非交互密钥协商综述

张明瑞 张 蕊 张 磊

(华东师范大学软件工程学院上海市高可信计算重点实验室 上海 200062)

(软硬件协同设计技术与应用教育部工程研究中心 上海 200062)

摘 要 非交互密钥协商作为一种重要的密码学原语是一种极具潜力的安全信道建立范式,持续受到学术界和工业界的密切关注.本文综述了非交互密钥协商协议的发展概况以及待解决的问题.有别于以往的综述,我们在对传统的非交互密钥协商协议进行全面回顾的同时,还对由消息层安全协议衍生的一类部分非交互密钥协商协议进行了深入的探讨.这类协议的突出特点在于,它们能够(部分)非交互式地为群组建立(初次)会话密钥;且后续在群组需要动态变化时,仅需其中一个参与者发送一条请求消息,其他参与者进行监听就能完成群组会话密钥的更新.此外,本文首次讨论了一种基于非对称群密钥协商构造多方非交互密钥协商协议的潜在技术路线,以及利用区块链技术作为公钥基础设施扩充组件用于解决非交互密钥协商协议设计中潜在风险的方法.

关键词 密钥协商;群密钥协商;非交互密钥协商;消息层安全协议

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.00558

A Survey of Non-Interactive Key Exchange

ZHANG Ming-Rui ZHANG Rui ZHANG Lei

(*Shanghai Key Laboratory of Trustworthy Computing*, *Software Engineering Institute*, *East China Normal University*, *Shanghai* 200062)

(*Engineering Research Center of Software/Hardware Co-design Technology and Application*, *Ministry of Education* (*East China Normal University*), *Shanghai* 200062)

Abstract Key exchange protocol serve as a fundamental cryptographic primitive, traditionally involving participants in one or multiple communication rounds to establish a shared session key. However, the innovation of non-interactive key exchange protocols revolutionizes this process, allowing participants to derive a session key without direct communication. This feature is particularly valuable in scenarios where real-time interaction is impractical, making non-interactive key exchange a promising paradigm for secure communication channels, drawing significant attention from academic and industrial communities. This paper aims to provide a comprehensive survey of the developmental trajectory in the field of non-interactive key exchange protocols and the current unresolved challenges in this domain. In contrast to prior survey papers, our survey involves not only an in-depth examination of the evolution of traditional non-interactive key exchange protocols, but also partially non-interactive key exchange protocols which stem from message-layer secure protocols proposed by researchers affiliated with the Internet Engineering Task Force (IETF). Notably, these partially non-interactive key exchange protocols enable a group of participants to establish session keys in a (partial) non-interactive manner. This partial non-interactivity offers a nuanced perspective, especially beneficial in dynamic group communication scenarios. In such a

收稿日期:2023-07-13;在线发布日期:2024-01-02.本课题得到国家自然科学基金(62372177,61972159)资助.**张明瑞**,博士研究生,主要研究方向为密码学、信息安全.E-mail:zhangmingrui@stu.ecnu.edu.cn.**张 蕊**,博士研究生,主要研究领域为信息安全、公钥密码学、车联网安全.**张 磊**(通信作者),博士,研究员,主要研究领域为密码学、车联网安全、云计算安全、大数据安全、隐私保护.E-mail:leizhang@sei.ecnu.edu.cn.

scenario, when there is a dynamic change in participant composition within the group, only one participant needs to send a request message, while the others simply listen to it in order to complete the update of the group session key. Consider a scenario where there is a dynamic change in participant composition within the group. This process enhances the adaptability and security of group communication. Additionally, this paper introduces, for the first time, a potential solution for constructing multi-party non-interactive key exchange protocols based on asymmetric group key agreement which allows a group of participants to negotiate a public group encryption key and each participant's own unique decryption key. We note that, currently, the existing multi-party non-interactive key exchange protocols rely on complex cryptographic primitives such as multilinear mappings and indistinguishability obfuscation. Our innovative approach offers a new potential solution for secure non-interactive key exchange in scenarios involving multiple participants without the need for complex cryptographic primitives such as multilinear mappings and indistinguishability obfuscation. Finally, this paper explores the integration of blockchain technology as an extended component of the Public Key Infrastructure (PKI) to mitigate potential risks in the design of non-interactive key agreement protocols. Specifically, within a non-interactive key exchange protocol based on PKI, a category of malicious behavior by adversaries, termed PKI attacks, is identified. In these attacks, an adversary has the capability to register an arbitrary public key in the PKI as the public key of a specific participant. This sophisticated form of attack not only undermines the trust of the PKI but also the security associated with non-interactive key exchange protocols. By leveraging blockchain technology, this approach enhances the security of participant public key registration, thereby mitigating the risk of adversaries manipulating the PKI and executing such malicious PKI attacks. In summary, non-interactive key exchange transforms secure communication, especially in dynamic group scenarios. This survey explores traditional and partially non-interactive protocols, introducing a novel multi-party solution and advocating blockchain integration to counter PKI attacks.

Keywords　key exchange; group key exchange; non-interactive key exchange; messaging layer security

1　引　言

密钥建立技术是密码学中的一项重要研究内容，广泛应用于视频会议、聊天、文件分享等应用系统(例如：WhatsApp、Threema 等即时通信软件[1]，Cisco Webbex Meetings、Skype 等视频会议软件[2])．它允许两个或多个参与方，在不安全信道条件下，安全建立一个所有参与方共享、共知的会话密钥．根据参与方是否需要贡献会话密钥生成材料，我们将密钥建立技术分为密钥分发和密钥协商两种技术．密钥分发技术借助可信的密钥分发中心独立生成会话密钥并通过安全信道将该会话密钥分发给所有需要通信的参与方．但该技术存在单点故障问题，即若密钥分发中心遭遇攻击或故障，则整个系统的通信安全将受影响．密钥协商技术允许所有通信参与方共同协商与影响会话密钥的生成，避免了可信密钥分发中心受到攻击带来的安全风险．

密钥协商协议最早在文献[3]中被公开提出，即 Diffie-Hellman 密钥协商协议．该协议允许两个参与方通过一轮或者非交互的形式协商出一个会话密钥．非交互密钥协商协议(Non-Interactive Key Exchange，NIKE)，允许各参与方在无需任何其他通信交互情况下，即可借助自身私钥与所知公开信息(公共参数和其他参与方公钥)计算得出本次通信的会话密钥．在整个过程中，由于该协议不需要交互通信，从而可以达到节约无线通讯设备能源的效果．另外，各参与方不需要使用随机信息，NIKE 亦可避免弱随机数等后门攻击威胁．在各类密码学协议的研究中，NIKE 可作为一种基础的密码原语用来构建其他交互式的密钥协商协议、密钥封装机制以及其他密码学原语与协议[4]．因此，NIKE 有着非常高

的实用价值.时至今日,经过四十多年的发展,NIKE已经产生了丰富的成果,并且正在向着更高效、更安全以及更实用的方向快速发展.

NIKE的研究大多集中在两方和三方参与方场景.在两方参与方场景下,以文献[5-6]为代表的一系列工作发展了两方NIKE的安全模型与安全性定义.目前,两方NIKE的主要研究方向是紧归约安全协议[7-8]与抗量子攻击协议[9].另外,以文献[10]为代表的身份基两方NIKE也有一些相关工作.文献[11]作者给出了首个三方NIKE,但是后续相关研究较少.而在参与方大于三时,NIKE目前效率不高.因为其基于有待解决的公开假设如多线性映射、不可区分混淆、椭圆曲线同源等.这些密码学原语候选协议存在安全风险或者效率不高等缺陷,导致现有的多方NIKE难以在现实世界中落地应用[12-14].在本文中,将上述协议称为传统非交互密钥协商.

然而,现实世界中对于高效的非交互群组通信需求却日渐增加.在多方NIKE不能落地之前,是否可以找到替代的实用协议也是密钥协商领域最近关注的热点问题之一.2018年,互联网工程任务组IETF提出的消息层安全协议项目(Messaging Layer Security,MLS)为实用的多方NIKE构造提供了一种可能的发展方向.该项目要求确保多个参与方组成的群组内部以及群组之间的通信安全.在现有MLS项目的相关实例中,参与方之间的通信是部分非交互的,即在执行群组操作(群密钥更新、群成员加入与退出)时,仅需群组操作发起者广播一条消息而其他群组参与方即可计算群组操作后的新会话密钥.这类协议可看作是一种可实用的多方NIKE折中协议[15].因此,在本文中我们将这类协议定义为一类特殊的多方NIKE,即部分NIKE.

除了上述NIKE技术路线,本文首次讨论了基于非对称群密钥协商技术构造NIKE的方法.该方法以非交互的方式协商出公共的群加密密钥和参与方各自的群解密密钥.任何人均可用群加密密钥加密消息(会话密钥)发送给群内成员.群成员利用各自群解密密钥即可在本地解密该消息.另外,本文还讨论了使用区块链作为PKI的补充组件,可作为潜在解决NIKE中PKI攻击的方法,即区块链组件分担部分公钥正确性验证功能,对NIKE协议设计的启发意义.

本文的整体叙述思路如图1所示.我们将非交互密钥协商分为传统非交互密钥协商和部分非交互密钥协商两类.传统非交互密钥协又包含两方NIKE(如迪菲赫尔曼密钥协商协议[3])和三方NIKE(如Joux三方密钥协商协议[11])和多方NIKE(如基于多线性映射的多方密钥协商协议[12]).部分非交互密钥协商是近年被提出的一类可以(部分)非交互的(动态)群组密钥协商协议[15],这类协议的突出特点在于,它们能够(部分)非交互式地为群组建立(初次)会话密钥.且后续在群组需要动态变化时,仅需其中一个参与者发送一条请求消息,其他参与者进行监听(不依赖于广播协议)就能完成群组会话密钥的更新.

<table>
<tr><td rowspan="3">非交互密钥协商</td><td rowspan="2">传统NIKE</td><td>传统两/三方NIKE</td><td>典型方案如文献[3,5,6,7,8,11,16,17,18,21,22]</td><td>讨论:区块链作为PKI扩充组件解决NIKE中的潜在风险</td></tr>
<tr><td>传统多方NIKE</td><td>典型方案如文献[12,14,26,28,29,33]</td><td>讨论:基于非对称群密钥协商的多方NIKE</td></tr>
<tr><td colspan="2">部分NIKE</td><td colspan="2">典型方案如文献[19,20,40,41,42,48]</td></tr>
</table>

图1 非交互密钥协商方案概况

本文第2节给出NIKE的概念和安全性;第3节给出传统两/三方/多方NIKE发展现状及面临的挑战,以及使用区块链作为公钥基础设置组件解决NIKE在实际应用中所面临的PKI攻击的潜在方法;第4节给出部分NIKE的发展现状以及面临的挑战.并首次探讨基于非对称群密钥协商技术构造实用多方NIKE的技术路线;本文第5节为对NIKE的总结与展望.

2 NIKE概念与安全性

本节介绍传统NIKE与部分NIKE相关概念及其相关安全性定义.

2.1 传统NIKE概念及其安全性

2.1.1 传统NIKE概念

定义1. NIKE允许多个参与方在只掌握系统

内其他参与方公钥、公共参数以及自身私钥的条件下，各参与方之间不进行任何通信交互，独立的在本地计算出该群组通信的会话密钥. NIKE 主要包括三个算法：公共参数生成算法，生成参与方共知的协议参数；密钥生成算法，生成参与方各自用于协商会话密钥的材料；密钥协商算法，生成各参与方本次协商的会话密钥. 但是，在传统 PKI 密码体制、基于身份的密码体制和无证书密码体制前提下，NIKE 的算法描述略有区别. 下文分别在不同的密码体制下对 NIKE 进行叙述.

在基于传统 PKI 密码体制下，根据文献[5-6]等对 NIKE 的定义，NIKE 由如下三个算法组成：

(1) 公共参数生成. 输入为安全参数 k，输出为系统公共参数 $params$，该算法一般由可信方执行.

(2) 密钥生成. 输入为系统参数 $params$、身份 ID_i，输出为参与方的一对公私钥 (pk_i, sk_i)，该算法一般由协议中参与方执行.

(3) 密钥协商. 输入为系统参数 $params$、某个参与方身份 id_i、公钥 pk_i 与私钥 sk_i 以及本轮所有其他参与协商的参与方身份集合与公钥集合，输出为本次通信的会话密钥 gsk，该算法一般由参与方执行.

在基于身份(ID-based)的密码体制下，存在一个可信的密钥生成中心(Key Generator Center，KGC)为参与方身份生成对应的私钥，根据文献[10，16-18]，基于身份的非交互密钥协商(ID-Based Non-Interactive Key Exchange，IB-NIKE)由如下三个算法组成：

(1) 公共参数生成. 输入为安全参数 k，输出为系统公共参数 $params$，系统主密钥 msk. 该算法由可信 KGC 执行.

(2) 密钥生成. 输入为系统参数 $params$、身份 id，输出为参与方身份 id 对应的私钥 sk_{id}. 该算法由可信 KGC 执行.

(3) 密钥协商. 输入为系统参数 $params$、某个参与方身份 id、私钥 sk_{id} 和目标协商参与方身份集合 I，输出为身份集合 I 的会话密钥 gsk. 该算法由集合 I 中各参与方执行.

如果无特殊说明，描述的协议都是基于传统 PKI 密码体制的.

2.1.2　传统 NIKE 安全性要求

根据文献[3，5-6，12]等对传统 NIKE 安全性研究，传统 NIKE 至少应该满足如下两个最基本的安全性要求：

(1) 正确性(Correctness). 所有的参与方在密钥协商算法执行完毕后，输出的都应该是相同的会话密钥.

(2) 独立性(Independence). 如果有某个群组的会话密钥泄露，这不会影响由其他不同参与方组成的群组生成的会话密钥的安全性.

2.2　部分 NIKE 概念及其安全性

2.2.1　部分 NIKE 概念

部分 NIKE 通常假设参与方的公私钥对仅用于群组初始化时消息的保密传输. 该协议侧重于群组秘密的生成. 因此，现有部分 NIKE 通常不专门提及参与方密钥生成算法. 此外，在部分 NIKE 中，通常假设存在消息传递服务器. 该服务器主要用于保证参与方都能收到一致的协议消息. 现有的部分 NIKE 协议均运行在传统 PKI 密码体制下.

定义 2.　部分 NIKE 允许多个参与方之间在进行群组秘密计算时是部分非交互的，仅需群组操作(增加成员、删除成员、更新)发起方广播一条消息，其他群组参与方监听收到该消息后，均可在本地计算得到群组操作执行后的新群组秘密. 文献[15，19-20]对这类部分 NIKE 算法进行了具体的形式化描述，一般由以下的六个算法组成：

(1) 初始化. 输入为一个执行初始化的参与方身份 id，输出为一个初始群组状态 γ. 该算法可由任意想要建群的参与方执行.

(2) 群组创建. 输入为初始群组状态 γ、本次群组创建的所有参与方身份列表 $G=\{id_1, \cdots, id_n\}$，输出为更新后的群组状态 γ' 和控制消息 W. 该算法由想要建群的参与方执行.

(3) 增加成员. 输入为一个群组状态 γ 和一个新加入参与方身份 id'，输出为更新后的群组状态 γ' 和控制消息 W、T，其中 W 仅发送给新入群参与方，T 被发送给群内所有参与方. 该算法由群内某一参与方执行，用于邀请协议新参与方入群.

(4) 删除成员. 输入为一个群组状态 γ 和一个待删除参与方的身份 id'，输出为更新后的群组状态 γ' 和 T，其中 T 需发送给群内所有参与方. 该算法由群内某一参与方执行，用于删除群内身份为 id' 的参与方.

(5) 更新. 输入为一个群组状态 γ，输出更新后的群组状态 γ' 和 T，其中 T 需发送给群内所有参与方. 该算法由群内某一参与方执行，用于发起群组秘密的更新.

(6) 事务执行. 该算法输入为一个群组状态 γ

和 W,T,输出为更新后的群组状态 γ' 和更新后的群组秘密 I(初始值为空). 该算法由所有收到控制消息的群内参与方执行.

在上述算法中,群组状态 γ 反映协议实例当前运行情况,包含群组标识符、群组运行阶段标识符、群组协议版本号等信息. 每当上述群组操作算法被执行一次,群组运行阶段标识符加 1,群组状态 γ 也随之改变. 控制消息 W 被称为"欢迎消息". 所有被邀请的参与方都会收到此消息. 该消息包含当前群组的上下文信息(如群组运行阶段标识符、群组协议所用密码组件等). 控制消息 T 被称为常规控制消息,用于通知已在群组内的成员执行具体的群组操作(如增加成员、删除成员等)以及被操作涉及的参与方信息(如参与方身份、密钥对等). 群组秘密 I 随着群组每个运行阶段改变. 在具体协议中,该秘密值可为群组会话密钥 gsk 的派生材料或会话密钥本身.

2.2.2 部分 NIKE 安全性

在 2020 年美密会上,文献[19]作者首次系统地提出了部分 NIKE 应满足四个最基本安全性,具体要求如下:

(1) 正确性(Correctness). 所有的群内参与方在每次群组运行状态改变后,即所有参与方均执行完成了同样的群组操作后,最终输出的群组秘密 I 应该是相同的.

(2) 隐私性(Privacy). 参与方通过执行消息 W、T 所指示的群组操作之后,输出的群组秘密 I 应该是一个秘密的随机值.

(3) 前向机密性(Forward Secrecy). 如果敌手获得了某个群内参与方某个时刻的秘密信息(如参与方随机数、群组秘密等),所有该群组先前生成的群组秘密 I 对于敌手依然保持机密性.

(4) 后向安全性(Post-compromise Security). 在任何一个群内参与方秘密信息泄露给敌手的情况下,只要此时群组内参与方发起并执行一次不被敌手影响的更新操作,更新后的群组秘密 I 对于敌手而言仍将是机密的.

3 传统 NIKE 现状与挑战

本节将传统 NIKE 按照支持最大参与方人数分为两类:传统两/三方 NIKE 和多方 NIKE,分别介绍这两类 NIKE 的发展现状与面临的挑战.

3.1 传统两/三方 NIKE 发展现状

本节介绍传统的支持两个参与方与三个参与方的 NIKE 协议发展概况. 如表 1 所示,我们以支持参与方数量、协议设定、构造技术、安全性假设对两方和三方 NIKE 的典型协议进行了分类.

表 1 传统两方/三方 NIKE 分析表

参与方数量	协议设定	构造技术	安全性假设	典型协议
两方	HKR	EC	DDH	文献[3]
两方	DKR	EC	TwinDH	文献[5]
两方	DKR	Pairing	DBDH	文献[6]
两方	DKR	QR	Factor	文献[6]
两方	HKR	Pairing	DLIN	文献[7]
两方	HKR	EC	DDH	文献[7]
两方	HKR	Pairing	DLIN、LWE	文献[8]
两方	DKR	LMmap	MDDH	文献[21]
两方	DKR	Isogeny	GA-CDH	文献[22]
两方	ID-Based	Pairing	BDH	文献[16]
两方	ID-Based	TDL	CDH	文献[17]
两方	ID-Based	Pairing	CBDH	文献[18]
三方	\	Pairing	BDH	文献[11]

在表 1 中,参与方数量即为该典型协议所能支持的最大参与方数量. 协议设定指敌手控制密钥的能力. 在两方 NIKE 中,我们根据敌手对于公钥的控制情况将敌手控制分为诚实密钥注册(Honest Key Registration,HKR)设定与不诚实密钥注册(Dishonest Key Registration,DKR)设定两类. 第一类设定假设整个系统中所有的参与方都是诚实的且参与方不能向 PKI 注册自己任意选择的公钥;第二类设定假设参与方可向 PKI 注册自己任意选择的公钥. DKR 设定意味着对 PKI 功能做最低程度的假设,即 PKI 不会提供任何对公钥的有效性检查,包括某个公钥是否被曾经注册过、公钥持有者是否持有对应的合法私钥. 另外,除了传统基于 PKI 的密码体制,NIKE 也可在基于身份密码体制或无证书密码体制下设计. 在表 1 中,我们记基于身份密码体制为 ID-based;构造技术为该典型协议所使用的底层密码学组件(如椭圆曲线群 EC[3]、双线性群 Pairing[6]、二次剩余群 QR[6]、陷门离散对数群 TDL[17]、层级多线性映射 Leveled multilinear maps,Lmmap[21]、椭圆曲线同源 Isogeny[22]). 安全性假设为所列典型协议所使用的密码学困难问题假设,如一系列基于迪菲赫尔曼问题(Diffie-Hellman assumption,DH)的困难假设:Computational Diffie-Hellman assumption,CDH 假设[3];Decisional Diffie-Hellman assumption,DDH 假设[3];Twin Diffie-Hellman assumption,TwinDH 假设[5];Bilinear Diffie-Hellman assumption,BDH 假设[16];Comptational Bilinear Diffie-Hellman assumption,CBDH 假设[18];Decisional Bilinear Diffie-Hellman assumption,DBDH 假设[6];Multilinear

Decisional Diffie-Hellman assumption，MDDH 假设[21]；GroupAction Computational Diffie-Hellman assumption，GA-CDH 假设[22]；判定线性假设 DLIN[7]；大整数分解假设 Factor[6]. 上述假设的完整定义可以查阅对应的参考文献.

3.1.1　基于 PKI 的密码体制下两/三方 NIKE 现状

两方 NIKE 允许两个参与方仅利用公共参数、自身私钥以及其他参与方的公钥即可计算获得本次通信的会话密钥. 本节重点介绍 Diffie 与 Hellman 的两方 NIKE 及其变种.

第一个两方 NIKE 由 Diffie 与 Hellman 在文献[3]中提出. 假设两个参与方为身份为 Alice 和 Bob. 该协议算法如下：

(1) 公共参数生成. 输入为安全参数 k，输出为公共参数 $params=(q,g,\mathbb{G},Hash,Z_q)$. 其中 $Hash$ 为一个哈希函数，$\mathbb{G}$为一个阶为素数 q、生成元为 g 的循环群，Z_q为一个模 q 整数群.

(2) 密钥生成. 输入为公共参数 $params$，输出为参与方的公私钥对. Alice 利用该算法生成私钥 $\alpha\in Z_q$和公钥 g^{α}. 同样的，另一参与方 Bob 利用该算法生成自己的私钥与公钥 $\beta\in Z_q, g^{\beta}$.

(3) 密钥协商. 输入为 Alice 的私钥和 Bob 的公钥或者 Alice 的公钥和 Bob 的私钥，输出为会话密钥 gsk. Alice 和 Bob 可以分别通过自己的私钥和对方公布的公钥以及哈希函数 $Hash$，计算得到会话密钥 $gsk=Hash(\text{Alice},\text{Bob},g^{\alpha\beta})$.

上述两方 NIKE 在 HKR 设定下满足第 2.1.1 节中描述的密钥正确性与密钥独立性. 但是，该协议容易遭受中间人攻击，即存在敌手能够控制网络消息传输，则敌手分别以 Alice 和 Bob 的身份将自己的公钥 g^{c}发送给对方. 最终导致 Alice 、Bob 分别与敌手完成密钥协商，但是 Alice 和 Bob 却无法察觉. 另外，文献[5]作者指出该协议面临 DKR 设定敌手(文献[5]称该设定为敌手的主动攻击)时存在一定安全风险. 具体来说，DKR 设定敌手可选择$\mathbb{G}$中任意的一个元素作为自己的公钥并向 PKI 进行注册(敌手此时不掌握该公钥对应的私钥)，随后使用该公钥与一个诚实的参与方建立会话密钥. 若敌手可获取到这个与诚实参与方协商获取的密钥 sk，则该敌手可以任选群$\mathbb{G}$上的一个元素 z，对等式 $gsk=Hash(\text{Alice},\text{Bob},z)$进行测试，直至找出符合该等式的 z. 那么此时敌手获得了一个 CDH 假设中正确的目标值 z，则敌手此时可解决 CDH 困难问题.

为了解决该安全风险，文献[5]作者提出了新的 NIKE 安全模型(即 CKS 模型). 该模型允许敌手不诚实密钥注册(即捕获了上述 DKR 敌手的攻击行为)，并允许敌手请求诚实密钥注册参与方与不诚实密钥注册参与方间的会话密钥. 文献[5]作者也提出在该模型下可证明安全的两方 NIKE. 协议如下：

(1) 公共参数生成. 输入为安全参数 k，输出为公共参数 $params=(q,g,\mathbb{G},Hash,Z_q)$. 其中 $Hash$ 为一个哈希函数，$\mathbb{G}$为一个阶为素数 q、生成元为 g 的循环群，Z_q为一个模 q 整数群.

(2) 密钥生成. Alice 生成私钥$(x_1,x_2)\in Z_q$、公钥$(X_1=g^{x_1},X_2=g^{x_2})\in\mathbb{G}$；相同的，Bob 生成私钥$(y_1,y_2)\in Z_q$、公钥$(Y_1=g^{y_1},Y_2=g^{y_2})\in\mathbb{G}$.

(3) 密钥协商算法. Alice 和 Bob 掌握自身私钥和对方公钥，可在本地计算会话密钥 $gsk=Hash(\text{Alice},\text{Bob},dh(X_1,Y_1),dh(X_1,Y_2),dh(X_2,Y_1),dh(X_2,Y_1))$. 其中 dh 计算如下 $dh(X,Y)=z, X=g^{x}, Y=g^{y}, z=g^{xy}$.

该协议在随机预言模型下被证明是安全的，安全性基于一个新的困难问题 Twin DH 问题. 文献[5]作者证明了解决困难问题等价于解决 CDH 困难问题.

文献[6]作者基于文献[5]中的 CKS 模型，给出了在 DKR 设定下的三种扩展模型 CKS-heavy，CKS-light，m-CKS-heavy. 这三种模型与原始 CKS 模型主要的区别是：(1) CKS 模型允许敌手可进行挑战的次数是任意次的，而 CKS-light 和 CKS-heavy 模型只允许一次挑战；(2) CKS-heavy 和 m-CKS-heavy 允许敌手询问已诚实注册的非目标诚实参与方公钥对应的私钥即提取询问(Extract query)和允许敌手请求两个自己选择的诚实注册参与方之间生成的会话密钥即揭示询问(Reveal query)，而 CKS 模型则未定义这两种询问. 文献[6]作者证明了文献[5-6]中提出的上述四种安全模型是多项式等价的. 此外，文献[6]作者也给出了 HKR 设定下的上述三种安全模型. 与 DKR 设定下的三种安全模型相比，HKR 设定下的三种安全模型不允许敌手注册随机公钥. 自然的，敌手也就不能询问诚实方-非诚实方协商会话密钥的能力. 随后，文献[6]作者分别基于 DBDH 假设和 Factor 假设构造了在 CKS-light 模型下安全的两方非交互密钥协商协议.

文献[21]作者指出如果存在层级多线性映射(Leveled multilinear maps，Lmmap)，则可在 HKR 和DKR设定下构造具备前向安全属性的两方NIKE. 主要思想为借助 Lmmap 可在保持参与方公钥不变

情况下支持参与方定期更新其私钥. 文献[21]作者给出了相关协议构造并证明该协议安全性归约到MDDH困难问题.

上述传统两方NIKE都不是紧归约安全的. 2018年,文献[7]作者首次提出了紧归约安全的NIKE. 作者给出了两个均借助哈希证明系统技术的协议构造实例,并且在CKS-heavy模型下证明了其安全性. 两个协议的安全性分别被归约到了DLIN假设和DDH假设,安全归约损失均达到$(1/2)n$,n为与敌手交互的诚实参与方数量. 最近,文献[8]作者给出了多个目前最优的紧归约安全两方NIKE. 这些协议被证明在HKR敌手设定下是半适应性安全的,安全性可归约到DLIN,LWE假设,归约损失为$O(N^2\log(\nu)/\nu^2)$,其中N为系统中所有参与方的数量,$2\leq\nu\leq N$是一个可以根据具体协议自由设定的协议参数(例如,在文献[8]中ν代表协议公共参数中所用随机对称矩阵的行列数). 文献[9]作者指出现有的使用了LWE困难假设的两方NIKE,往往失去了非交互的属性,或存在使用polynomial LWE-modulus技术导致的巨大计算开销问题. 文献[9]作者对基于LWE困难假设的两方NIKE进行了形式化的描述与定义,并探讨了现在基于(ring)LWE困难假设构造两方非交互密钥协商协议的困难性. 在2023年,文献[22]作者给出了首个基于椭圆曲线同源的抵抗DKR敌手攻击的NIKE,并借助量子随机谕言机在CKS模型下证明了协议的安全性.

在三方NIKE方面,文献[11]作者所提的基于双线性映射的三方密钥协商可通过简单转换转化为一个三方NIKE. 假设双线性映射为$e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_T$,其中$\mathbb{G}_1$,$\mathbb{G}_2$,$\mathbb{G}_T$均为素数阶循环群. e为双线性映射运算可以将群$\mathbb{G}_1$和$\mathbb{G}_2$的两个元素映射到群$\mathbb{G}_T$. 当$\mathbb{G}_1=\mathbb{G}_2=\mathbb{G}$时,$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$称为对称群双线性映射,否则称为非对称群双线性映射. 设有参与方Alice,Bob,Charlie. 文献[11]三方NIKE如下:

(1)公共参数生成. 输出为满足$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$的双线性映射和阶为$q$的循环群$\mathbb{G}$,$\mathbb{G}_T$,生成元$P\in\mathbb{G}$,模$q$整数群$Z_q$. 公共参数设置为$params=(q,P,\mathbb{G},\mathbb{G}_T,Z_q)$.

(2)密钥生成. 输出为三个参与方的公钥aP,bP,cP. 上述三个参与方分别选择三个随机数$a,b,c\in Z_q$作为自己的私钥,每个参与方计算自己的公钥aP,bP,$cP\in\mathbb{G}$.

(3)密钥协商. 输出为三个参与方共享的会话密钥gsk. 每个参与方根据自己私钥和其他人公钥计算得到会话密钥$gsk=e(P,P)^{abc}$.

该协议安全性可被归约到BDH假设.

另外,随着区块链技术的发展,是否能利用区块链技术作为公钥基础设施扩充组件用于解决非交互密钥协商协议设计中潜在风险也是值得讨论的一个问题. 基于PKI的NIKE中存在一类被称为PKI攻击[6,23]的敌手恶意行为,例如:敌手向PKI注册任意的公钥等. 前文所述DKR敌手即为这类攻击的一种具体实例. 目前,NIKE设计者往往期望对PKI系统做最小限度的假设,将公钥有效性检测嵌入至NIKE内部,以此来抵抗DKR敌手攻击. 但是,这需要在NIKE中嵌入其他密码学工具,如文献[6]作者使用变色龙哈希函数来解决该问题. 这加大了协议复杂度. 另外,对于部分NIKE来说,文献[19]作者指出,如何为上述恶意行为建模还是一个公开问题.

要求参与方提供私钥的零知识证明来验证公钥的合规性也是常用的抵抗PKI攻击的方法. 但传统PKI系统容易遭受单点失效、根证书节点腐败等风险. 区块链技术为解决上述问题提供了一种可能的方法. 区块链可作为参与方公钥与公钥验证信息(例如,私钥的零知识证明相关信息)的载体. 所有人都可通过检查区块链上的公钥验证信息检测参与方公钥的合规性,或者借助智能合约技术自动对参与方公钥进行验证[24-25]. 因此,区块链可作为PKI的扩充组件,使协议设计者可以将更多的精力集中在核心NIKE的设计上. 这对于设计高效NIKE具较大积极意义.

3.1.2 基于身份密码体制下传统两方NIKE现状

基于身份的密码体制下也有不少的两方NIKE成果. 文献[10]提出了第一个基于身份的非交互密钥协商协议(ID-based Non-Interactive Key Exchange, ID-based NIKE). 该协议也通常被称为SOK协议. 具体协议如下:

(1)公共参数生成. 输入为安全参数k,输出协议公共参数$params=(q,e,x,IH,GH,mpk,msk,Z_q)$,其中$q$为一个素数,$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$为双线性映射,$IH$为$I\rightarrow\mathbb{G}$将身份$id\in I$映射到群$\mathbb{G}_T$中元素的映射函数,$GH$为将$\mathbb{G}_T\rightarrow\{0,1\}^n$群$\mathbb{G}_T$元素映射为$n$长二进制串的编码函数,$x\in Z_q$为随机数,$g\in\mathbb{G}$是一个群生成元,$mpk=(g,h,IH,GH)$为KGC主公钥,$msk=x$为KGC的主私钥.

(2)密钥生成. 输入为安全参数$params$和参与方身份id,输出该参与方私钥$sk_{id}=IH(id)^x$.

(3)密钥协商. 输入为参与方A的私钥sk_a和参

与方 B 的身份 id_b，参与方 A 和 B 均可在本地计算两方会话密钥 gsk 为

$$gsk=GH(e(sk_a,IH(id_b)))=GH(e(sk_b,IH(id_a))).$$

SOK 协议被提出时并没有给出形式化的安全性证明. 文献[16]作者对 SOK 协议进行了扩展，并且首次在随机谕言机模型下将该扩展协议的安全性归约到了 BDH 困难假设上. 文献[17]作者给出了一个新的 ID-based NIKE 安全模型. 该模型允许敌手询问一对任意参与方(非敌手挑战的)协商的会话密钥，文献[16]则不允许这样的敌手询问. 文献[17]作者还基于通用陷门离散对数群给出了一个在 CDH 假设下可证明安全的 ID-based NIKE 构造. 2016 年，文献[18]作者给出了 SOK 协议在随机谕言机模型下的一个紧归约证明和首个标准模型下适应性安全的 ID-based NIKE. 这里 ID-based NIKE 中适应性指：在安全证明算法运行过程中，敌手可根据挑战者的回复信息，自由的进行 Extract 询问和 Reveal 询问.

3.1.3　传统两/三方 NIKE 待解决的问题

两/三方 NIKE 待解决的问题主要涉及模型间的安全归约、紧归约构造与抗量子构造，具体包括：

(1) 是否存在 CKS-light、CKS、CKS-heavy 与 m-CKS-heavy 四种安全模型之间的紧归约转换证明.

CKS 模型及其相关变体是被广泛认可的两方 NIKE 安全模型. 虽然文献[6]作者证明了这四个安全模型是多项式等价的，但证明的归约损失较大. 解决该问题的主要难点在于模型之间的归约需要处理不同能力的敌手. 例如 CKS-heavy 和 m-CKS-heavy 的区别在于前者只允许敌手进行一次挑战询问(Test 询问)，而后者允许敌手进行多次挑战询问. 这导致在证明二者的等价性时，CKS-heavy 模型中的敌手优势和 m-CKS-heavy 的敌手优势存在一个与挑战询问次数相等的损失因子.

(2) 是否存在不使用双线性映射且在标准模型下可证明安全的紧归约两方 NIKE.

目前，尽管有一些不使用双线性映射的两方 NIKE 协议被提出[7]，但它们的安全性证明都需借助随机谕言机模型且都不是严格紧归约的. 虽然基于双线性映射可构造标准模型下的相对紧归约的两方 NIKE[7-8]. 但双线性映射的计算开销通常认为较高，且这些协议也未做到严格紧归约. 解决该问题的主要难点在于两方 NIKE 的安全归约中挑战者需要猜测敌手在挑战询问中选定的目标参与方. 这往往与系统中参与方数量 n 相关，从而导致较高的归约损失因子. 例如在最早的 DH 协议[3]中，归约损失平凡的达到 n^2. 又例如文献[7]作者所提协议归约损失为 $n/2$.

(3) 是否可以构造抵抗适应性敌手的紧归约两方 NIKE.

为了捕获现实中敌手的攻击能力，CKS 模型首次定义了两方 NIKE 中的适应性敌手. 但现有抵抗适应性敌手的协议都存在归约损失过大的问题. 解决该问题难点与问题(2)相同.

(4) 是否可以给出仅基于(ring)LWE 困难假设的两方 NIKE.

目前还没有基于 LWE 或 Ring-LWE 构造的安全实用的两方 NIKE 协议. 其中 Ring-LWE 的参数为多项式形式而非矩阵，因此基于 Ring-LWE 构造密码学原语时，密钥长度会大幅降低且运算速度更快. 文献[9]作者指出解决这个问题的主要难点在于对(ring)LWE 中误差的协调处理. 如果协调函数(Reconciliation Function)首先计算接收到的(ring)LWE 样本与其私有(ring)LWE 秘密的内积或者其中一个协调函数不依赖于传输的(ring)LWE 样本的误差. 那么就可以基于(ring)LWE 困难假设构造两方 NIKE. 但是，前者需要交互通信交换误差，这不符合非交互定义. 后者协议若无需使用对方的误差，又不符合(ring)LWE 困难问题定义.

(5) 是否能够基于 Joux 协议构造紧归约的三方 NIKE.

本问题包括问题“是否存在不使用双线性映射且在标准模型下可证明安全的紧归约三方 NIKE.”，“是否可以构造抵抗适应性敌手的紧归约三方 NIKE.”解决这两个子问题的难点分别与问题(2)，(3)中涉及的难点类似.

3.2　传统多方 NIKE 现状

本节主要介绍传统的多方 NIKE. 传统多方 NIKE 支持 $n(n>3)$ 个参与方在仅掌握所有参与方公钥信息与自身私钥以及公共参数的条件下，以非交互的形式协商出会话密钥.

如表 2 所示，我们从安全模型、技术路线、构造技术与安全性假设多个维度，对多方 NIKE 的典型协议进行了分类. 依据文献[26]作者定义，安全模型主要有半静态安全模型(Semi-static)、静态安全模型(Static)、适应性安全模型(Adaptive)三类.

半静态安全模型要求在安全性证明初始化阶段后公布一个参与方集合 $\hat{S}$，敌手只能对集合 $S^*\subseteq\hat{S}$

的内部成员之间协商的会话密钥进行挑战询问，且敌手只能对参与方 i，$i\notin\hat{S}$ 进行 Extract 询问和 Reveal 询问. 这里 Extract 询问与两方 NIKE 中 Extract 询问含义相同，需要注意的是在两方 NIKE 中敌手 Reveal 的是一对诚实参与方的会话密钥，在多方 NIKE 中敌手 Reveal 的是一组诚实参与方的会话密钥.

静态安全模型是半静态安全模型概念的弱化，要求在安全性证明的初始化阶段前需公布一个参与方集合 $\hat{S}$，只允许敌手对 $S^*\subseteq\hat{S}$ 的内部成员之间协商的会话密钥进行一次挑战询问，只能对参与方 i，$i\notin\hat{S}$ 进行 Extract 询问和 Reveal 询问. 半静态和静态两种安全模型的区别主要是敌手选择公布攻击目标成员集合的时机不同.

适应性模型无需要求在安全证明初始化阶段前后公布一个目标参与方集合 $\hat{S}$. 敌手可在安全证明算法运行过程中任意性地对诚实参与方进行 Extract 询问和 Reveal 询问. 文献[27]作者所提协议是目前为止最优的适应性 NIKE，但其仍然限制了敌手 Extract 询问次数.

由于部分文献仅仅给出了协议，没有详细讨论安全性证明的具体情况，因此在表 2 中将这类文献的安全模型栏填写“\”. 构造技术为该典型协议所使用的底层密码学组件，如多线性映射(Multilinear Map)[12]、可穿刺伪随机函数(Puncturable-Pseudorandom Function, P-PRF)[26]、不可区分混淆(Indistinguishability Obfuscation, IO)[26]、椭圆曲线同源(Isogenise)[14]. 安全性假设为所列典型协议安全性被归约到的密码学困难假设，或者协议所用构造技术的存在性假设，如判定性迪菲赫尔曼假设(Decisional Diffie-Hellman, DDH)[28]、多线性迪菲赫尔曼假设(MultilinerMap DH, MDH)[12]、多线性计算迪菲赫尔曼假设(Multiliner Computational DH, MCDH)[29]、N 方计算迪菲赫尔曼假设(N-way CDH)[14]. 上述假设完整定义可参考下述如表 2 典型协议的引用文献.

表 2 传统多方非交互密钥协商协议分析表

参与方数量	安全模型	构造技术	安全性假设	典型协议
多方	\	MultilinerMap	MDH	文献[12]
多方	\	Isogenise	N-WayCDH	文献[14]
多方	Semi-Static	p-PRF、IO	IO	文献[26]
多方	Adaptive	IO	IO、DDH	文献[28]
多方	\	MultilinerMap	MCDH	文献[29]
多方	Static	IO	IO	文献[33]

3.2.1 传统多方 NIKE 现状

本节主要介绍典型的基于 MultilinerMap 和 IO 的多方 NIKE.

最早文献[12]作者预测如果存在安全的 MultilinerMap，那么就可以构造多方 NIKE. 随后多个基于 MultilinerMap 的协议被提出. 依据文献[12]作者所提协议基本可以概述如下：

(1) 公共参数生成. 输入为安全参数 k，参与方数量 $K+1$，输出为公共参数 $params=(e,g,l)$. 其中 e 为满足 $e:\mathbb{G}_1^n\to\mathbb{G}_2$ 的 n 方多线性映射，g 为群 $\mathbb{G}_1$ 的生成元，l 为群 $\mathbb{G}_1$ 的阶数，参与方数量 $K+1$ 和 n 方线性映射存在 $n=K+1$ 的数量关系.

(2) 密钥生成. 输入为公共参数 $params$ 和参与方身份 $i\in\{1,\cdots,n\}$. 选择随机数 $a_i\in[1,l-1]$ 为参与方 i 的私钥，计算 $g^{a_i}\in\mathbb{G}_1$ 为公钥. 输出为参与方 i 的一对公私钥 $(pk_i=g^{a_i},sk_i=a_i)$.

(3) 密钥协商. 输入为公共参数 $params$、参与方 i 的私钥 a_i、目标参与方公钥 $(pk_1,\cdots,pk_j)_{j\neq i}$，输出为多方协商的会话密钥 gsk. 参与方 i 均可在本地计算 $K+1$ 个参与方协商的会话密钥为

$$gsk=e(pk_1,\cdots,pk_{i-1},pk_{i+1},\cdots,pk_{K+1})^{a_i}\in\mathbb{G}_2.$$

文献[29]作者给出了基于文献[12]的两个扩展协议，扩展了原始协议中参与方人数与多线性映射之间存在 $n=K+1$ 的固定关系，允许参与方人数在小于等于 n 时也可运行多方 NIKE，并将这两个协议的安全性都归约到了 MCDH 假设上. 然而，构造多线性映射困难实例是相当困难的. 近年来，多线性映射候选协议相继被攻破[27,30-31]或多线性映射的候选协议还存在不安全或者不实用的地方. 文献[32]作者对多线性映射假设做了全面的总结，供有兴趣的读者参考.

IO 亦被广泛用于构造多方 NIKE. 文献[26]作者首次基于 IO 构造了多方 NIKE. 该协议是基于 IO 技术路线构造 NIKE 的代表性协议，具体描述如下：

(1) 公共参数生成. 输入为安全参数 k，输出为公共参数 $params=(N,G,P_{\mathrm{IO}},x_0,PRF,PRG)$. 其中 $PRF:\{0,1\}^{\lambda}\to\{0,1\}^{2\lambda}$ 为一个受约束的伪随机数函数、IO 为一个不可区分混淆器、N 为系统允许的最大参与方数量、$G\leq N$ 为实际参与方数量. 选择一个伪随机数函数及该伪随机函数的密钥 key. 构建一个会话密钥生成程序 PK_E，$x_0\in\{0,1\}^{2\lambda}$ 为一个随机数. 使用 IO 对程序 PK_E 进行混淆，得到一个混淆程序 $P_{io}=\mathrm{IO}(P_{KE})$，$PRG:\{0,1\}^{\lambda}\to\{0,1\}^{2\lambda}$ 是一个伪随机数生成器. 将 $(N,G,P_{\mathrm{IO}},x_0,PRF,PRG)$ 作

为公共参数 $params$.

(2) 密钥生成. 输入为公共参数 $params$. 输出为公钥 x_i. 每个参与方 i 选择一个随机种子 $s_i \in \{0,1\}^\lambda$ 作为自己的私钥，公布 $x_i = PRG(s_i)$ 作为自己的公钥.

(3) 密钥协商. 输入为参与方 i 的公私钥对和随机数种子 s_i、公共参数 $params$、S，$\{x_i\}_{i\in S}$，输出为多方会话密钥 gsk. 其中 S 为本次协商密钥的所有参与方集合，$\{x_i\}_{i\in S}$ 为本次所有参与密钥协商的参与方的公钥. 如果本次密钥协商参与方数量 $|S|$ 大于额定允许参与人数 G，或者当前参与方不属于本次密钥协商集合 S，则终止协议. 定义 $S(j)$ 为参与方 j 在 S 中的序号，定义 $S^{-1}(k)$，$k \in S$ 为其逆，即输入序号 k 得到相应的参与方. 通过 $\hat{x}_j = x_{S(j)}$，$j \leq |S|$ 获得所有参与方公钥，若额定允许参与人数大于 G 则设置 $\hat{x}_j = x_0$. 运行混淆程序 $P_{io}(\hat{x}_1, \cdots, \hat{x}_G, S^{-1}(i), S_i)$ 得到本次会话密钥 $gsk = PRF(\hat{x}_1, \cdots, \hat{x}_G)$ 或者终止符 $\perp$.

文献[26]作者给出了该协议在半静态(semi-static)安全模型下的安全性证明，将安全性归约到了 IO 的安全性. 文献[33]作者基于不可区分混淆提出了第一个不限制参与方人数的多方 NIKE 并且证明了该协议在 IO 假设下是静态安全的(static). 2022 年，文献[28]作者在 IO 和 DDH 假设下构造了适应性安全的 NIKE. 该协议要求可以被适应性 Extract 询问的参与方数量是有界的，即那些初始化时是诚实参与方然后被 Extract 询问的参与方数量是有界的. 诚实参与方数量和敌手生成的诚实参与方数量是不受限制的. 改进了之前文献[26]要求参与方总人数必须初始化设定有界的条件. 目前 IO 的构造也是一个公开问题，有两类关于 IO 的研究技术路线被认为是有希望的[34]. 一类为通过基本假设构造[13,35]；另一类是基于同态加密构造[36].

传统多方非交互密钥协商协议的另一个潜在技术路线为基于椭圆曲线同源问题来进行构造. Boneh 等人在文献[14]中给出了一个框架用来构造多方 NIKE. 该框架假设计算椭圆曲线同源问题是困难的. 然而，因为其中的一些步骤依赖于尚且没有解决的公开数学困难问题，作者称目前无法给出一个实际的协议.

3.2.2　传统多方 NIKE 待解决的问题

多方 NIKE 待解决的问题主要涉及多线性映射、不可区分混淆以及椭圆曲线同源等用于构造协议的工具目前难以实用. 具体包括：

(1) 是否存在实用的基于多线性映射的多方 NIKE.

多线性映射一直被认为是构造多方 NIKE 的关键技术. 然而，可潜在用于构造多方 NIKE 的多线性映射候选协议相继被攻破[30-31]，或安全性分析有待考证，或效率不高导致多方 NIKE 无法实际投入应用. 因此，解决该问题的主要难点在于安全高效多线性映射构造本身是一个公开难题.

(2) 是否可以使用 IO 技术设计(完全)适应性安全的多方 NIKE.

虽然文献[26]作者给出了一个基于 IO 构造的多方 NIKE，但该协议仅能在半静态安全模型下证明是安全的，无法抵抗(完全)适应性敌手. 解决该问题的关键难点在于两点：(1) 不可区分混淆 IO 的构造本身也是一个公开难题；(2) 抗(完全)适应性敌手存在挑战者需要猜测正确敌手攻击目标参与方的问题.

(3) 是否能够基于椭圆曲线同源构造有效的多方 NIKE.

基于椭圆曲线同源可构造抗量子攻击的多方 NIKE. 但已知的成果只有 Boneh 等人首次在文献[14]中提出的一个底层基于椭圆曲线同源的多方 NIKE 框架. 然而，针对该框架目前并没有具体的基于椭圆曲线同源构造的多方 NIKE 被提出. 解决这个问题的难点在于椭圆曲线同源构造本身也是一个公开难题.

3.2.3　基于非对称群密钥协商的多方 NIKE

多方 NIKE 还存在一些不使用多线性映射、不可区分混淆或椭圆曲线同源的潜在的构造方法. 在 2009 年欧密会上提出的非对称群密钥协商[37](Asymmetric Group Key Agreement，AGKA)是潜在的技术之一. 本节介绍一种基于 AGKA 构造多方 NIKE 的新思路.

AGKA 允许一组参与方通过协商生成一个公开的群加密密钥以及每个参与方各自不同的解密密钥. 任何知道这个群加密密钥的参与方都可向群内参与方发送加密消息. 群内参与方可用他们各自的解密密钥对消息进行解密. 在文献[37]作者首次提到了基于 AGKA 的 NIKE，即非交互非对称群密钥协商(Non-Interactive AGKA，NI-AGKA)的平凡构造方法以及一个单轮的 AGKA 协议. 之后，诸多学者相继提出满足更多安全属性的 AGKA 协议[38-39]. 但后继的协议都不是非交互的.

文献[37]作者首次提到了 NI-AGKA 的平凡构造方法. 具体的，由参与方生成其公私钥对并公开公

钥.发送方在发送消息时,首先选定接收者集合,集合内所有参与方的公钥即为群加密密钥,每个参与方的私钥即为其解密密钥;其次使用公钥加密机制(PKE)为每一位接收者/参与方生成其专属的密文,即用集合中每位参与方的公钥加密同一消息并得到对应的密文;将每个密文发送给对应的参与方.接收者集合中的每位参与方须用其私钥解密与其对应的密文方可获取消息.尽管该平凡构造方法以非交互的方式实现了多参与方间的安全通信,但该方法在效率方面存在诸多限制,例如:密文总长度随接收者集合大小线性增加、发送者加密过程计算复杂度较大等.

我们注意到,单轮的 Diffie-Hellman 密钥协商协议可通过简单转换变为非交互的 Diffie-Hellman 密钥协商协议.现有的 AGKA 协议几乎都为单轮的密钥协商协议.我们似乎也可以用这种思路来构造 NI-AGKA.

我们以文献[37]中的 AGKA 协议为例,讨论 NI-AGKA 的潜在构造思路.AGKA 协议基于一特殊设计的签名协议来构造,该协议被称为基于聚合签名的广播协议(Aggregatable Signature-Based Broadcast,ASBB),其主要包括密钥生成算法、签名算法和验证算法.潜在构造的 NI-AGKA 也需使用 ASBB 协议.

假设系统中总共有 N 个用户 $\{U_1,\cdots,U_N\}$.每个用户 $U_i(1\leq i\leq N)$ 有一唯一的身份标识符 ID_i(通常为字符串),所有用户的身份标识符号组成集合 $ID_i=\{ID_1,\cdots,ID_N\}$.每个用户需执行 ASBB 协议中的密钥生成算法得到一对临时公私钥对.

若当前存在 $n,n\leq N$ 个用户 $\{U_1,\cdots,U_n\}$ 参与密钥协商,则这 n 个用户形成一个规模为 n 的群组.用户 $\{U_1,\cdots,U_n\}$ 具体协商过程如下:

每个用户 $U_i(1\leq i\leq n)$ 首先确定其在群组中的序号 i'(代表 U_i 为群中第 i 个成员).接着,用户 U_i 运行 ASBB 协议的签名算法生成 n 个签名,表示为 $\sigma_{i'}(ID_1),\cdots,\sigma_{i'}(ID_j),\cdots,\sigma_{i'}(ID_n),1\leq j\leq n$,其中第 j 个签名 $\sigma_{i'}(ID_j)$ 为 U_i 在运行 ASBB 协议的签名算法时,以第 j 个用户的身份标识符 ID_j 和 U_i 的临时私钥为算法输入生成得到的签名.随后,U_i 公开除 $\sigma_{i'}(ID_j)$ 外的所有签名.至此,U_i 生成其长期公私钥对 $(PK_{i'},SK_{i'})$,其中 $PK_{i'}$ 包括 U_i 公开的签名、验证签名的临时公钥以及群序号 i',$SK_{i'}$ 为 U_i 未公开的签名 $\sigma_{i'}(ID_i)$.最终,用户 U_i 利用其他用户长期公钥及自身的长期私钥即可计算出一共同的群公钥 PK 以及 U_i 的解密密钥 $dk_{i'}$,具体的,U_i 计算 $PK=\prod_{i'=1}^{n}PK_{i'}$ 及 $dk_{i'}=\prod_{j=1,j\neq i'}^{n}\sigma_j(ID_i)SK_{i'}$.

在上述潜在构造的 NI-AGKA 中,参与协商的用户在仅看到其他用户公钥的情况下,利用自身私钥即可计算出群加解密密钥,此密钥协商过程满足非交互性质.然而,目前这种潜在构造的 NI-AGKA 所能达到的安全性还未有研究.

4 部分 NIKE 现状与待解决问题

本节主要介绍部分 NIKE,在第 4.1 节主要介绍部分 NIKE 的发展概况与典型协议,在第 4.2 节主要介绍部分 NIKE 待解决的问题.

4.1 部分 NIKE 发展概况

部分 NIKE 是在传统多方 NIKE 落地困难的背景下的一种折中协议.部分 NIKE 可以看作是起源于互联网工程任务组 IETF 所提的消息层安全项目(Messaging Layer Security,MLS).该项目期望实现抵抗窃听、消息篡改等敌手攻击,并且提供良好的前向机密性与后向安全性的群组通信密钥协商协议.同时 MLS 还能作为异步端到端加密(End to End Encryption,E2EE)中建立对称加密密钥的核心组件.

如表 3 所示,我们以支持参与方数量、安全模型、构造技术与安全性假设对部分 NIKE 的典型协议进行了分类.

表 3 部分 NIKE 密钥协商协议分析表

参与方数量	安全模型	构造技术与安全假设	典型协议
多方	Semi-Static	PRG、Updatable Public-key Encryption	文献[19]
多方	Adaptive	HIBE、Key-Updatable Signatures、NIZK	文献[20]
多方	Semi-Static	PRG、CPA-Encryption	文献[40]
多方	Adaptive	PRF、CPA-Encryption	文献[41]
多方	Non-adaptive	PRG、KDF、AEAD	文献[42]
多方	Semi-Static	PRF-ODH	文献[48]

安全模型主要包含适应性模型和半静态模型两类,这里的适应性模型、半静态模型概念与第 3.2 节传统多方 NIKE 中适应性相同.部分 NIKE 和传统多方 NIKE 的敌手询问略有区别,部分 NIKE 中敌手的 Extract 询问,不仅可以获得诚实参与方的私钥还能获得参与方的随机硬币信息,在不少文献中也称为腐化询问(Corrupt).

构造技术与安全假设即为典型协议所使用的主要密码组件和密码学安全性假设.这些协议的安全性

证明主要是将自身的安全性均归约到了所使用的密码学组件安全性，如安全伪随机数生成器(Pseudo Random Generator，PRG)[40]、选择明文安全的加密(CPA-Encryption)[41]、密钥可更新的公钥加密(Updatable Public-key Encryption，UPKE)[19]、分层身份基加密(Hierarchical Identity Based Encryption，HIBE)[20]、带关联数据的认证(对称)加密(Authenticated Encryption with Associated Data，AEAD)[42]、可更新密钥的数字签名(Key-Updatable Signatures，KUS)[20]、密钥派生函数(Key Derivation Function，KDF)[42]、零知识证明(Non-Interactive Zero Knowledge，NIZK)[20]或者密码学困难假设如PRF-ODH 假设.

TreeKEM 作为 MLS 的候选协议在文献[40]中被提出. 该协议主要使用了三种通用密码学原语，分别是哈希函数 $Hash$，密钥派生函数 KDF 和公钥加密 $PKE=(Kgen,Enc,Dec)$. 这里假设有四个参与方需要协商群组秘密值. 每个参与方持有各自的秘密值分别为 A,B,C,D. 这里假设由持有秘密值 A 的参与方来分别初始赋予其他三个参与方秘密值 B,C,D，并以该秘密值为私钥，派生出对应的公钥(例如，$(A,PK_A)=Kgen(1^k)$). 需要注意的是参与方秘密值本质即为参与方自己掌握的一种秘密随机数，群组秘密值则特指群组中所有参与方共享共知的一个秘密随机数.

TreeKEM 具体算法描述如下：

(1) 初始化. 输入为执行初始化的参与方身份，输出为群组初始状态标识符 i，初始 $i=0$.

(2) 群组创建. 输入为初始群组状态 i 和各参与方身份与初始秘密值，输出为更新后群组状态 i 和欢迎消息 W. 群组创建者建立一个二叉树结构计算群组秘密值 K_0，群组秘密值可被用作群组会话密钥的派生元素. 具体来说，假设有四个参与方建立群组过程如图 2 所示. 群组创建者将每个参与方的秘密值 A,B,C,D 放置于二叉树的叶子节点，并赋予对应公私钥对. 从叶子节点所在层开始，每个非叶子节点选取其右孩子的秘密值的哈希值为该节点的秘密值，然后重复这个过程直到根节点秘密值诞生(图 2 中树根秘密值为 $H^2(D)$，表示对秘密值 D 进行两次连续的哈希运算)，其中非根节点均有一对由秘密值派生的公私钥对. 群组创建者使用密钥派生函数计算得到本次协商的群组秘密 $K_i=KDF(H^2(D),K_{i-1}),i=0,K_{i-1}=i$，其中 K_{i-1} 是上一阶段的群组秘密值，此时群组初创，故设定 $K_{i-1}=i$. 群组创建者分别为每个参与方发送一个欢迎消息 W，该消息包含该参与方对应叶子节点到根的路径上所有的节点的公私钥对、以该路径节点的兄弟节点的公钥，这些内容被该参与方的公钥加密(如图 2 中流程，对于持有秘密值 B 的参与者，其获得欢迎消息为：$W=\{Enc_{PK_B}(H(B),H^2(D)),PK_A,PK_{H(D)}\}$. 值得注意的是，后续随着协议中各参与方发起的更新算法不断执行，群组创建者将不再掌握所有参与方的初始的秘密信息.

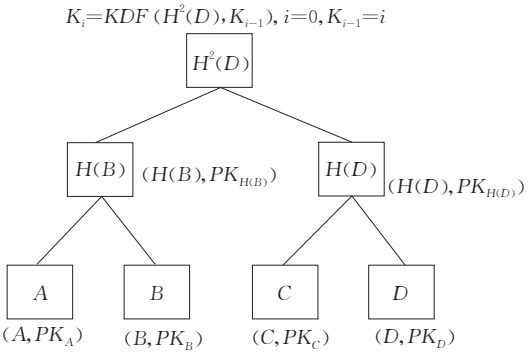

图 2　TreeKEM 技术路线群密钥协商协议群组建立流程图

(3) 更新. 输入为群组状态 i，输出为控制消息 T 和更新的群组状态 i. 当某个参与方发起更新密钥操作，那么该节点首先更新自己对应的二叉树叶子节点的秘密值，其次逐级计算该秘密值的哈希值，作为叶子节点到根路径节点的秘密值(如某个叶子节点更新秘密值为 x，从该节点到根路径上依次第 i 层节点秘密值为 $H^i(x)$，叶子层为第 0 层). 发起更新操作的参与方在本地使用新根节点秘密值和原群组秘密值计算更新后的群组秘密值. 最后将该路径上变化的秘密值和新会话状态标识符 $i=i+1$ 写入控制消息 T 发送给群内其他参与方. 对于群内参与方而言，控制消息内容包括因为本次更新导致的树上节点变化的秘密值和密钥对，同样消息内容使用群内其他参与方的公钥或者共同未变动祖先节点公钥加密). 其他节点接收到上述消息后需执行事务执行算法.

(4) 增加成员. 输入为群组状态 i 和新加入参与方身份，输出为更新的群组状态 i 和消息 W、T. 增加成员算法本质上也是一种更新操作，等价于在二叉树结构中空叶子节点位置设置一个新秘密值，然后执行上述更新算法，故其原理类似，这里不再赘述. 需要注意的是，如果二叉树结构叶子层已满，则可以朴素扩充二叉树结构(例如，创建一个当前二叉树的空白镜像，与现有二叉树组成一棵新的树).

(5)删除成员.输入为群组状态 i 和待删除参与方身份,输出为更新的群组状态 i 和消息 T.发起删除成员的参与方使用一个新的秘密值,替换二叉树上待删除参与方所对应的叶子节点的秘密值(新的秘密值删除成员不掌握).然后发起删除成员的参与方执行与更新算法类似的操作,首先使用新的叶子节点秘密值的多次哈希值,更新叶子节点到根节点的路径上的秘密值.进一步,使用密钥派生函数以新的根秘密值和原群组秘密值为输入,输出为更新的群组秘密值.并向其他参与方发送消息 T(消息的生成和更新算法相同).

(6)事务执行算法.输入为群组状态 i,各参与方收到消息 W 或者 T,输出为更新后的群组状态 i 和群组秘密值 K_i.当参与方收到 W,T 消息后,首先解密消息内容,并更新自己对应叶子节点到根节点路径上变化的节点的秘密值和密钥对,同时更新群组状态 $i=i+1$.最后,使用密钥派生函数以新的根节点秘密值和原群组秘密值为输入,输出是更新的群组秘密值 K_i.

TreeKEM 被提出时并没有给出形式化的安全性证明.在 2020 年,文献[19]作者分析了 TreeKEM 的安全性,证明 TreeKEM 具备较弱的前向安全性并给出了一个改进的 TreeKEM.该改进的 TreeKEM 被证明是半静态安全的.此外,文献[19]作者指出如果要实现抵抗适应性敌手的 TreeKEM,归约损失因子将达到 $n^{\log n}$,n 为群组最大容纳成员数量.此外,诸如文献[41]作者声称的能够通过采用一些特殊的证明技术降低损失因子到 $n^2Q^{\log n}$.其中 Q 为该群组可以执行的群组操作次数(增加、删除成员、更新密钥等).然而,这要求 Q 必须远小于 n 才有实际意义.

文献[20]作者基于 TreeKEM 及其变种,使用 HIBE、KUS 以及NIZK技术构造了主动安全(Active Secure)的部分 NIKE.主动安全概念下敌手可以发起内部攻击(Insider Attacks),即协议中存在攻击者可仿冒被执行过 Extract 询问的参与方身份向系统内参与者发送使协议偏离执行的任意消息.文献[41]作者给出了被称为TTKEM(Tainted TreeKEM)的 TreeKEM 变体.相较于 TreeKEM,TTKEM 增加了对节点状态信息的跟踪机制.TTKEM 在随机谕言机模型和标准模型下被证明在一定程度上满足适应性安全.文献[42]作者提出了一种适用于去中心化网络环境的 TreeKEM 变种.相比于 TreeKEM 需要可信服务器来提供收发消息一致性服务,该协议可在无可信服务器的情况下安全运行.该协议使用的密码学原语有PRG、KDF以及AEAD.该协议被证明是半静态安全的.另外,还有一些针对 TreeKEM 特定问题的研究,如文献[43]作者给出了一个新的 TreeKEM 协议构造,允许通信群组高效并发执行会话密钥更新操作.该协议在不牺牲安全性的前提下,当群组中 n 个用户同时需要执行密钥更新时,群中任意用户也仅需要处理大约 $(\log(n))^2$ 条协议消息,与现有的各种 TreeKEM 协议相比,确实有效的降低了实际通信复杂度.文献[44]作者研究了 TreeKEM 内部攻击者问题,内部攻击指群组内的恶意成员通过发向不同参与者发送不同的协议信息,达到破坏协议正确执行的目的,文献[44]作者对这些攻击行为进行了安全建模与分析,并给出了多个可能解决协议.文献[45]作者研究了群组中参与者元数据泄露的问题,参与者元数据指用户的静态信息(例如:群组中发送消息的用户身份、成员邀请加入关系、成员之间关系等),并且给出了通用可组合安全的捕获元数据泄露的形式化协议安全模型,并基于数字签名技术、多接收者公钥加密技术以及对称密码原语给出了一个具体的协议实例.

另外,分布式架构 TreeKEM 和带有管理员角色的 TreeKEM 也是当前研究的热点问题.文献[46]作者借助区块链技术,设计了分布式架构的 TreeKEM 框架,达到参与者之间消息共识与提升协议执行并发更新时的安全性和稳定性的目的.文献[47]作者通过使用数字签名技术构造了两种带有群组管理员角色的 TreeKEM 并给出了形式化安全分析.第一种称为单管理员签名(Individual Admin Signatures,IAS)协议.该协议要求每个管理员掌握一对独立的签名密钥对,所有的群组操作指令及密钥材料信息均由管理员签名后发出,群组中参与者维持一个列表跟踪所有管理员的签名验证公钥.第二种协议称为动态群组签名(Dynamic Group Signatures,DGS)协议.该协议要求所有群组内的管理员共同维持一个独立的群组信道,共享一对签名公私钥对,所有的群组操作指令及密钥材料信息均由管理员签名后发出,群组中参与者无需维持用于追踪所有管理员签名公钥的列表.

文献[48]作者提出了 MLS 的另一种候选技术路线,即以传统的两方 DH 密钥协商协议为基础,使用二叉树作构造的一种异步棘轮树协议(Asynchronous Ratcheting Trees,ART).在 ART 中,仅

需要单方面广播协议信息，即可完成群组密钥的建立、更新操作. ART 是一个针对静态数量群组成员的协议，目前只支持群组创建和成员密钥更新. 但是文献[48]作者也指出根据参考文献[49]中的工作，容易为 ART 扩展增加成员、删除成员的功能. 文献[47]作者给出了 ART 的安全模型并在随机谕言机模型下将该协议的安全性归约到了 PRF-ODH 假设. 协议具体算法描述如下：

(1) 初始化. 输入为执行初始化的参与方身份，输出为群组初始状态标识符 i，初始 $i=0$.

(2) 群组创建. 输入为群组初始状态标识符 i 和各参与方身份与初始秘密值，输出为更新后的群组状态标识符 i 和欢迎消息 W. 假设有四个参与方需要协商共享的群组秘密值，这四个参与方分别持有自己的秘密信息 A,B,C,D. 这里假设由持有 A 的参与方作为群组建立者，其他参与方的秘密值 B,C,D 由各参与方分别与群组建立者进行一次两方密钥协商(ART 中选用两方 DH 密钥协商协议[3])获得. 需要注意的是秘密值本质即为参与方自己掌握的一种秘密随机数，群组秘密值则特指群组中所有参与方共享共知的一个秘密随机数. 群组创建者计算群组秘密值 K_i，群组秘密值可被用作群组会话密钥的派生元素. 群组建立者将各参与方秘密值设置在二叉树的叶子节点，然后从叶子节点所在的层开始，令同一个父亲节点的两个孩子节点之间执行一次两方 DH 密钥协商协议[3]，然后使用哈希函数将两个孩子节点之间协商的 DH 密钥映射为比特串，作为该父亲节点的私钥(如图 3，A 和 B 的父亲节点私钥 $H(g^{AB})$)，使用该私钥计算一个群元素作为该父亲节点的公钥(例如，A 和 B 的父亲节点公钥 $g^{H(g^{AB})}$)，对其他树节点重复这个过程，直到根节点公钥生成. 最终使用 KDF 以根节点公钥的哈希值和上阶段群组秘密值(群组初创时，以群组状态 $i=0$ 替换上阶段群组秘密值)为输入，输出本次群组协商的群组秘密值 $K_0=KDF(H(pk_{\text{root}}),i)$，$PK_{\text{root}}=g^{H(g^{H(g^{AB})}H(g^{CD}))}$. 然后，群组创建者将每个叶子节点到根节点路径上所有节点的公钥，和该路径上所有节点的兄弟节点的公钥信息，写入欢迎消息 W，发送给其他群内参与方. 后续随着协议中各参与方发起的更新算法不断执行，群组创建者将不再掌握所有参与方的秘密信息.

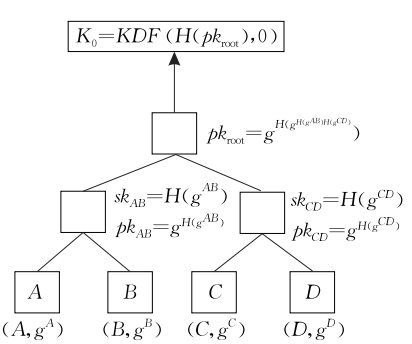

图 3　ART 技术路线群密钥协商协议流程图

(3) 更新. 输入为群组状态标识符 i，输出为控制消息 T 和更新的群组状态标识符 i. 当有一个节点发起群密钥更新操作时，发起节点仅需要更新自己的对应叶子节点的秘密值，并按照群组创建算法中描述的计算方法更新叶子到根路径节点的公私钥对，在本地使用更新后根节点公钥和更新的群组状态计算新的群组秘密值以及更新的群组状态 $i=i+1$. 将本次改变的非叶子节点的公钥信息写入控制消息 T，发送给群内其他各参与方.

(4) 事务执行. 输入为群组状态标识符 i 和消息 w、消息 T，输出为更新后的群组状态标识符 i 和群组秘密 K_i. 其他节点根据接收到的消息 w 或者 T，获取更新的树节点公钥信息，在本地使用更新后根节点公钥和更新的群组状态计算新的群组秘密值 K_i 并更新本地群组状态 $i=i+1$. 群组秘密值可被用作群组会话密钥的派生元素.

4.2　部分 NIKE 待解决的问题

部分 NIKE 待解决的问题主要涉及建立通用安全模型间和紧归约，具体包括：

(1) 部分 NIKE 涉及的参与方多、系统内角色庞杂，目前未有实际可用的通用安全模型.

目前部分 NIKE 的安全性分析基本基于研究者自己提出的安全模型[20,45,48]. 虽然文献[50]作者提出了一个通用部分 NIKE 安全模型. 但文献[50]作者并没有提供任何在该安全模型下可证明安全的具体协议. 因此目前未有广泛认可的通用安全模型. 解决本问题的难点在于现有安全模型捕获的安全性质侧重点不同，涉及的相关安全概念的定义也存在差异. 例如，在捕获具体安全性时，不同模型定义的匹配(如 Matching、Partnering 等)存在差异.

(2) 是否能够形式化地证明 TreeKEM 是紧归约且抵抗适应性敌手的或提出紧归约且抵抗适应性敌手的部分 NIKE.

同两方、三方 NIKE 类似，多方 NIKE 也存在如何构造抵抗适应性敌手和紧归约的 NIKE 的问题. 解决该问题的难点与“构造抵抗适应性敌手且满足

紧归约的两方、三方 NIKE”问题相同.

5 总结与展望

NIKE 作为一种重要的密码学原语,自从诞生起就一直伴随着公钥密码学的发展.本文结合 NIKE 的发展,将当前的 NIKE 分为传统的 NIKE 和部分 NIKE.传统两方 NIKE 的研究历程较长,成果也相对丰富,不少协议也逐渐被部署应用.但是三方和多方 NIKE 则发展缓慢,多方 NIKE 甚至还没有一个堪称可用的协议实例.多方 NIKE 不但是目前密钥协商的研究重点,在可见的未来也是整个密码学领域必须要面对的难题,因此多方 NIKE 值得被深入研究.另外,部分 NIKE 以其极强的实用性成为了近年学术界和工业界研究的热点.然而,部分 NIKE 仍面临未有统一的形式化安全模型、无法给出相对紧致的安全归约等问题.最后,本文也探讨了基于 AGKA 构造多方 NIKE 的潜在技术路线,以及将区块链技术作为 PKI 补充组件对 NIKE 设计的影响.相信在未来,研究者们将会不断推进 NIKE 的发展,这将对密码学和相关产业带来积极影响.

参 考 文 献

[1] Rösler P, Mainka C, Schwenk J. More is less: On the end-to-end security of group chats in signal, WhatSapp, and Threema//Proceedings of the 3rd IEEE European Symposium on Security and Privacy (EuroS&P). London, UK, 2018: 415-429

[2] Cremers C, Fairoze J, Kiesl B, Naska A. Clone detection in secure messaging: Improving post-compromise security in practice//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Online, 2020: 1481-1495

[3] Diffie W, Hellman M E. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[4] Boyd C, Mao W, Paterson K G. Key agreement using statically keyed authenticators//Proceedings of the International Conference on Applied Cryptography and Network Security. Mount Huangshan, China, 2004: 248-262

[5] Cash D, Kiltz E, Shoup V. The twin Diffie-Hellman problem and applications. Journal of Cryptology, 2009, 22(4): 470-504

[6] Freire E S V, Hofheinz D, Kiltz E, Paterson K G. Non-interactive key exchange//Proceedings of the International Workshop on Public Key Cryptography. Nara, Japan, 2013: 254-271

[7] Hesse J, Hofheinz D, Kohl L. On tightly secure non-interactive key exchange//Proceedings of the 38th Annual International Cryptology Conference. Santa Barbara, USA, 2018: 65-94

[8] Hesse J, Hofheinz D, Kohl L, Langrehr R. Towards tight adaptive security of non-interactive key exchange//Proceedings of the Theory of Cryptography: The 19th International Conference. Raleigh, USA, 2021: 286-316

[9] Guo S, Kamath P, Rosen A, Sotiraki K. Limits on the efficiency of (ring) lwe-based non-interactive key exchange. Journal of Cryptology, 2022, 35(1): 1-24

[10] Sakai R, Ohgishi K, Kasahara M. Cryptosystems based on pairing//Proceedings of the 2000 Symposium on Cryptography and Information Security. Okinawa, Japan, 2000, 45: 26-28

[11] Joux A. A one round protocol for tripartite Diffie-Hellman. Journal of Cryptology, 2004, 17(4): 263-276

[12] Boneh D, Silverberg A. Applications of multilinear forms to cryptography. Contemporary Mathematics, 2003, 324(1): 71-90

[13] Lin H, Tessaro S. Indistinguishability obfuscation from trilinear maps and block-wise local PRGs//Proceedings of the 37th Annual International Cryptology Conference. Santa Barbara, USA, 2017: 630-660

[14] Boneh D, Glass D, Krashen D, et al. Multiparty non-interactive key exchange and more from isogenies on elliptic curves. Journal of Mathematical Cryptology, 2020, 14(1): 5-14

[15] Omara E, Beurdouche B, Rescorla E, et al. The messaging layer security (MLS) architecture. Internet-Draft draft-ietf-mls-architecture-02. Internet Engineering Task Force. https://datatracker. ietf. org/doc/html/draft-ietf-mls-architecture-02 Work in Progress, 2019

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

[17] Paterson K G, Srinivasan S. On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups. Designs, Codes and Cryptography, 2009, 52(2): 219-241

[18] Chen Y, Huang Q, Zhang Z. Sakai—ohgishi—kasahara identity-based non-interactive key exchange revisited and more. International Journal of Information Security, 2016, 15(1): 15-33

[19] Alwen J, Coretti S, Dodis Y, Tselekounis Y. Security analysis and improvements for the IETF MLS standard for group messaging//Proceedings of the 40th Annual International Cryptology Conference. Santa Barbara, USA, 2020: 248-277

[20] Alwen J, Coretti S, Jost D, Mularczyk M. Continuous group key agreement with active security//Proceedings of the Theory of Cryptography: 18th International Conference. Durham, USA, 2020: 261-290

[21] Pointcheval D, Sanders O. Forward secure non-interactive key exchange//Proceedings of the International Conference on Security and Cryptography for Networks. Amalfi, Italy, 2014: 21-39

[22] Duman J, Hartmann D, Kiltz E, et al. Group action key encapsulation and non-interactive key exchange in the QROM //Proceedings of the 28th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China, 2023: 36-66

[23] Dodis Y, Katz J, Smith A, Walfish S. Composability and on-line deniability of authentication//Proceedings of the 6th Theory of Cryptography Conference. San Francisco, USA, 2009: 146-162

[24] Yakubov A, Shbair W, Wallbom A, Sanda D. A blockchain-based PKI management framework//Proceedings of the 1st IEEE/IFIP International Workshop on Managing and Managed by Blockchain Colocated with IEEE/IFIP NOMS 2018. Taipei, China, 2018

[25] Orman H. Blockchain: The emperors new PKI? IEEE Internet Computing, 2018, 22(2): 23-28

[26] Boneh D, Zhandry M. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. Algorithmica, 2017, 79(4): 1233-1285

[27] Coron J S, Lepoint T, Tibouchi M. Practical multilinear maps over the integers//Proceedings of the 33rd Annual Cryptology Conference. Santa Barbara, USA, 2013: 476-493

[28] Koppula V, Waters B, Zhandry M. Adaptive multiparty NIKE// Proceedings of the Theory of Cryptography: The 20th International Conference. Chicago, USA, 2022: 244-273

[29] Jia H, Hu Y, Wang X A, et al. Extensional schemes of multipartite non-interactive key exchange from multilinear maps //Proceedings of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC). Krakow, Poland, 2015: 771-774

[30] Garg S, Gentry C, Halevi S. Candidate multilinear maps from ideal lattices//Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Athens, Greece, 2013: 1-17

[31] Gentry C, Gorbunov S, Halevi S. Graph-induced multilinear maps from lattices//Proceedings of the Theory of Cryptography: The 12th Theory of Cryptography Conference. Warsaw, Poland, 2015: 498-527

[32] Zhang Fang-Guo. From bilinear pairings to multilinear maps. Journal of Cryptologic Research, 2016, 3(3): 211-228(in Chinese)
(张方国. 从双线性对到多线性映射. 密码学报, 2016, 3(3): 211-228)

[33] Khurana D, Rao V, Sahai A. Multi-party key exchange for unbounded parties from indistinguishability obfuscation// Proceedings of the 21st International Conference on the Theory and Application of Cryptology and Information Security. Auckland, New Zealand, 2016: 52-75

[34] Zhang Zheng, Zhang Fang-Guo. Garbled circuits and indistinguishability obfuscation. Journal of Cryptologic Research, 2019, 6(5): 541-560(in Chinese)
(张正, 张方国. 混淆电路与不可区分混淆. 密码学报, 2019, 6(5): 541-560)

[35] Lin H. Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 PRGs//Proceedings of the 37th Annual International Cryptology Conference. Santa Barbara, USA, 2017: 599-629

[36] Brakerski Z, Döttling N, Garg S, Malavolta G. Candidate IO from homomorphic encryption schemes//Proceedings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Zagreb, Croatia, 2020: 79-109

[37] Wu Q, Mu Y, Susilo W, et al. Asymmetric group key agreement//Proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cologne, Germany, 2009: 153-170

[38] Zhang L, Wu Q, Domingo-Ferrer J, et al. Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications. IEEE Transactions on Information Forensics and Security, 2015, 10(11): 2352-2364

[39] Li J, Zhang L, Sender Dynamic. Non-repudiable, privacy-preserving and strong secure group communication protocol. Information Sciences, 2017, 414: 187-202

[40] Bhargavan K, Barnes R, Rescorla E. TreeKEM: Asynchronous Decentralized Key Management for Large Dynamic Groups a Protocol Proposal for Messaging Layer Security (MLS)[Ph. D. dissertation]. Inria Paris, France, 2018

[41] Klein K, Pascual-Perez G, Walter M, et al. Keep the dirt: Tainted TreeKEM, adaptively and actively secure continuous group key agreement//Proceedings of the 2021 IEEE Symposium on Security and Privacy. Online, 2021: 268-284

[42] Weidner M, Kleppmann M, Hugenroth D, Beresford A R. Key agreement for decentralized secure group messaging with strong security guarantees//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. Online, 2021: 2024-2045

[43] Alwen J, Auerbach B, Noval M C, et al. CoCoA: Concurrent continuous group key agreement//Proceedings of the 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Trondheim, Norway, 2022: 815-844

[44] Alwen J, Jost D, Mularczyk M. On the insider security of MLS//Proceedings of the 42nd Annual International Cryptology Conference. Santa Barbara, USA, 2022: 34-68

[45] Hashimoto K, Katsumata S, Prest T. How to hide metadata in MLS-like secure group messaging: Simple, modular, and post-quantum//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. Los Angeles, USA, 2022: 1399-1412

[46] Alwen J, Auerbach B, Noval M C, et al. DeCAF: Decentralizable continuous group key agreement with fast healing. Cryptology ePrint Archive, 2022: https://ia.cr/2022/559

[47] Balbás D, Collins D, Vaudenay S. Cryptographic administration for secure group messaging. Cryptology ePrint Archive, 2022: https://ia.cr/2022/1411

[48] Cohn-Gordon K, Cremers C, Garratt L, et al. On ends-to-ends encryption: Asynchronous group messaging with strong security guarantees//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 1802-1819

[49] Kim Y, Perrig A, Tsudik G. Communication-efficient group key agreement//Proceedings of the International Information Security Conference. Boston, USA, 2001: 229-244

[50] Poettering B, Rösler P, Schwenk J, Stebila D. SoK: Game-based security models for group key exchange//Proceedings of the Cryptographers' Track at the RSA Conference. San Francisco, USA, 2021: 148-176

ZHANG Ming-Rui, Ph. D. candidate. His research interests include cryptography and information security.

ZHANG Rui, Ph. D. candidate. Her research interests include information security, public key cryptography, and VANET security.

ZHANG Lei, Ph. D., professor. His research interests include cryptography, VANET security, cloud security, big data security, and privacy protection.

Background

Non-interactive key exchange (NIKE), examined in this paper, belongs to the category of public key cryptography, serving as a foundational element in public key cryptography research. NIKE can be categorized into two main types. The first involves traditional two/three/multi-party NIKE, facilitating the establishment of a shared session key without direct interaction. The second centers on partial NIKE, evolving from the Messaging Layer Security protocol (MLS).

In the case of the first category, a significant challenge in two/three-party NIKE is achieving tight security. For multi-party NIKE, the primary challenge is overcoming limitations in protocol construction tools. Although a multi-party NIKE protocol has been proposed by Dan Boneh et al., the construction tool, multilinear mapping, lacks proven security and efficiency, and the protocol remains unimplemented. Similarly, other multi-party protocols based on multilinear maps, indistinguishability obfuscation, and isogenies lack the required security and efficiency.

Turning to the second category of NIKE, the primary challenge faced by partial NIKE is the absence of comprehensive security analysis for existing protocols. This paper provides a summary of NIKE's development, current issues, and challenges. Additionally, a potential method based on asymmetric group key agreement is proposed for constructing multi-party NIKE, and the potential impact of blockchain technology on NIKE design is discussed. This research is supported by the National Natural Science Foundation of China under Grant Nos. 62372177 and 61972159.