

特色专题

基于异构认证密钥协商协议的抗量子密码协议敏捷迁移

路献辉, 李清之, 刘凯博, 贺婧楠

摘要 抗量子密码协议迁移是整个抗量子密码迁移工程中的核心环节,其核心工作是将现有 TLS (transport layer security)、IPSec(Internet protocol security)、SSH(secure shell)等安全协议中的密钥交换、身份认证、数字签名等基础密码算法替换成抗量子密码算法,并且在迁移过程中保持系统的稳定,兼容现有已经部署的协议版本。介绍面对抗量子密码迁移过程中只有一方完成抗量子迁移的异构场景下如何实现基于异构认证的密钥协商协议(authenticated key exchange, AKE)。首先梳理同构与异构 AKE 的典型构造及主流安全协议中的经典认证密钥交换机制;随后基于 TLS 1.3 双向认证框架,实现基于经典算法 RSA(Rivest-Shamir-Adleman)和 SM2 签名认证与基于抗量子算法的 Dilithium 数字签名(signature, SIG)和 Kyber 密钥封装机制(key encapsulation mechanism, KEM)分别承担不同认证方向的异构认证组合,并扩展证书、密钥加载、握手认证及密钥派生过程。实验对 8 种异构组合进行比较。结果说明,在不要求通信双方同步完成密码算法升级的条件下,异构 AKE 能够支持经典密码与抗量子密码的组合认证,为安全协议的渐进式、敏捷迁移提供一种可实现的过渡方案。

关键词 抗量子密码;公钥加密;数字签名;密钥交换;敏捷迁移

密钥交换协议(key exchange, KE)是密码学中的基本原语,用于使通信双方在不安全信道上协商得到相同密钥,从而建立安全通信信道。其安全性可分为被动安全和主动安全:被动攻击者只能窃听并获取公开参数和通信内容,主动攻击者还可以实施篡改、伪造和重放等攻击。1976 年,Diffie 和 Hellman 提出 Diffie-Hellman(DH)密钥交换协议^[1],奠定了该领域的基础。认证密钥交换协议在密钥交换过程中增加身份鉴别功能,以抵御主动攻击。随后, Law 等^[2]提出 MQV(Menezes-Qu-Vanstone)方案,在协议交互过

程中引入通信双方公钥信息,使只有持有相应私钥的用户才能计算出相同的会话密钥,从而实现隐式身份认证。

认证的密钥协商协议(authenticated key exchange, AKE)的设计主要包括 3 类基本框架:(1) 基于离散对数结构的 HMQV(Hash Menezes-Qu-Vanstone)类协议,采用隐式认证;(2) 基于密钥封装机制和公钥加密的隐式认证框架;(3) 被动安全密钥交换与数字签名结合的显式认证框架。现有大量 AKE 协议均基于这些基本框架构造。

随着 AKE 研究的发展,研究者提出了多种安全模型。1993 年, Bellare 和 Rogaway^[3]首次基于复杂度理论对密钥交换协议进行提出了 Bellare-Rogaway

中国科学院信息工程研究所,北京 100085

收稿日期: 2026-05-13; 修回日期: 2026-08-19

基金项目: 国家重点研发计划项目(2023YFC3305503)

作者简介: 路献辉,教授,研究方向为可证明安全理论、抗量子密码算法设计、同态密码算法设计、物理层安全密码算法设计,电子信箱: luxianhui@iie.ac.cn

引用格式: 路献辉, 李清之, 刘凯博, 等. 基于异构认证密钥协商协议的抗量子密码协议敏捷迁移[J]. 科技导报, 2026, 44(16): 85-95;

doi:10.3981/j.issn.1000-7857.2026.05.00054

(BR)模型, Canetti 和 Krawczyk^[4]进一步提出 Canetti-Krawczyk(CK)模型, 通过会话状态泄露询问、会话 ID 和匹配会话等概念刻画 AKE 安全性。随后, Krawczyk^[5]提出 C 模型, 以增强对密钥泄露伪装和弱完美前向安全等攻击的抵抗能力; LaMacchia 等^[6]进一步提出 eCK(extended Canetti-Krawczyk)模型, 对临时秘密信息泄露等攻击场景进行了更细致的刻画。与此同时, SIGMA(SIGn-and-MAc)^[7]、HMQV 和 FSXY(Fujioka-Suzuki-Xagawa-Yoneyama)^[8]等典型协议分别从数字签名、离散对数和密钥封装机制等角度构造 AKE, 为后续经典和抗量子 AKE 研究提供了基础。

除基本认证和密钥协商功能外, AKE 协议还会根据应用需求考虑匿名性、可否认性、模糊性及口令、证书、生物特征等认证方式。例如, Lyu 等^[9]提出了具有前向安全和显式认证能力的 PPAKE(privacy-preserving authenticated key exchange)构造; Erwig 等^[10]研究了支持模糊口令的 PAKE(fuzzy asymmetric password-authenticated key exchange); Liu 等^[11]提出基于“KEM+SIG(signature)”的双消息显式 AKE; Brendel 等^[12]和 Ishibashi 等^[13]分别研究了可否认 AKE 和单边匿名 AKE。

AKE 协议已广泛应用于网站登录、移动终端访问服务器及金融系统等场景, 用于建立经过身份认证的安全通信信道, 传输层安全协议(transport layer security, TLS)、安全外壳协议(secure shell, SSH)、互联网协议安全(Internet protocol security, IPsec)等主流安全协议的连接建立过程均包含 AKE 机制。

1 认证密钥交换协议与抗量子密码迁移基础

AKE 协议是构建安全通信系统的核心基础, TLS、SSH 与 IPsec 等主流安全协议均通过认证密钥交换机制建立安全信道, 现有协议普遍采用 RSA(Rivest-Shamir-Adleman)、ECC(elliptic curve cryptography)等经典公钥算法, 但经典算法面临潜在的量子攻击威胁, 因此, 安全协议正将认证密钥交换协议由经典密码体系迁移至抗量子密码体系, 在这一过程中, 通信双方可能采用相同功能类型的长期密钥完成同构认证, 也可能分别持有 SIG 密钥与 KEM 密钥, 或

者分别采用经典算法与抗量子算法, 从而形成异构认证场景。与同构认证相比, 异构认证能够适应不同实体迁移进度不一致的现实条件, 是实现抗量子密码敏捷迁移的重要过渡机制。

1.1 同构抗量子认证密钥交换协议

同构认证密钥交换是指通信双方在协议执行前持有相同功能类型的长期密钥对, 并据此完成身份认证与密钥协商。现有抗量子 AKE 大多沿用经典认证密钥交换的基本框架, 通过引入抗量子公钥加密、密钥封装机制和抗量子数字签名等原语, 使协议具备抵抗量子攻击的能力。

张江等^[14]基于 Ring-LWE(ring learning with errors)构造的类 HMQV 的认证密钥交换协议, 不仅具有 HMQV 的隐式密钥认证、效率高等优点, 且基于抗量子的底层困难问题, 使得这一协议可以抵抗量子计算机的攻击。这一方案具有弱完美前向安全性, 安全性不能在 CK 模型中得到证明, 但可以在 BR 模型中证明。

Hvelmanns 等^[15]对 FSXY 进行模块化分析给出了更加简洁的转换并给出了双消息认证密钥交换协议基于游戏的安全性定义。Pan 等^[16]基于 lossy PKE(public key encryption)对 FSXY 的框架进行变形, 给出了 QROM(quantum random oracle model)中一个更紧致的 AKE 的证明。2020 年发布的不使用错误协调机制的 NewHope-Simple 方案, 基于 LWE 和小整数解问题(short integer solution, SIS)问题的 Kyber 方案和基于模上舍入学习问题(module learning with rounding, MLWR)问题的 Saber 方案都是此类密钥交换协议。

Peikert^[17]对 SIGMA 协议进行变形, 将 KEM 与数字签名、消息认证码相结合, 构造后量子认证密钥交换协议。Bos 等^[18]将格上的 KEM 作为 DH 类型的密钥交换协议嵌入到传统的认证体制中如 TLS, 使用 RSA 签名或者 ECC 签名等传统认证机制实现身份认证。del Pino 等^[19]将具有消息恢复功能的数字签名与密钥交换协议相结合。

此外, Xu 等^[20]提出超奇异同源认证密钥交换协议(SIAKE), 并分析了其在量子随机预言机模型下的安全性。该协议的安全性可归约到 SIDH(supersingular isogeny Diffie-Hellman)问题。之后, Jager 等^[21]

也给出了一种新型的抗量子认证密钥建立协议。

Boyd 等^[22]进一步提出模块化 AKE 设计方法, 用基于 KEM 的被动安全密钥交换代替 DH, 并分别设计基于 KEM(KEM-based)和基于签名(SIG-based)的 2 类认证器。通信双方可灵活选择不同认证器, 从而形成多种 AKE 组合, 这种模块化思想也为异构认证密钥交换协议的设计提供了基础。

1.2 异构抗量子认证密钥交换协议

在抗量子密码算法的实际部署中, 由于不同系统在迁移进度、技术路径和密码原语选择上的差异, 通信双方可能持有不同功能类型的长期密钥对, 例如一方使用 SIG 密钥, 另一方使用 KEM 密钥。能够兼容不同密码原语的异构认证密钥交换协议, 可以适应通信实体迁移进度不一致的场景, 是实现抗量子密码协议敏捷迁移的重要技术。

在异构抗量子认证密钥交换协议中, 认证方式、密钥交换和安全性需求如下。

1) 认证方式 2 种。(1) 基于签名的认证: A 方发送挑战给持有签名密钥的 B 方。B 方对挑战进行签名以证明其身份并返回签名。A 方验证签名, 若验证失败则终止通信。这实现了显式认证, 防止伪造者与 A 方建立会话密钥。(2) 基于 KEM 的认证: A 方使用 B 方的 KEM 公钥封装共享密钥, 并将生成的密文发送给 B 方。封装过程包含一个随机值, 该随机值实际上充当挑战。B 方解封装以获得相同的共享密钥。在双消息 AKE 中, 没有从 B 方到 A 方的单独密钥确认步骤, 因此本文将此共享密钥嵌入最终的会话密钥派生中。只有合法的 B 方才能派生出相同的会话密钥, 从而实现隐式认证。Schwabe 等^[23]提出的 KEMTLS 即基于这类 KEM 隐式认证实现了无握手签名的抗量子 TLS。

2) 密钥交换。在 PQC 环境中, 双方之间安全协商共享会话密钥通常通过 KEM 方案实现: 一方使用另一方的公钥封装共享密钥, 将密文发送给对方, 后者解封装以获得相同的密钥。

3) 安全性需求。(1) 前向安全性: 即使长期密钥被泄露, 先前建立的会话密钥也应保持安全。引入临时 KEM 用于密钥交换, 通过为每个会话生成新的密钥对来确保前向安全性。(2) 交叉泄露: 由于每个会话除了长期密钥外还维护自己的秘密状态, 协议必须

在一方的长期密钥和另一方的会话状态同时泄露时仍保持安全。通过确保各方的长期密钥和临时密钥均参与会话密钥派生, 以避免这种交叉泄露的情况下攻击者恢复会话密钥。

下面介绍一方使用签名密钥, 另一方使用 KEM 密钥的异构抗量子认证密钥交换协议, HetAKE 协议^[24]对这类异构 AKE 给出了完整的描述, 不仅涵盖了基本的认证密钥交换流程, 还涉及如何在统一安全模型下集成 KEM 与签名等后量子密码原语。

1.2.1 KEM 发起 SIG 响应

在此场景中, 发起方使用基于 KEM 的长期密钥, 响应方持有基于签名的长期密钥。这种场景与主流的 AKE 设计(如签名 Diffie-Hellman 和 FSXY)非常相似, 其中签名和 KEM 各自发挥标准作用。

1) 认证: 发起方发送新的随机挑战。响应方使用其长期密钥对挑战进行签名, 发起方验证签名。同时, 响应方使用发起方的 KEM 公钥封装一个挑战返回给发起方。只有持有正确长期 KEM 密钥的发起方能够解封装, 再将解封装的共享密钥与会话密钥生成绑定, 防止没有正确密钥的攻击者建立相同的会话密钥。

2) 密钥交换和前向安全性: 使用 KEM 进行临时密钥交换, 确保前向安全性。发起方生成临时密钥对并将其临时公钥发送给响应方, 响应方封装一个临时密钥。发起方随后解封装临时密文以获得相同的密钥。

3) 交叉泄露: 发起方将其临时密钥存储在会话状态中。在双消息设置中, 响应方在向发起方发送消息后不处理数据, 因此没有会话状态。为了使会话密钥在发起方会话状态泄露下仍具有机密性, 会话密钥派生结合了长期 KEM 共享密钥(来自发起方的长期密钥)和临时密钥, 确保仅泄露其中一个组件不足以恢复最终的会话密钥。

1.2.2 SIG 发起 KEM 响应

在此场景中, 发起方持有基于签名的长期密钥, 而响应方使用基于 KEM 的长期密钥。与第一种场景不同, 挑战—响应流程被反转, 为方案设计带来了难度。

1) 认证。响应方的认证可以采用典型的 KEM 方式: 发起方使用响应方的长期 KEM 公钥封装共享密钥, 响应方利用长期私钥解封装, 并将得到的共享

密钥纳入最终会话密钥。对于发起方,由于其在收到响应方挑战之前就需要发送消息,因此不能直接采用普通的挑战——签名方式完成认证。

2) 密钥交换和前向安全性:发起方生成临时 KEM 密钥对,并将临时公钥发送给响应方;响应方使用该公钥封装临时共享密钥,发起方随后进行解封装。响应方返回的临时密文可以视为对发起方的挑战,而发起方成功解封装并得到相同共享密钥则构成响应。由于临时 KEM 密钥本身不能表明发起方身份,因此发起方还需要使用长期签名私钥对临时公钥进行签名,将身份与临时密钥绑定。由此,发起方认证通过长期签名与临时 KEM 共同完成。

3) 交叉泄露:发起方的长期签名私钥本身不能像长期 KEM 私钥一样直接产生共享秘密。为使长期密钥参与最终会话密钥的安全性,发起方生成随机值 r ,并将 r 与长期签名私钥共同作为确定性密钥派生过程的输入,用于生成临时 KEM 密钥,而会话状态仅保存 r 。收到临时密文后,发起方利用 r 和长期签名私钥重新生成临时私钥并完成解封装。这样,攻击者必须同时获得长期签名私钥和会话状态中的 r ,才能恢复相应的会话秘密,从而抵抗交叉泄露。

1.3 主流安全协议及其经典认证密钥交换机制

尽管前文所述的同构与异构抗量子 AKE 为 KEM 和数字签名算法的组合及其安全性分析建立了理论基础,但相关研究目前仍较多地集中于协议构造、安全模型和形式化证明,其在证书体系、算法协商、实现兼容性及部署成本等方面仍有待进一步验证。当前,部分抗量子 KEM 和签名算法已经完成标准化,主流安全协议也开始抗量子算法的试验性部署;然而,抗量子算法尚未全面取代现有密码体系,实际大规模使用的标准化协议仍主要依赖 RSA、DH/ECDH、ECDSA(elliptic curve digital signature algorithm)和 EdDSA(edwards-curve digital signature algorithm)等经典公钥算法完成密钥交换与身份认证。因此,现阶段正处于由经典密码向抗量子密码逐步迁移的过渡时期。下面将以 TLS、SSH 和 IPsec 为例,分别介绍 3 种主流安全协议的流程及其当前采用的经典密钥交换与身份认证算法。

1.3.1 3 种主流安全协议

1) TLS 协议:TLS 是一种广泛应用于互联网通信

的安全协议,主要用于在客户端和服务端之间建立经过身份认证和加密保护的通信信道。TLS 通常部署在传输层协议之上,为上层应用提供身份认证、密钥协商、机密性保护和完整性保护等安全功能。

以 TLS 1.3 为例,其握手过程主要包括协商密码套件、验证通信实体身份、建立共享密钥以及确认握手消息完整性等步骤(图 1)。客户端和服务端首先交换握手参数,并通过密钥交换机制生成共享的临时密钥材料。随后,服务端通常通过发送数字证书和证书验证(certification verify)消息证明其身份以及对握手上下文的控制权。在双向认证场景下,客户端也需要向服务端发送客户端证书和对应的签名证明。

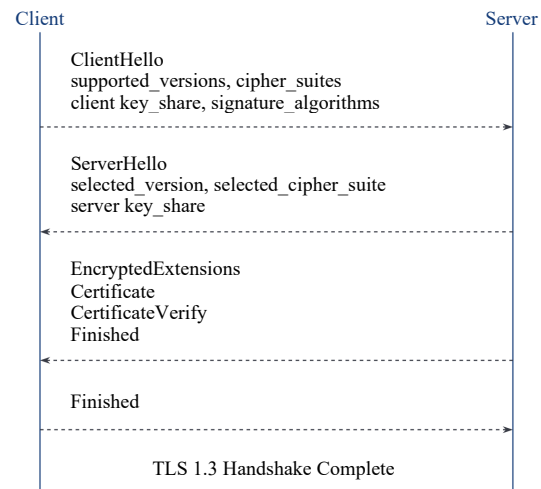


图 1 TLS 1.3 经典握手流程

2) SSH 协议:安全外壳协议(secure shell, SSH)是一种面向远程登录、命令执行、文件传输和端口转发等场景的安全通信协议,通常由传输层协议、用户认证协议和连接协议构成。SSH 通过协商会话算法、验证服务器和用户身份、建立会话密钥等过程,为不安全网络中的远程通信提供安全保护。

以 SSHv2 为例,完整的经典 SSH 安全会话建立过程如图 2 所示,客户端与服务器首先建立 TCP(transmission control protocol)连接,并完成协议版本交换和算法协商;随后通过 ECDH(以使用 ECDH 密钥交换和公钥用户认证为例)计算共享秘密,客户端结合服务器主机密钥及其签名验证服务器身份。双方交换 SSH_MSG_NEWKEYS 后启用受保护的传输,再依次完成用户认证和 SSH 通道建立,最终通过该通道传输应用数据。

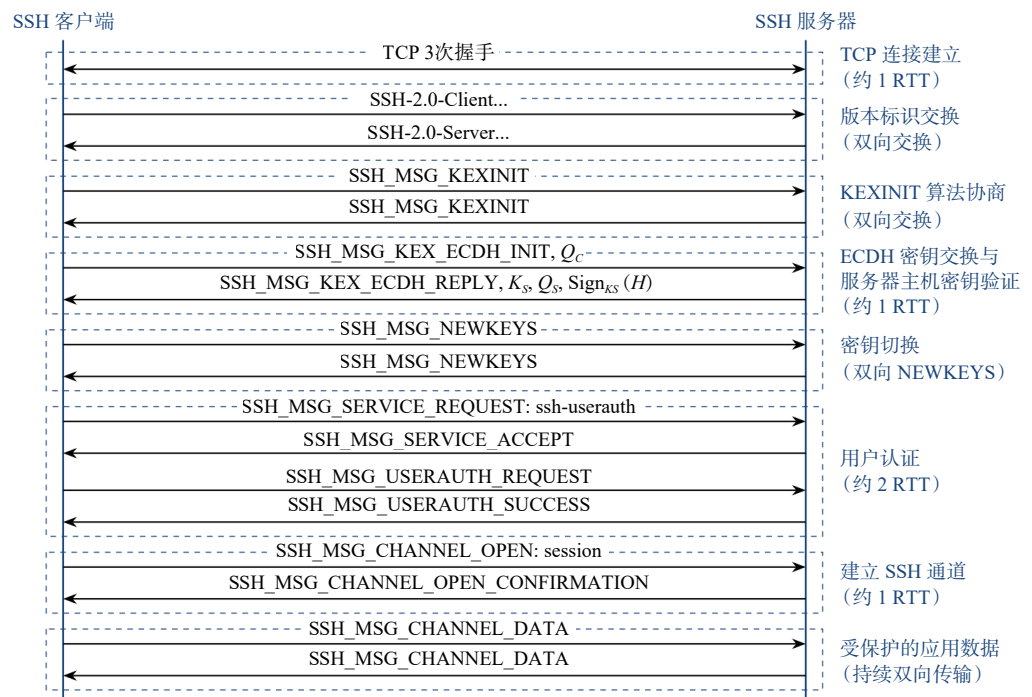


图 2 SSHv2 会话建立完整流程

3) IPsec 协议: IPsec 是一组用于保护网络层通信的安全协议,能够为 IP 数据报提供认证、完整性保护、机密性保护以及抗重放保护等安全功能。IPsec 通常应用于虚拟专用网络、站点到站点安全连接和远程接入等场景。在实际部署中,IPsec 通常使用 IKEv2 协商双方支持的密码算法、建立共享密钥、验证通信实体身份,并生成后续 IPsec 数据通道所需的密钥。

图 3 展示了 IKEv2 的典型初始协商流程:通信双方首先通过 IKE_SA_INIT 协商算法、完成 DH 密钥交换并派生 IKE SA 密钥,随后在受保护的 IKE_AUTH

交换中完成身份认证并建立首对 IPsec Child SA,后续信息由 ESP(encapsulating security payload)保护。

1.3.2 经典认证密钥交换机制

TLS、SSH 和 IPsec 是面向不同应用场景的安全通信协议。三者虽然在协议层次、消息格式、认证对象和安全目标等方面存在差异,但其在握手或连接建立阶段均涉及 AKE,尽管主流安全协议已纷纷启动抗量子密码迁移工作,但就大规模实际部署现状而言,其 AKE 实现仍然主要依赖 RSA、ECDH 以及 ECDSA 等基于大整数分解或离散对数困难问题的密码算法。

这些算法在经典计算模型下具有较高的安全性,然而,量子计算模型已经对基于 RSA 的签名与密钥交换算法,以及基于椭圆曲线离散对数问题这些相关算法产生威胁,因此,本文将上述算法统称为经典非抗量子算法。表 1 是 TLS 1.3、SSHv2、IKEv2/IPsec 中现行的已由 IETF 标准化的经典算法。

随着量子计算的发展,这些经典公钥算法面临着安全威胁,因此 TLS、SSH 和 IPsec 目前正逐步引入抗量子算法,但迁移仍主要集中在密钥交换环节,身份认证的抗量子化相对滞后,因此在过渡阶段可能出现经典长期密钥与抗量子长期密钥并存的异构认证场景。

其中,TLS 协议作为互联网安全的基础设施,支撑着超过 95% 的 Web 流量,其认证机制的异构化升

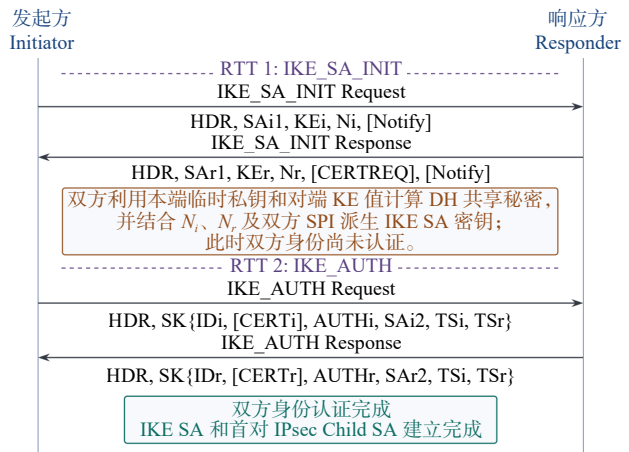


图 3 IKEv2 基本初始协商流程

表 1 3 个主流安全协议中 AKE 使用的经典算法

协议	经典密钥交换算法	经典身份认证算法
TLS 1.3	ECDHE、FFDHE、PSK、PSK-DHE	RSA-PSS、ECDSA、Ed25519、Ed448; 另支持 PSK 认证
SSHv2	Curve25519 ECDH; NIST 曲线 ECDH; 有限域 DH group14/group16/group18	Ed25519、ECDSA、RSA-SHA2-256、RSA-SHA2-512
IKEv2/IPsec	有限域 DH MODP 2048 位及以上; NIST 曲线 ECDH; Curve 25519、Curve448; Brainpool ECDH	RSA-PSS、ECDSA、Ed25519、Ed448; 另支持 PSK 和 EAP

级直接影响着整个互联网的抗量子迁移进程。与其他协议相比, TLS 的握手设计在模块化与可扩展性上具有天然优势, 为嵌入异构认证提供了理想原型平台。鉴于此, 本文基于 TLS 1.3 的握手框架, 将基于量子算法的认证与经典签名显式认证相结合, 构建异构认证密钥交换协议来实现抗量子密码协议敏捷迁移的过渡, 并实验分析方案在耗时、通信量方面的性能。

2 面向抗量子算法敏捷迁移的异构 AKE 设计与实现

2.1 抗量子迁移中的异构认证场景与实现需求

2.1.1 抗量子密码算法的敏捷迁移

现有的主流通信安全协议中的认证密钥交换大多依赖于 RSA、DH、ECDH 等不具备抗量子能力的经典公钥密码算法, 所以量子计算机的发展会对现有网络安全协议构成潜在威胁。为应对这一问题, 包括 TLS 在内的众多安全协议开始了基于格等数学问题的抗量子密码算法的标准化和工程应用部署。

然而, 从经典密码算法迁移到抗量子密码算法并不是一个能够一次性完成的过程。一方面, 不同通信实体的软件版本、硬件能力和安全需求可能存在较大差异, 现有网络中的协议实现、密码库、证书体系、硬件设备和密钥管理基础设施具有较强的历史兼容性, 不同通信实体的升级能力和迁移进度也不可能完全一致, 导致部分实体能够较早完成抗量子算法升级, 而另一些实体可能由于计算资源受限、软硬件更新周期较长或需要兼容既有密码基础设施, 仍需继续使用经典算法。另一方面, 抗量子 KEM 与数字签名算法通常具有不同于经典算法的密钥长度、报文长度和计算特征, 其部署还需要对证书格式、算法标识、握手消息和协议状态进行相应调整。因此, 在较长一段时

间内, 经典算法与抗量子算法将同时存在于实际网络环境中。

因此, 抗量子算法迁移不仅要求安全协议能够在经典算法和抗量子算法之间进行整体切换, 还要求协议具备更细粒度的算法敏捷性, 即能够根据通信双方的能力、配置和安全需求, 分别为 2 个认证方向灵活选择不同的密码算法, 允许双方使用不同类型长期密钥的异构 AKE, 可以在不要求所有实体同步更新的情况下建立经过认证的会话密钥, 为经典密码体系向抗量子密码体系的迁移提供一种过渡方式。

2.1.2 异构 AKE 的认证方式

对于经典认证方向, 本文采用 RSA 和 SM2 作为长期公钥算法。在 TLS 1.3 中, RSA 是作为数字签名算法进行身份认证的。具体而言, 通信实体使用 RSA/SM2 长期私钥生成证书验证签名, 对端利用证书中的 RSA/SM2 公钥验证签名, 从而将实体身份、证书公钥和当前握手会话绑定。对于抗量子认证方向, 本文分别研究基于 KEM 和基于数字签名的 2 种实现方式。

在基于数字签名认证的 AKE 中, 抗量子实体持有 Dilithium2 长期密钥对, 并使用其私钥对握手转录进行签名。对端根据证书或其他可信公钥载体获得 Dilithium 公钥, 并验证该签名。其基本认证逻辑与 TLS 1.3 原有的证书验证消息机制相近, 主要差异在于公钥、私钥和签名数据的长度, 以及对应的算法标识与密码库接口。

在基于 KEM 认证的 AKE 中, 抗量子实体持有 Kyber768 长期密钥对。KEM 本身不具备生成数字签名的能力, 为了利用长期 KEM 密钥完成身份认证, 对端需要使用证书中经过认证的长期 KEM 公钥执行封装, 并将封装密文发送给抗量子实体; 抗量子实体则使用对应的长期私钥进行解封装。封装方和解封装方获得的 KEM 共享秘密被纳入握手密钥派生, 抗量

子实体随后使用由该共享秘密派生的密钥生成 finished 或专门的密钥确认数据。除执行封装并已知共享秘密的一方外,只有持有对应长期 KEM 私钥的抗量子实体才能从封装密文中恢复该共享秘密,并基于共享秘密生成有效的确认数据,因此,对端在验证该确认数据后,可以获得本端抗量子实体持有相应长期 KEM 私钥的证明。基于以上 KEM 私钥持有证明的身份认证过程可以看出,KEM 认证并不是“KEM 直接生成签名”,而是通过“长期公钥封装、长期私钥

解封装、握手密钥派生以及密钥确认”实现。本文的实现会扩展 TLS 1.3 的证书和密钥派生过程,以支持基于长期 KEM 密钥的身份认证。

2.1.3 本文面向敏捷性迁移的异构 AKE 实现

基于上述需求,本文对 TLS 1.3 的双向认证过程进行扩展,使客户端和服务端作为经典实体的一方配置 RSA 或 SM2 长期密钥,作为抗量子实体的一方配置 Kyber768 或 Dilithium2 长期密钥,实现经典算法与抗量子算法在不同认证方向上的组合(表 2)。

表 2 实验认证组合

认证组合	客户端认证模式	服务器认证模式	方案类型
RSA→Kyber768	RSA	Kyber768	经典签名—抗量子KEM
RSA→Dilithium2	RSA	Dilithium2	经典签名—抗量子签名
Kyber768→RSA	Kyber768	RSA	抗量子KEM—经典签名
Dilithium2→RSA	Dilithium2	RSA	抗量子签名—经典签名
SM2→Kyber768	SM2	Kyber768	经典签名—抗量子KEM
SM2→Dilithium2	SM2	Dilithium2	经典签名—抗量子签名
Kyber768→SM2	Kyber768	SM2	抗量子KEM—经典签名
Dilithium2→SM2	Dilithium2	SM2	抗量子签名—经典签名

其中,箭头表示客户端与服务端之间长期身份认证算法的配置方向。以“RSA →Kyber768”为例,客户端使用 RSA 长期密钥完成经典身份认证,服务器使用 Kyber768 长期密钥完成抗量子身份认证。

为了评估异构 AKE 的性能开销,本文对 RSA、SM2、Kyber768 和 Dilithium2 在通信双方组合使用形成的 8 种异构组合,测试并比较了其在 TLS 1.3 握手过程中的执行耗时和通信量,从而分析不同算法配置对抗量子迁移过渡方案性能的影响。

2.2 异构认证场景的实验实现与性能评估

2.2.1 实验目的

本实验的主要目的是在相同的 TLS 通信环境下,对比 RSA→Dilithium2、RSA→Kyber768、Dilithium2→RSA、Kyber768→RSA、SM2→Dilithium2、SM2→Kyber768、Dilithium2→SM2、Kyber768→SM2 这 8 种认证组合的时间开销与通信开销,并验证修改后的 Go TLS 协议栈能否正确支持异构 AKE。实验重点考察以下 2 个性能指标。

1) TLS 连接建立耗时。该指标用于衡量客户端从发起连接开始到 TCP 连接建立、TLS 握手及身份

认证成功完成所经历的时间。每种认证模式分别独立建立 100 次连接,并计算平均连接建立耗时。通过比较 8 种认证模式的测量结果,可以分析不同认证机制及其组合对 TLS 连接建立性能的影响。

2) 单次连接通信量。该指标用于衡量客户端与服务端建立并关闭 1 条 TCP/TLS 连接时产生的双向网络通信量,包括客户端发送量、客户端接收量及二者之和。该指标为 Wireshark 捕获的网络传输字节数,包含 TCP 连接控制、TLS 握手认证和连接关闭等数据。通过比较 8 种认证模式的通信量,可以分析证书、认证消息、签名值及 KEM 相关数据对协议通信开销的影响。

因此,本实验并非单独在 TLS 中实现基于某一种签名算法或 KEM 算法的 AKE,而是从 TLS 协议实际运行的角度,对比异构认证方案在采取不同算法连接建立耗时和双向通信量方面的整体表现,从而评估异构认证密钥交换机制在 TLS 协议中的工程可行性。

2.2.2 实验测量方法

为在统一的 TLS 环境下比较不同算法下的异构认证密钥交换方案,本文基于 Go 原生 crypto/TLS 协

议栈,对证书处理、抗量子密钥加载、握手认证流程及认证模式配置机制进行扩展,在保留 TLS 连接建立、密钥派生、加密通信框架以及经典的 RSA 签名认证的基础上,引入 SM2 签名、SIG 和 KEM 3 类认证方式。其中, SIG 认证采用 CRYSTALS-Dilithium2 算法,认证端对握手相关数据进行签名,对端使用证书中携带的公钥完成验证;KEM 认证采用 CRYSTALS-Kyber768 算法,通过公钥封装、私钥解封装及后续握手确认完成密钥持有证明和实体认证。为实现上述认证,实验首先对 TLS 原生证书生成方式进行拓展,加入经典 SM2 签名算法,然后自定义证书生成模块,分别生成了 SIG 证书、KEM 证书。SIG 证书在自定义扩展中携带 Dilithium2 公钥,并与本地 Dilithium2 私钥配套使用;KEM 证书在自定义扩展中携带 Kyber768 公钥,并与本地 Kyber768 私钥配套使用,使同一通信实体能够根据实验配置进入相应的认证分支。证书公钥与本地私钥必须属于同一密钥对,否则协议栈无法正确完成签名验证或 KEM 解封装,握手过程将直接终止。

1) 耗时测量方法。本文在客户端以 `tls.Dial` 函数作为连接建立与握手的触发接口,在测试开始前完成根证书、客户端证书链及本地私钥的加载,以避免文件读取和证书解析操作对测量结果产生影响。

对于每一种认证模式,客户端连续向服务端发起 100 次独立 TLS 连接。每次测试开始时记录系统时间,随后建立 TCP 连接并完成 TLS 握手;当 `tls.Dial` 成功返回后立即记录结束时间,并关闭当前连接,最后记录 100 次连接的平均耗时、最短耗时以及最长耗时。

由于计时从 TCP 连接建立开始,且 `tls.Dial` 在返回前会完成 TLS 握手,因此该指标反映的是一次完整 TLS 连接建立过程的总耗时,包含 TCP 建连、证书认证、密钥协商及握手确认等环节。

2) 通信量测量方法。通信量实验使用 Wireshark 对客户端与服务器之间的通信过程进行抓包。由于客户端和服务端运行在同一台设备上,实验选择本机环回网络接口进行捕获。针对每种认证模式,客户端均重新发起 TCP/TLS 连接,并从捕获结果中筛选客户端第一次调用 `tls.Dial` 所对应的 TCP 流。该连接在 TLS 握手完成后立即关闭,不包含后续连接中的固

定应用层消息及服务器回显。

本文统计的通信量是 Wireshark 在上述单条 TCP/TLS 连接中观测到的抓包级字节数,而不是单独的 TLS 握手消息长度或纯认证密钥交换数据长度。该数据包含 TCP 连接建立、TLS 握手与认证以及连接关闭过程中产生的通信数据,同时包含 TCP/IP 协议头、确认报文等传输控制开销。8 种认证模式均采用相同的软硬件环境、网络条件、连接流程和统计口径,并分别加载与相应认证模式匹配的证书和密钥。因此, TCP 连接控制开销对各模式的影响基本一致,通信量差异主要来源于 TLS 握手阶段所传输的完整证书链、认证公钥、签名、KEM 密文及其他协议数据结构的不同。

2.3 实验结果与分析

2.3.1 TLS 连接建立耗时测量结果与分析

8 种认证模式的连接建立耗时如表 3 所示。RSA→Dilithium 模式平均耗时为 4.02 ms, Dilithium→RSA 模式的平均耗时为 3.97 ms,两者处于较低水平;而 Kyber768→SM2 模式的平均耗时最高,达 16.85 ms。从算法组合来看,凡是涉及 SM2 算法的认证模式,其平均耗时均显著高于仅涉及 RSA 与后量子算法组合的模式,例如 SM2→Dilithium(14.57 ms)约为 RSA→Dilithium(4.02 ms)的 3.6 倍,表明 SM2 算法在该实现中的计算开销较大。

表 3 耗时测量结果

认证模式	平均耗时/ms	最长耗时/ms	最短耗时/ms
RSA→Dilithium2	4.02	13.79	2.66
RSA→Kyber768	4.61	14.54	3.47
Dilithium2→RSA	3.97	15.14	3.79
Kyber768→RSA	4.10	8.62	3.26
SM2→Dilithium2	14.57	18.31	7.97
SM2→Kyber768	16.55	18.68	15.70
Dilithium2→SM2	15.97	19.04	9.78
Kyber768→SM2	16.85	20.14	15.69

在仅涉及 RSA 与后量子算法的 4 种模式中,平均耗时整体处于 3.97~4.61 ms,波动较小,说明 RSA 与后量子算法(Dilithium2、Kyber768)之间能够实现较为高效的协同工作。进一步观察发现,包含 Kyber768 算法的认证模式(RSA→Kyber768 平均 4.61 ms、Kyber768→RSA 平均 4.10 ms)平均耗时略高于对应

的 Dilithium2 组合 (RSA→Dilithium2 平均 4.02 ms、Dilithium2→RSA 平均 3.97 ms), 但差异在 1 ms 以内, 整体仍在可接受范围内。

总体而言, 基于签名的认证模式(含 Dilithium2)耗时略低于基于 KEM 的认证模式(含 Kyber768), 但两者差距不大; 而 SM2 与后量子算法的异构组合耗时明显偏高, 这与 SM2 算法的实现效率和硬件加速支持不足有关, 在实际部署中需根据性能需求权衡选用。

2.3.2 通信量测量结果与分析

8 种异构认证组合的通信量如图 4 所示(数据已经取整, 故分项之和可能与总量存在少量出入)。在经典认证端为 RSA 的组合中, 总通信量在 36~38 kB 之间; 而经典端为 SM2 的组合总通信量仅为 13~14 kB, 前者约为后者的 2.6 倍。这主要是由于本实验中, RSA 方案将 Dilithium/Kyber 等抗量子材料以自定义 X.509 扩展的形式写入证书, 并且根证书、中间证书和终端证书均携带相关扩展; 同时, 部分二进制抗量子数据经十六进制字符串编码后存储, 使其表示长度进一步增加。TLS 握手传输完整证书链时, 上述额外数据会随证书链一并传输并产生累积开销。相比之下, SM2 方案直接基于原本标准的 X.509 证书机制集成抗量子信息, 证书编码与扩展组织更紧凑, 因此在相同抗量子算法组合下表现出更小的通信量。该差异主要由证书抗量子算法扩展配置不同导致, 不能直接归因于 SM2 算法本身的通信开销更低。这恰恰反映出抗量子算法为了达到相应的安全强度并保证解封装或签名验证的正确性, 需要使用较高维度的代数结构, 同时传输多项式系数、随机性信息和校验数据,

从而增加了认证消息及证书相关数据的长度。只从抗量子算法角度看, Kyber768 替换为 Dilithium2 时, RSA 侧总通信量仅增加 2 kB, SM2 侧仅增加 1 kB, KEM 类抗量子算法在通信量上略优于签名类抗量子算法, 但算法不同造成的影响相对有限。

3 结论

抗量子密码迁移是一项复杂的系统工程, 需要在密码算法、协议、软件、硬件、固件、终端、系统等不同形态不同规模的替换中保持协同的正常运行。而抗量子算法类型和标准的多样性, 以及抗量子密码算法的功能、尺寸、性能等核心指标的巨大差异性给迁移工作带来了严峻挑战。相较于目前基于经典公钥密码体制的主流模式, 本文讨论的基于密钥封装和数字签名 2 类不同的原语实现认证密钥交换的思路为 TLS 等安全协议的迁移提供了更好的灵活性, 针对不同国家、不同机构、不同产品持有不同类型的长期身份数字证书的场景可以提供更好的兼容性和敏捷性。

参考文献 (References)

- [1] Diffie W, Hellman M E. New directions in cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644-654.
- [2] Law L, Menezes A, Qu M H, et al. An efficient protocol for authenticated key agreement[J]. *Designs, Codes and Cryptography*, 2003, 28(2): 119-134.
- [3] Bellare M, Rogaway P. Entity authentication and key distribution[C]//*Advances in Cryptology—CRYPTO '93*. Berlin, Heidelberg: Springer, 1994: 232-249.
- [4] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[C]//*Advances in Cryptology—EUROCRYPT 2001*. Berlin, Heidelberg: Springer, 2001: 453-474.
- [5] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol: Extended abstract[C]//*Advances in Cryptology—CRYPTO 2005*. Berlin, Heidelberg: Springer, 2005: 546-566.
- [6] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange[C]//*Provable Security*. Berlin, Heidelberg: Springer, 2007: 1-16.

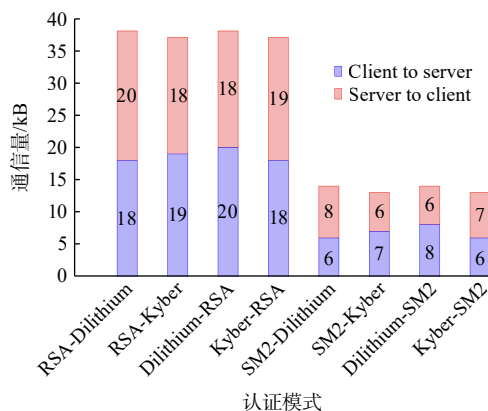


图4 不同认证模式下的通信量

- [7] Krawczyk H. SIGMA: The "SIGn-and-MAC" approach to authenticated Diffie-Hellman and its use in the IKE protocols[C]//Advances in Cryptology—CRYPTO 2003. Berlin, Heidelberg: Springer, 2003: 400–425.
- [8] Fujioka A, Suzuki K, Xagawa K, et al. Strongly secure authenticated key exchange from factoring, codes, and lattices [C]//Public Key Cryptography—PKC 2012. Berlin, Heidelberg: Springer, 2012: 467–484.
- [9] Lyu Y, Liu S L, Han S, et al. Privacy-preserving authenticated key exchange in the standard model[C]//Advances in Cryptology—ASIACRYPT 2022. Cham: Springer Nature Switzerland, 2022: 210–240.
- [10] Erwig A, Hesse J, Orlt M, et al. Fuzzy asymmetric password-authenticated key exchange[C]//Advances in Cryptology—ASIACRYPT 2020. Cham: Springer International Publishing, 2020: 761–784.
- [11] Liu X Y, Liu S L, Gu D W, et al. Two-pass authenticated key exchange with explicit authentication and tight security[C]//Advances in Cryptology—ASIACRYPT 2020. Cham: Springer International Publishing, 2020: 785–814.
- [12] Brendel J, Fiedler R, Günther F, et al. Post-quantum asynchronous deniable key exchange and the signal handshake [C]//Public-Key Cryptography—PKC 2022. Cham: Springer International Publishing, 2022: 3–34.
- [13] Ishibashi R, Yoneyama K. Post-quantum anonymous one-sided authenticated key exchange without random oracles [C]//Public-key cryptography—PKC 2022. Cham: Springer International Publishing, 2022: 35–65.
- [14] Zhang J, Zhang Z F, Ding J T, et al. Authenticated key exchange from ideal lattices[C]//Advances in Cryptology—EUROCRYPT 2015. Berlin, Heidelberg: Springer, 2015: 719–751.
- [15] Hvelmanns K, Kiltz E, Schge S, et al. Generic authenticated key exchange in the quantum random oracle model[C]//Public-Key Cryptography—PKC 2020. Cham: Springer International Publishing, 2020: 389–422.
- [16] Pan J X, Wagner B, Zeng R Z. Tighter security for generic authenticated key exchange in the QROM[C]//Advances in Cryptology—ASIACRYPT 2023. Singapore: Springer Nature Singapore, 2023: 401–433.
- [17] Peikert C. Lattice cryptography for the Internet[C]//Post-Quantum Cryptography. Cham: Springer International Publishing, 2014: 197–219.
- [18] Bos J W, Costello C, Naehrig M, et al. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem[C]//Proceedings of the IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE, 2015: 553–570.
- [19] del Pino R, Lyubashevsky V, Pointcheval D. The whole is less than the sum of its parts: Constructing more efficient lattice-based AKEs[C]//Security and Cryptography for Networks. Cham: Springer International Publishing, 2016: 273–291.
- [20] Xu X, Xue H Y, Wang K P, et al. Strongly secure authenticated key exchange from supersingular isogenies[C]//Advances in Cryptology—ASIACRYPT 2019. Cham: Springer International Publishing, 2019: 278–308.
- [21] Jager T, Kiltz E, Riepel D, et al. Tightly-secure authenticated key exchange, revisited[C]//Advances in Cryptology—EUROCRYPT 2021. Cham: Springer International Publishing, 2021: 117–146.
- [22] Boyd C, de Kock B, Millerjord L. Modular design of KEM-based authenticated key exchange[C]//Information Security and Privacy. Cham: Springer Nature Switzerland, 2023: 553–579.
- [23] Schwabe P, Stebila D, Wiggers T. Post-quantum TLS without handshake signatures[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 1461–1480.
- [24] Lu X H, Cheng Y, He J N, et al. HetAKE: Heterogeneous authenticated key exchange for post-quantum migration[C]//Information Security and Privacy. Singapore: Springer Nature Singapore, 2026: 24–77.

Agile migration of post-quantum cryptographic protocols heterogeneous authenticated based key exchange

LU Xianhui, LI Qingzhi, LIU Kaibo, HE Jingnan

Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China

Abstract The migration of post-quantum cryptographic protocols is a core part of the overall transition to post-quantum cryptography. Its main task is to replace the key exchange, identity authentication, digital signature, and other basic cryptographic algorithms used in existing security protocols, such as TLS (transport layer security), IPsec (Internet protocol security), and SSH (secure shell), with post-quantum algorithms, while maintaining system stability and compatibility with deployed protocol versions. This paper investigates heterogeneous authenticated key exchange (AKE) in migration scenarios where only one communicating party has completed the transition to post-quantum cryptography. First, typical homogeneous and heterogeneous AKE constructions and classical authenticated key exchange mechanisms in mainstream security protocols are reviewed. Then, based on the TLS 1.3 mutual authentication framework, heterogeneous authentication combinations are implemented, in which classical RSA and SM2 signature authentication and post-quantum Dilithium signatures (SIG) and Kyber key encapsulation mechanisms (KEM) are used in different authentication directions. The certificate, key loading, handshake authentication, and key derivation processes are extended accordingly. Experiments on eight heterogeneous combinations show that heterogeneous AKE supports combined classical and post-quantum authentication without requiring both parties to upgrade simultaneously, providing a practical transition approach for gradual and agile protocol migration.

Keywords post-quantum cryptography; public-key encryption; digital signature; key exchange; agile migration ●



(责任编辑 王志敏)