域认证密钥协商协议，随后介绍了如何设计安全的认证密钥协商协议，最后介绍了可证明安全性理论的相关知识。

第3章介绍了具有已知密钥安全的基于标识的零交互认证密钥协商协议 IB-ZIAKE, 通过引入随机因子, 本文将原有的 IB-NIKE 协议的安全性从密钥不可区分安全拓展到了已知密钥安全, 然后将 IB-ZIAKE 协议应用到 T-IP 协议中, 使得协议

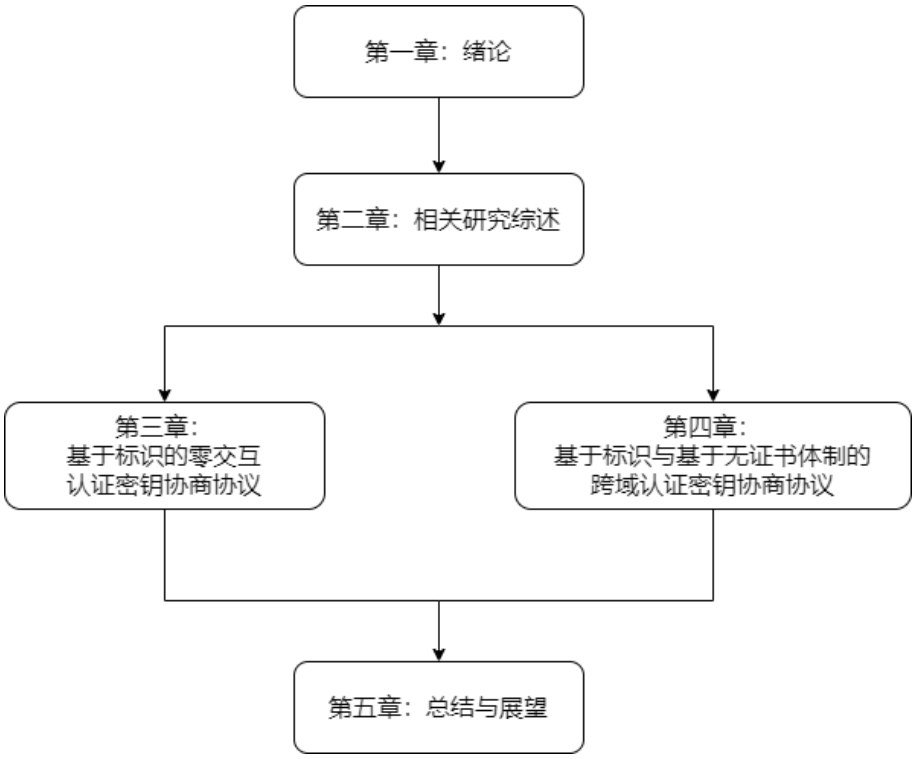

图 1.6　本文组织结构

能够抵抗已知密钥攻击和重放攻击。最后基于 BLS-12381 曲线对比了 IB-ZIAKE 协议和原始的 SOK 协议，发现协议的安全性得到显著提升的同时，对于协议性能并无明显影响。

第4章介绍了基于标识与基于无证书体制的跨域认证密钥协商协议 CDAKE, 并在改进的无证书 eCK 模型下对协议提供严格的安全证明，证明该协议满足已知密钥安全，已知会话临时信息安全，前向安全，抗密钥泄漏伪装安全，抗未知密钥共享安全。最后，基于 BLS-12381 曲线，在 Ubuntu 系统上实现了 CDAKE 协议。

第5章总结本文的主要工作, 对设计的具有已知密钥安全的基于标识的零交互密钥协商协议协议 IB-ZIAKE 和基于标识与基于无证书体制的跨域认证密钥协商协议 CDAKE 进行总结，并分析当前工作的不足，针对可以改进的对未来工作给予展望。

第二章　相关研究综述

2.1　无交互认证密钥协商协议研究

设计高效的认证密钥协商协议持续受到广泛关注和深入的研究。在 1976 年, Diffie-Hellman[3] 首次提出了公钥密码体制的密钥协商协议 Diffie-Hellman 协议 (简称为 DH 协议）, 但由于协议缺乏认证性, 容易遭受中间人攻击[32], 在传统的公钥密码体制下的解决方式是使用证书将用户信息与身份进行绑定[33], 通过数字证书对公钥进行验证, 由此出现了大量改进的 DH 协议如 MTI 协议[34]、MQV 协议[4]、HMQV 协议[5], FHMQV 协议[6] 等。

为了减少交互次数, 降低通信延迟, 大量学者针对无交互密钥协商协议进行了研究。Bernstein[35] 给出了第一个 NIKE 的安全模型。此后, Cash、Kiltz 和 Shoup [13] 对其进行了增强, 允许不诚实地生成公钥。该模型模拟了现实生活中的情况, 其中公钥是由用户发布的, 没有证书, 或者只有 (当认证机构不检查关联密钥的知识, 而仅检查公钥所有者的身份时) 弱证书。然而, Freire 等人[14] 指出了他们模型中的一些弱点, 例如敌手不能破坏诚实用户, 从而得到诚实生成的密钥或两个诚实参与方之间的共享密钥。他们提出了不诚实的密钥注册模型, 作为最强的安全模型, 并提出了一个在配对友好环境下的协议, 且证明了此协议在标准模型下是安全的。后续的研究一方面提出了更高效的 NIKE 协议[36, 37], 另一方面提出了对 NIKE 协议更紧密的规约安全[38, 39]。

然而, 上述协议隐含地依赖于证书体制, 涉及隐式公钥查询和验证, 要求参与者之间知道彼此的真实公钥。因此, 这些协议只做到了无交互密钥协商，并不能真正意义上的实现零交互认证密钥协商。只有满足无需公钥查询、无公钥验证、无事先交互的认证密钥协商协议才能称为零交互认证密钥协商协议。两方 NIKE 协议分析如表2.1所示。在表2.1中, 构造技术为该协议使用的底层密码学组件如椭圆曲线群 EC、双线性群 Pairing、二次剩余群 QR、离散对数群 TDL, 安全假设为协议是用的密码学困难问题假设, 如 Decisional Diffie-Hellman assumption, DDH 假设；Twin Diffie-Hellman assumption, Twin DH 假设；Decisional Bilinear Diffie-Hellman assumption, DBDH 假设；Decisional Diffie-Hellman assumption, DDH 假设；Computational Diffie-Hellman assumption, CDH 假设；Computational Bilinear Diffie-Hellman assumption, CBDH 假设。由表可以看出, 只有基于标识的无交互认证密钥协商协议能实现真正意义上的零交互认证密钥协商。

为了消除对证书的依赖, 人们引入了基于标识的密码学（Identity-based Cryptography, IBC)。首先, Shamir[7] 提出了一种基于标识的公钥系统, 每个用户的公钥

表 2.1　两方 NIKE 分析

协议	构造技术	安全性假设	公钥查询与验证
[3]	EC	DDH	Yes
[13]	EC	Twin DH	Yes
[14]	Pairing	DBDH	Yes
[14]	QR	Factor	Yes
[38]	EC	DDH	Yes
[20]	TDL	CDH	No
[21]	Pairing	CBDH	No
IB-ZIAKE	Pairing	CBDH	No

直接对应于其身份标识, 从而实现了对公钥的直接验证。相应的私钥由可信的密钥生成中心（KGC）通过陷门单向函数得到。2000 年, Joux [40] 首次提出将密码分析中的双线性配对整合到密钥协商协议的构建中。Dan Boneh 与 Matthew Franklin[41] 于 2001 年利用 weil 对实现了 IBE 协议的构造, 从而引发了大量双线性对密码学的研究热潮。随后, 许多利用双线性配对的协议相继被提出来 [2, 42–52]。

然而, 只有 Sakai、Ohgishi 和 Kasahara[2] 引入了基于双线性配对的初始 IB-NIKE 结构, 命名为 SOK, 使双方无需交互即可生成共享密钥，如图2.1所示。但 SOK 协议的安全性一直没有出现严格的证明, 直到 2006 年, Dupont[19] 才给出了 IB-NIKE 协议的正式安全证明。Dupont 基于随机谕言机模型, 定义了第一个无交互密钥协商协议的安全模型, 将 SOK 稍微扩展到了一般的配对环境中。随后, Kenneth[20] 参照 Dupont 的证明建立了一个更强的 IB-NIKE 安全模型, 其中允许对手除了可以获得[19] 中定义的获取用户私钥的能力外，还可以通过访问揭露会话密钥的随机谕言机，获得非挑战会话的会话密钥。在这个增强的安全模型中, Kenneth 提供了严格的安全证明, 并强调了无交互密钥协商协议无法实现某些交互式对应协议所展示的前向安全性。此外, Chen [21] 完善了来自 [20] 的安全分析, 提供了更紧密的安全规约。为了增强 IB-NIKE 协议的安全性, Steinwandt[17] 提出了一种具有前向安全的基于标识的无交互密钥协商协议, 允许用户定期更新自己的私钥, 并无交互地生成共享会话密钥。然而, Xi[18] 等人随后证明了这一协议缺乏前向安全性。

2.2　跨域认证密钥协商协议研究

协议[22, 23] 在传统的基于证书的公钥密码体制的基础上，提出了分布式认证和密钥协商协议，但两种协议都需要大量的签名。文献[53] 提出了一种新的基于标识

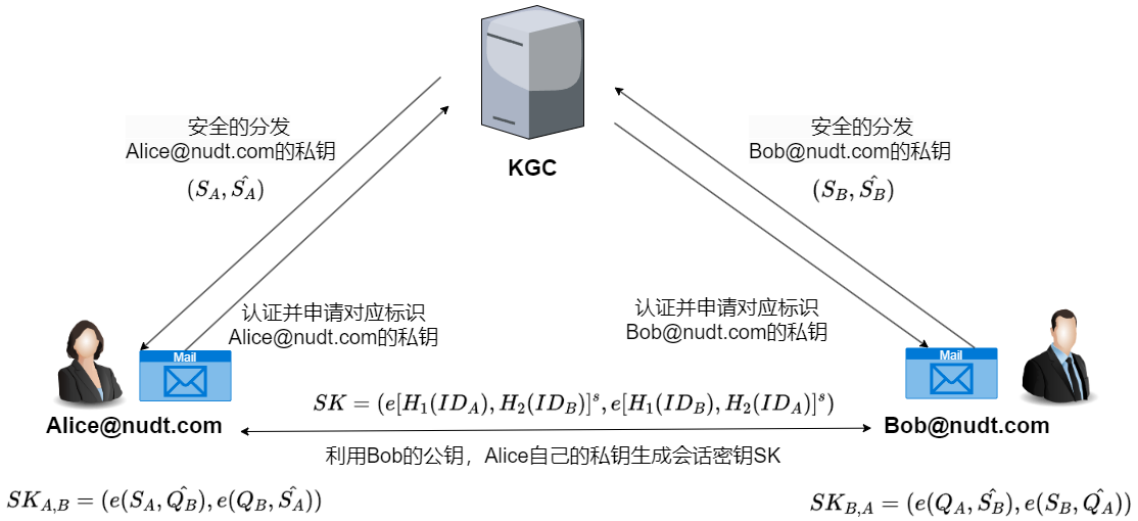

图 2.1　SOK 协议

的安全架构，以实现大规模多域无线网络中的安全通信。在该协议下，来自域 A 的用户 U 向其他域 B 请求安全通信服务时，总共需要进行 8 次消息交互。此外，U 需要与域 B 中的可信机构 TB 进行通信，TB 进一步与可信机构 TA 进行通信。因此，可信机构 TA 和 TB 很容易成为系统的瓶颈。可信机构在两个域中的参与也增加了认证延迟。He 等人[54] 改进了[53] 的协议，实现了客户端和服务器之间的分布式认证，但是该密钥协商协议需要进行大量的消息传递，导致较长的认证延迟。文献[55–59] 提出了几种跨域协议和模型。然而，它们由一个可信机构 (TA) 管理，TA 需要参与每个注册和认证过程。

公钥基础设施 (PKI) 是保障网络安全的重要实用化密码技术。在基于 PKI 的身份认证中，证书服务系统将数字证书与通信实体的公钥绑定，通信参与方可以利用证书对另一方公钥的签名实现对对方公钥的验证。Zhang 等人[60] 采用基于门限协议的椭圆曲线密码体制，借助虚拟桥 CA 模型构建企业跨域认证系统。然而，由于通过拆分密钥因子的阈值导致协议的高交互成本，使得加入和退出成员的扩展性不强。Bin [61] 对现有的证书撤销机制进行了改进，但是证书验证需要从待验证的证书到根证书进行检测，使得验证路径过长，路径验证效率较低，极大地影响了跨域身份认证技术的应用范围。Basin 等人[62] 提出了一种新的 PKI 体系结构，ARPKI ，它通过使用形式化模型来设计，以确保与证书相关的操作 (如证书的颁发、更新、撤销、验证等) 的透明性和可靠性，并有效地处理安全问题。然而，随着合法用户数量的增加，证书维护过程的计算和通信开销随之增加。跨域身份认证存在信任路径长、证书验证效率低、域间信任复杂等问题。

Wong 和 Lim [63] 以及 Chen 等人[64] 在基于标识的密码体制的基础上提出了一个基于口令的认证域间密钥协商协议。然而，它是基于两个用户在认证之前必须

共享一个密码的假设。这种假设是不切实际的。因为两个用户可能属于不同的域。当用户第一次进入一个陌生的域时，他们可能不同意同一个密码。Chen 等人[25]拓展了单域中的密钥协商协议，利用两个双线性对构造了在 IBC 体制下不同 KGC 域的跨域认证密钥协商算法（CK 算法），Lee 等人[65] 则专门针对不同 KGC 用户之间进行跨域认证密钥协商提出了 Lee 算法，并将其拓展到三方密钥协商协议。周寰[8] 针对 DK 域（相同根 KGC）和 DP 域（不同根 KGC）利用四个双线性对提出了安全性更高的跨域认证密钥协商协议，三个协议的计算开销如表2.2所示。然而，基于 KGC 的跨域认证密钥协商协议用户私钥由 KGC 生成，KGC 可以解密任意用户的信息，存在密钥托管问题，跨域通信出现用户身份多重性，使得跨域身份认证异常。

表 2.2　IBC 体制下的跨域认证密钥协商计算开销

协议	双线性对运算（次）	点乘运算（次）
Chen[25]	2	3
Lee[65]	2	4
周寰[8] DK 域	2	4
周寰[8] DP 域	2	4.5

Li[27] 等人提出的跨域认证密钥协商协议，使用了过多的对称加密，从而导致大量的计算开销。2018 年，Yang[55] 提出了一种在电子健康系统下的跨域无证书密钥协商协议。虽然它实现了动态用户管理、认证和会话密钥的安全保证，但它没有实现真正的跨域，不能抵抗 Luo[66] 等人提出的已知临时密钥攻击。2018 年，Semal 等人[67] 提出了在不可信的无人机网络中进行安全通信的无证书群组认证密钥协商协议，2020 年，Luo 等人[66] 提出了面向 5G 网络切片的跨域无证书认证群组密钥协商协议。然而，在 2022 年，Ren 等人[68] 指出 Semal 等人提出的协议不能抵抗公钥替换攻击，Luo 等人提出的协议只能抵抗公钥替换攻击。

针对跨体制的密钥协商需求，一个简单的解决方案需要每个用户维护两个体制下的静态密钥，以容纳所有的对等方通信需求，但维护多个秘钥的成本，密钥与协议的匹配，而防止不希望的干扰，可以说是不切实际的。另一种协议是用户可以使用证书链和交叉证书在不同的 CA 之间进行交互。但是因为存在多个 CA 和多个 KGC，为每个 CA 和 KGC 维护一个秘钥意味着大量的内存和维护成本。当前，很少有工作关注不同体制之间的认证密钥协商。Ustaouglu[29] 提出了针对证书体制与标识密码体制的跨体制密钥协商协议，用户只需要维护单个静态密钥对，然后可以与持有证书或基于标识的密钥的对等体进行会话密钥建立。但他们的协

议仍然要求参与者使用来自同一代数群的参数。后来，Guo 等人[30] 基于[24] 的通用构造思想（如图2.2所示），通过构造基于证书的实体的陷门单向函数 $f_Z(X)$ 和基于标识的陷门单向函数 $g_{ID}(X)$，提出了一个两方认证密钥协商协议，其中一个实体是基于证书的，另一个实体是基于标识的，并且两个实体的参数可能来自不同的代数群。同时，Guo 等人[30] 还改进了基于证书与基于标识的跨域认证密钥协商协议，提出了具有前向安全和抗临时密钥泄露安全的跨域认证密钥协商协议。[69] 定义了多个域的密钥协商协议，并在 PKI 和 IBC 域之间建立了新的身份验证通道。Yuan 等人[70] 实现了 PKI 域和 IBC 域之间的密钥协商协议，但是他们的协议仍然要求所有参与者使用来自相同密码设置的参数，仍然没有做到真正的跨域。

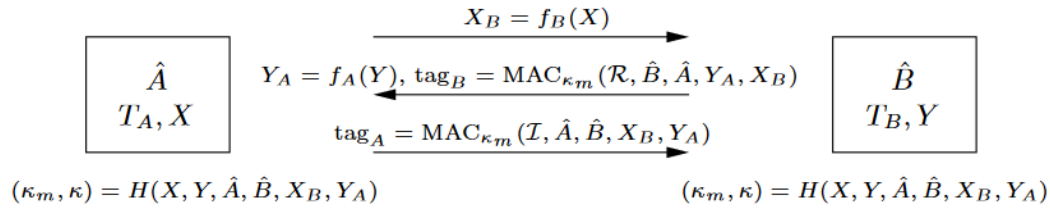

图 2.2　认证密钥协商协议的通用构造

2.3　认证密钥协商协议安全分析

2.3.1　认证密钥协商协议的设计需求

认证密钥协商协议的设计需求包括协议性能和协议安全性两个方面。认证密钥协商协议在效率方面应该尽可能地减少交互的回合数，即协议的信息交互次数尽可能少；其次通信占用带宽要尽可能小，即降低交互信息的长度；还要考虑尽可能低的计算消耗，即运算尽可能采取高效的运算操作。

在公开网络环境中运行的认证密钥协商协议应该能够同时抵抗敌手的被动攻击（攻击者只是被动监听协议）和主动攻击（攻击者可以插入、更改、删除或重放消息）在此，将敌手的主动攻击总结归纳如下：

- 已知会话密钥攻击（Known Key Attack）：针对每次会话密钥相同的密钥协商协议，敌手通过获得过去的会话密钥，获取新鲜会话密钥的攻击。

- 基本的假冒攻击（Basic Impersonation Resilience）：针对没有身份认证的协议，敌手通过假冒参与方 A 与其他合法用户进行通信。

- 密钥泄露伪装（Key Compromise Impersonation，KCI）攻击：针对不满足 KGC 前向安全的密钥协商协议，设 A 和 B 是两个正确执行协议的合法参与方，

若 A 的长期私钥被敌手获得，敌手能够冒充 A 与其它的协议参与者（例如 B）进行通信；同时，A 的长期私钥泄露，敌手能结合 KGC 私钥，使得敌手反过来在 A 面前冒充其它的参与者（例如 B）。

- 未知密钥共享（Unknown Key Share，UKS）攻击：针对没有身份认证的协议，敌手分别与参与方 A，B 协商生成一个会话密钥，令 A，B 都错误地认为该会话密钥是和对方协商得到的。

- 非密钥控制（No Key Control）：针对各协议参与者对生成的会话密钥没有做出同等贡献的协议，即没有双方都交互临时信息，未贡献临时信息的一方能提前预计算会话密钥，只要敌手掌握一方的私钥，就可以通过同样的方式获得会话密钥。

- 公钥替换攻击：针对在公钥没有验证的 AKE 中，敌手通过替换参与方的公钥信息达到攻击协议的目的。在基于数字证书的体制中，敌手可能向认证中心注册自己并不持有对应私钥的公钥，或者在基于无证书体制中直接替换用户的公钥。

2.3.2 认证密钥协商协议安全属性

根据不同的安全目标，认证密钥协商协议可以分为隐式认证、密钥确认和显示认证。隐式认证是指参与密钥协商的一方能够确保，除了指定的用户外，其他任何用户都不能获取会话密钥。密钥确认则意味着参与密钥协商的一方可以验证其他合法参与者已经获得了本次协商的会话密钥。为了实现这一安全目标，文献[5] 指出通常需要在实现隐式认证的基础上增加一次额外的通信。如果一个密钥协商协议同时实现了隐式认证和密钥确认，那么就称此协议实现了显示认证。

定义 2.1 认证密钥协商（Authenticate Key Exchange,AKE）：对于两方密钥协商，如果在两个方向上 (A 对 B，B 对 A) 都实验了隐式认证，则称此密钥协商协议为认证密钥协商协议，也称为 AK(Authenticate Key) 协议。

定义 2.2 带密钥确认的认证密钥协商协议 (Authenticate Key Exchange with Key Confirmation,AKC)：如果一个密钥协商协议同时提供双向隐式认证和双向密钥确认，则称之为带有密钥确认的认证密钥协商协议。

对于安全的两方认证密钥协商协议，参与方分别为用户 A 和用户 B，协议应至少具备以下属性：

- 已知会话密钥安全 (Known Key Security, KKS)：即使用户 A、B 之前的一些会话密钥被泄露，敌手无法根据这些泄露的会话密钥计算出当前的或者以后的会话密钥。

- 前向安全性 (Forward Security, FS): 前向安全分为部分前向安全和完美前向安全。部分前向安全是指，如果参与通信的一方的长期私钥泄露，敌手不能有效计算旧的会话密钥；完美前向安全是指如果参与密钥协商的双方的长期私钥全部泄露，敌手仍然不能有效计算旧的会话密钥。对于事先没有建立共享安全状态的一轮 (两向) 消息的 AKE 协议，不可能达到真正意义的完美前向安全。针对无证书体制，存在 KGC 前向安全的概念。KGC 前向安全是指即使敌手获得私钥生成中心 KGC 的主密钥，仍然无法计算参与双方的会话密钥。如果一个密钥协商协议满足 KGC 前向安全，则表明协议具有无会话密钥托管的特性。

- 抗私钥泄露伪装安全 (Key Compromise Impersonation, KCI)：对于协议的参与方 A,B，如果一方 (假设为 A) 的长期私钥被泄露，敌手无法模拟 B 与 A 进行通信，即一方长期私钥的泄露不会影响最终的会话密钥安全。

- 未知会话密钥共享安全 (Unknown Key Share, UKS)：参与方 A 通过身份认证，确定与他进行通信的是参与方 B，敌手无法做出干扰，令 A 误认为与自己进行通信的是参与方 C。

- 抗临时密钥泄露安全（Ephemeral Key Reveal, EKR)：临时密钥的泄露不能导致攻击者计算出会话密钥。

2.3.3 认证密钥协商安全模型

可证明安全的思想起源于 Goldwasser 和 Micali[71], 文中定义了概率加密和语义安全，随后，Bellare 和 Rogaway[72] 于 1993 年将在对称密钥协商协议中将可证明安全性理论成功应用, 提出了著名的 BR 模型, BR 模型通过允许敌手查询谕言机, 定义了敌手攻击协议的能力，并针对敌手能力定义了协议满足的安全属性。Blake-Wilson 等人[73, 74] 在 BR 模型的基础上定义了改进的安全模型, 首次将认证密钥协商安全模型拓展到非对称密码体制。2001 年, Canetti 和 Krawczyk[75] 进一步优化了安全模型, 提出著名的 CK 模型, 允许敌手进行会话状态揭露查询和腐蚀用户, 考虑了弱前向安全问题和会话相关临时密钥泄露安全问题, 但 CK 模型下安全的协议不允许会话结束前泄露长期私钥, 无法抵抗密钥泄露伪装攻击（Key Compromise Impersonation, KCI）, 也不能抵抗双方临时密钥泄露攻击。Lamacchia

等人[76] 在 2007 年提出了拓展的 eCK 模型, 将 CK 模型中的 Corrupt 查询分解为三个查询, 即长期私钥查询（Long-Term Key Reveal）, 临时密钥查询（Ephemeral Key Reveal）和会话密钥查询（Session Key Reveal）, eCK 模型能提供双方认证密钥协商协议的最强的安全定义。随后 Lippold 等人[1] 基于 eCK 模型, 提出了无证书 eCK 模型, 并指出在无证书 eCK 模型下, 对于双方认证密钥协商协议, 只要双方至少有一个未妥协的秘密, 那么协议是安全的。

2.4 可证明安全性理论

本论文设计的认证密钥协商协议的安全性都是基于某些计算复杂性困难假设的。所谓困难，或者称为计算不可行，指的是问题的解决没有有效的多项式时间算法。

可证明安全性理论是指基于数学困难问题假设，通过特定安全模型定义敌手能力，证明协议在特定安全模型可被严格证明安全的理论。其基本思想是利用数学中的反证法，通过归约的方式将密码算法的安全性规约到某个公认的数学难题上，若不存在解决困难问题的有效算法，则不存在针对密码协议攻击的有效算法。一般包括以下步骤:

（1）定义安全模型。通过模拟真实环境抽象出问题中的对象（包括协议的参与者和用户）并赋予对象相应的能力。根据敌手的攻击行为和目标，建立形式化安全模型。目前安全模型主要包括随机谕言机模型和标准模型。本文主要采用随机谕言机模型。

（2）定义安全游戏。根据协议执行的算法和敌手能力，模拟协议的执行过程，在游戏执行过程中，嵌入协议相关的困难问题，通过判断敌手赢得游戏的概率是否是可忽略的定义敌手成功的概率。

（3）困难问题归约。通过反证法，假设存在有效的算法攻击底层困难问题，从而构造具有不可忽略优势赢得游戏的敌手。最后通过底层困难问题的复杂性，反正不存在有效攻击协议的敌手，证明协议的安全性。

密码协议归纳转化的困难问题假设越弱，那么安全性更强。一个安全度高的协议一定是在最强的安全模型下基于较弱的困难性假设证明是安全的。

2.4.1 计算复杂性理论

定义 2.3 *可忽略函数 $\varepsilon(n)$。如果对于任意多项式 $p(n)$, 存在一个自然数 N, 使得对于所有 $n > N$, 都有 $\varepsilon(n) < \frac{1}{p(n)}$，则称函数 $\varepsilon(n)$ 是可忽略的。*

定义 2.4 *多项式时间算法：如果算法的运行时间可以用输入规模 n 的某个多项式函数来表示，称这个算法在多项式时间内运行，或者说这个问题可以在多项*

式时间内求解。

定义 2.5 概率多项式时间算法：概率多项式时间算法是一种在多项式时间内运行的算法，但可以访问一些提供真正随机比特的谕言机，对于输入 X，输出并不是确定的值 $y = A(X)$，而是得到一个随机变量 Y，而且 Y 有一定的概率是一组不同的值。

2.4.2 安全模型

目前，基于标识的零交互认证密钥协商协议最强的安全模型是 Kenneth[20] 提出的 ID-NIKD 模型, 本文在文献[20] 提出的安全模型的基础上，在敌手对会话揭露谕言机进行询问时，赋予了敌手额外获取过去会话密钥的能力。因此在新的安全模型下, 协议具有已知密钥安全。

在无证书体制下, 由于公钥缺乏证书的绑定, 所以根据文献[9], 攻击无证书密码体制的敌手可以分为两类：$\mathcal{A}_{\mathcal{I}}$ 和 $\mathcal{A}_{\mathcal{II}}$ 。敌手 $\mathcal{A}_{\mathcal{I}}$ 代表恶意用户, 无权获取主密钥, 但是 $\mathcal{A}_{\mathcal{I}}$ 可以将用户公钥替换为其选择的值；敌手 $\mathcal{A}_{\mathcal{II}}$ 代表恶意的 KGC, 可以获取主密钥, 并基于此主密钥计算部分私钥, 但是不能替换用户的公钥。在基于标识与基于无证书体制的跨域认证密钥协商协议中, 本文改进了文献[1] 提出的无证书 eCK 模型。使得协议在改进的无证书 eCK 模型下具有已知会话密钥安全、前向安全、抗临时密钥泄露安全、抗未知密钥共享安全等属性。

2.5 小结

本章通过分析当前无交互认证密钥协商协议和跨域认证密钥协商协议的不足，指出本文工作的必要性。此外，本章定义了认证密钥协商协议的设计需求和对应的安全性，为后文设计认证密钥协商协议提供参考。同时简要概述了后文对认证密钥协商协议进行证明采取的是拓展的 ID-NIKD 模型和改进的无证书 eCK 模型。

第三章　基于标识的零交互认证密钥协商

基于标识的无交互密钥协商（IB-NIKE）是基于标识的密码学中一个强大的原语。然而, 现有的 IB-NIKE 协议不满足已知密钥安全性。一个会话密钥的泄露将导致损害所有其他会话密钥。本章首先定义了 IB-NIKE 的已知密钥安全模型, 将密钥协商协议的安全性从共享密钥不可区分性（Indistinguishability of Shared Key (IND-SK)) 扩展到已知密钥安全。然后提出了第一个具有已知密钥安全的 IB-NIKE 协议, 称为基于标识的零交互认证密钥协商（IB-ZIAKE）协议。通过引入每个会话特有的共享随机因子, IB-ZIAKE 使用单向哈希函数从双线性对计算生成唯一的会话密钥。在提出的已知密钥安全模型下, 本文给出了 IB-ZIAKE 安全性的形式证明。此外, 本文还演示了 IB-ZIAKE 协议在自信任和安全的互联网协议（T-IP）中的应用, 展示了它如何有效地减轻已知密钥攻击和重放攻击。

3.1　预备知识

3.1.1　双线性对

双线性对是一个映射，将两个具有相同阶数的加法群 $(\mathbb{G}_1, +)$ 和 $(\mathbb{G}_2, +)$ 映射到一个乘法群 $(\mathbb{G}_T, \times)$，两个群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 在映射中都能保持线性即为双线性，形式化定义如下:

若存在映射：$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$，对于 $\forall P_1, P_2 \in \mathbb{G}_1$，$\forall Q_1, Q_2 \in \mathbb{G}_2$，满足:

$$\hat{e}(P_1 + P_2, Q_1) = \hat{e}(P_1, Q_1) \cdot \hat{e}(P_2, Q_1) \tag{3.1}$$

$$\hat{e}(P_1, Q_1 + Q_2) = \hat{e}(P_1, Q_1) \cdot \hat{e}(P_1, Q_2) \tag{3.2}$$

则称映射 $\hat{e}$ 为 $\mathbb{G}_1 \times \mathbb{G}_2$ 到 $\mathbb{G}_T$ 的一个双线性对。双线性映射 $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ 还应该满足以下属性:

1) 双线性：$\forall P \in \mathbb{G}_1, \forall Q \in \mathbb{G}_2$, 对于整数 s，有 $\hat{e}(nP, Q) = \hat{e}(P, nQ) = \hat{e}(P, Q)^s$

2) 非退化性: $\forall P \in \mathbb{G}_1$ 且 P 不是 $\mathbb{G}_1$ 的零元，$\exists Q \in \mathbb{G}_2$，使得 $\hat{e}(P, Q)$ 不为 $\mathbb{G}_T$ 的单位元。同样地，$\forall Q \in \mathbb{G}_2$ 且 Q 不是 $\mathbb{G}_2$ 的零元，$\exists P \in \mathbb{G}_1$，使得 $\hat{e}(P, Q)$ 不为 $\mathbb{G}_T$ 的单位元。

3）可计算性：$\forall P \in \mathbb{G}_1$，$\forall Q \in \mathbb{G}_2$，$\hat{e}(P, Q)$ 可在多项式时间内完成计算。

值得注意的是本文在下列提出的协议中选取的 $\mathbb{G}_1$ 群和群 $\mathbb{G}_2$ 群的生成元分别为 P_1 和 P_2，存在 $\mathbb{G}_2$ 到 $\mathbb{G}_1$ 的同构映射 ψ，即满足 $\psi(P_2) = P_1$，更详细的解释可参考文献[77]。

3.1.2 配对友好曲线

密码学中的椭圆曲线通过对椭圆曲线弧长的积分引入的，通常情况下是用 Weierstrass 方程描述的平面曲线，一般用 E 表示。

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a^4x + a^6 \tag{3.3}$$

通过仿射变换，可以将椭圆曲线化简为 $E: y^2 = x^3 + ax + b$，且为了保证曲线没有奇异点，即处处光滑可导，其判别式必须不等于 0，即 $\Delta = 4a^3 + 27b^2 \neq 0$，椭圆曲线上的点用坐标 (x, y) 表示，完整的椭圆曲线公式为：

$$E = \{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b, \Delta = 4a^3 + 27b^2 \neq 0\} \cup \{0\} \tag{3.4}$$

根据不同从参数选择，可以得到不同表现形式的椭圆曲线，如图3.1所示：

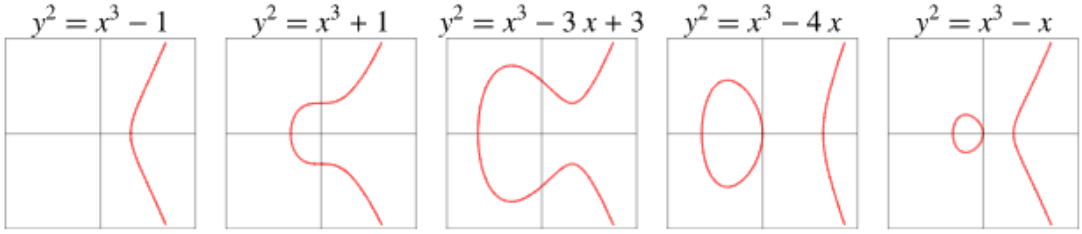

图 3.1 椭圆曲线表现形式

椭圆曲线的选择对实现双线性对的效率具有较大影响，双线性配对曲线不能随机选取，而是要通过特殊的构造方式构造的特定曲线，即需要找到一些具有较大素数阶（r）子群、较小嵌入度 (k) 的椭圆曲线，具体定义如下：

定义 3.1 *E 为定义在有限域 $\mathbb{F}_q$ 上的椭圆曲线，当 E 满足：*

（1）存在素数 $r \geq \sqrt{q}$，并且满足 $r \# E(\mathbb{F}_q)$；

（2）与 r 对应的 E 的嵌入次数 $k \leq log_2(r)/8$。

则称椭圆曲线 E 是配对友好型曲线，令 $\rho(E) = \frac{log\ q}{log\ r}$，配对友好型曲线满足 $\rho \leq 2$，ρ 越接近 1 越好。配对友好曲线能够提高曲线的安全水平，同时曲线的嵌入度较低，有利于加速双线性对的运算。

普通的配对友好的椭圆曲线有两种形式，一种是属于曲线族的，另一种则是非族曲线。对于非族曲线，每次计算参数 p、r、k 和 t 时都需要分别进行。对于固定的 k 值，曲线族中的配对友好椭圆曲线的 p、r 和 t 由单变量多项式 $p(u)$、$r(u)$ 和 $t(u)$ 来确定。目前，大多数构造配对友好曲线的方法均是基于复乘（CM）[78]

去构造基于素数域的椭圆曲线。CM 方法是输入整数 n 和素数 p，在 $\mathbb{F}_q$ 上构造一个阶为 n 的椭圆曲线 E，基本思想是求解 CM 方程：

$$Dy^2(u) = 4q^2(u) - t^2(u) \tag{3.5}$$

其中 $q(u) = p(u)^d$，$d \geq 1$，$p(u)$ 代表素数，$t(u)$ 素数。相关参数的详细解释可参考[79]。Freeman [79] 对近些年配对友好曲线做了详细的综述，目前应用（NIST 或者国密算法 SM9）较为广泛的配对友好曲线主要有 BLS 曲线[80] BN 曲线[81]，和 KSS 曲线[82]。本文后续对于协议的实现主要是基于 BLS 曲线，下面主要针对 BLS 曲线进行介绍。

BLS 曲线采用 $y^2 = x^3 + b$ 的形式，曲线参数 p，r，t，定义在一个参数化的素域 $\mathbb{F}_q$ 上。对于双线性映射，需要构造取自相同阶 q 的群 $\mathbb{G}_1$，$\mathbb{G}_2$，域 $\mathbb{F}_q$ 内包含 $\mathbb{G}_1$ 群，而域 $\mathbb{F}_q$ 的扩张域 $\mathbb{F}_{q^k}$ 内包含 $\mathbb{G}_2$ 群，BLS 曲线上的配对定义在 q 阶的扭转子群。BLS 曲线的阶可被一个很大的参数化的素数整除, 但曲线的阶不是素数。上，目前针对 BLS 曲线，研究的最多的是嵌入度为 12 和 24 的曲线，即 BLS12 和 BLS24，具体参数如下所示：

BLS12：

$$\begin{aligned} p(u) &= (u-1)^2(u^4 - u^2 + 1)/3 + u \\ r(u) &= u^4 - u^2 + 1 \\ t(u) &= u + 1 \end{aligned}$$

BLS24：

$$\begin{aligned} p(u) &= (u-1)^2(u^8 - u^4 + 1)/3 + u \\ r(u) &= u^8 - u^4 + 1 \\ t(u) &= u + 1 \end{aligned}$$

本文设计的认证密钥协商协议的实现采取的是 BLS12-381 曲线，即采取嵌入度为 12，并且具有 6 阶的扭转，域的模为 381 位素数，子群大小为 255 位素数的 BLS 曲线。BLS12-381 为 BLS 曲线族的成员之一，381 为表示曲线上坐标所需的 bit 位数，是一个很方便的数字，每个域元素可用 48 字节表示，剩余的 3 个 bit 可用作标签或计算优化。

对于 BLS12-381 的曲线，双线性映射就是在两个非对称群上任意选择点 $P \in \mathbb{G}_1 \subset \mathbb{F}_q$ 和点 $Q \in \mathbb{G}_2 \subset \mathbb{F}_{q^2}$，并输出群 $\mathbb{G}_T \subset \mathbb{F}_{q^{12}}$ 中的一个点，即 $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$。

3.1.3 困难问题假设

CBDH(Computational Bilinear Diffie-Hellman) 问题：设 P_1 为循环群 $\mathbb{G}_1$ 的生成元, P_2 为循环群 $\mathbb{G}_2$ 的生成元，存在同构映射 ψ，满足 $P_1 = \psi(P_2)$，随机选择整数 $x, y, z \in_R \mathbb{Z}_N^*$，存在双线性 $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$，给定 $(P_1, P_2, xP_2, yP_2, zP_2)$，求解 $\hat{e}(P_1, P_2)^{xyz}$。假设存在算法 $\mathcal{A}$ 以优势 ϵ 解决 CBDH 问题，$Pr[\mathcal{A}(P_1, P_2, xP_2, yP_2, zP_2) = \hat{e}(P_1, P_2)^{xyz}] = \epsilon$，若 ϵ 是可忽略的，则称 BDH 问题是困难的。

DBDH (Decisional Bilinear Diffie-Hellman) 问题：设 P_1 为循环群 $\mathbb{G}_1$ 的生成元, P_2 为循环群 $\mathbb{G}_2$ 的生成元，随机选择整数 $x, y, z \in_R \mathbb{Z}_N^*$，存在双线性 $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$，给定 $(P_1, P_2, xP_2, yP_2, zP_2)$，判定 $\hat{e}(P_1, P_2)^{xyz} = \hat{e}(P_1, P_2)^d$ 是否成立。假设存在算法 $\mathcal{A}$ 以优势 ϵ 解决 DBDH 问题，$Pr[\mathcal{A}(\hat{e}(P_1, P_2)^d) = \hat{e}(P_1, P_2)^{xyz} | P_1, P_2, xP_2, yP_2, zP_2] = \epsilon$，若 ϵ 是可忽略的，则称 DBDH 问题是困难的。

GBDH（Gap-Bilinear Diffie-Hellman）问题: 设 P_1 为循环群 $\mathbb{G}_1$ 的生成元, P_2 为循环群 $\mathbb{G}_2$ 的生成元，随机选择整数 $x, y, z \in_R \mathbb{Z}_N^*$，存在双线性 $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$，给定 $(P_1, P_2, xP_2, yP_2, zP_2)$ 和 DBDH 谕言机，求解 $Pr[\mathcal{A}(\hat{e}(P_1, P_2)^{xyz}] = \epsilon$，若 ϵ 是可忽略的，则称 GBDH 问题是困难的。

3.2 安全模型

在本节提出一个新的安全模型, 用于对基于标识的零交互密钥协商协议的研究。首先简要介绍了具有已知密钥安全的零交互认证密钥协商协议 IB-ZIAKE, 在原有的 ID-NIKD 模型下证明了此协议满足密钥不可区分安全。随后本文改进了原有的 ID-NIKD 模型, 将密钥协商协议的安全性从共享密钥不可区分性（IND-SK）扩展到已知密钥安全（Known-Key Security，KKS）, 并在此安全模型下证明了 IB-ZIAKE 满足已知密钥安全。

IB-ZIAKE 协议由以下三个算法组成：启动算法（Setup）, 私钥提取算法（Extract）, 共享密钥计算算法（SharedKey）。

Setup (κ)：选取一个安全参数 κ 并生成系统参数 $params$ 和系统主密钥 msk, msk 由 KGC 秘密保留。

Extract $(params, ID_i, msk)$：输入 $params$, msk 和用户 i 的身份标识 ID_i, 返回用户私钥 d_i 。

SharedKey(d_i**,** ID_j**,** r_m**)**：输入用户 ID_i 的私钥 d_i, 用户 j 的身份标识 ID_j 和随机因子 r_m, 其中 $ID_i \neq ID_j$, 输出会话密钥 $sk_{i,j}^{r_m}$ 。 .

3.2.1 共享密钥不可区分安全

下面通过描述挑战者 $\mathcal{C}$ 与敌手 $\mathcal{A}$ 之间的游戏（Game）定义本文提出的 IB-ZIAKE 协议具有共享密钥不可区分安全（Indistinguishability of Shared Key (IND-SK)）。

- Setup(κ)：挑战者首先输入安全参数 κ, 生成系统参数 $params$ 并秘密保留主密钥 msk。

- Phase 1：敌手可以自适应地执行下列查询：

  StaticKeyReveal (ID_i)：接收到该询问后, 挑战者返回 ID_i 的私钥 d_i 。

  SessionKeyReveal (ID_i, ID_j, r_m)：接收到该询问后, 挑战者返回相关的会话密钥 $sk_{i,j}^{r_m}$ 。

- Challenge (ID_I, ID_J, r_M)：一旦敌手决定 $Phase$ 1 结束。它会选择两个用户 (ID_I, ID_J) 和一个随机因子 r_M, 询问相关的会话密钥，要求 $Phase$ 1 中没有出现针对挑战 ID 的密钥询问，即没有出现 StaticKeyReveal (ID_I) , StaticKeyReveal(ID_J)，也没有出现针对挑战 ID 双方的会话密钥的询问，即在 SessionKeyReveal (ID_i, ID_j, r_m) 中，$\{ID_i, ID_j\} \neq \{ID_I, ID_J\}$。此时挑战者随机掷出一个无偏的硬币 b, 如果 $b = 0$, 则挑战者从会话密钥的分布域 $\{0, 1\}$ 中随机选择一个值返回给敌手, 如果 $b = 1$, 则返回真实的会话密钥 $sk_{I,J}^{r_M}$ 给敌手。

- Phase 2：敌手可以重复执行 $Phase$ 1, 但是同样要保证没有出现 StaticKeyReveal (ID_I) , StaticKeyReveal(ID_J)，在 SessionKeyReveal (ID_i, ID_j, r_m) 中，$\{ID_i, ID_j\} \neq \{ID_I, ID_J\}$，如果不满足条件则终止游戏。

- Guess：当敌手决定阶段 2 结束后, 敌手输出猜测 $b' \in \{0, 1\}$, 如果 $b' = b$, 则敌手赢得游戏。敌手赢得游戏的优势被定义为：

$$Adv_{\mathcal{A}}^{IND-SK}(\kappa) = |Pr(b' = b) - \frac{1}{2}| \tag{3.6}$$

定义 3.2 *如果对于任意多项式有界的敌手 $\mathcal{A}$, 函数 $Adv_{\mathcal{A}}^{IND-SK}(\kappa)$ 是可忽略的, 则协议具有共享密钥不可区分安全。*

3.2.2 已知密钥安全

下面通过描述挑战者 $\mathcal{C}$ 与敌手 $\mathcal{B}$ 之间的游戏（Game）定义本文提出的 IB-ZIAKE 协议具有已知密钥安全（Known-Key Security（KKS））。

- Setup(κ)：挑战者首先输入安全参数 κ, 生成系统参数 $params$ 并秘密保留主密钥 msk, 同时挑战者掌握所有过去会话的会话密钥。

- Phase 1：敌手可以自适应地执行下列查询：

  StaticKeyReveal (ID_i)：接收到该询问后, 挑战者返回 ID_i 的私钥 d_i 。

  SessionKeyReveal (ID_i, ID_j, r_m)：接收到该询问后, 挑战者返回相关的会话密钥 $sk_{i,j}^{r_m}$ 。

- Challenge (ID_I, ID_J, r_M)：一旦敌手决定 $Phase$ 1 结束。它会选择两个用户 ID_I，ID_J 和一个随机因子 r_M, 询问相关的会话密钥，要求 $Phase$ 1 中没有出现针对挑战 ID 的密钥询问，即没有出现 StaticKeyReveal (ID_I)，StaticKeyReveal(ID_J)，也没有出现针对挑战会话的会话密钥的询问，即没有出现 SessionKeyReveal (ID_I, ID_J, r_M)。此时挑战者随机掷出一个无偏的硬币 b。如果 $b = 0$, 则挑战者从会话密钥的分布域 $\{0, 1\}$ 中随机选择一个值返回给敌手, 如果 $b = 1$, 则返回真实的会话密钥 $sk_{I,J}^{r_M}$ 给敌手。

- Phase 2：敌手可以重复执行 $Phase$ 1, 但是要保证 ID_I 和 ID_J 不能出现在 $StaticKeyReveal$ 查询中, (ID_I, ID_J, r_M) 不能出现在 $SessionKeyReveal$ 查询中，如果不满足条件则终止游戏。但是只要 $r_m \neq r_M$, 敌手就可以发起针对目标用户的 $SessionKeyReveal$ (ID_I, ID_J, r_m) 询问。

- Guess：当敌手决定阶段 2 结束后, 敌手输出猜测 $b' = 1$, 如果 $b' = b$, 则敌手赢得游戏。敌手赢得游戏的优势被定义为：

$$Adv_{\mathcal{B}}^{KKS}(\kappa) = |Pr[\mathcal{B} \rightarrow 1] - \frac{1}{2} \tag{3.7}$$

定义 3.3 *如果对于任意多项式有界的敌手 $\mathcal{B}$, 函数 $Adv_{\mathcal{B}}^{KKS}(\kappa)$ 是可忽略的, 则协议具有已知密钥安全。*

3.3 协议设计

3.3.1 生成共享随机因子

随机因子的获取应结合通信本身设定作用阈值。目前，在零交互的情况下通信双方共享随机因子的实现方式主要有两类，一类是基于通信双方消息流提取流共有的独特随机因子，例如使用 IP 报文头中的分段标识，另一类是提取本地时间作为随机因子。网络报文在传输过程中受限于最大传输单元（Maximum

Transmission Unit，MTU)，需要将报文分段发送，分段生成的每个 IP 报文都会携带对应的分段标识，而报文传输过程要求分段标识不会改变，以便于接收方根据分段标识重组报文，因此可以将报文的分段标识作为随机因子 r_m。另一个可行的方案是提取本地时间作为随机因子 r_m。新用户在接入通信系统时都需要进行时钟同步，通过设定适宜的时间窗口使得通信双方在发送消息和接收消息处于相同的时间窗口内，利用相同的时间窗口，通信双方能获得相同的时间，实现零交互的情况下生成共享随机因子。进一步利用哈希函数将随机因子 r_m 映射到 $\mathbb{Z}_q$ 域，增强随机性。本文后续实验采用的是提取本地时间时间作为共享随机因子。

3.3.2 协议描述

本节给出一个基于标识的具有已知密钥安全的零交互密钥协商协议 IB-ZIAKE, 通信双方可以在不进行交互的情况下协商出会话密钥, 能实现首次发送数据时立即开始数据传输, 而无需等待传统的往返时间（0-RTT)。系统初始化如图3.2所示，密钥协商过程如图3.3所示。协议具体过程如下所示:

Setup (κ)：输入安全参数 κ, KGC 选择 q 阶加法循环群 $\mathbb{G}_1$, $\mathbb{G}_2$ 和乘法循环群 $\mathbb{G}_T$, P_1, P_2 分别是 $\mathbb{G}_1$, $\mathbb{G}_2$ 的生成元。存在双线性映射 $\hat{e}:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$, 随机选择 $s\in_R\mathbb{Z}_q^*$, 计算 $P_{pub_1}=sP_1$, $P_{pub_2}=sP_2$。选择哈希函数 $H_1:\{0,1\}^*\to\mathbb{G}_1$, $H_2:\{0,1\}^*\to\mathbb{G}_2$, $H_3:\{0,1\}^*\to\{0,1\}^N$, N 为密钥长度, $H_4:\mathbb{G}_T\to\{0,1\}^*$, 输出系统参数 $params=(P_1,P_2,P_{pub1},P_{pub2},H_1,H_2,H_3,H_4)$, 并秘密保留系统主密钥 s。

Extract $(params,s,ID_i)$：输入系统参数 $params$, 主密钥 s 和用户身份标识 ID_i, 计算用户私钥 $d_{i_1}=sH_1(ID_i)$ 和 $d_{i_2}=sH_2(ID_i)$。

SharedKey (d_{i_2},ID_j,r_m)：对于用户 i 作为会话发起方, 用户 j 作为会话接收方, 输入 $params$, 私钥 d_{i_2}, 用户 j 的身份标识 ID_j 和随机因子 r_m, 计算会话密钥 $sk_{i,j}^{r_m}=H_4[\hat{e}(H_1(ID_j),d_{i_2})^{H_3(r_m)}]$。对于用户 j 来说, 利用私钥 d_{j_1}, 用户 i 的身份标识 ID_i 和随机因子 r_m, 计算会话密钥 $sk_{j,i}^{r_m}=H_4[\hat{e}(d_{j_1},H_2(ID_i))^{H_3(r_m)}]$。

正确性验证。下面分别从发送方 A 与接收方 B 的角度验证会话密钥的正确性。

$$\begin{aligned}
sk_{A,B}^{r_m} &= H_4[\hat{e}(H_1(ID_B),d_{A_2})^{H_3(r_m)}]\\
&= H_4[\hat{e}(H_1(ID_B),sH_2(ID_A))^{H_3^{(r_m)}}]\\
&= H_4[\hat{e}(H_1(ID_B),H_2(ID_A))^{sH_3^{(r_m)}}]\\
&= H_4[\hat{e}(sH_1(ID_B),H_2(ID_A))^{H_3^{(r_m)}}]\\
&= H_4[\hat{e}(d_{B_1},H_2(ID_A))^{H_3(r_m)}]\\
&= sk_{B,A}^{r_m}
\end{aligned}$$

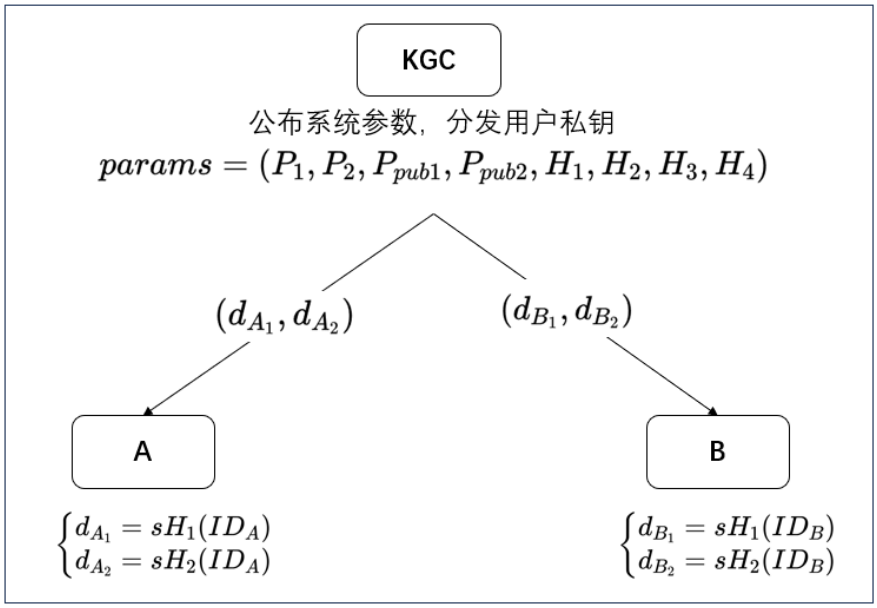

图 3.2　IB-ZIAKE 协议系统初始化

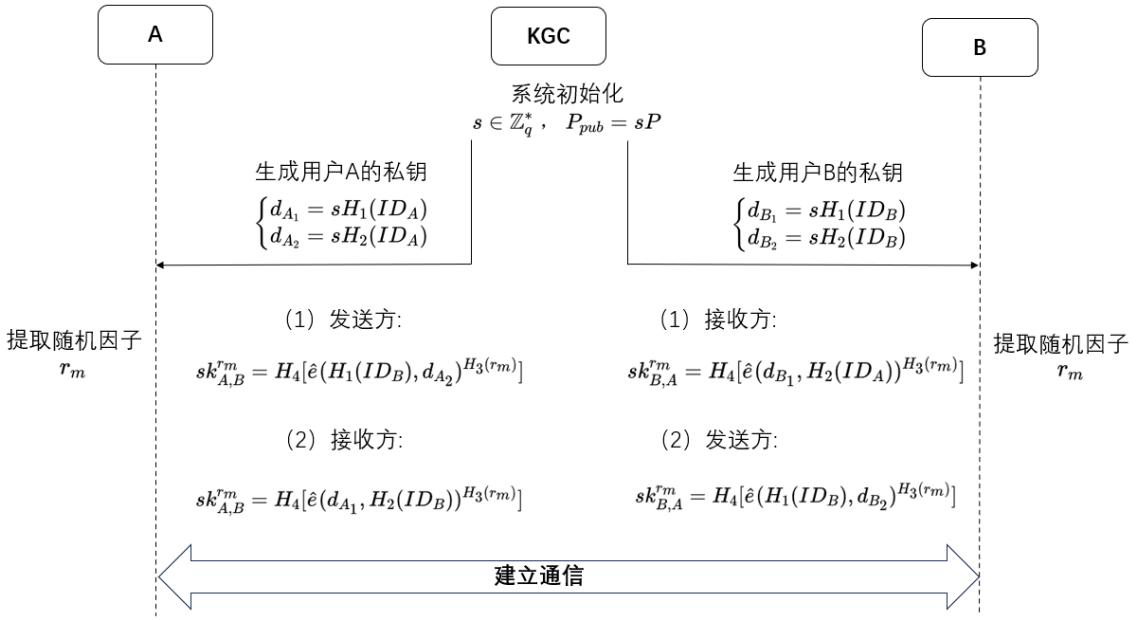

图 3.3　IB-ZIAKE 协议密钥协商示意图

3.3.3　安全证明

定理 3.1　如果 CBDH 假设成立, H_1, H_2, H_3, H_4 是随机谕言机, 那么 IB-ZIAKE 协议在随机谕言机模型下是 IND-SK 安全的。

假设任意多项式有界的敌手 $\mathcal{A}$ 能够以 $Adv_{\mathcal{A}}^{IND-SK}(\kappa)$ 的优势攻破 IB-ZIAKE 协议, 假设 $\mathcal{A}$ 最多进行 q_e 次 $StaticKeyReveal$ 查询, q_r 次 $SessionKeyReveal$ 查询,

q_f 次对 H_3 的查询, q_g 次对 H_4 的查询, 存在算法 $\mathcal{C}$ 能够至少以下列的优势解决 CBDH 困难问题:

$$Adv_{\mathcal{B}}^{CBDH}(\kappa) \geq Adv_{\mathcal{A}}^{IND-SK}(\kappa)\frac{4}{(q_e+q_r)^2 q_f q_g}\cdot(1-\frac{2}{q_e+q_r+2})^{(q_e+q_r+2)}$$

证明： 给定 CBDH 问题实例 $(P_1, P_2, xP_2, yP_2, zP_2)$, 其中 $P_1 \in \mathbb{G}_1$，$(P_2, xP_2, yP_2, zP_2) \in \mathbb{G}_2$，在3.1.1中提到 $\mathbb{G}_1$ 群与 $\mathbb{G}_2$ 群存在同构映射 ψ，$P_1 = \psi(P_2)$，$Adv_{\mathcal{B}}^{CBDH}(\kappa)$ 为挑战者 $\mathcal{C}$ 利用 $\mathcal{A}$ 解决 CBDH 问题的优势, $\mathcal{C}$ 与 $\mathcal{A}$ 的交互如下:

- Setup: $\mathcal{C}$ 运行启动算法, 生成系统参数 $params = (P_1, P_2, P_{pub1}, P_{pub2}, H_1, H_2, H_3, H_4)$ 和系统主密钥 $msk = x$ ($\mathcal{C}$ 不知道 x 的具体值), 其中 $P_{pub_1} = \psi(P_{pub_2})$, 将 H_1, H_2, H_3, H_4 建模为随机谕言机，给 $\mathcal{A}$ 返回 $params$。

- 随机谕言机询问: 为了处理随机谕言机询问, 挑战者维护四个相关的列表 $L_{H_1}, L_{H_2}, L_{H_3}, L_{H_4}$, 四个列表初始化为空。

  H_1 **谕言机：** 在表 L_{H_1} 中的每个条目的形式为 $(ID_i, mark, coin, t_i, pk_i)$, 其中 $ID_i \in I, mark, coin \in \{0,1\}, t_i \in \mathbb{Z}_q^*, pk_i \in \mathbb{G}_1$.。当敌手对 $< ID_i >$ 进行 H_1 询问时, 如果表中已经定义过了这个条目, 则挑战者返回相关的值 pk_i, 否则借助 H_2 谕言机, 对 ID_i 进行 H_2 询问, 得到相应的条目 $(ID_i^*, mark, coin, t_i, pk_i^*)$, 再通过同构映射将表 L_{H_2} 中 $\mathbb{G}_2$ 群上的元素转换为 $\mathbb{G}_1$ 群上的元素, $pk_i = \psi(pk_i^*)$, 然后将条目 $(ID_i, mark, coin, t_i, pk_i)$ 插入到表 L_{H_1} 中。

  H_2 **谕言机：** 在表 L_{H_2} 中的每个条目的形式为 $(ID_i, mark, coin, t_i, pk_i)$, 其中 $ID_i \in I, mark, coin \in \{0,1\}, t_i \in \mathbb{Z}_q^*, pk_i \in \mathbb{G}_2$.。当敌手对 $< ID_i >$ 进行 H_2 询问时, 如果表中已经定义过了这个条目, 则挑战者返回相关的值 pk_i, 否则随机选择 $t_i \in_R \mathbb{Z}_q^*$, 按照如下方式更新条目信息:

  - 以 $1-\delta$ 的概率设定 $mark = 1$, 然后随机投掷一个无偏的硬币 $coin$, 如果 $coin = 0$, 计算 $pk_i = t_i yP_2$, 如果 $coin = 1$, 计算 $pk_i = t_i zP_2$, 然后将条目 $(ID_i, mark, coin, t_i, pk_i)$ 插入到表 L_{H_2} 中。
  - 以 δ 的概率设定 $mark = 0$, 设定 $coin = \perp$, $\perp$ 代表未定义, 计算 $pk_i = t_i P_2$, 然后将条目 $(ID_i, mark, coin, t_i, pk_i)$ 插入到表 L_{H_2} 中。

  令 $P : I \to \{0,1\}$ 是一个谓词, 并且 $mark = 1$ 时, $P(ID) = 1$, $mark = 0$ 时, $P(ID) = 0$。

  H_3 **谕言机：** 在表 L_{H_3} 中的每个条目的形式为 (r_m, f_i), 其中 $r_m \in \{0,1\}^*$, $f_i \in \{0,1\}^N$。当敌手对 $< r_m >$ 进行 H_3 询问时, 如果表中已经定义过了这

个条目, 则挑战者返回相关的值 f_i, 否则随机选择 $f_i \in_R \{0,1\}^N$, 并将条目 (r_m, f_i) 插入到表 L_{H_3} 中。

H_4 **谕言机：** 在表 L_{H_4} 中的每个条目的形式为 (k, shk), 其中 $k \in \mathbb{G}_T$, $shk \in \{0,1\}^N$ 。当敌手对 $< k >$ 进行 H_4 询问时, 如果表中已经定义过了这个条目, 则挑战者返回相关的值 shk, 否则随机选择 $shk \in_R \mathbb{Z}_q^*$, 并将条目 (k, shk) 插入到表 L_{H_4} 中。

- Phase 1: $\mathcal{A}$ 能发起下列询问:

  StaticKeyReveal (ID_i) **：** 接收到该询问后, 挑战者查询列表 L_{H_2}, 得到对应的条目 $(ID_i, mark, coin, t_i, pk_i)$, 如果 $P(ID_i) = 0$, 计算 $d_i = t_i x P_2$ 。

  SessionKeyReveal $(ID_i, ID_j.r_m)$ **：** 挑战者维护会话密钥的列表 L_{sk}, 在 L_{sk} 中的每个条目的形式为 $(ID_i, ID_j, r_m, sk_{i,j}^{r_m})$, 如果表中已经定义过了这个条目, 则挑战者返回相关的值 $sk_{i,j}^{r_m}$, 否则, 如果 $P(ID_i) = 0 \vee P(ID_j) = 0$, 挑战者选择其中 $mark = 0$ 的任意一个用户（假设为用户 ID_i ）并利用 $Extract$ 算法查询其对应的私钥 d_i, 然后利用 $SharedKey$ 算法计算会话密钥 $sk_{i,j}^{r_m}$, 然后将条目 $(ID_i, ID_j, r_m, sk_{i,j}^{r_m})$ 插入到表 L_{sk} 中, 并将 $sk_{i,j}^{r_m}$ 返回给敌手。如果 $P(ID_i) = 1 \wedge P(ID_j) = 1$, 则挑战者终止游戏。

- Challenge: 敌手选择两个用户 ID_I, ID_J 和随机因子 r_M, 但是要求 ID_I 和 ID_J 不能出现在 $StaticKeyReveal$ 查询中, 而且不能出现针对目标用户 ID_I 和 ID_J 的会话密钥查询, 即对于任意的随机因子 r_m, (ID_I, ID_J, r_m) 不能出现在 $SessionKeyReveal$ 查询中。令 $(t_I, coin_I)$ 为表 L_{H_1} 中与 ID_I 相关的值 $(t_J, coin_J)$ 是表 L_{H_2} 与 ID_J 相关的值。如果 $P(ID_i) = 1 \wedge P(ID_j) = 1 \wedge coin_a \neq coin_b \wedge r_m = r_M$, 此时挑战者随机掷出一个无偏的硬币 b, 如果 $b = 0$, 则挑战者从会话密钥的分布域 $\{0,1\}$ 中随机选择一个值返回给敌手, 如果 $b = 1$, 则返回真实的会话密钥 $sk_{I,J}^{r_M}$ 给敌手, 否则挑战者终止游戏。

- Phase 2: 敌手可以重复执行 Phase 1, 但是要求 ID_I 和 ID_J 不能出现在 $StaticKeyReveal$ 查询中, 而且不能出现针对目标用户 ID_I 和 ID_J 的会话密钥查询, 即对于任意的随机因子 r_m, (ID_I, ID_J, r_m) 不能出现在 $SessionKeyReveal$ 查询中。

- Guess: 敌手输出他的猜测 b' 。

在游戏结束后, 挑战者从列表 L_{H_4} 中找到含有正确 $k_{I,J}^{r_M}$ 的相应条目, $k_{I,J}^{r_M} = e(t_I y P_2, t_J z P_2)^{x f_M}$, 则 $(k_{I,J}^{r_M})^{t_I^{-1} t_J^{-1} f_M^{-1}}$ 是 CBDH 困难问题的解。通过上面的游戏可

以看出, 只要游戏过程中挑战者没有终止游戏, 从敌手 $\mathcal{A}$ 的角度来看, 游戏过程与真实的 IB-ZIAKE 协议是一致的。假设敌手最多进行 q_g 次对 H_4 谕言机的查询, 令 F 代表挑战者 $\mathcal{C}$ 不会终止游戏的事件, $Pr[F]$ 代表挑战者 $\mathcal{C}$ 不会终止游戏的概率, 则可以得到 $Adv_{\mathcal{C}}(\kappa) = Pr[F]\cdot\frac{2}{q_g}\cdot Adv_{\mathcal{A}}^{IND-SK}$, 假设 $\mathcal{A}$ 最多进行 q_e 次 $StaticKeyReveal$ 查询, q_r 次 $SessionKeyReveal$ 查询, q_f 次对 H_3 谕言机的查询。为了简化分析过程, 进一步定义下列事件, 其中 F_1 代表挑战者在进行 $StaticKeyReveal$ 查询时不会终止游戏的事件, F_2 代表挑战者在进行 $SessionKeyReveal$ 查询时不会终止游戏的事件, F_3 代表挑战阶段, 挑战者不会终止游戏且在对 H_4 谕言机的询问中询问的事件, 具体表示如下:

$$
\begin{aligned}
&F_1 : \wedge_{i=1}^{q_e}(P(ID_i) = 0)\\
&F_2 : \wedge_{k=1}^{q_r}(P(ID_i) = 0 \vee P(ID_j) = 0)\\
&F_3 : P(ID_I) = 1 \wedge P(ID_J) = 1 \wedge coin_I \neq coin_J \wedge r_m = r_M
\end{aligned}
$$

显然, 通过分析可以得到 $F = F_1 \wedge F_2 \wedge F_3$, 因此, 可以得到:

$$Pr[F] = Pr[F_1]\cdot Pr[F_2 \wedge F_3|F_1]$$

因为针对不同用户进行私钥查询的事件是独立的, 每次查询以 δ 的概率设置 $P(ID_i) = 0$, 因此 $Pr[F_1] = \delta^{q_e}$ 。而针对会话密钥查询时, 每次只需两个身份中至少有一个 $mark = 0$, 且至少有一个不是目标身份, 所以 F_2 与 F_3 非完全独立事件, 由于 $coin_I$ 和 $coin_J$ 的选择是随机的, 所以 $Pr[F_2 \wedge F_3|F_1] \geq \delta^{q_r}\cdot\frac{(1-\delta)^2}{2}\cdot\frac{1}{q_f}$ 。所以得到 $Pr[F] \geq \delta^{q_r+q_e}\frac{(1-\delta)^2}{2q_f}$ 。令函数 $f(\delta) = \delta^{q_r+q_e}\frac{(1-\delta)^2}{2q_f}$, 通过计算可得, 当 $\delta = 1-\frac{2}{q_e+q_r+2}$, $f'(\delta) = 0$, $f(\delta)$ 取最小值, 因此可以得到:

$$Pr[F] \geq \frac{2}{(q_e+q_r)^2 q_f}\cdot(1-\frac{2}{q_e+q_r+2})^{q_e+q_r+2)}$$

根据极限公式 $\lim_{x\to 0}(1+x)^{\frac{1}{x}} = e$, 函数的最小值为 $\frac{2}{e^2(q_e+q_r)^2}$ 。所以如果存在敌手 $\mathcal{A}$ 能够以不可忽略的优势 $Adv_{\mathcal{A}}^{IND-SK}(\kappa)$ 攻破 IB-ZIAKE 协议, 那么就存在敌手 $\mathcal{C}$ 能够以至少 $\frac{4}{e^2(q_e+q_r)^2 q_g q_f}\cdot Adv_{\mathcal{A}}^{IND-SK}(\kappa)$ 的优势解决 CBDH 困难问题, 这与困难问题假设相矛盾, 所以敌手 $\mathcal{A}$ 攻破 IB-ZIAKE 协议的优势 $Adv_{\mathcal{A}}^{IND-SK}(\kappa)$ 是可忽略的, 所以 IB-ZIAKE 协议是 IND-SK 安全的。

定理 3.2 *如果 CBDH 假设成立, H_1, H_2, H_3, H_4 是随机谕言机, 那么 IB-ZIAKE 协议在随机谕言机模型下是已知密钥安全的。*

假设任意多项式有界的敌手 $\mathcal{B}$ 能够以 $Adv_{\mathcal{B}}^{KKS}(\kappa)$ 的优势在已知密钥安全的游戏中获胜, $\mathcal{B}$ 最多掌握两个用户之间 n 个过去的会话密钥, 存在算法 $\mathcal{C}$ 能够以下

列优势在共享密钥不可区分安全的游戏中获胜:

$$Adv_{\mathcal{A}}^{IND-SK}(\kappa) = \frac{1}{2(n+1)} Adv_{\mathcal{B}}^{KKS}(\kappa)$$

证明：在下列证明过程中, 定义了一系列安全游戏 $G_0, G_1, \cdots, G_{n+1}$。安全游戏的具体过程如下:

Game G_0 **：** 挑战者掌握所有会话过去的会话密钥的列表 L_{psk}, 表 L_{psk} 中的每个条目的形式为 $(ID_i, ID_j, r_m, sk_{i,j}^{r_m})$, 其中包含 n 个针对挑战阶段中出现用户 ID_I, ID_J 过去的会话密钥, 对应的随机因子为 $r_1, r_2, \cdots, r_n \in R$。$R$ 代表随机因子的集合。

- Setup：挑战者首先输入安全参数 κ, 生成系统参数 $params$ 并秘密保留主密钥 msk, 同时挑战者掌握所有会话过去的会话密钥的列表 L_{psk}。

- 随机谕言机询问：与定理3.1中证明过程相同。

- Phase 1：敌手 $\mathcal{B}$ 发起下列询问:

  StaticKeyReveal (ID_i)**：** 与定理3.1中证明过程相同。

  SessionKeyReveal $(ID_i, ID_j.r_m)$**：** 当接收到该询问后, 挑战者首先查询列表 L_{psk}, 如果表中定义过了这个条目, 则挑战者返回相关的值 $sk_{i,j}^{r_m}$；否则挑战者维护会话密钥的列表 L_{sk}, 在 L_{sk} 中的每个条目的形式为 $(ID_i, ID_j, r_m, sk_{i,j}^{r_m})$, 如果表中已经定义过了这个条目, 则挑战者返回相关的值 $sk_{i,j}^{r_m}$, 否则, 如果 $P(ID_i) = 0 \vee P(ID_j) = 0$, 挑战者选择其中 $mark = 0$ 的任意一个用户（假设为用户 ID_i）并利用 $Extract$ 算法查询其对应的私钥 d_i, 然后利用 $SharedKey$ 算法计算会话密钥 $sk_{i,j}^{r_m}$, 然后将条目 $(ID_i, ID_j, r_m, sk_{i,j}^{r_m})$ 插入到表 L_{sk} 中, 并将 $sk_{i,j}^{r_m}$ 返回给敌手；如果 $P(ID_i) = 1 \wedge P(ID_j) = 1 \wedge r_m \notin R$, 则挑战者终止游戏。

- Challenge：敌手选择两个用户 ID_I, ID_J 和随机因子 r_M, 但是要求 ID_I 和 ID_J 不能出现在 $StaticKeyReveal$ 查询中, (ID_I, ID_J, r_M) 不能出现在 $SessionKeyReveal$ 查询中。令 $(t_I, coin_I)$ 为表 L_{H_1} 中与 ID_I 相关的值，$(t_J, coin_J)$ 是表 L_{H_2} 与 ID_J 相关的值。如果 $P(ID_i) = 1 \wedge P(ID_j) = 1 \wedge coin_a \neq coin_b \wedge r_m = r_M$, 此时挑战者随机掷出一个无偏的硬币 b, 如果 $b = 0$, 则挑战者从会话密钥的分布域 $\{0, 1\}$ 中随机选择一个值返回给敌手, 如果 $b = 1$, 则返回真实的会话密钥 $sk_{I,J}^{r_M}$ 给敌手, 否则挑战者终止游戏。

- Phase 2：敌手可以重复执行 $Phase$ 1, 但是要保证 ID_I 和 ID_J 不能出现在 $StaticKeyReveal$ 查询中, (ID_I, ID_J, r_M) 不能出现在 $SessionKeyReveal$ 查询中。

- Guess：敌手输出猜测 $b' = 1$ 。

定义敌手在 Game G_0 中输出 1 的概率为 $Pr[\mathcal{B}(G_0) \to 1]$ 。

Game G_1 **：** 挑战者掌握所有会话过去的会话密钥的列表 L_{psk}, 表 L_{psk} 中的每个条目的形式为 $(ID_i, ID_j, r_m, sk_{i,j}^{r_m})$, 其中包含 n 个针对挑战阶段中出现用户 ID_I, ID_J 过去的会话密钥, 对应的随机因子为 $r_1, r_2, \cdots, r_n \in R$ 。任选其中一个会话密钥, 将其替换为随机数, 游戏的其余阶段与 Game G_0 相同。定义敌手在 Game G_0 中输出 1 的概率为 $Pr[\mathcal{B}(G_1) \to 1]$ 。

⋮

Game G_{n+1} **：** 挑战者掌握所有会话过去的会话密钥的列表 L_{psk}, 表 L_{psk} 中的每个条目的形式为 $(ID_i, ID_j, r_m, sk_{i,j}^{r_m})$, 其中包含 n 个针对挑战阶段中出现用户 ID_I, ID_J 过去的会话密钥, 对应的随机因子为 $r_1, r_2, \cdots, r_n \in R$, 其中 n 个会话密钥都被替换为随机数, 游戏的其余阶段与 Game G_0 相同。定义敌手在 Game G_0 中输出 1 的概率为 $Pr[\mathcal{B}(G_{n+1}) \to 1]$ 。

引理 3.1 在上述的游戏中, 对于任意相邻的游戏 G_i 和 G_{i+1}, 其中 $i \in \{0, n\}$, 下列等式成立:

$$|Pr[\mathcal{B}(G_{i+1}) \to 1] - Pr[\mathcal{B}(G_i) \to 1]| = \frac{1}{2} Adv_{\mathcal{A}}^{IND-SK}(\kappa) \tag{3.8}$$

证明： 这是一个简单的计算。粗略的说, 游戏 G_i 和游戏 G_{i+1} 的区别为在游戏 G_i 中, 敌手能获得额外的一个真实密钥, 而游戏在 G_{i+1} 中, 对应的密钥为随机值。定义 b' 是敌手输出的猜测, b 代表挑战者的选择。令 p_0 代表敌手在游戏 G_i 中输出 1 的概率, 即 $Pr[b' = 1|b = 0] = p_0$, p_1 为敌手在游戏 G_{i+1} 中输出 1 的概率, 即 $Pr[b' = 1|b = 1] = p_1$ 。因此可以得到下列等式:

$$\begin{aligned} Pr[b' = b] &= Pr[b' = b \mid b = 0]Pr[b = 0] + Pr[b' = b \mid b = 1]Pr[b = 1] \\ &= Pr[b' = 0 \mid b = 0] \cdot \frac{1}{2} + Pr[b' = 1 \mid b = 1] \cdot \frac{1}{2} \\ &= \frac{1}{2}\left(1 - Pr[b' = 1 \mid b = 0] + Pr[b' = 1 \mid b = 1]\right) \\ &= \frac{1}{2}(1 - p_0 + p_1). \end{aligned}$$

在共享密钥不可区分安全的游戏中, 敌手的优势被定义为 $Adv_{\mathcal{A}}^{IND-SK}(\kappa) = |Pr[b' = b] - \frac{1}{2}|$, 根据上述的游戏序列, 可以得到下列等式:

$$Adv_{\mathcal{A}}^{IND-SK}(\kappa) = \frac{1}{2}|p_1 - p_0| = \frac{1}{2} \cdot |Pr[\mathcal{B}(G_{i+1}) \to 1] - Pr[\mathcal{B}(G_i) \to 1]|$$

$$\begin{aligned}
|Pr[\mathcal{B}(G_1) \to 1] - Pr[\mathcal{B}(G_0) \to 1]| &= 2 \cdot Adv_{\mathcal{A}}^{IND-SK}(\kappa) \\
|Pr[\mathcal{B}(G_2) \to 1] - Pr[\mathcal{B}(G_1) \to 1]| &= 2 \cdot Adv_{\mathcal{A}}^{IND-SK}(\kappa) \\
&\vdots \\
|Pr[\mathcal{B}(G_{n+1}) \to 1] - Pr[\mathcal{B}(G_n) \to 1]| &= 2 \cdot Adv_{\mathcal{A}}^{IND-SK}(\kappa) \\
|Pr[\mathcal{B}(G_0) \to 1] - Pr[\mathcal{B}(G_{n+1}) \to 1]| &= 2(n+1) \cdot Adv_{\mathcal{A}}^{IND-SK}(\kappa)
\end{aligned}$$

在游戏 G_{n+1} 中, 敌手 $\mathcal{B}$ 得到 n 个关于挑战阶段中出现用户 ID_I, ID_J 过去的会话密钥, 但全部被替换为随机数, 相当于敌手在未知信息的情况下直接猜测挑战阶段的会话密钥, $|Pr[\mathcal{B}(G_{n+1}) \to 1] = \frac{1}{2}$, 因此, 可以得到下列等式:

$$Adv_{\mathcal{B}}^{KKS}(\kappa) = |Pr[\mathcal{B}(G_0) \to 1] - \frac{1}{2}| = 2(n+1) \cdot Adv_{\mathcal{A}}^{IND-SK}(\kappa) \tag{3.9}$$

所以如果存在敌手 $\mathcal{B}$ 能够以不可忽略的优势 $Adv_{\mathcal{B}}^{KKS}(\kappa)$ 在已知密钥安全的游戏中获胜, 那么就存在敌手 $\mathcal{A}$ 能够以不可忽略的优势 $\frac{1}{2(n+1)}Adv_{\mathcal{B}}^{KKS}(\kappa)$ 在共享密钥不可区分安全的游戏中获胜。然后通过定理3.1可知, 敌手 $\mathcal{A}$ 在共享密钥不可区分安全的游戏中获胜的概率是可忽略的, 所以 $Adv_{\mathcal{B}}^{KKS}(\kappa)$ 是可忽略的, 所以 IB-ZIAKE 协议具有已知密钥安全。

3.3.4 性能分析

本节主要为 IB-ZIAKE 协议的实现和测试，主要测试协议的正确性和通信开销。本节模拟实验在 Ubuntu 20.04 操作系统上进行，该系统搭载了一款 Intel i5 处理器，基于 BLS-12381 曲线参数和 MIRACL 库对协议进行实现。MIRACL 库（Multiprecision Integer and Rational Arithmetic C/c++ Library）是设计与大数运算相关函数库，实验环境如表3.1所示。

实验流程如图3.4所示。首先基于生成元 P_1，P_2 生成两个非对称群 $\mathbb{G}_1$，$\mathbb{G}_2$，利用随机数生成函数 Get_RNG 生成随机数 RNG，将随机数传入到函数 IDC_383_MASTKEY_GEN1 中，生成主密钥 s_0 和对应的 $\mathbb{G}_1$ 群上的主公钥 s_0P，接着用户基于标识向 KGC 申请用户私钥，调用函数 IDC_383_PRVKEY_GEN2 生成对应的 $\mathbb{G}_2$ 群上的用户私钥 d_A，提取本地时间，调用 IB-ZIAKE 函数计算会话密钥 SK_A。SOK 协议实现过程省去了提取本地时间的过程，其余过程和 IB-ZIAKE

表 3.1　实验环境配置

名称	配置信息
操作系统	Ubuntu 20.04
CPU	Intel(R) Core(TM) i5
内存	8 GB
开发语言	C 语言
代码库	MIRACL 库

协议相同。SOK 协议与 IB-ZIAKE 协议中，采用相同的用户公私钥，如表3.2所示。

图 3.4　IB-ZIAKE 协议密钥计算流程图

SOK 协议与 IB-ZIAKE 协议实验结果如表3.3，表3.4所示，SOK 协议计算的是 $\mathbb{G}_T$ 群上的双线性对的值，而 IB-ZIAKE 协议在会话密钥计算过程中，通过引入每个会话特有的共享随机因子, 并采用哈希函数 SHA-512 对 $\mathbb{G}_T$ 群上的双线性对进行哈希运算，计算生成唯一的会话密钥。实验结果表明，IB-ZIAKE 协议与 SOK 协议的耗时均为 0.013588 秒，尽管 IB-ZIAKE 协议比 SOK 协议需要多执行时间提取算法和额外的两次 Hash 算法，但由于这两个算法耗时相对于密钥计算过程耗时低得多，可以得出结论，IB-ZIAKE 协议性能几乎与 SOK 协议相同，但是 IB-ZIAKE 协议比 SOK 协议增加了已知密钥安全，协议安全性对比如表3.4所示。在 SOK 协

表 3.2　基于标识的零交互密钥协商协议参数

	公钥	私钥
用户 Alice	([489783d8 48d06339 415f870d 00d67b8c 00da604b fc58647d 0da3ae6d 3393647a 9fe2ce7a 81dec582 4e5850c5 81deac55,47db8da3 227cee9a 1ebbad8b 9a8a75e0 5fcee0ad 62e8b11f 479df5e4 714e2206 d60f147f 8595bf8d ad5b76e7 52e6e3b3],[783c3c19 fa178f96 9a177a64 e0da1351 95d0bd47 0f61e940 b266a915 76fe6a63 6e282869 a96f08ad 13120bdd 258713fc,3602a4a8 696b90c5 648e3c4e 3a25a29f bdd7e129 f8991140 88286a1c cd5a20fc 8a8dc61e 07b6a8bc 1e60c967 8aca97af])	([75c496e6 625ec01b e23c9b26 23b8c2bb 57f3fa11 fa6ac628 fd917db3 78e81f0c f4ef6b0e 891806dc 7d26a6db 3bd0dc12,228c875f ea1be42d 60da55bb 9360c0fc cd49f131 900752f6 e10aaa38 0fd25ae2 f759e4bd a54c8116 e8461235 940c19f8],[6f1c586d 4154bd42 f19483e0 43b518ef 70af8433 3398feba 264557b4 f843206a 410f5042 2fa0dbac f4195c48 ccad2a61,72aad91c 24ffda3e c812f53e 208369f6 b285e260 9c4c42d6 92202b88 d47ccc0c a6132e76 0761a9c7 98aae2b4 327cd2be])
用户 Bob	(3f0aa330 d2e69120 6ffd73a5 be861fa2 f584bddc 6678bfb9 4e941d0e 840b5cc5 8329f62f d2edc890 82408208 926d6abc,2c5bd24e 49ce80e1 7d4d640f 9c9e1927 b50d187c 94448347 c5ce9781 c6bd47f9 e6867f4d 3a9995df 4a510dbb abe0530d)	(261d65e6 abef94eb 85ca2d98 0840c04f 8deb6d78 2ce78c3b 0021c324 1bb542d9 5fd41d60 171b84fe 161eef0c 33c0f111,69e036db 8f246413 4590a35d 6ecc59ea 1016057f 6c7b7ebd d6b43350 2fa6ceae 43b86730 dcd9f401 465ea31b cb0d11c2)

议与 IB-ZIAKE 协议中，会话密钥计算均包含双方身份标识，因此两个协议均满足未知密钥共享安全（KKS），但是由于是零交互的密钥协商协议，SOK 协议与 IB-ZIAKE 协议仍然无法实现前向安全（FS）和抗私钥泄露伪装安全（KCI）。

3.4　IB-ZIAKE 协议在 T-IP 协议中的应用

王等人[83] 提出了自信任安全的互联网协议（T-IP）, 该协议采用基于标识的加密技术, 将 IP 地址作为公钥。他们的研究表明, T-IP 的传输开销和连接延迟比 IPsec 低得多。它为低延时、计算资源有限的网络环境提供了高效的安全协议。不过, 他们在 T-IP 协议中使用了 IB-NIKE 协议。这种密钥协商协议无法满足已知密钥的安全性要求。因此, 本文用 IB-ZIAKE 协议取而代之, 以增强协议的安全性。

表 3.3　基于标识的零交互密钥协商协议实验结果

协议	会话密钥
SOK 协议	1791913a 8d899b22 baf2b852 0c80ffd4 4058fe50 c1466e0c f8c46b24 2162b2a3 ee5889e3 abe55938 ee6c9c6e 7bc0549b 44fbc33d f16b3498 d7e84cbc d5bdad0c 07d24780 8eb51fe4 9a255ef5 85e5dba4 159b6d72 139d398e f07939f5 c05d61c5 3250a681 34c24aa3 516715d5 5724ccc0 8acb0613 5116ba15 a57b2d46 a843b033 b637ca8d c29545d3 756d306e 158659b9 1bf6cae4 33e2b2b0 a7077341 5b3722f2 41426013 bc3de05d 67d2f19f 6934129e 518ca68f dd96a802 0bfb1779 dc547b1d 3a3a918c 9c4ca8bc d088cd89 9f14518d 18f150e9 b6b6309e 4e713c19 f7b5b498 a8e8fbb8 33153d15 89622139 b98b278d 56714d7a 4bdd2a7c 63d7bfa7 c65a9f49 e4f47dbc 14eb2bbb 49a62489 2ba8c9c6 b57a9b68 7c3a4979 5e31ce66 94bbf857 2a33e6b9 b6fdd16b 00918a43 bcf675b8 d3657e1b b292670a 89ba6525 50bff0e7 c8fa6ee7 81b1b999 67467513 79a22b43 31760cb1 2e0c7eb8 3c527b3b f1a30861 c58f42ba e60dc3a7 5b845c6b b24ad672 a77560da cecf65b3 a972a444 09daee2d 4f3abbf8 4304ff11 d70253ef 32c6b803 9e9a3b90 04afe41b 184c7d51 06807ce5 69cf924b cd5e064a f63d8f62 f7489047 01020d66 acaaea02 865f2cee 45a3cfe5 e01e0030 56363703 10a0f1ba 2cae069b 804c057d ea13d3e3 f71ed9c3 1a72bb6d 32e40264 b5bf0094 9d6ee7a1 e7de3766 44b85e65 0eed17c1 6aae9e43 3eaed953 f6ad6430 48d450a0 11f6224c 9c47a196 44f234f4 583ae7e7 dbae76a8 1670fda8 80c777be e8b9a316 1be058f8 f67e352b acc7758d e85405c7 bf2de3cb 78048408
IB-ZIAKE 协议	99b98cd8 0cbf0df5 537bd1fd d8c3132b 4552fe40 18809a18 70cde830 d4eee8e5 4f4bcd72 67ffa75c 0a4d004d f77ed83c 2156fa04 044cbe8e 0e2235b8 acdd8dc7

表 3.4　基于标识的零交互密钥协商协议对比

协议	计算开销 (s)	安全性			
		UKS	KKS	FS	KCI
SOK	0.0114	✓	×	×	×
IB-ZIAKE	0.0114	✓	✓	×	×

3.4.1　改进的 T-IP 协议

T-IP 协议通信过程确保了通信双方的身份验证和信息的加密传输。图3.5展示了改进后的 T-IP 协议通信过程。

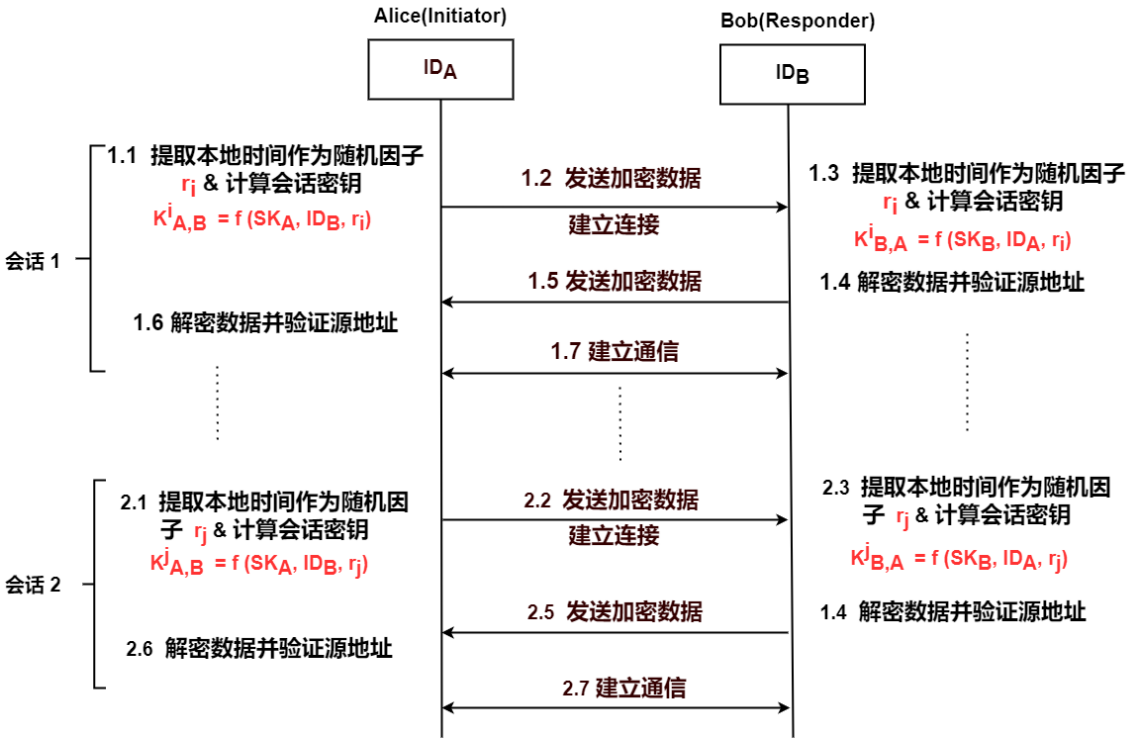

图 3.5　改进的 T-IP 协议

Alice 和 Bob 在加入通信系统时运行网络时间协议（Network Time Protocol，NTP）来同步时钟。有关 NTP 的详细信息, 请参阅文献[84]。然后通信双方从密钥生成中心 (KGC) 获取自己的私钥。在密钥协商过程中，Alice 首先提取本地时间并进行哈希运算以创建随机因子, 使用 IB-ZIAKE 协议生成会话密钥。然后, 她根据协议格式构建信息, 并将加密数据包发送给 Bob。收到 Alice 发送的数据包后, Bob 在相同的时间窗口内提取本地时间进行哈希运算，获得相同的随机因子并计算会话密钥。然后, 他会解密信息并验证源地址。如果源地址是伪造的（即 Alice 是假冒的）, 解密后的信息将与 T-IP 协议格式不符, 因为攻击者无法获得与 Alice 的 IP 地址相对应的 T-IP 私钥, 因此无法计算出与 Bob 相同的密钥[83]。同样, Bob 向 Alice 发送加密数据包, Alice 验证源地址, 建立安全通道。

当 Alice 想要与 Bob 建立新会话时, 她会提取此刻的本地时间并进行哈希运算, 以创建一个新的随机因子。这样, 她就可以与 Bob 共享一个新的会话密钥。这样就确保了每次会话密钥的唯一性，并防止在过去的会话密钥被泄露的情况下, 所有会话密钥都会暴露。

3.4.2　安全性分析

如文献[83] 中提到的, T-IP 协议可以认证源地址, 抵抗中间攻击和拒绝服务攻击。随着 IB-ZIAKE 协议的应用, T-IP 协议进一步实现了已知密钥安全。由于每个

协议运行中包含不同的随机因子, 每个会话生成唯一的会话密钥。即使对手获得了过去会话密钥, 也不会影响未来会话的安全性。改进后的 T-IP 协议可以抵抗以下攻击:

已知密钥攻击：假设敌手获取了过去会话的密钥，敌手使用相同的会话密钥加密信息发给用户 A 或 B，由于每个会话密钥都包含唯一的随机因子, 敌手获取的会话密钥是基于过去的随机因子生成的，又基于哈希函数的单项性，即使攻击者获得了过去会话的会话密钥，也无法计算双线性对的值，无法利用公开的随机因子计算当前的会话密钥。所以对于用户来说，一旦发现加密信息无法使用当前的会话密钥解密，用户就放弃该信息，敌手无法实现已知密钥攻击。

重放攻击：提取本地时间作为随机因子, 为每个会话密钥提供唯一的生命周期。这允许通信双方在零交互的情况下进行会话密钥更新。在最初的 T-IP 协议中, 密钥协商协议采用的是 SOK 协议，一旦通信双方确定后，会话密钥不再进行更新。由于每次会话的会话密钥相同，如果对手重放过去的会话，则用户无法有效地识别这种攻击。然而, 将 IB-ZIAKE 协议替换 SOK 协议后, 如果敌手重放过去的会话, 由于新的会话使用新的会话密钥，接收方会因为会话密钥不一致拒绝会话。因此, 敌手无法执行重放攻击。

3.5 小结

本章首先定义了双线性对的相关知识，并阐述了后续实验采用的 BLS12-381 曲线的相关知识。其次，定义了基于标识的零交互密钥协商的已知密钥安全模型。该安全模型将密钥协商协议的安全性从共享密钥的不可区分性（IND-SK）扩展到了已知密钥安全性。它超越了现有框架, 允许对手获取过去的会话密钥, 但确保未来会话的安全性不受影响。, 然后，本文介绍了具有已知密钥安全性的 IB-ZIAKE 协议。IB-ZIAKE 通过在双线性配对会话密钥计算中引入共享随机因子和单向哈希函数来生成唯一的会话密钥。这一改进大大降低了与已知密钥攻击和重放攻击相关的风险, 而这正是安全通信协议中的关键问题。通过将 IB-ZIAKE 协议集成到 T-IP 协议中, 本文证明, 与 IPsec 相比, 改进后的协议不仅保留了其固有的低传输开销和减少连接延迟的优势, 而且还增强了抵御高级安全威胁的能力。具体地说, 每次会话都使用唯一的会话密钥, 这就确保了过去会话密钥的泄露不会危及未来的通信。通过实验对比 IB-ZIAKE 协议与 SOK 协议，实验结果表明 IB-ZIAKE 协议在保持 SOK 协议性能的前提下，满足了已知密钥安全。

第四章　基于标识与基于无证书体制的跨域认证密钥协商

随着网络设备的多样化和应用场景的复杂化，跨域认证密钥协商协议成为确保通信安全的关键技术。传统的基于标识的密钥协商和基于无证书的密钥协商在各自领域内具有独特的优势，但面对跨域通信时，如何实现高效、安全的密钥协商成为亟待解决的问题。本章设计一种基于标识与无证书体制的跨域认证密钥协商协议（Cross-Domain Authenticated key Exchange，CDAKE），旨在提高跨域通信设备间通信的安全性和效率，为跨域通信的广泛应用提供坚实的安全保障。同时在改进了无证书 eCK 模型，在改进的的模型下证明了协议安全性。

4.1　预备知识

4.1.1　强不可伪造安全

消息认证码 (Message authentication codes [MAC])：消息认证码由以下三个算法组成:

- 密钥生成算法 $KG(\kappa)$: 输入安全参数 κ, 返回密钥 sk 。
- 签名算法 $MAC_{sk}(sk, x)$: 输入消息 $x \in \{0,1\}^*$ 和密钥 sk, 产生标签 tag 。
- 验证算法 $Ver_{sk}(x, tag)$: 输入密钥 sk, 消息 x 和标签 tag, 如果 $Ver(sk, x, tag) = 1$, 则证明标签有效, 否则无效。

强不可伪造 (Strong Unforgeability against chosen-message attacks, SU-CMA) 安全模型可以用如下 Game 描述:

- Setup：假设 SP 为系统参数. 挑战者执行密钥生成算法, 生成用户公私钥对 (pk, sk) 并将用户公钥 pk 发送给敌手. 挑战者保留 sk 用来回答敌手的签名查询。
- Query：敌手自适应地选取任意消息 m_i 进行签名查间. 对于敌手提交的消息 m_i，挑战者执行签名算法生成 σ_{m_i}，并将其发送给敌手。
- Forgery：敌手返回一个伪造的对于某个消息 m^* 的签名 σ_{m^*}。

对于任意多项式时间的敌手 $\mathcal{F}$ 企图伪造签名, 给定 MAC 谕言机 $MAC_{sk}(\cdot)$, 挑战者通过谕言机回答敌手的标签查询, 维护消息 m_i 与对应标签 tag_i 的集

合 $\mathcal{Q}=\{m_i,tag_i\}$, 概率 $Pr[sk\leftarrow KG(\kappa),(x,tag)\leftarrow\mathcal{F}^{MAC_{sk}(\cdot)}(\lambda),(x,tag)\notin\mathcal{Q}:Ver_{sk}(x,T)=1]$ 是可忽略的, 则说 MAC 协议是强不可伪造的。

基于跨域认证密钥协商协议显示认证的需求，本小节定义了强不可伪造安全的安全模型并进行了简单的证明，后文中提到的 MAC 算法默认是强不可伪造安全的，后续不再进行赘述。

4.1.2 困难问题假设

CDH(Computational Diffie-Hellman) 问题：设 P 为循环群 $\mathbb{G}$ 的生成元, 阶为素数 q, 输入 $aP\in\mathbb{G}$ 和 $bP\in\mathbb{G}$, 求解 abP。假设存在算法 $\mathcal{A}$ 以优势 ϵ 解决 CDH 问题，$Pr[\mathcal{A}(aP,bP)=abP]=\epsilon$，若 ϵ 是可忽略的，则称 CDH 问题是困难的。

DDH(Decisional Diffie-Hellman) 问题：设 P 为循环群 $\mathbb{G}$ 的生成元, 阶为素数 q, 随机选择整数 $a,b,c\in_R\mathbb{Z}_N^*$，给定 (P,aP,bP,cP)，判定 $abP=cP$ 是否成立。假设存在算法 $\mathcal{A}$ 以优势 ϵ 解决 DDH 问题，$Pr[\mathcal{A}(abP)=cP|P,aP,bP,cP]=\epsilon$，若 ϵ 是可忽略的，则称 DDH 问题是困难的。

DCDH(Divisible Computational Diffie-Hellman) 问题：设 P 为循环群 $\mathbb{G}$ 的生成元, 输入 $aP\in\mathbb{G}$ 和 $bP\in\mathbb{G}$, 求解 $a^{-1}bP$ 。假设存在算法 $\mathcal{A}$ 以优势 ϵ 解决 DCDH 问题，$Pr[\mathcal{A}(aP,bP)=a^{-1}bP]=\epsilon$，若 ϵ 是可忽略的，则称 DCDH 问题是困难的。根据文献[85]，CDH 问题与 DCDH 问题等价。

4.2 安全模型

在本节, 本文提出一个新的安全模型, 用于对跨域认证密钥协商协议的研究。基于标识与基于无证书体制的跨域认证密钥协商协议所使用的形式化安全模型, 实际上是对无证书 eCK 模型[1] 的改造, 使其能够适用于跨域通信的情形。

根据参与方类型不同, 将参与者分为两个集合, 其中有 n_1 个基于标识密码体制的用户, n_2 个基于无证书体制的用户, 将每个参与者建模为一个概率多项式（PPT, probabilistic polynomial-time）的图灵机, 任意两个在不同体制内的用户可以运行此协议, 会话是协议的一个实例, 每个用户可并行执行多个会话, 用户 ID_i 与用户 ID_j 执行的第 t 个会话用 $\Pi_{i,j}^t$ 表示, 其中将会话的发起方 ID_i 称为会话的拥有者（Owner）, 而 ID_i 希望通信的另一方 ID_j, 即此会话的响应者称为此会话的伙伴（Peer）。会话 $\Pi_{i,j}^t$ 的标识符为 $(role,ID_i,ID_j,comm_i,comm_j)$, 其中 $role\in\{\mathcal{I},\mathcal{R}\}$, $\mathcal{I}$ 代表会话的发起者, $\mathcal{R}$ 代表会话的响应者, $comm_i$ 和 $comm_j$ 分别代表会话发起者 ID_i 和其伙伴 ID_j 通信过程中传递的信息。对于攻击此协议的敌手 $\mathcal{A}$, 同样将其建模为一个概率多项式的图灵机, 且 $\mathcal{A}$ 控制了整个通信网络。

定义 4.1 已接受的会话：如果会话的拥有者计算出一个会话密钥 $k_{i,j}^t$, 就将会话 $\Pi_{i,j}^t$ 标记为可接受的。当协议成功结束时（并规定不再接受消息）, 会话拥有者就将会话标记为已完成。一个已完成的会话必须是可接受的。

定义 4.2 匹配会话：对于会话 $\Pi_{i,j}^t$, 其会话标识 $sid_i^t = (role, ID_i, ID_j, comm_i, comm_j)$, 对于会话 $\Pi_{j,i}^w$, 其会话标识 $sid_j^w = (\overline{role}, ID_j, ID_i, \overline{comm_i}, \overline{comm_j})$, 若 $role \neq \overline{role}$, $comm_i$ 是 $\overline{comm_j}$ 的前缀, 反之亦然, 称会话 $\Pi_{i,j}^t$ 与会话 $\Pi_{j,i}^w$ 是匹配会话。

下面通过描述挑战者 $\mathcal{C}$（Challenger）与敌手 $\mathcal{A}$ (Adversary) 之间的游戏（Game）定义本文提出的跨域认证密钥协商协议的安全性:

- Setup: 挑战者首先输入安全参数 κ, 选择所有的诚实用户并运行启动（Setup）算法从而获得系统参数和公钥信息。

- Phase 1, 敌手可以按照任意顺序执行下列询问:

  Create(ID_i**,** $type$ **)**：该查询模拟敌手任意注册一个合法的用户, 代表某个参与者 ID_i。挑战者接收到此询问后, 如果 $type = 0$, 返回基于标识密码体制用户的公私钥对, 如果 $type = 1$, 返回基于无证书密码体制用户的公私钥对。若一个用户不是由敌手注册的，则称此用户为诚实用户。

  SessionKeyReveal($\Pi_{i,j}^t$ **)**：接收到该询问后, 若该会话处于已接受的状态, 那么挑战者返回该会话密钥, 否则返回 $\perp$。接受到此查询的会话被称作是开放的。

  MasterPrivateKeyReveal(ID_i**,** $type$ **)**：接收到该询问后, 如果 $type = 0$, 挑战者返回管理标识密码体制用户的 KGC_1 的系统主密钥, 如果 $type = 1$, 挑战者返回管理无证书密体制用户的 KGC_2 的系统主密钥。

  StaticKeyReveal(ID_i**,** $type$ **)**：接收到该询问后, 如果 $type = 0$, 挑战者返回用户 ID_i 的长期私钥, 否则返回 $\perp$。若已进行了 MasterPrivateKeyReveal 查询, 则发起此查询是多余的。

  PartialPrivateKeyReveal(ID_i**,** $type$ **):** 接收到该询问后, 如果 $type = 1$, 挑战者返回用户 ID_i 的部分私钥, 否则返回 $\perp$。

  PublicKeyReplace(ID_i**,** $type$**,** X' **)**：接收到该询问后, 如果 $type = 1$, 挑战者使用新的公钥 X' 替换用户 ID_i 的旧公钥, 否则返回 $\perp$。

SecretValueReveal(ID_i**,** $type$ **)**：接收到该询问后, 如果 $type = 1$ 挑战者返回用户 ID_i 的秘密值, 该秘密值用于生成 ID_i 的无证书公钥。如果针对 ID_i 已经进行过了 PublicKeyReplace 询问, 则返回 $\perp$ 。如果 $type = 0$, 返回 $\perp$ 。

EphemeralKeyReveal($\Pi_{i,j}^t$ **)**：接收到该询问后, 挑战者返回会话 $\Pi_{i,j}^t$ 中参与方的临时密钥。

Send($\Pi_{i,j}^t$**,** $comm$ **)**：敌手代表 ID_j 向会话 $\Pi_{i,j}^t$ 的另一个参与方 ID_i 发送消息 $comm$, 返回用户 ID_i 对此消息的响应。若 $comm = \lambda$, 则 ID_i 作为消息的发起方。如果之前尚未初始化参与方, 则会创建相应的公私钥对。此查询允许敌手命令 ID_i 发起一个与 ID_j 的会话 $\Pi_{i,j}^t$, 并提供从 ID_j 到 ID_i 的通信。在 ID_i 发送和接收协议指定的最后一组消息后, 它会输出一个决定, 指示接受或拒绝会话。通常要求 $ID_i \neq ID_j$, 即一个参与方不会与自己执行一个会话。

定义 4.3 *新鲜会话：会话的两个参与方 ID_i, ID_j 都是诚实的, 称会话 $\Pi_{i,j}^t$ 是新鲜的, 如果以下条件成立：*

(1) $\Pi_{i,j}^t$ 是可接受的, 即 $\Pi_{i,j}^t$ 已经产生会话密钥。

(2) $\Pi_{i,j}^t$ 不是开放的, 即 $\Pi_{i,j}^t$ 没有受到会话密钥查询。

(3) 参与会话 $\Pi_{i,j}^t$ 的双方都没有被完全腐化, 即敌手没有同时获得基于标识密码体制用户的长期私钥和临时密钥, 也没有同时获得基于无证书密体制用户的秘密值、部分私钥和临时密钥。

(4) 不存在某个开放的会话 $\Pi_{j,i}^w$ 与 $\Pi_{i,j}^t$ 相匹配。

- Test($\Pi_{i,j}^t$): 一旦敌手决定阶段 1 结束。它会选择一个新鲜会话 $\Pi_{i,j}^t$ 并发起对会话 $\Pi_{i,j}^t$ 的会话密钥查询。此时挑战者随机掷出一个无偏的硬币 b。如果 $b = 0$, 则挑战者从会话密钥的分布域 $\{0,1\}^\kappa$ 中随机选择一个值返回给敌手, 如果 $b = 1$, 则返回真实的会话密钥 $sk_{i,j}^t$ 给敌手。另外, 在敌手选择测试会话后, 敌手可以针对任意参与方发起公钥替换查询。

- Phase 2：敌手可以重复执行 Phase 1, 但是保证测试会话 $\Pi_{i,j}^t$ 及其匹配会话 (如果存在的话) 的新鲜性。

- Guess：当敌手决定阶段 2 结束后, 敌手输出猜测 $b' \in \{0,1\}$, 如果 $b' = b$, 则敌手赢得游戏。敌手赢得游戏的优势被定义为：

$$Adv_{\mathcal{A}}(\kappa) = |Pr(b' = b) - \frac{1}{2}| \tag{4.1}$$

定义 4.4 *如果对于任意多项式有界的敌手 $\mathcal{A}$, 函数 $Adv_{\mathcal{A}}(\kappa)$ 是可忽略的, 则协议在改进的无证书 eck 模型下是安全的。*

实际上, 上述定义的新鲜会话已经囊括了无证书密码体制下定义的两类敌手, 因此, 在本文的安全模型中只考虑一个单一的敌手, 证明过程不对敌手进行区分。另一方面，原始的无证书 eck 模型[1] 所描述的基于无证书密码体制的协议涉及到双方的部分私钥、秘密值和临时秘密共六块秘密信息。本节给出的模型与此不同, 因为该模型只涉及到五块秘密信息：基于标识密码体制的用户的长期私钥、临时密钥；基于无证书密体制的用户的部分私钥、秘密值和临时密钥。要求一个跨域认证密钥协商协议是安全的, 只要每个参与方仍有至少一个秘密未被泄露。

4.3 协议设计

4.3.1 协议描述

本节给出一个基于标识与无证书体制的跨域认证密钥协商协议（CDAKE），通过三次消息交互实现显示认证的密钥协商。假设基于标识密码体制的用户有一个可信的 KGC_1 负责产生并安全地分发用户的静态私钥, 基于无证书体制的用户有一个可信的 KGC_2 负责产生并安全地分发用户的部分私钥。协议初始化如图4.1所示，基于表示密钥体制用户 A 由所属的 KGC_1 通过安全的信道分发用户私钥 d_A，公布系统主公钥 P_{pub_1}。基于无证书密码体制的用户 B 由所属的 KGC_2 通过安全的信道分发部分私钥 y，公布对应的公钥 R 和主公钥 P_{pub_2}，用户 B 选择秘密值 x 并公布对应的公钥 X。

（一）对于基于标识密码体制的用户, 生成系统参数和用户公私钥对：

Setup (κ)：输入安全参数 κ, 选定阶为素数 q 的加法循环群 $\mathbb{G}_1$, 乘法循环群 $\mathbb{G}_2$, $\mathbb{G}_1$ 的生成元为 P, 存在双线性映射 $\hat{e}:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$。随机选取 $s_1\in_R\mathbb{Z}_q^*$ 作为系统主密钥, 计算 $P_{pub_1}=s_1P$, 选择哈希函数 $H_1:\{0,1\}^*\to\mathbb{G}_1$, 输出系统参数 $params_1=\{q,\mathbb{G}_1,\mathbb{G}_2,\hat{e},P,P_{pub_1},H_1\}$ 并秘密保存系统主密钥 s_1。

Extract $(params_1,s_1,ID_A)$：对于用户 A, 输入系统参数 $params_1$, KGC_1 的主密钥 s_1, 用户标识 ID_A, KGC_1 输出用户 A 的私钥 $d_A=s_1H_1(ID_A)$。

（二）对于基于无证书体制的用户, 生成系统参数和用户公私钥对：

Setup (κ)：输入安全参数 κ, 选定阶为素数 q 的加法循环群 $\mathbb{G}_1$, 乘法循环群 $\mathbb{G}_2$, $\mathbb{G}_1$ 的生成元为 P, 存在双线性映射 $\hat{e}:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$。随机选取 $s_2\in_R\mathbb{Z}_q^*$, 计算 $P_{pub_2}=s_2P$, 选择哈希函数 $H_2:\{0,1\}^*\times\mathbb{G}_1\to\mathbb{Z}_q^*$, 输出系统参数 $params_2=\{q,\mathbb{G}_1,\mathbb{G}_2,\hat{e},P,P_{pub_2},H_2\}$ 及系统主密钥 s_2。

PartialPrivateKeyExtract $(params_2,ID_B)$：输入系统参数 $params_2$ 和用户 B 的身份标识 ID_B, KGC_2 选择 $r\in\mathbb{Z}_q^*$, 计算 $R=rP$, $y=r+s_2H_2(ID_B,R)$, 输出 R

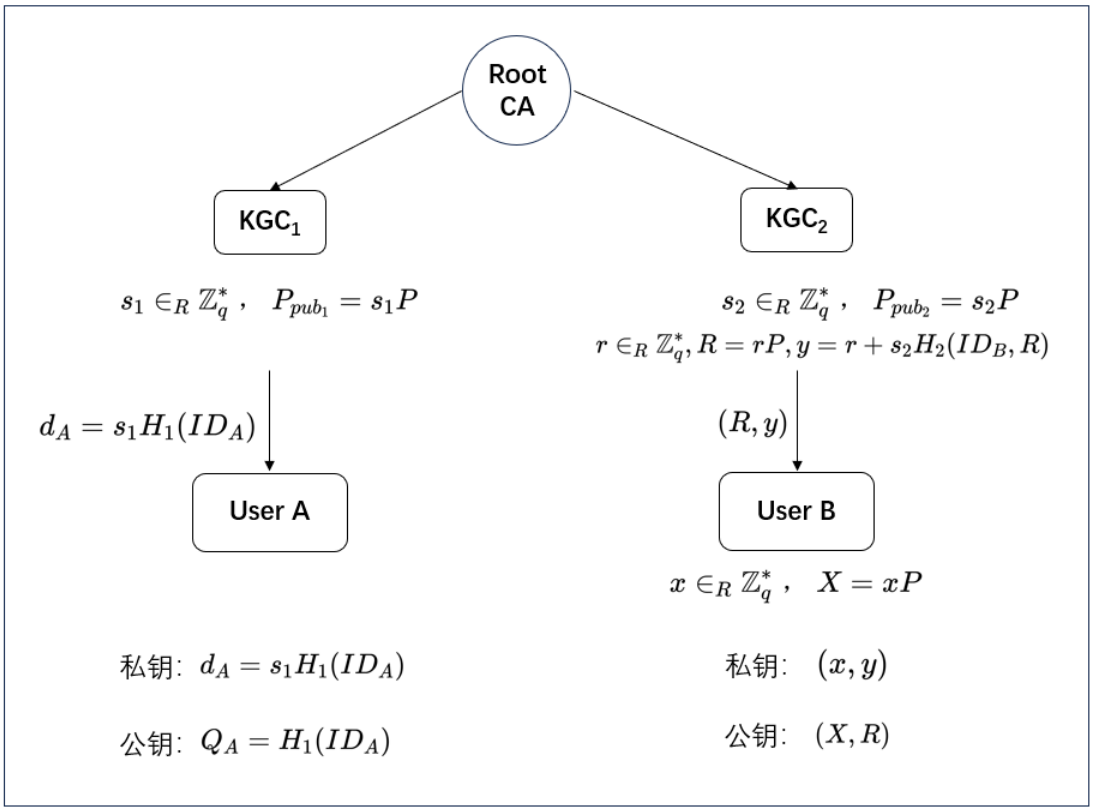

图 4.1　CDAKE 协议初始化

和 y, KGC_2 将 R 和 y 发送给用户 B, B 可以通过等式 $yP = R + H_2(ID_B, R)P_{pub_2}$ 是否成立判断 (R, y) 的有效性。

SetSecretKey $(params_2, ID_B)$：输入系统参数 $params_2$ 和用户 B 的身份标识 ID_B, 输出随机数 $x \in \mathbb{Z}_q^*$ 作为秘密值。

SetPublicKey $(params_2, ID_B, x)$：输入系统参数 $params_2$, 用户 B 的身份标识 ID_B 和秘密值 x, 计算 $X = xP$, 输出公钥 (X, R) 。

SetFullPrivateKey $(params_2, ID_B, x, y)$：输入系统参数 $params_2$, 用户 B 的身份标识 ID_B, 秘密值 x 和部分私钥 y, 输出用户的完整私钥 (x, y)

（三）密钥协商:

密钥协商过程如图4.2所示，协议具体过程如下所示:

（1）Alice 选择随机数 $a \in_R \mathbb{Z}_q^*$, 计算 $T_A = aP$, 设置会话标识为 $sid_i^t = (\mathcal{I}, ID_A, ID_B, T_A)$, 发送 (ID_A, T_A) 给 Bob。

（2）Bob 收到消息 (ID_A, T_A) 后, 选择随机数 $b \in_R \mathbb{Z}_q^*$, 计算 $T_B = bP$, $K_1^B = \hat{e}(H_1(ID_A), (x+b)P_{pub_1})$, $K_2^B = \hat{e}(H_1(ID_A), yP_{pub_1})$, $K_3^B = bT_A$, $K_4^B = (x+y)T_A$, $(k_m, k) = H(ID_A \| ID_B \| T_A \| T_B \| X \| R \| K_1^B \| K_2^B \| K_3^B \| K_4^B)$, $tag_B = MAC_{k_m}(\mathcal{R} \| K_1^B \| ID_A \| ID_B \| T_A \| T_B \| X \| R \| K_2^B \| K_3^B \| K_4^B)$，设置会话标识为 $sid_j^w = (\mathcal{R}, ID_B, ID_A, T_A, T_B, X, R, tag_B)$, 发送 (ID_B, T_B, X, R, tag_B) 给 Alice。

（3）Alice 收到消息 (ID_B, X, R, T_B, tag_B) 以后, 计算 $K_1^A = \hat{e}(d_A, (X + T_B))$, $K_2^A = \hat{e}(d_A, R + H_2(ID_B, R)P_{pub_2})$, $K_3^A = aT_B$, $K_4^A = a[R + H_2(ID_B, R)P_{pub_2} + X]$, $(k_m, k) = H(ID_A \| ID_B \| T_A \| T_B \| X \| R \| K_1^A \| K_2^A \| K_3^A \| K_4^A)$, 令 $SB = MAC_{k_m}(\mathcal{R} \| K_1^A \| ID_A \| ID_B \| T_A \| T_B \| X \| R \| K_2^A \| K_3^A \| K_4^A)$, 验证 $Ver_{k_m}(SB, tag_B) \stackrel{?}{=} 1$, 如果验证通过, 计算 $tag_A = (\mathcal{I} \| K_1^A \| ID_A \| ID_B \| T_A \| T_B \| X \| R \| K_2^A \| K_3^A \| K_4^A)$, 发送 tag_A 给 Bob。更新会话标识符为 $sid_i^t = (\mathcal{I}, ID_A, ID_B, T_A, T_B, X, R, tag_B, tag_A)$, 接受会话密钥 (k_m, k) 并完成会话。

（4）令 $SA = (\mathcal{I} \| K_1^B \| ID_A \| ID_B \| T_A \| T_B \| X \| R \| K_2^B \| K_3^B \| K_4^B)$, Bob 验证 $Ver_{k_m}(SA, tag_A) \stackrel{?}{=} 1$, 如果验证通过, 则更新会话标识符 $sid_j^w = (\mathcal{R}, ID_B, ID_A, T_A, T_B, X, R, tag_B, tag_A)$, 接受会话密钥 (k_m, k) 并完成会话。

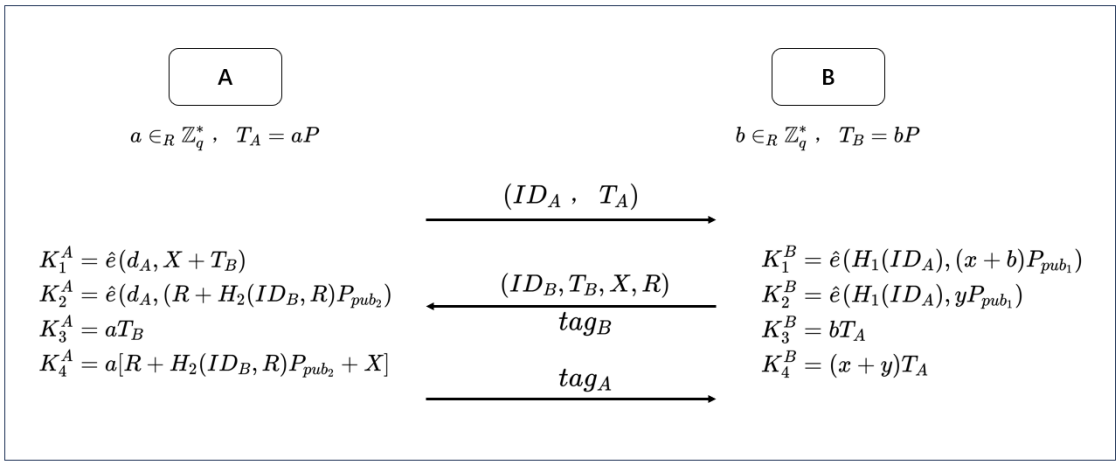

图 4.2　CDAKE 协议密钥协商过程

简单验证会话密钥的正确性。

$$K_1 = K_1^A = \hat{e}(d_A, X + T_B) = \hat{e}(H_1(ID_A), (x + b)P_{pub_1}) = K_1^B$$
$$K_2 = K_2^A = \hat{e}(d_A, R + [H_2(ID_B, R)P_{pub_2}]) = \hat{e}(H_1(ID_A), yP_{pub_1}) = K_2^B$$
$$K_3 = K_3^A = aT_B = bT_A = K_3^B$$
$$K_4 = K_4^A = a[R + H_2(ID_B, R)P_{pub_2} + X] = (x + y)T_A = K_4^B$$

则会话双方能协商出一致的密钥。$(k_m, k) = H(ID_A \| ID_B \| T_A \| T_B \| X \| R \| K_1 \| K_2 \| K_3 \| K_4)$, 协议具备正确性。

4.3.2　安全证明

定理 4.1　如果 CBDH 假设成立, H, H_1, H_2 是随机谕言机, 那么协议 ϵ 在 4.2 节提出的改进的无证书 eck 模型中是安全的。

证明：假设敌手最多激活 n_1 个基于标识密码体制的用户, n_2 个基于无证书体制的用户, 且最多激活 n_s 个会话, 假设敌手在上述安全游戏中获胜的概率 $Adv^{\epsilon}_{\mathcal{A}}(\kappa)$ 是不可忽略的。由于 H 被建模为随机谕言机, 敌手发起 $Test(\Pi^{T}_{I,J})$ 查询后, 只能通过以下三种方式赢得游戏:

- 密钥猜测攻击。敌手正确猜测出会话密钥。
- 密钥复制攻击。敌手建立了与测试会话 $\Pi^{T}_{I,J}$ 非匹配但是有相同会话密钥的会话。敌手通过查询该会话可以获得测试会话对应的会话密钥。
- 密钥伪造攻击。敌手向 H 查询了测试会话 $\Pi^{T}_{I,J}$ 的有关值 $(ID_A \parallel ID_B \parallel T_A \parallel T_B \parallel K_1 \parallel K_2 \parallel K_3 \parallel K_4)$, 显然在这种情况下, 敌手自行计算出了正确的 (K_1, K_2, K_3, K_4) 。

然而, 通过分析可以知道, 由于 H 是随机谕言机, 密钥猜测攻击相当于是要从密钥空间中正确猜测密钥, 所以敌手能正确猜测 $\Pi^{T}_{I,J}$ 的会话密钥的概率是 $O(\frac{1}{2^{\kappa}})$, 是可忽略的。而在针对 H 的询问中, 输入包含参与会话双方的公钥及临时公钥等信息, 密钥复制攻击需要找到一个关于 H 的碰撞, 碰撞发生的概率为 $O(\frac{n_s^2}{2^{\kappa}})$, 又因为碰撞的概率是可忽略的, 所以下面主要针对敌手的密钥伪造攻击进行分析。

下面的证明中挑战者 $\mathcal{C}$ 通过将敌手 $\mathcal{A}$ 在安全游戏中区分真实密钥和随机密钥的优势转化为它解决 CBDH 问题或 CDH 问题的优势。假设给定 CBDH 问题的实例 (uP, vP, wP), 其中 $uP, vP, wP \in \mathbb{G}_1^*$, $\mathcal{C}$ 的目标是计算出 $BDH(uP, vP, wP) = \hat{e}(P, P)^{abc}$, $Adv_{\mathcal{C}}^{CBDH}(\kappa)$ 为挑战者 $\mathcal{C}$ 在给定安全参数 κ 和利用敌手 $\mathcal{A}$ 的情况下所获得的解决 CBDH 问题的优势。假设给定 CDH 问题的实例 (uP, vP), 其中 $uP, vP \in \mathbb{G}_1^*$, $\mathcal{C}$ 的目标是计算出 $CDH(uP, vP) = uvP$, $Adv_{\mathcal{C}}^{CDH}(\kappa)$ 为挑战者 $\mathcal{C}$ 在给定安全参数 κ 和利用敌手 $\mathcal{A}$ 的情况下所获得的解决 CDH 问题的优势。

在安全游戏开始前, 挑战者试图猜测测试会话及敌手采取的策略。挑战者随机选取参与会话的双方 $I \in_R \{1, \cdots, n_1\}$, $J \in_R \{1, \cdots, n_2\}$, 身份标识分别为 ID_I, ID_J。在基于标识密码体制的用户 ID_I 与基于无证书体制的用户 ID_J 的会话中任选一个会话 $T \in \{1, \cdots, n_s\}$, 猜定测试会话为 $\Pi^{T}_{I,J}$。依据新鲜会话的定义, 敌手 $\mathcal{A}$ 的策略如下所示:

1. 敌手 $\mathcal{A}$ 可能既不知道 ID_I 的标识私钥 d_I, 也不知道 ID_J 的秘密值 x_J （并且不替换 ID_J 的公钥)。
2. 可能既不知道 ID_I 的临时密钥 a, 也不知道 ID_J 的秘密值 x_J （并且不替换 ID_J 的公钥)。

3. 可能既不知道 ID_I 的标识私钥 d_I, 也不知道 ID_J 的部分私钥 y。

4. 可能既不知道 ID_I 的临时密钥 a, 也不知道 ID_J 的部分私钥 y。

5. 可能既不知道 ID_I 的标识私钥 d_I, 也不知道 ID_J 的临时密钥 b。

6. 敌手可能既不知道 ID_I 的临时密钥 a, 也不知道 ID_J 的临时密钥 b。

通过敌手的策略和用户空间，可以得出挑战者猜中敌手策略和测试会话的概率至少为 $\frac{1}{6n_sn_1n_2}$。若敌手 $\mathcal{A}$ 实际选取的测试会话与挑战者 $\mathcal{C}$ 预想的不符, 那么 $\mathcal{C}$ 终止游戏, 否则, $\mathcal{C}$ 选取随机值 $\xi \in_R \{0,1\}^\kappa$ 返回给敌手。根据猜测的策略, 挑战者模拟游戏并回应敌手的测试查询如下:

策略 1： 敌手既不掌握 ID_I 的长期私钥 d_I, 又不掌握 ID_J 的秘密值 b。敌手可能获得 ID_I 的临时密钥 a 和 ID_J 的部分私钥 y 及临时密钥 b。挑战者 $\mathcal{C}$ 利用敌手 $\mathcal{A}$ 来解决 CBDH 问题实例 (uP, vP, wP)。

- Setup：$\mathcal{C}$ 运行启动算法, 生成基于标识密码体制用户的系统参数 $params_1 = \{q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub_1}, H_1\}$ 和 KGC_1 对应的主密钥 u （$\mathcal{C}$ 不知道 u 的具体值）和基于无证书体制用户的系统参数 $params_2 = \{q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub_2}, H_2\}$ 和 KGC_2 对应的主密钥 s_2 （$\mathcal{C}$ 掌握 s_2 ）。$\mathcal{C}$ 将 $params_1, params_2, s_2$ 发给敌手。

- 随机谕言机询问：为了处理随机谕言机询问, 挑战者维护三个相关的列表 L_{H_1}, L_{H_2}, L_H, 三个列表初始化为空。

  H_1 **谕言机：** 在表 L_{H_1} 中的每个条目的形式为 (ID_i, l_i, pk_i), 其中 $l_i \in \mathbb{Z}_q^*$, $pk_i \in \mathbb{G}_1$。当敌手对 $< ID_i >$ 进行 H_1 询问时, 如果 $type = 1$, 则返回 $\perp$, 如果 $type = 0$, 则查询 L_{H_1}, 如果表中已经定义过了这个条目 (ID_i, l_i, pk_i), 则挑战者返回相关的值 pk_i, 否则选择 $l_i \in_R \mathbb{Z}_q^*$, 计算 $pk_i = l_iP$, 并将条目 (ID_i, l_i, pk_i) 插入到表 L_{H_1} 中。

  H_2 **谕言机：** 在表 L_{H_2} 中的每个条目的形式为 (ID_j, R_j, h_j), 其中 $R_j \in \mathbb{G}_1$, $h_j \in \mathbb{Z}_q^*$。当敌手对 $< ID_j, R_j >$ 进行 H_2 询问时, 如果 $type = 0$, 则返回 $\perp$, 如果 $type = 1$, 则查询 L_{H_2}, 如果表中已经定义过了这个条目 (ID_j, R_j, h_j), 则挑战者返回相关的值 h_j, 否则选择 $h_j \in_R \mathbb{Z}_q^*$, 并将条目 (ID_j, R_j, h_j) 插入到表 L_{H_2} 中。

  H **谕言机：** 在表 L_H 中的每个条目的形式为 $(ID_i, ID_j, T_i, T_j, X_j, R_j, K_1, K_2, K_3, K_4, h_1 \parallel h_2)$, 其中 $K_1, K_2 \in \mathbb{G}_2, T_i, T_j, X_j, R_j\ K_3, K_4 \in \mathbb{G}_1, h_1 \times h_2 \in \{0,1\}^{k_m} \times \{0,1\}^k$。当敌手对 $< ID_i, ID_j, T_i, T_j, X_j, R_j, K_1, K_2, K_3, K_4 >$ 进行

H 询问时, 如果表中已经定义过了这个条目, 则挑战者返回相关的值 $(h_1 \parallel h_2)$, 否则在表 L_S 中查找条目 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$, 在表 L_{IBC} 查找条目 (ID_i, l_i, pk_i, d_i), 在表 L_{CL} 中查找对应的条目 $(ID_j, x_j, y_j, X_j, R_j)$, 在表 L_{H_1} 中查找对应的条目 (ID_i, l_i, pk_i), 在表 L_{H_2} 中查找对应的条目 $(ID_j, x_j, y_j, X_j, R_j)$ 。

(1) 如果表 L_S 中存在相应条目, 并满足 $T_i^t = T_i$, $T_j^t = T_j$, $X_j^t = X_j$, $R_j^t = R_j$, $K_1 = \hat{e}(d_i, X_j + T_j)$, $K_2 = \hat{e}(d_i, (R_j + H_2(ID_j, R_j))P_{pub_2})$, $K_3 = r_{i,j}^t T_j$, $K_4 = r_{i,j}^t[R_j + H_2(ID_j, R_j)P_{pub_2} + X_j]$ 及 $sk_{i,j}^t \neq \perp$, 那么令 $(h_1 \parallel h_2) = sk_{i,j}^t$, 返回 $(h_1 \parallel h_2)$ 并更新表 L_H 中对应的值。

(2) 如果表 L_S 中不存在相应条目, 则在表 L_S 中寻找条目 $(\Pi_{j,i}^w, r_{j,i}^w, T_i^w, T_j^w, X_j^w, R_j^w, sk_{j,i}^w)$,

(2.1) 如果存在相应条目, 并满足 $T_i^w = T_i$, $T_j^w = T_j$, $X_j^w = X_j$, $R_j^w = R_j$, $K_1 = \hat{e}(H_1(ID_i), (x_j + r_{j,i}^w)P_{pub_1})$, $K_2 = \hat{e}(H_1(ID_i), yP_{pub_1})$, $K_3 = r_{j,i}^w T_i$, $K_4 = (y_j + x_j)T_i$ 及 $sk_{j,i}^w \neq \perp$, 那么令 $(h_1 \parallel h_2) = sk_{j,i}^w$, 返回 $(h_1 \parallel h_2)$ 并更新表 L_H 中对应的值。

(2.2) 如果表 L_S 中仍不存在相应条目, 则选取 $h_1 \in_R \{0,1\}^{k_m}, h_2 \in_R \{0,1\}^k$, 并将条目 $(ID_i, ID_j, T_i, T_j, X_j, R_j, K_1, K_2, K_3, K_4, h_1 \parallel h_2)$ 插入到表 L_H 中。

- Create($ID_i, type$): $\mathcal{C}$ 维护列表 L_{IBC}, L_{CL}, 初始化为空, 表 L_{IBC} 中的每个条目的形式为 (ID_i, l_i, pk_i, d_i), 表 L_{CL} 中的每个条目的形式为 $(ID_i, x_i, y_i, X_i, R_i)$。接收到该询问后, 挑战者作出如下回答:

  如果 $type = 0$,

  - 如果 $ID_i \neq ID_I$, 则选取 $l_i \in_R \mathbb{Z}_q^*$, 计算 $pk_i = l_i P$, $d_i = l_i uP$, 将 (ID_i, l_i, pk_i, d_i) 添加至表 L_{IBC} 中, 将 (ID_i, l_i, pk_i) 添加至表 L_{H_1} 中。
  - 如果 $ID_i = ID_I$, 则选取 $l_I \in_R \mathbb{Z}_q^*$, 计算 $pk_I = l_I vP$, 将 $(ID_I, l_I, pk_I, \perp)$ 添加至表 L_{IBC} 中, 将 (ID_I, l_I, pk_I) 添加至表 L_{H_1} 中。

  如果 $type = 1$,

  - 如果 $ID_i \neq ID_J$, 则选取 $x_i, y_i, h_i \in_R \mathbb{Z}_q^*$, 计算 $X_i = x_i P$, $R_i = y_i P - h_i P_{pub}$, 并将 (ID_i, R_i, h_i) 添加至表 L_{H_2} 中, 将 $(ID_i, x_i, y_i, X_i, R_i)$ 添加至表 L_{CL} 中。

– 如果 $ID_i = ID_J$, 则令 $X_J = wP$, 选取 $y_J, h_J \in_R \mathbb{Z}_q^*$, 计算 $R_J = y_J P - h_J P_{pub_2}$, 将 (ID_J, R_J, h_J) 添加至表 L_{H_2} 中, 将 $(ID_J, \perp, y_J, X_J, R_J)$ 添加至表 L_{CL} 中。

假设敌手在进行其他询问时, 已询问过 Create(ID_i, $type$)。

- MasterPrivateKeyReveal(ID_i, $type$): 接收到该询问后, 如果 $type = 0$, 则返回 $\perp$, 如果 $type = 1$, 则返回 KGC_2 对应的系统主密钥 s_2

- StaticKeyReveal(ID_i, $type$): 接收到该询问后, 如果 $ID_i = ID_I$, 则返回 $\perp$, 如果 $type = 0$, 挑战者在表 L_{IBC} 中寻找以 ID_i 为索引的条目, 将 d_i 返回给敌手, 如果 $type = 1$, 则返回 $\perp$ 。

- PartialPrivateKeyReveal(ID_i, $type$): 接收到该询问后, 如果 $type = 1$, 挑战者在表 L_{CL} 中寻找以 ID_i 为索引的条目, 将 y_i 返回给敌手, 如果 $type = 0$, 则返回 $\perp$ 。

- SecretValueReveal(ID_i, $type$): 接收到该询问后, 如果 $type = 1$, 且 $ID_i = ID_J$, 则终止游戏, 否则在 L_{CL} 中寻找以 ID_i 为索引的条目, 将 x_i 返回给敌手。如果 $type = 0$, 则返回 $\perp$ 。

- Send($\Pi_{i,j}^t$, $comm$): 挑战者维护列表 L_S, 初始化为空, 表 L_S 中的每个条目的形式为 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$, 其中 $r_{i,j}^t$ 是会话 $\Pi_{i,j}^t$ 的临时密钥, T_i^t 和 T_j^t 是 ID_i 的第 t 个会话中发送与接收到的临时公钥, (X_j^t, R_j^t) 是 ID_j 的公钥, $sk_{i,j}^t$ 是会话 $\Pi_{i,j}^t$ 的会话密钥。接收到该询问后, 挑战者作出如下回答:

  – 如果 $comm = \lambda$, 则挑战者选择 $r_{i,j}^t \in_R \mathbb{Z}_q^*$, 返回 $(ID_i, T_i^t = r_{i,j}^t P)$ 。

  – 如果 $comm = (ID_j, X_j^t, R_j^t, T_j^t)$, 则挑战者选择 $r_{i,j}^t \in_R \mathbb{Z}_q^*$, 返回 $(ID_i, T_i^t = r_{i,j}^t P)$, 令 $sk_{i,j}^t = \perp$, 添加 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$ 至表 L_S 中。

- EphemeralKeyReveal($\Pi_{i,j}^t$): 接收到该询问后, 挑战者在表 L_S 中寻找以 $\Pi_{i,j}^t$ 为索引的条目中临时秘密值返回给敌手。

- SessionKeyReveal($\Pi_{i,j}^t$): 接收到该询问后, $\mathcal{C}$ 在表 L_S 中寻找以 $\Pi_{i,j}^t$ 为索引的条目 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_j^t)$, 挑战者作出如下回答:

  (1) 如果 $\Pi_{i,j}^t = \Pi_{I,J}^T$ 或是与 $\Pi_{I,J}^T$ 相匹配的会话 $\Pi_{J,I}^W$, 那么 $\mathcal{C}$ 终止游戏。

  (2) 如果 $sk_{i,j}^t \neq \perp$, 返回 $sk_{i,j}^t$; 如果 $sk_{i,j}^t = \perp$, 查询对应的匹配会话 $\Pi_{j,i}^w$ 对应的条目, 如果 $sk_{j,i}^w \neq \perp$, 则返回 $sk_{j,i}^w$, 如果 $sk_{j,i}^w = \perp$, 则执行第三步操作:

(3) 判断表 L_H 中是否存在条目 $(ID_i, ID_j, T_i, T_j, X_j, R_j, K_1, K_2, K_3, K_4, h_1 \parallel h_2)$。

(3.1) 如果 L_H 中存在相应条目, 判断下列等式是否均成立: $T_i^t = T_i, T_j^t = T_j, X_j^t = X_j, R_j^t = R_j, K_1 = \hat{e}(d_i, X_j + T_j), K_2 = \hat{e}(d_i, (R_j + H_2(ID_j, R_j))P_{pub_2}), K_3 = r_{i,j}^t T_j, K_4 = r_{i,j}^t[R_j + H_2(ID_j, R_j)P_{pub_2} + X_j]$。如果等式均成立, 则返回 $(h_1 \parallel h_2)$, 并更新表 L_S 中的 $sk_{i,j}^t$。

(3.2) 如果 L_H 中不存在相应条目, 则选择 $h_1 \in_R \{0,1\}^{k_m}, h_2 \in_R \{0,1\}^k$, 并更新表 L_S 中的 $sk_{i,j}^t$。

- Test($\Pi_{i,j}^t$): 如果 $\Pi_{i,j}^t \neq \Pi_{I,J}^T$, 那么游戏终止, 如果 $\Pi_{i,j}^t = \Pi_{I,J}^T$, 挑战者选择 $h_1 \in_R \{0,1\}^{k_m}, h_2 \in_R \{0,1\}^k$ 作为输出结果。

若敌手成功实施密钥伪造攻击, 且最多对 H 谕言机进行 q_H 次询问, 则 $\mathcal{C}$ 能够以至少 $\frac{1}{q_H}$ 的概率在表 L_H 中找到含有正确 K_1 的相应条目, $K_1 = \hat{e}(l_I vP, (w + r_{i,j}^t)P_{pub_1})$, 则 $\hat{e}(vP, wP)^u = K_1^{{l_I}^{-1}} \cdot \hat{e}(l_I vP, r_{i,j}^t P_{pub_1})^{-1}$ 即为 CBDH 问难问题的解, 从而 $\mathcal{C}$ 有 $\frac{1}{6n_s n_1 n_2 q_H}$ 的优势解决 CBDH 困难问题, 这与困难问题假设相矛盾, 所以该协议在敌手选择策略 1 的情况下是安全的。

策略 2: 敌手既不掌握 ID_I 的临时密钥 a, 也不掌握 ID_J 的秘密值 x_J。敌手获得 ID_I 的长期私钥 d_I 和 ID_J 的部分私钥 y 及临时密钥 b。挑战者 $\mathcal{C}$ 利用敌手 $\mathcal{A}$ 解决 CDH 问题实例 (vP, wP)。

- Setup: $\mathcal{C}$ 运行启动算法, 生成基于标识密码体制用户的系统参数 $params_1 = \{q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub_1}, H_1\}$ 和 KGC_1 对应的主密钥 s_1 ($\mathcal{C}$ 知道 s_1 的具体值) 和基于无证书体制用户的系统参数 $params_2 = \{q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub_2}, H_2\}$ 和 KGC_2 对应的主密钥 s_2 ($\mathcal{C}$ 掌握 s_2)。$\mathcal{C}$ 将 $params_1, params_2, s_2$ 发给敌手。

- 随机谕言机询问: 与策略 1 一致。

- Create($ID_i, type$): $\mathcal{C}$ 维护列表 L_{IBC}, L_{CL}, 初始化为空, 表 L_{IBC} 中的每个条目的形式为 (ID_i, l_i, pk_i, d_i), 表 L_{CL} 中的每个条目的形式为 $(ID_i, x_i, y_i, X_i, R_i)$。接收到该询问后, 挑战者作出如下回答:

  如果 $type = 0$, 选取 $l_i \in_R \mathbb{Z}_q^*$, 计算 $pk_i = l_i P, d_i = l_i s_1 P$, 将 (ID_i, l_i, pk_i, d_i) 添加至表 L_{IBC} 中, 将 (ID_i, l_i, pk_i) 添加至表 L_{H_1} 中。

  如果 $type = 1$,

  - 如果 $ID_i \neq ID_J$, 则选取 $x_i, y_i, h_i \in_R \mathbb{Z}_q^*$, 计算 $X_i = x_iP$, $R_i = y_iP - h_iP_{pub}$, 并将 (ID_i, R_i, h_i) 添加至表 L_{H_2} 中, 将 $(ID_i, x_i, y_i, X_i, R_i)$ 添加至表 L_{CL} 中。
  - 如果 $ID_i = ID_J$, 则令 $X_J = wP$, 选取 $y_J, h_J \in_R \mathbb{Z}_q^*$, 计算 $R_J = y_JP - h_JP_{pub_2}$, 将 (ID_J, R_J, h_J) 添加至表 L_{H_2} 中, 将 $(ID_J, \perp, y_J, X_J, R_J)$ 添加至表 L_{CL} 中。

    假设敌手在进行其他询问时, 已询问过 Create($ID_i, type$)。

- MasterPrivateKeyReveal($ID_i, type$): 接收到该询问后, 如果 $type = 0$, 则返回 KGC_1 对应的系统主密钥 s_1, 如果 $type = 1$, 则返回 KGC_2 对应的系统主密钥 s_2

- StaticKeyReveal($ID_i, type$): 如果 $type = 0$, 由于敌手掌握 KGC_1 对应的系统主密钥 s_1, 所以无需发起此询问, 敌手可以通过对随机谕言机 H_1 的询问计算得到 ID_i 的固定私钥 $d_i = s_1H_1(ID_i)$, 如果 $type = 1$, 则返回 $\perp$ 。

- PartialPrivateKeyReveal($ID_i, type$): 与策略 1 一致。

- SecretValueReveal($ID_i, type$): 与策略 1 一致。

- EphemeralKeyReveal($\Pi_{i,j}^t$): 接收到该询问后, 若 $\Pi_{i,j}^t = \Pi_{I,J}^T$, 挑战者终止游戏, 否则在表 L_S 中寻找以 $\Pi_{i,j}^t$ 为索引的条目中临时密钥返回给敌手。

- Send $(\Pi_{i,j}^t, comm)$: 挑战者维护列表 L_S, 初始化为空, 表 L_S 中的每个条目的形式为 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$, 其中 $r_{i,j}^t$ 是会话 $\Pi_{i,j}^t$ 的临时密钥, T_i^t 和 T_j^t 是 ID_i 的第 t 个会话中发送与接收到的临时公钥, (X_j^t, R_j^t) 是 ID_j 的公钥, $sk_{i,j}^t$ 是会话 $\Pi_{i,j}^t$ 的会话密钥。接收到该询问后, 挑战者作出如下回答:
  - 如果 $comm = \lambda$, 则挑战者选择 $r_{i,j}^t \in_R \mathbb{Z}_q^*$, 返回 $(ID_i, T_i^t = r_{i,j}^tP)$ 。
  - 如果 $comm = (ID_j, X_j^t, R_j^t, T_j^t)$, 则挑战者选择 $r_{i,j}^t \in_R \mathbb{Z}_q^*$, 返回 $(ID_i, T_i^t = r_{i,j}^tP)$, 令 $sk_{i,j}^t = \perp$, 添加 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$ 至表 L_S 中。若 $n = T$, $ID_i = ID_I$, $ID_j = ID_J$, 那么令 $r_{I,J}^T = \perp$, $T_I^T = vP$, $sk_{i,j}^t = \perp$, 然后添加 $(\Pi_{I,J}^T, \perp, T_I^T, T_J^T, X_J^T, R_J^T, \perp)$ 至表 L_S 中。

- SessionKeyReveal($\Pi_{i,j}^t$): 与策略 1 一致。

- Test($\Pi_{i,j}^t$): 如果 $\Pi_{i,j}^t \neq \Pi_{I,J}^T$, 那么游戏终止, 如果 $\Pi_{i,j}^t = \Pi_{I,J}^T$, 挑战者选择 $h_1 \in_R \{0,1\}^{k_m}, h_2 \in_R \{0,1\}^k$ 作为输出结果。

若敌手成功实施密钥伪造攻击, 且最多对 H 谕言机进行 q_H 次询问, 则 $\mathcal{C}$ 能够以至少 $\frac{1}{q_H}$ 的概率在表 L_H 中找到含有正确 K_4 的相应条目, $K_4 = vP(w + y_J) = T_I^T(w + y_J)$, 则 $vwP = K_4 - T_I^T y_J$ 即为 CDH 困难问题的解, 从而 $\mathcal{C}$ 有 $\frac{1}{6n_s n_1 n_2 q_H}$ 的优势解决 CDH 困难问题, 这与困难问题假设相矛盾, 所以该协议在敌手选择策略 2 的情况下是安全的。

策略 3： 敌手既不掌握 ID_I 的长期私钥 d_I, 也不掌握 ID_J 的部分私钥 y。敌手获得 ID_I 的临时密钥 a 和 ID_J 的秘密值 x_J 及临时密钥 b。挑战者 $\mathcal{C}$ 利用敌手 $\mathcal{A}$ 解决 CBDH 问题实例 (uP, vP, wP)。

- Setup: $\mathcal{C}$ 运行启动算法, 生成基于标识密码体制用户的系统参数 $params_1 = \{q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub_1}, H_1\}$ 和 KGC_1 对应的主密钥 u （$\mathcal{C}$ 不知道 u 的具体值) 和基于无证书体制用户的系统参数 $params_2 = \{q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub_2}, H_2\}$ 和 KGC_2 对应的主密钥 s_2 （$\mathcal{C}$ 不掌握 s_2)。$\mathcal{C}$ 将 $params_1, params_2$ 发给敌手。

- Create($ID_i, type$): $\mathcal{C}$ 维护列表 L_{IBC}, L_{CL}, 初始化为空, 表 L_{IBC} 中的每个条目的形式为 (ID_i, l_i, pk_i, d_i), 表 L_{CL} 中的每个条目的形式为 $(ID_i, x_i, y_i, X_i, R_i)$。接收到该询问后, 挑战者作出如下回答:

  如果 $type = 0$, 回答和策略 1 一致。

  如果 $type = 1$,

  - 如果 $ID_i \neq ID_J$, 则随机选取 $x_i, y_i, h_i \in_R \mathbb{Z}_q^*$, 计算 $X_i = x_i P$, $R_i = y_i P - h_i P_{pub}$, 并将 (ID_i, R_i, h_i) 添加至表 L_{H_2} 中, 将 $(ID_i, x_i, y_i, X_i, R_i)$ 添加至表 L_{CL} 中。
  - 如果 $ID_i = ID_J$, 则随机选取 $x_J \in_R \mathbb{Z}_q^*$, 计算 $X_J = x_J P$, 令 $Y_J = wP$, 随机选取 $r_J, h_J \in_R \mathbb{Z}_q^*$, 计算 $R_J = r_J P$, $P_{pub_2} = (Y_J - R_J)h_J^{-1}$, 添加 (ID_J, R_J, h_J) 至表 L_{H_2} 中, 最后添加 $(ID_J, x_J, \perp, X_J, R_J)$ 到表 L_{CL} 中。

  假设敌手在进行其他询问时, 已询问过 Create(ID_i, $type$)。

- MasterPrivateKeyReveal(ID_i, $type$): 接收到该询问后, 返回 $\perp$。

- StaticKeyReveal(ID_i, $type$): 和策略 1 一致。

- PartialPrivateKeyReveal(ID_i, $type$): 接收到该询问后, 如果 $type = 1$, 且 $ID_i = ID_J$, 则挑战者终止游戏, 否则在表 L_{CL} 中寻找以 ID_i 为索引的条目, 将 y_i 返回给敌手, 如果 $type = 0$, 则返回 $\perp$。

- SecretValueReveal($ID_i, type$): 接收到该询问后, 如果 $type = 1$, 在表 L_{CL} 中寻找以 ID_i 为索引的条目, 返回 x_i 给敌手。如果 $type = 0$, 则返回 $\perp$ 。

- PublicKeyReplace($ID_i, type, X'$): 接收到该询问后, 如果 $type = 1$, 挑战者在表 L_{CL} 中寻找并更新以 ID_i 为索引的条目, 使用新公钥替换旧公钥, 令 $X_i = X', x_i = \perp$, 并且在后续的会话使用新公钥。如果 $type = 0$, 则返回 $\perp$ 。

- Send($\Pi_{i,j}^t, comm$): 和策略 1 一致。

- EphemeralKeyReveal($\Pi_{i,j}^t$): 和策略 1 一致。

- SessionKeyReveal($\Pi_{i,j}^t$): 和策略 1 一致。

- Test($\Pi_{i,j}^t$): 如果 $\Pi_{i,j}^t \neq \Pi_{I,J}^T$, 那么游戏终止, 如果 $\Pi_{i,j}^t = \Pi_{I,J}^T$, 挑战者选择 $h_1 \in_R \{0,1\}^{k_m}, h_2 \in_R \{0,1\}^k$ 作为输出结果。

若敌手成功实施密钥伪造攻击, 且最多对 H 谕言机进行 q_H 次询问, 则 $\mathcal{C}$ 能够以至少 $\frac{1}{q_H}$ 的概率在表 L_H 中找到含有正确 K_2 的相应条目, $K_2 = \hat{e}(l_I vP, wP)$, 则 K_2 即为 CBDH 困难问题的解, 从而 $\mathcal{C}$ 有 $\frac{1}{6n_s n_1 n_2 q_H}$ 的优势解决 CDH 困难问题, 这与困难问题假设相矛盾, 所以该协议在敌手选择策略 3 的情况下是安全的。

策略 4: 敌手既不掌握 ID_I 的临时密钥 a, 也不掌握 ID_J 的部分私钥 y 。敌手获得 ID_I 的长期私钥 d_I 和 ID_J 的秘密值 x_J 及临时密钥 b 。挑战者 $\mathcal{C}$ 利用敌手 $\mathcal{A}$ 解决 CDH 问题实例 (vP, wP) 。

- Setup: $\mathcal{C}$ 运行启动算法, 生成基于标识密码体制用户的系统参数 $params_1 = \{q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub_1}, H_1\}$ 和 KGC_1 对应的主密钥 s_1 ($\mathcal{C}$ 知道 s_1 的具体值) 和基于无证书体制用户的系统参数 $params_2 = \{q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub_2}, H_2\}$ 和 KGC_2 对应的主密钥 s_2 ($\mathcal{C}$ 不掌握)。$\mathcal{C}$ 将 $params_1, params_2$ 发给敌手。

- Create($ID_i, type$): 如果 $type = 0$, 回答和策略 2 一致, 如果 type=1, 回答和策略 3 一致。

- MasterPrivateKeyReveal($ID_i, type$): 接收到该询问后, 如果 $type = 0$, 则返回 KGC_1 对应的系统主密钥 s_1, 如果 $type = 1$, 则返回 $\perp$ 。

- StaticKeyReveal($ID_i, type$): 和策略 2 一致。

- PartialPrivateKeyReveal($ID_i, type$): 和策略 3 一致。

- SecretValueReveal($ID_i, type$): 和策略 3 一致。

- PublicKeyReplace($ID_i, type, X'$): 和策略 3 一致。
- Send($\Pi_{i,j}^t, comm$): 和策略 2 一致。
- EphemeralKeyReveal($\Pi_{i,j}^t$): 和策略 1 一致
- SessionKeyReveal($\Pi_{i,j}^t$): 和策略 1 一致。
- Test($\Pi_{i,j}^t$): 如果 $\Pi_{i,j}^t \neq \Pi_{I,J}^T$, 那么游戏终止, 如果 $\Pi_{i,j}^t = \Pi_{I,J}^T$, 挑战者选择 $h_1 \in_R \{0,1\}^{k_m}, h_2 \in_R \{0,1\}^k$ 作为输出结果。

若敌手成功实施密钥伪造攻击, 且最多对 H 谕言机进行 q_H 次询问, 则 $\mathcal{C}$ 能够以至少 $\frac{1}{q_H}$ 的概率在表 L_H 中找到含有正确 K_4 的相应条目, $K_4 = vP(x_J + w) = T_I^T(x_J + w)$, 则 $vwP = K_4 - T_I^T w_J$ 即为 CDH 困难问题的解, 从而 $\mathcal{C}$ 有 $\frac{1}{6n_s n_1 n_2 q_H}$ 的优势解决 CDH 困难问题, 这与困难问题假设相矛盾, 所以该协议在敌手选择策略 2 的情况下是安全的。

策略 5: 敌手既不掌握 ID_I 的长期私钥 d_I, 也不掌握 ID_J 的临时密钥 b 。敌手获得 ID_I 的临时密钥 a 和 ID_J 的秘密值 x_J 及部分私钥 y 。挑战者 $\mathcal{C}$ 利用敌手 $\mathcal{A}$ 解决 CBDH 问题实例 (uP, vP, wP) 。

- Setup: 和策略 3 一致。
- Create($ID_i, type$): $\mathcal{C}$ 维护列表 L_{IBC}, L_{CL}, 初始化为空, 表 L_{IBC} 中的每个条目的形式为 (ID_i, l_i, pk_i, d_i), 表 L_{CL} 中的每个条目的形式为 $(ID_i, x_i, y_i, X_i, R_i)$ 。接收到该询问后, 挑战者作出如下回答:

  如果 $type = 0$, 回答和策略 1 一致。如果 type=1, 随机选取 $x_i, y_i, h_i \in_R \mathbb{Z}_q^*$, 计算 $X_i = x_i P$, $R_i = y_i P - h_i P_{pub}$, 并将 (ID_i, R_i, h_i) 添加至表 L_{H_2} 中, 将 $(ID_i, x_i, y_i, X_i, R_i)$ 添加至表 L_{CL} 中。
- MasterPrivateKeyReveal($ID_i, type$): 和策略 3 一致。
- StaticKeyReveal($ID_i, type$): 和策略 1 一致。
- PartialPrivateKeyReveal($ID_i, type$): 和策略 1 一致。
- SecretValueReveal($ID_i, type$): 和策略 3 一致。
- PublicKeyReplace($ID_i, type, X'$): 和策略 3 一致。

- Send($\Pi_{i,j}^t, comm$): 挑战者维护列表 L_S, 初始化为空, 表 L_S 中的每个条目的形式为 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$, 其中 $r_{i,j}^t$ 是会话 $\Pi_{i,j}^t$ 的临时密钥, T_i^t 和 T_j^t 是 ID_i 的第 t 个会话中发送与接收到的临时公钥, (X_j^t, R_j^t) 是 ID_j 的公钥, $sk_{i,j}^t$ 是会话 $\Pi_{i,j}^t$ 的会话密钥。接收到该询问后, 挑战者作出如下回答:
  - 如果 $comm = \lambda$, 则挑战者选择 $r_{i,j}^t \in_R \mathbb{Z}_q^*$, 返回 $(ID_i, T_i^t = r_{i,j}^t P)$ 。
  - 如果 $comm = (ID_j, X_j^t, R_j^t, T_j^t)$, 则挑战者选择 $r_{i,j}^t \in_R \mathbb{Z}_q^*$, 返回 $(ID_i, T_i^t = r_{i,j}^t P)$, 令 $sk_{i,j}^t = \perp$, 添加 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$ 至表 L_S 中。若 $\Pi_{i,j}^t$ 是 $\Pi_{I,J}^T$ 的匹配会话 $\Pi_{J,I}^W$, 则令 $r_{J,I}^W = \perp$, $T_J^T = wP$, $sk_{i,j}^t = \perp$, 然后添加 $(\Pi_{J,I}^W, \perp, T_I^T, T_J^T, X_J^T, R_J^T, \perp)$ 至表 L_S 中。
- EphemeralKeyReveal($\Pi_{i,j}^t$): 和策略 2 一致。
- SessionKeyReveal($\Pi_{i,j}^t$): 和策略 1 一致。
- Test($\Pi_{i,j}^t$): 如果 $\Pi_{i,j}^t \neq \Pi_{I,J}^T$, 那么游戏终止, 如果 $\Pi_{i,j}^t = \Pi_{I,J}^T$, 挑战者选择 $h_1 \in_R \{0,1\}^{k_m}, h_2 \in_R \{0,1\}^k$ 作为输出结果。

若敌手成功实施密钥伪造攻击, 且最多对 H 谕言机进行 q_H 次询问, 则 $\mathcal{C}$ 能够以至少 $\frac{1}{q_H}$ 的概率在表 L_H 中找到含有正确 K_1 的相应条目, $K_1 = \hat{e}(l_I vP, (w + r_{i,j}^t)P_{pub_1})$, 则 $\hat{e}(vP, wP)^u = K_1^{{l_I}^{-1}} \cdot \hat{e}(l_I vP, r_{i,j}^t P_{pub_1})^{-1}$ 即为 CBDH 问难问题的解, 从而 $\mathcal{C}$ 有 $\frac{1}{6n_s n_1 n_2 q_H}$ 的优势解决 CBDH 困难问题, 这与困难问题假设相矛盾, 所以该协议在敌手选择策略 5 的情况下是安全的。

策略 6: 敌手既不掌握 ID_I 的临时密钥 a, 也不掌握 ID_J 的临时密钥 b 。敌手获得 ID_I 的长期私钥 d_I 和 ID_J 的秘密值 x_J 及部分私钥 y 。挑战者 $\mathcal{C}$ 利用敌手 $\mathcal{A}$ 解决 CBDH 问题实例 (vP, wP) 。

- Setup: 和策略 4 一致。
- Create($ID_i, type$): 如果 $type = 0$, 回答和策略 2 一致。如果 $type = 1$, 回答和策略 5 一致。
- MasterPrivateKeyReveal($ID_i, type$): 和策略 4 一致。
- StaticKeyReveal($ID_i, type$): 和策略 4 一致。
- PartialPrivateKeyReveal($ID_i, type$): 和策略 1 一致。
- SecretValueReveal($ID_i, type$): 和策略 3 一致。

- PublicKeyReplace($ID_i, type, X'$): 和策略 3 一致。

- Send($\Pi_{i,j}^t, comm$): 挑战者维护列表 L_S, 初始化为空, 表 L_S 中的每个条目的形式为 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$, 其中 $r_{i,j}^t$ 是会话 $\Pi_{i,j}^t$ 的临时密钥, T_i^t 和 T_j^t 是 ID_i 的第 t 个会话中发送与接收到的临时公钥, (X_j^t, R_j^t) 是 ID_j 的公钥, $sk_{i,j}^t$ 是会话 $\Pi_{i,j}^t$ 的会话密钥。接收到该询问后, 挑战者作出如下回答:

  - 如果 $comm = \lambda$, 则挑战者选择 $r_{i,j}^t \in_R \mathbb{Z}_q^*$, 返回 $(ID_i, T_i^t = r_{i,j}^t P)$ 。
  - 如果 $comm = (ID_j, X_j^t, R_j^t, T_j^t)$, 则挑战者选择 $r_{i,j}^t \in_R \mathbb{Z}_q^*$, 返回 $(ID_i, T_i^t = r_{i,j}^t P)$, 令 $sk_{i,j}^t = \perp$, 添加 $(\Pi_{i,j}^t, r_{i,j}^t, T_i^t, T_j^t, X_j^t, R_j^t, sk_{i,j}^t)$ 至表 L_S 中。那么令 $r_{I,J}^T = \perp, T_I^T = vP, sk_{i,j}^t = \perp$, 然后添加 $(\Pi_{I,J}^T, \perp, T_I^T, T_J^T, X_J^T, R_J^T, \perp)$ 至表 L_S 中。

    若 $\Pi_{i,j}^t = \Pi_{I,J}^T$, 那么令 $r_{I,J}^T = \perp, T_I^T = vP, sk_{i,j}^t = \perp$, 然后添加 $(\Pi_{I,J}^T, \perp, T_I^T, T_J^T, X_J^T, R_J^T, \perp)$ 至表 L_S 中。若 $\Pi_{i,j}^t$ 是 $\Pi_{I,J}^T$ 的匹配会话 $\Pi_{J,I}^W$, 则令 $r_{J,I}^W = \perp, T_J^T = wP, sk_{i,j}^t = \perp$, 然后添加 $(\Pi_{J,I}^W, \perp, T_I^T, T_J^T, X_J^T, R_J^T, \perp)$ 至表 L_S 中。

- EphemeralKeyReveal($\Pi_{i,j}^t$): 接收到该询问后, 如果 $\Pi_{i,j}^t = \Pi_{I,J}^T$ 或其匹配会话 $\Pi_{J,I}^W$, 挑战者终止游戏, 否则在表 L_S 中寻找以 $\Pi_{i,j}^t$ 为索引的条目中临时密钥值返回给敌手。

- SessionKeyReveal($\Pi_{i,j}^t$): 和策略 1 一致。

- Test($\Pi_{i,j}^t$): 如果 $\Pi_{i,j}^t \neq \Pi_{I,J}^T$, 那么游戏终止, 如果 $\Pi_{i,j}^t = \Pi_{I,J}^T$, 挑战者选择 $h_1 \in_R \{0,1\}^{k_m}, h_2 \in_R \{0,1\}^k$ 作为输出结果。

若敌手成功实施密钥伪造攻击, 且最多对 H 谕言机进行 q_H 次询问, 则 $\mathcal{C}$ 能够以至少 $\frac{1}{q_H}$ 的概率在表 L_H 中找到含有正确 K_3 的相应条目, $K_3 = vwP$, 则 K_3 即为 CDH 困难问题的解, 从而 $\mathcal{C}$ 有 $\frac{1}{6n_s n_1 n_2 q_H}$ 的优势解决 CDH 困难问题, 这与困难问题假设相矛盾, 所以该协议在敌手选择策略 2 的情况下是安全的。

综上所述, 基于标识与基于无证书体制的跨域认证密钥协商协议在改进的无证书 eck 模型下是安全的。

4.3.3 安全性分析

通过上述协议对敌手攻击方式的模拟，证明了基于标识与基于无证书体制的跨域认证密钥协商协议在改进的无证书 eCK 模型下是安全的，下面对照第2章中提到的认证密钥协商协议的安全性，对所提协议进行形式化分析。

- 已知密钥安全：假设敌手获得了过去的会话的会话密钥，但是在本文设计的跨域认证密钥协商协议中，基于哈希函数的单向性，敌手无法计算哈希函数内的 K_1，K_2，K_3，K_4 的值。同时每次密钥协商过程，用户 A，B 均会随机选择唯一的临时密钥 a，b，由于每次会话选取的临时密钥不同，所以敌手无法根据过去的会话密钥计算当前会话的会话密钥。此外，基于 DL 困难问题，敌手无法从公开信息 T_A，T_B 中求解临时密钥 a，b。所以哈希函数的单向性与临时密钥的唯一性确保了协议符合已知密钥安全。

- 完美前向安全：即使用户双方的长期私钥（d_A，x，y）均泄露后，基于 DL 困难问题，敌手无法从公开信息 T_A，T_B 中求解临时密钥 a，b。由于敌手无法求出 K_3 的具体值，敌手仍旧无法获取当前会话的会话密钥，协议满足完美前向安全。

- KGC 前向安全：即使敌手获取了不同体制下用户的系统主密钥 s_1 和 s_2，即敌手控制了 KGC，由于敌手无法解决 CDH 困难问题，敌手无法求出 K_4 的具体值，敌手无法获取会话密钥，协议满足 KGC 前向安全。

- 非密钥控制：协议由双方独立生成随机值作为临时密钥，能确保没有任何一方能控制密钥的结果，协议满足非密钥控制。

- 抗临时密钥泄露安全：即使敌手获得了临时密钥 a，b，敌手只能通过公开信息计算 $K_3 = abP, K_4 = K_4^A = a[R + H_2(ID_B, R)P_{pub_2} + X]$, 由于敌手无法获取用户私钥（$d_A$，$x$，$y$），无法求解 K_1，K_2，协议满足抗临时密钥泄露安全。

- 抗私钥泄露伪装安全：如果 A 的长期私钥被敌手获得，该敌手能够冒充 A 与其他协议的参与者（例如 B）进行通信。然而，协议中用户公私钥包含唯一的用户 ID，A 的长期私钥泄露不能使得敌手反过来向参与方 A 冒充为其他参与者（例如 B），所以协议满足抗私钥泄露伪装安全。

- 未知会话密钥共享安全：结合协议分析可知，$(k_m, k) = H(ID_A \| ID_B \| T_A \| T_B \| X \| R \| K_1 \| K_2 \| K_3 \| K_4)$，会话密钥的生成过程中包含了用户身份信息 ID_A，ID_B，确保了参与会话用户的合法身份，协议满足未知会话密钥共享安全。

4.3.4 性能分析

本节主要为基于标识与基于无证书体制的跨域认证密钥协商协议的实现和测试，主要测试协议的正确性和通信开销，实验环境如表3.1所示。实验流程如

图4.3所示。首先基于生成元生成两个群 $\mathbb{G}_1$，$\mathbb{G}_2$，利用随机数生成器生成 4 个随机数 RNG_S0，RNG_S1，RNG_R，RNG_X，分别调用 IDC_383_MASTKEY_GEN1 中，生成主密钥 s_0 和对应的 $\mathbb{G}_1$ 群上的主公钥 s_0P，主密钥 s_1 和对应的 $\mathbb{G}_1$ 群上的主公钥 s_1P，$\mathbb{G}_1$ 群上的用户公钥 R，X。调用函数 IDC_383_PRVKEY_GEN2 生成对应的 $\mathbb{G}_2$ 群上的用户私钥，计算基于标识密码体制用户的私钥 d_A，基于无证书密码体制用户的部分私钥 $y = r + s_2H_2(ID_B, R)$。基于不同体制的用户密钥如表4.1所示。

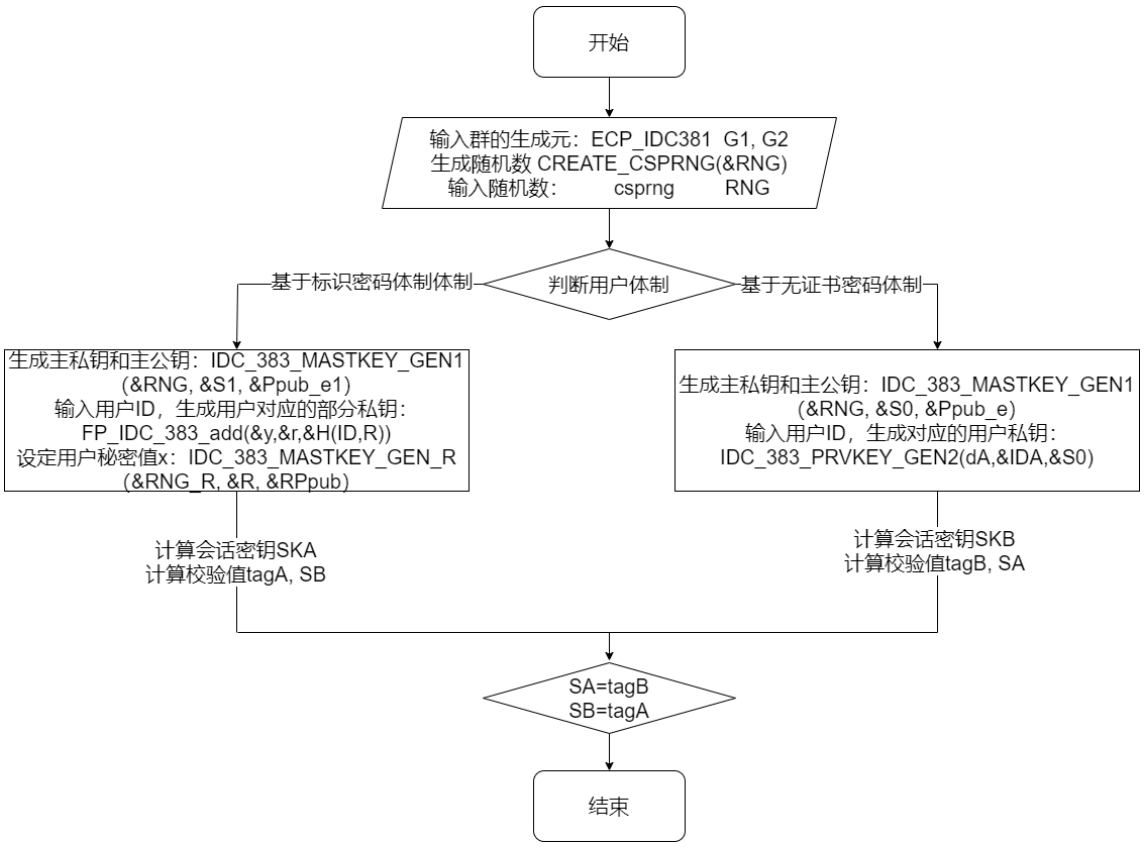

图 4.3　跨域密钥协商协议计算流程图

根据 CDAKE 协议进行密钥协商，实验结果如表4.2所示，协议通过引入 MAC 算法，对比 tag_B 与 SB，tag_A 与 SA，实现了密钥确认。通过结果发现，基于标识密码体制的用户计算耗时 34.961ms，基于无证书用户计算耗时 19.644ms，基于标识密码体制的用户计算耗时更高，这是因为基于标识密码体制用户计算密钥包含了 2 个双线性对、3 个椭圆曲线上的加法运算和 3 个椭圆曲线上的乘法运算，基于无证书体制用户计算密钥包含了 2 个双线性对，四个椭圆曲线上的乘法运算，无证书体制的用户多了 1 个椭圆曲线上的乘法运行运算。CDAKE 协议耗时为 34.961 毫秒。

如表4.3所示为当前跨体制密钥协商协议对比分析，表中展示了不同体制的跨

表 4.1　基于不同体制的用户密钥

	公钥	私钥
基于无证书体制用户	X =0212c153 42b00156 34864cd1 395aa90a 954cc55c b45544fd 80de3740 967bae81 56392976 ecafbf48 85e3aaa0 6369e765 50	x =00000000 00000000 00000000 00000000 e9047c65 057faa4e ffbba973 4a2606e8 49cabd7b 4b474a9e 4679da80 b57e83f7
	R = 0372e5ec dff90e1d 79acf3de 32812e7d f9f69fb4 fc61b1fc 1a8a5af3 060d97e1 62d1d9e8 a96093bd 576f19ee 27803cbd 27	y =79ae263a fc3017f9 7292e873 5f2bca67 49e3daf9 ca1a06e8 d2fb55a6 d2ab2df0 62c8b394 f5683f0a 67e92ebd 32a829ec
基于标识体制用户	Q_A =([74bd09e8 9a74066a 918e5f8e 8451c5f4 bed96f3d 5fb731e6 5115dca0 041574ef 7c8a9c77 3db43a4b 8d8ae872 12d3152e, 761e13d8 29fa9732 9fac4b28 14df057e 1f257175 97ae87eb f61c396b c157d66e e7661d40 5c4ad017 13e5eb5b ab185846 0a37bd45 6e58d682 d1f2c8b6 d358cc28 4dfd3604 5a4c05ba 837e5d28 f18b26bc 8e85b7c0, 1d0ecbbc b9af6f6d ac1fe31a 56f9d12e 79c9fc08 4924795c df50c40d 5909b25f 55519949 f2ce54c3 f1585d84 1d13ec6a])	d_A = ([33e182b2 73be3273 e56fe7fd 35d0ebcb 51a373d9 33f28d1f dac50b36 92c345b2 2624622d 213bea6a 25f6f0af 414ab3a3, 6dd931f9 45505ad7 4e7d61a3 013e924e 7a8b7744 378b09e2 3c59b334 111b4f6f 854fa674 01cb4f33 c1179bfe 602babcd], [5be0d1f2 055adeab f3ffa73a cfad316e 3d7d04bd d92c40f9 967aba5e fbefb1e1 2c013a76 b82d4a21 5ec10639 d6014588, 0e7d4077 825c7dea ccd6b545 161862fe 1daa6dce 4071d5b7 e7b07710 ba93bd34 7dac84ff ff651124 46e89cea 5a895e87])

域密钥协商算法的计算开销。与协议[29] 相同，CDAKE 协议同样利用用户 A 的长期私钥和临时密钥分别与用户 B 的长期公钥和临时公钥进行了四次运算，所以理论上来说来说，密钥协商总开销相同，但是文献[30] 中设计的协议与 CDAKE 协议附带了额外的消息认证码，实现了密钥确认。文献[30] 是针对文献[29] 中提出的协议的优化，通过构造单向陷门函数减少了双线性对的使用，提高了方案的效率，这为下一步优化 CDAKE 协议给出启发。

协议的安全性对比如表4.4所示。从表格中的安全性分析可知，eck 模型是目前针对密钥协商协议安全性最强的模型，在 eck 模型及其变体下证明安全的协议

表 4.2　跨域认证密钥协商协议实验结果

	会话密钥	验签	标签	耗时 (s)
基于无证书体制用户	(SK_B)	/	(tag_B)	0.019644
	7881712b		29dea4a9	
	35ab4840		6ebd4256	
	3c08a00e		d28a8ee7	
	330ef961		4b2c54ca	
	359ca9c7		a425bb66	
	a1c0fe06		bd333704	
	a7481203		4574d37d	
	a3a00d0c		a8aa5ffd	
	0024d645		afb853ef	
	e3524580		32682a94	
	368ef8b3		906f0a7d	
	87ffb692		0f4a058d	
基于标识体制用户	(SK_A)	$SB = tag_B$	(tag_A)	0.034961
	7881712b		399c2b0d	
	35ab4840		906bc74f	
	3c08a00e		7068c0df	
	330ef961		de24ec77	
	359ca9c7		7010d919	
	a1c0fe06		1e4dc647	
	a7481203		9bd79616	
	a3a00d0c		d9e00df1	
	0024d645		a9da8626	
	e3524580		20d94243	
	368ef8b3		e1adfd6c	
	87ffb692		3712ce64	
基于无证书体制用户	(SK_B)	$SA = tag_A$	/	/

具有最强的安全性，协议满足抗未知密钥共享安全 (UKS)，已知密钥安全 (KKS)，前向安全（FS)，抗私钥泄露伪装安全（KCI)，非密钥控制安全（EKR)。

4.4　小结

本章针对跨域通信的需求设计了首个基于标识与基于无证书体制的跨域认证密钥协商协议 CDAKE，具有以下优势：

表 4.3　跨域认证密钥协商协议性能对比

协议	跨域体制	密钥协商总开销
[8]	ID-ID	$2T_{BP}$+$4T_{G_{Mul}}$
[29]	ID-Cert	$4T_{BP}$+$7T_{G_{Mul}}$+$3T_{G_{Add}}$
[30]	ID-Cert	$2T_{BP}$+$9T_{G_{Mul}}$
CDAKE	ID-(CL-PKC)	$4T_{BP}$+$7T_{G_{Mul}}$+$3T_{G_{Add}}$
[28]	(CL-PKC)-(CL-PKC)	$13T_{G_{Mul}}$

表 4.4　跨域认证密钥协商协议安全性对比

协议	安全模型	安全性				
		UKS	KKS	FS	KCI	EKR
[8]	eck	✓	✓	✓	✓	✓
[29]	eck 变体[29]	✓	✓	✓	✓	✓
[30]	eck 变体[29]	✓	✓	✓	✓	✓
CDAKE	改进的无证书 eCK 变体	✓	✓	✓	✓	✓
[28]	无证书 eCK	✓	✓	✓	✓	✓

（1）降低管理复杂性：该协议不需要复杂的证书管理，适合需要管理大量用户的场景；基于标识密码体制简化了公钥分发，适合用户动态变化的场景。

（2）高效的资源利用：在资源丰富的云服务器端使用无证书密码体制，在资源受限的客户端使用标识密码体制，优化了计算和存储资源的利用。

（3）具有较强的灵活性和可扩展性：混合使用两种体系可以适应不同的通信需求和安全要求，提高系统的灵活性和可扩展性。同时本文改进了 Lippold[1] 提出的无证书 eCK 模型, 在此安全模型下，基于 CDH 假设和 CBDH 假设, 对本文提出的跨域协议进行严格安全证明，该协议满足已知密钥安全，前向安全，KGC 前向安全，抗密钥泄露伪装安全，抗未知会话密钥共享安全。

第五章　总结与展望

5.1　总结

针对即时通信的需求，设计高效安全的无证书低交互认证密钥协商协议一直是密码学者的研究热点。本文针对无证书体制下的两方密钥协商协议进行了研究，提出了具有已知密钥安全的基于标识的零交互认证密钥协商协议 IB-ZIAKE 和基于标识与基于无证书体制的跨域认证密钥协商协议 CDAKE，具体来说，本文完成的工作有：

首先，本文针对高安全的即时通信需求，提出了首个具有已知密钥安全的基于标识的零交互认证密钥协商协议 IB-ZIAKE。与原始的 SOK 协议不同，IB-ZIAKE 协议通过加入了每个会话独有的共享随机因子，使用单向哈希函数从双线性配对会话密钥计算中生成唯一的会话密钥，在原有 SOK 协议的基础上增强了协议的安全性，同时实验结果表明协议性能并未有明显变化。其次，本文提出的针对标识体制下的零交互密钥协商安全模型能够将密钥协商协议的安全性从共享密钥的不可区分性（IND-SK）扩展到已知密钥安全，并在文中对 IB-ZIAKE 协议进行了详细的安全证明。然后，通过将 IB-ZIAKE 协议集成到 T-IP 协议中，本文证明，与 IPsec 相比，改进后的协议不仅保留了其固有的低传输开销和减少连接延迟的优势，而且还增强了抵御已知密钥攻击和重放攻击的能力。具体来说，每次会话都使用唯一的会话密钥，这就确保了前一次会话密钥的泄露不会影响未来会话密钥的安全。

另一方面，随着网络环境的日趋复杂，不同的认证服务器有各自的认证域，跨域通信的问题影响着网络通信效率。本文针对基于标识与基于无证书体制下的跨域通信需求，首次提出了基于标识与基于无证书体制下的跨域认证密钥协商协议 CDAKE。然后，本文根据改进的无证书 eCK 模型下对 CDAKE 协议进行了严格的安全证明，证明协议满足已知会话密钥安全、已知会话临时信息安全、前向安全、抗密钥泄露伪装安全、抗未知会话密钥共享安全。最后基于 BLS12-381 曲线，模拟实现了 CDAKE 协议，并计算了协议开销，为协议将来可能的实际部署提供了理论支撑。

5.2　展望

本文集中于无证书低交互认证密钥协商协议的设计和安全性分析，关于该方向的后续工作可以围绕以下几点展开：

1、虽然 IB-ZIAKE 协议在确保通信协议安全方面有了显著改进，但未来的

研究仍有几个方向。最有希望的方向是将 IB-ZIAKE 与其他加密协议和系统集成，从而扩大其应用范围。探索 IB-ZIAKE 与各种网络架构的互操作性及其在现实世界中的应用，将有助于深入了解其实际优势和局限性。此外，有必要进行广泛的实验评估和实地测试，以验证 IB-ZIAKE 在不同操作环境中的理论优势。此外，具有前向安全性的基于标识的零交互密钥协商协议仍有待探索。

2、随着跨域通信需求的增加，针对不同体制下的高效跨域认证密钥协商协议是待探索的方向。本文提出的跨域认证密钥协商协议包含双线性对运算，计算开销仍旧较大，如何降低跨域认证密钥协商协议的计算开销将是本文的下一步工作。

3、标准模型下可证明安全的认证密钥协商协议研究。尽管目前随机预言模型下的协议往往比标准模型下的同类协议具有更高的性能优势，但是模型标准模型更贴近实际，要求哈希函数具备特定性质（如抗碰撞性、单向性等），而不是依赖于对哈希函数的完全随机性假设。因此，在标准模型下证明安全的协议更具现实意义。因此，基于标准模型对所提协议进行安全证明仍值得我们探索。

致　谢

行文至此，百感交集，提笔谢辞，落笔为终。

涓涓师恩，铭记于心。硕士生涯最要感谢的就是我的指导老师王小峰老师和邢倩倩老师，从论文选题、课程入门到后续的深入研究，两位老师都给予了我很多帮助。短短的两年，王老师不仅教会了我如何搞研究，也教会了我很多为人处世的道理，目标清晰才有干劲！

山水一程，三生有幸。感谢硕士期间认识的很多小伙伴，课题组优秀的工程师佳朴哥、烨哥，还有更优秀的麻将搭子杰文哥、秋雷哥、雷莹姐、家璇姐，当然还有同门许欣悦，第一个让我觉得我是 i 人的超级 e 人，很庆幸见证了他和烨哥的爱情！还有就是我的健身搭子张龙辉，我的篮球兄弟们，当然还有一直以来的铁三角清全和宫贺，唐梦晨和谢泽毅，很开心和大家一起度过了欢快的硕士生涯。

感谢父母对我一直以来的支持，也感谢哥哥嫂子姐姐一直以来的关心，一家人要一直健健康康平平安安开开心心快快乐乐顺顺利利才是最大的福！

始于 2022 年秋，亦终于 2024 年秋。短短的两年硕士生涯还是太短了，感觉才刚刚入门研究，就又要匆匆离去，但是两年的时光也收获满满，唯一遗憾的是没能如愿申博咯，那就让学生生涯暂时画个逗号吧，先去工作，如果有机会，一定会回来的！加油！

参考文献

[1] Lippold G, Boyd C, Gonzalez Nieto J. Strongly secure certificateless key agreement [C]. In International conference on pairing-based cryptography. 2009: 206–230.

[2] R Sakai M K, K Ohgishi. Cryptosystems based on pairing [J]. The 2000 Symposium on Cryptography and Information Security. 2000.

[3] Hellman M. New directions in cryptography [J]. IEEE transactions on Information Theory. 1976, 22 (6): 644–654.

[4] Law L, Menezes A, Qu M, et al. An efficient protocol for authenticated key agreement [J]. Designs, Codes and Cryptography. 2003, 28: 119–134.

[5] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol [C]. In Annual international cryptology conference. 2005: 546–566.

[6] Sarr A P, Elbaz-Vincent P, Bajard J-C. A secure and efficient authenticated Diffie–Hellman protocol [C]. In Public Key Infrastructures, Services and Applications: 6th European Workshop, EuroPKI 2009, Pisa, Italy, September 10-11, 2009, Revised Selected Papers 6. 2010: 83–98.

[7] Shamir A. Identity-based cryptosystems and signature schemes [C]. In Advances in Cryptology: Proceedings of CRYPTO 84 4. 1985: 47–53.

[8] 周寰. 轻量级的网络自信任传输机制研究与实现 [D]. [S. l.]: 国防科学技术大学, 2014.

[9] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C]. In International conference on the theory and application of cryptology and information security. 2003: 452–473.

[10] 刘小琼, 潘进, 李国朋. 基于无证书的两方跨域认证密钥协商协议 [J]. 计算机应用研究. 2012, 29 (2): 4.

[11] 陈虹, 郑艳艳, 肖振久. 无双线性对无证书两方跨域认证密钥协商协议 [J]. 计算机工程与应用. 2015, 000 (007): 74–79,153.

[12] 许盛伟. 可证安全的无证书两方认证密钥协商协议 [J/OL]. 密码学报. 2020, 7 (6): 886–898. http://www.jcr.cacrnet.org.cn/CN/10.13868/j.cnki.jcr.000414.

[13] Shoup D C E K V. The Twin Diffie–Hellman Problem and Applications [J]. Journal of Cryptology. 2009: 470–504.

[14] Freire E S, Hofheinz D, Kiltz E, et al. Non-interactive key exchange [C]. In

Public-Key Cryptography–PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26–March 1, 2013. Proceedings 16. 2013: 254–271.

[15] 傅晓彤, 刘晓晓. 一个无证书型非交互式密钥协商协议 [J]. 密码学报. 2014: 334–340.

[16] Wei Y, Wei F, Ma C. Certificateless non-interactive key exchange protocol without pairings [C]. In 2014 11th International Conference on Security and Cryptography (SECRYPT). 2014: 1–12.

[17] Corona R S A S. Identity-based non-interactive key distribution with forward security [J]. Designs, Codes and Cryptography. 2012: 195–208.

[18] Sun; X J L R W. Comment on ”Identity-based non-interactive key distribution with forward security”. [J]. DESIGNS CODES AND CRYPTOGRAPHY. 2015: 1–7.

[19] Dupont R, Enge A. Provably secure non-interactive key distribution based on pairings [J]. Discrete Applied Mathematics. 2006, 154 (2): 270–276.

[20] Paterson K G, Srinivasan S. On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups [J]. Designs, Codes and Cryptography. 2009, 52: 219–241.

[21] Chen Y, Huang Q, Zhang Z. Sakai–Ohgishi–Kasahara identity-based non-interactive key exchange revisited and more [J]. International Journal of Information Security. 2016, 15: 15–33.

[22] Ren K, Lou W. A sophisticated privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks [C]. In 2008 The 28th International Conference on Distributed Computing Systems. 2008: 286–294.

[23] Ren K, Yu S, Lou W, et al. PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks [J]. IEEE Transactions on Parallel and Distributed Systems. 2009, 21 (2): 203–215.

[24] Chatterjee S, Menezes A, Ustaoglu B. A generic variant of NIST’s KAS2 key agreement protocol [C]. In Information Security and Privacy: 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings 16. 2011: 353–370.

[25] Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings [C]. In 16th IEEE Computer Security Foundations Workshop, 2003. Proceedings. 2003: 219–233.

[26] McCullagh N, Barreto P S. A new two-party identity-based authenticated key

agreement [C]. In Topics in Cryptology–CT-RSA 2005: The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005. Proceedings. 2005: 262–274.

[27] Li Y, Chen W, Cai Z, et al. CAKA: a novel certificateless-based cross-domain authenticated key agreement protocol for wireless mesh networks [J]. Wireless Networks. 2016, 22: 2523–2535.

[28] Cao L, Liang M, Zhang Z, et al. Certificateless Cross-Domain Group Authentication Key Agreement Scheme Based on ECC [J]. Wireless Communications and Mobile Computing. 2022, 2022 (1): 7519688.

[29] Ustaoğlu B. Integrating identity-based and certificate-based authenticated key exchange protocols [J]. International Journal of Information Security. 2011, 10: 201–212.

[30] Guo Y, Zhang Z. Authenticated key exchange with entities from different settings and varied groups [C]. In International Conference on Provable Security. 2012: 276–287.

[31] Liu X, Ma W. CDAKA: A provably-secure heterogeneous cross-domain authenticated key agreement protocol with symptoms-matching in TMIS [J]. Journal of medical systems. 2018, 42: 1–15.

[32] Lowe G. An attack on the Needham- Schroeder public- key authentication protocol [J]. Information processing letters. 1995, 56 (3).

[33] Adams C, Lloyd S. Understanding public-key infrastructure: concepts, standards, and deployment considerations [M]. Sams Publishing, 1999.

[34] Matsumoto T, Takashima Y, Imai H. On seeking smart public-key-distribution systems [J]. IEICE TRANSACTIONS (1976-1990). 1986, 69 (2): 99–106.

[35] Bernstein D J. Curve25519: new Diffie-Hellman speed records [C]. In Public Key Cryptography-PKC 2006: 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24-26, 2006. Proceedings 9. 2006: 207–228.

[36] Bala S, Verma A K. A non-interactive certificateless two-party authenticated key agreement protocol for wireless sensor networks [J]. International Journal of Ad Hoc and Ubiquitous Computing. 2016, 21 (2): 140–155.

[37] Pan M, He D, Li X, et al. A lightweight certificateless non-interactive authentication and key exchange protocol for IoT environments [C]. In 2021 IEEE Symposium on Computers and Communications (ISCC). 2021: 1–7.

[38] Hesse J, Hofheinz D, Kohl L. On Tightly Secure Non-Interactive Key Exchange [C]. In Advances in Cryptology –CRYPTO 2018. 2018: 65–94.

[39] Hesse J, Hofheinz D, Kohl L, et al. Towards tight adaptive security of non-interactive key exchange [C]. In Theory of Cryptography: 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part III 19. 2021: 286–316.

[40] Joux A. A one round protocol for tripartite Diffe-Hellman [J]. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2000: 385–393.

[41] Boneh D. Identity-Based Encryption from the Weil Pairing [C]. 2001.

[42] Shim; K. Efficient ID-based authenticated key agreement protocol based on Weil pairing [J]. Electronics Letters. 2003: 653–654.

[43] kyung;Yoon Eun-Jun; Yoo Kee-Young R E. An efficient ID-based authenticated key agreement protocol from pairings [J]. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2004: 1458–1463.

[44] Yuan Q, Li S. A new efficient ID-based authenticated key agreement protocol [J]. Cryptology ePrint Archive. 2005.

[45] Choo S S M C-K R. Strongly-Secure Identity-Based Key Agreement and Anonymous Extension [J]. Lecture Notes in Computer Science. 2007: 203–220.

[46] Terada W D B. An IBE Scheme to Exchange Authenticated Secret Keys [J]. 2004.

[47] Takeshi Okamoto R T O. One-Way and Two-Party Authenticated ID-Based Key Agreement Protocols Using Pairing [J]. Lecture Notes in Computer Science. 2005: 122–133.

[48] Nieto M C G B M G. ID-based One-pass Authenticated Key Establishment [J]. Conferences in Research and Practice in Information Technology. 2008.

[49] Suzuki J T A F A N K. Strongly Secure Identity-Based Key Exchange with Single Pairing Operation [J]. Computer Security –ESORICS 2019. 2019: 484–503.

[50] Daniel R M, Rajsingh E B, Silas S. An efficient ECK secure identity based two party authenticated key agreement scheme with security against active adversaries [J]. Information and Computation. 2020, 275: 104630.

[51] Lian H, Pan T, Wang H, et al. Identity-Based Identity-Concealed Authenticated Key Exchange [C]. In Computer Security –ESORICS 2021. 2021: 651–675.

[52] Zahednejad B, Chong-zhi G. Two-Round ID-PAKE with strong PFS and single pairing operation [J]. Cryptology ePrint Archive. 2024.

[53] Zhu X, Fang Y, Wang Y. How to secure multi-domain wireless mesh networks [J]. Wireless Networks. 2010, 16: 1215–1222.

[54] He B, Agrawal D P. An identity-based authentication and key establishment scheme for multi-operator maintained wireless mesh networks [C]. In The 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2010). 2010: 71–78.

[55] Yang Y, Zheng X, Liu X, et al. Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system [J]. Future Generation Computer Systems. 2018, 84: 160–176.

[56] He D, Kumar N, Wang H, et al. A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network [J]. IEEE Transactions on Dependable and Secure Computing. 2016, 15 (4): 633–645.

[57] Wang C, Liu C, Niu S, et al. An authenticated key agreement protocol for cross-domain based on heterogeneous signcryption scheme [C]. In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). 2017: 723–728.

[58] Qikun Z, Yong G, Quanxin Z, et al. A dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application [J]. IEEE Access. 2018, 6: 24064–24074.

[59] Luo M, Luo Y, Wan Y, et al. Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT [J]. Security and Communication Networks. 2018, 2018 (1): 6140978.

[60] Zhang W, Wang X, Guo W, et al. An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem [J]. Acta Electronica Sinica. 2014, 42 (6): 1095–1102.

[61] Bin H. Improvement and Research on Mechanism of Certificate Revocation Based on PKI [J]. SHANGHAI JIAO TONG UNIVERSITY. 2015.

[62] Basin D, Cremers C, Kim T H-J, et al. Design, analysis, and implementation of ARPKI: An attack-resilient public-key infrastructure [J]. IEEE Transactions on Dependable and Secure Computing. 2016, 15 (3): 393–408.

[63] Wong F L, Lim H W. Identity-based and inter-domain password authenticated key exchange for lightweight clients [C]. In 21st International Conference on Advanced

Information Networking and Applications Workshops (AINAW'07). 2007: 544–550.

[64] Chen L, Lim H W, Yang G. Cross-domain password-based authenticated key exchange revisited [J]. ACM Transactions on Information and System Security (TISSEC). 2014, 16 (4): 1–32.

[65] Lee H, Kim D, Kim S, et al. Identity-based key agreement protocols in a multiple PKG environment [C]. In Computational Science and Its Applications–ICCSA 2005: International Conference, Singapore, May 9-12, 2005, Proceedings, Part IV 5. 2005: 877–886.

[66] Luo M, Wu J, Li X. Cross-domain certificateless authenticated group key agreement protocol for 5G network slicings [J]. Telecommunication Systems. 2020, 74 (4): 437–449.

[67] Semal B, Markantonakis K, Akram R N. A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks [C]. In 2018 IEEE/AIAA 37th digital avionics systems conference (DASC). 2018: 1–8.

[68] Ren H, Kim S, Seo D, et al. A certificateless-based one-round authenticated group key agreement protocol to prevent impersonation attacks [J]. KSII Transactions on Internet and Information Systems (TIIS). 2022, 16 (5): 1687–1707.

[69] Lan X, Xu J, Guo H, et al. One-round cross-domain group key exchange protocol in the standard model [C]. In Information Security and Cryptology: 12th International Conference, Inscrypt 2016, Beijing, China, November 4-6, 2016, Revised Selected Papers 12. 2017: 386–400.

[70] Yuan C, Zhang W, Wang X. EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system [J]. Arabian Journal for Science and Engineering. 2017, 42: 3275–3287.

[71] Goldwasser S, Micali S. Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information [J]. Stoc. 1982.

[72] Bellare M, Rogaway P. Entity authentication and key distribution [C]. In Annual international cryptology conference. 1993: 232–249.

[73] Blake-Wilson S, Menezes A. Entity authentication and authenticated key transport protocols employing asymmetric techniques [C]. In International Workshop on Security Protocols. 1997: 137–158.

[74] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis [C]. In IMA international conference on cryptography and coding. 1997: 30–45.

[75] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels [C]. In International conference on the theory and applications of cryptographic techniques. 2001: 453–474.

[76] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange [C]. In International conference on provable security. 2007: 1–16.

[77] Chen L, Cheng Z. Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme [C] // Smart N P. In Cryptography and Coding. Berlin, Heidelberg, 2005: 442–459.

[78] Devegili A J, Scott M, Dahab R. Implementing cryptographic pairings over Barreto-Naehrig curves [C]. In International Conference on Pairing-Based Cryptography. 2007: 197–207.

[79] Freeman D, Scott M, Teske E. A taxonomy of pairing-friendly elliptic curves [J]. Journal of cryptology. 2010, 23: 224–280.

[80] Barreto P S, Lynn B, Scott M. Constructing elliptic curves with prescribed embedding degrees [C]. In Security in Communication Networks: Third International Conference, SCN 2002 Amalfi, Italy, September 11–13, 2002 Revised Papers 3. 2003: 257–267.

[81] Barreto P S, Naehrig M. Pairing-friendly elliptic curves of prime order [C]. In International workshop on selected areas in cryptography. 2005: 319–331.

[82] Kachisa E J, Schaefer E F, Scott M. Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field [C]. In International conference on pairing-based cryptography. 2008: 126–135.

[83] Wang X, Zhou H, Su J, et al. T-IP: A self-trustworthy and secure Internet protocol [J]. China Communications. 2018, 15 (2): 1–14.

[84] Kasch D M M B. Network Time Protocol Version 4: Protocol and Algorithms Specification [J]. IETF. 2010.

[85] Bao F, Deng R H, Zhu H. Variations of Diffie-Hellman Problem [C]. In Information and Communications Security. Berlin, Heidelberg, 2003: 301–312.

作者在学期间取得的学术成果

发表的学术论文

[1] **Jing Jiang**, Xiaofeng Wang, Qianqian Xing, and Jin Tang. ECC-based certificateless multi-factor authentication scheme[C].The 2024 International Conference on Internet of Things, Cybersecurity, and Software Engineering(ITCSE), Guilin, China, 2024.

[2] **Jing Jiang**, Xiaofeng Wang. Certificateless cross-domain authentication key agreement[C]. The 2024 International Conference on Informatics, Cybersecurity, and Computers(ICICC), Xian, China, 2024.