# 【研究成果】IPSeQ: 集成量子密钥分发的安全增强型IPSec协议（IEEE Commun Mag）

信息网络安全杂志 2025年3月6日 17:00 上海

以下文章来源于InfonetLab，作者李忠辉

近日，实验室硕士研究生高旭民作为第一作者的论文“IPSeQ: A Security-Enhanced IPSec Protocol Integrated with Quantum Key Distribution”被通信领域旗舰期刊IEEE Communications Magazine录用，中国科学技术大学为第一单位和唯一通讯单位。

## 研究背景

随着互联网的发展，信息安全已提升为全球关注的焦点。互联网协议安全（IPSec）凭借其在网络层提供的认证、机密性和数据完整性，成为保护公共互联网安全通信的核心。然而，量子计算技术的迅猛发展，尤其是Shor算法和Grover算法的出现，给传统的加密方法带来了前所未有的挑战。Shor算法能够高效分解大数和计算离散对数，直接威胁到IPSec依赖的RSA和椭圆曲线Diffie–Hellman（ECDH）密码算法。同时，Grover算法能将对称加密密钥长度的有效安全性减半，进一步削弱了IPSec协议的整体安全性。虽然现代加密系统尚未完全被量子计算攻破，但全球范围内量子计算的进步预示着这种威胁可能在未来数十年内成为现实，因此设计抗量子攻击的IPSec协议显得尤为紧迫。

量子密钥分发（Quantum Key Distribution, QKD）依托量子力学原理，通过信息论安全方法在通信双方之间分配对称密钥，保证密钥交换在量子时代的安全性。因此，将QKD技术整合入IPSec协议，提供了一种有前景的长期解决方案。目前，IPSec与QKD的集成方案主要分为两类。第一类结合量子密钥和经典密钥以补充互联网密钥交换协议（IKE）；第二类则用QKD替代IKE的密钥交换功能。尽管这些方法在某些方面取得了进展，但在安全性、效率和灵活性方面仍存在诸多限制，推动着我们进一步探索如何在IPSec中高效整合QKD技术，以全面提升其在量子计算时代的安全性。

## 主要贡献

针对现有方法的局限性，本文提出了一种名为IPSeQ的安全增强型IPSec协议，IPSeQ在不改变原有IKE架构的基础上，通过引入高效的量子密钥管理设计，确保协议的灵活性和高效集成，该方案的具体贡献主要包括以下三个方面：

1.安全增强型协议IPSeQ：通过将QKD技术融入密钥交换、认证和加密过程，IPSeQ有效缓解了量子计算威胁，并在保留原有IKE架构的同时，为IPSec提供了全面的安全保障。此外，我们设计了一种高效的量子密钥管理方案以支持此集成。

2. 动态密钥更新机制：根据量子密钥生成率和加密密钥需求动态调整更新频率，实现了快速的量子密钥更新以提升通信安全性，并避免了密钥资源耗尽导致的传输效率下降。此外，我们采用滑动窗口机制来实现快速密钥更新过程中的密钥同步。

3. IPSeQ原型系统：基于真实QKD设备搭建了IPSeQ原型系统，并验证了IPSeQ的有效性。实验结果表明，即使在量子密钥资源稀少的情况下，IPSeQ也能显著提升传输效率并保持稳定性。

## 方案设计

### 一、系统框架

针对现有IPSec协议易受量子计算攻击这一安全隐患，我们提出了一种融合QKD的安全增强型IPSec安全协议——IPSeQ。为了减轻不安全的非对称加密算法带来的威胁，IPSeQ将量子密钥融入到密钥交换、身份验证和加密过程中，保护整个IPSec协议。同时，我们保留了标准IKE协议的框架，既保证了灵活的协商能力，又可以与传统IPSec无缝集成。对于已经部署了 IPSec VPN 隧道的用户，他们可以通过访问 QKD 网络并从密钥管理系统获取量子密钥；也可直接连接 QKD 设备获取量子密钥。我们通过引入量子密钥接口（QKI）中间件来扩展使用场景，并解决密钥管理问题。

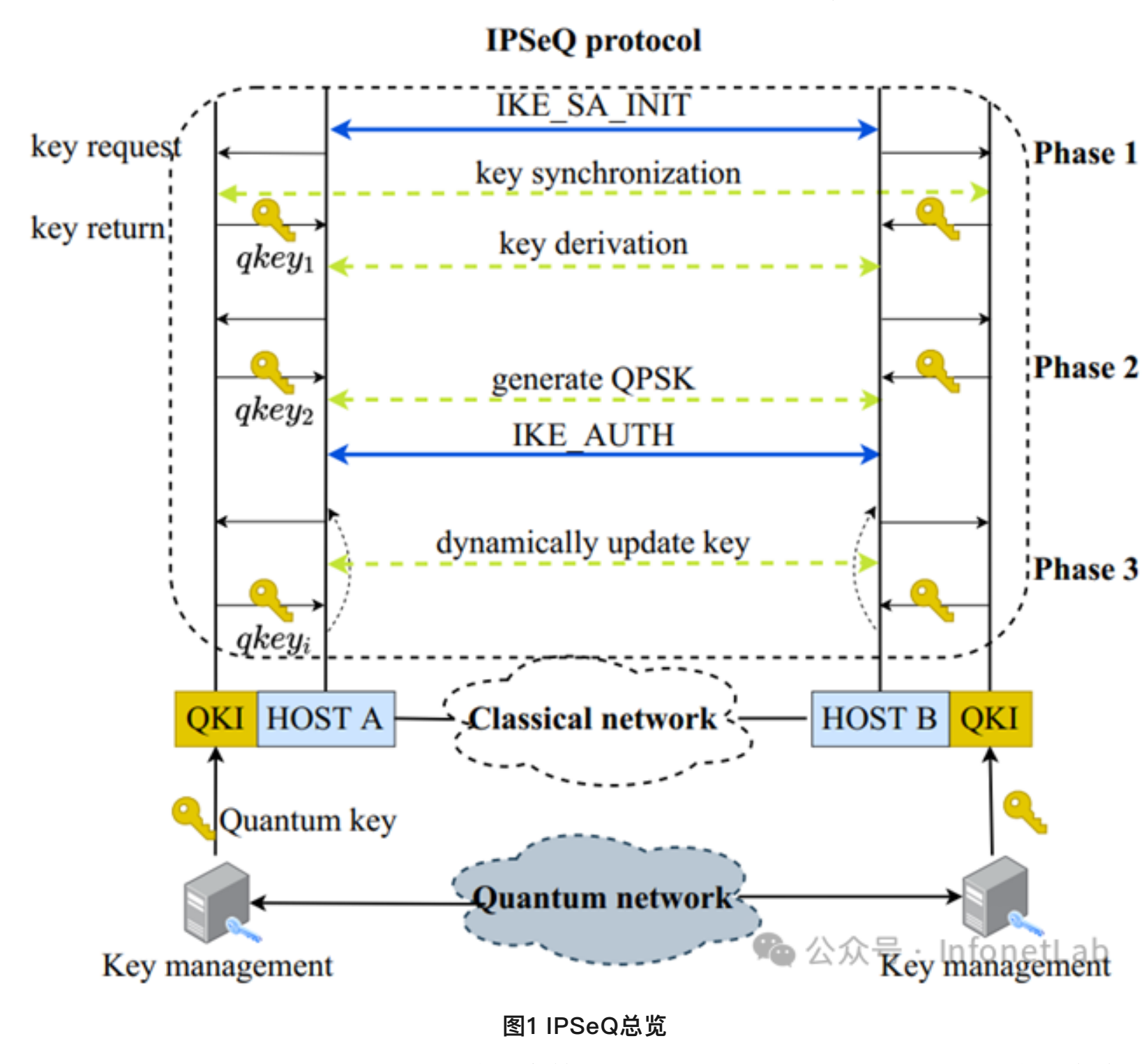


图1 IPSeQ总览

如图1所示，IPSeQ由三个阶段组成。在第一阶段，IPSeQ引入了基于QKD的密钥交换机制，为DH交换生成的密钥材料提供抗量子安全性，从而保护IPSec SA和IKE SA。在第二阶段，IPSeQ通过结合PSK和量子密钥来增强认证安全性，并以OTP形式使用量子密钥，有效降低PSK安全性退化的风险。在第三阶段，IPSeQ使用量子密钥快速更新会话密钥，进一步提升PFS，并通过滑动窗口机制实现密钥同步。此外，IPSeQ动态调整密钥重用参数，充分利用量子密钥资源并保持传输效率。

### 二、QKI设计

QKI 进程通过API从密钥管理器获取量子密钥，该流程遵循基于 ETSI 标准协议的简化设计，以确保互操作性和安全性。QKI之间的通信使用TCP协议，消息完整性由基于哈希的消息验证码（HMAC）保护。同时，IPSec 进程使用内部密钥获取协议向 QKI 申请加密和解密密钥。IPSec 进程首先向QKI 提交注册请求，通过 SPI 识别。然后，QKI 为请求分配一个密钥缓冲区。鉴于SA的单向性，QKI在SA对之间划分双向加密和解密密钥池。IPSec VPN之间可以存在多对SA，实现各种安全策略。因此，QKI有必要对量子密钥池的划分进行有效管理。由于每个SA加密的流量是不确定的、动态变化的，固定速率请求会导致量子密钥资源的不公平分配并导致饥饿问题。为了解决这个问题，我们利用公平划分密钥管理模型，为每个请求分配相同大小的密钥缓冲区，通过监控密钥缓冲区大小并优先为密钥消耗速度更快的请求补充密钥，即使在任意SA出现突发流量的极端情况下，密钥供给服务的稳健性仍然能够得到保证。

### 三、IPSeQ设计

第一阶段：为了保护IKE SA和IPSec SA免受量子计算攻击，我们提出了基于QKD的密钥交换机制，使用量子密钥来增强不安全的DH密钥。我们参考RFC 8784中的实现，并通过以下方式组合量子密钥$qkey_1$：通信双方将添加$qkey_1$到派生密钥材料$SK_d$中，为IPSec SA和后续的IKE SA使用的密钥提供抗量子安全性；然后，通信双方将$qkey_1$添加到用于计算签名对象的$SK_{pi}$和$SK_{pr}$中，使通信双方能够检测到密钥不匹配情况。

第二阶段：为了避免使用不安全的公钥认证方法并确保基于PSK的认证的长期安全性，我们在IPSeQ中使用PSK和量子密钥的组合进行认证。具体来说，IPSeQ要求通信双方共享一个长期密钥psk，作为握手过程中的认证基础。在IKE_AUTH阶段之前，双方都会获得一个32字节的量子密钥$qkey_2$。然后，他们将$psk$和$qkey_2$组合起来得到量子预共享密钥$QPSK$，计算方法如下所示：$QPSK=HMAC(qkey_2,psk)$,并使用$QPSK$生成AUTH有效负载。双方比较计算所得AUTH值是否一致。如果$psk$或$qkey_2$不一致，双方都会检测到AUTH不匹配，即认证失败。

第三阶段：在完成IKE_SA_INIT交换以及IKE_AUTH交换之后，一对IPSec SA将会被生成并用于保证数据的安全传输。但是，在IPSec SA生效期间，加密密钥和完整性保护密钥保持不变，其被破解的风险随着数据传输量的增大而不断增加。为了解决与IPSec SA密钥相关的安全退化问题并实现安全高效的密钥更新，我们提出了一种快速密钥更新方案，通过使用量子密钥不断更新会话密钥来增强PFS。我们直接从本地QKI获取新的量子密钥，无需进行DH密钥交换或IPSec SA频繁更换，从而减少了通信开销。

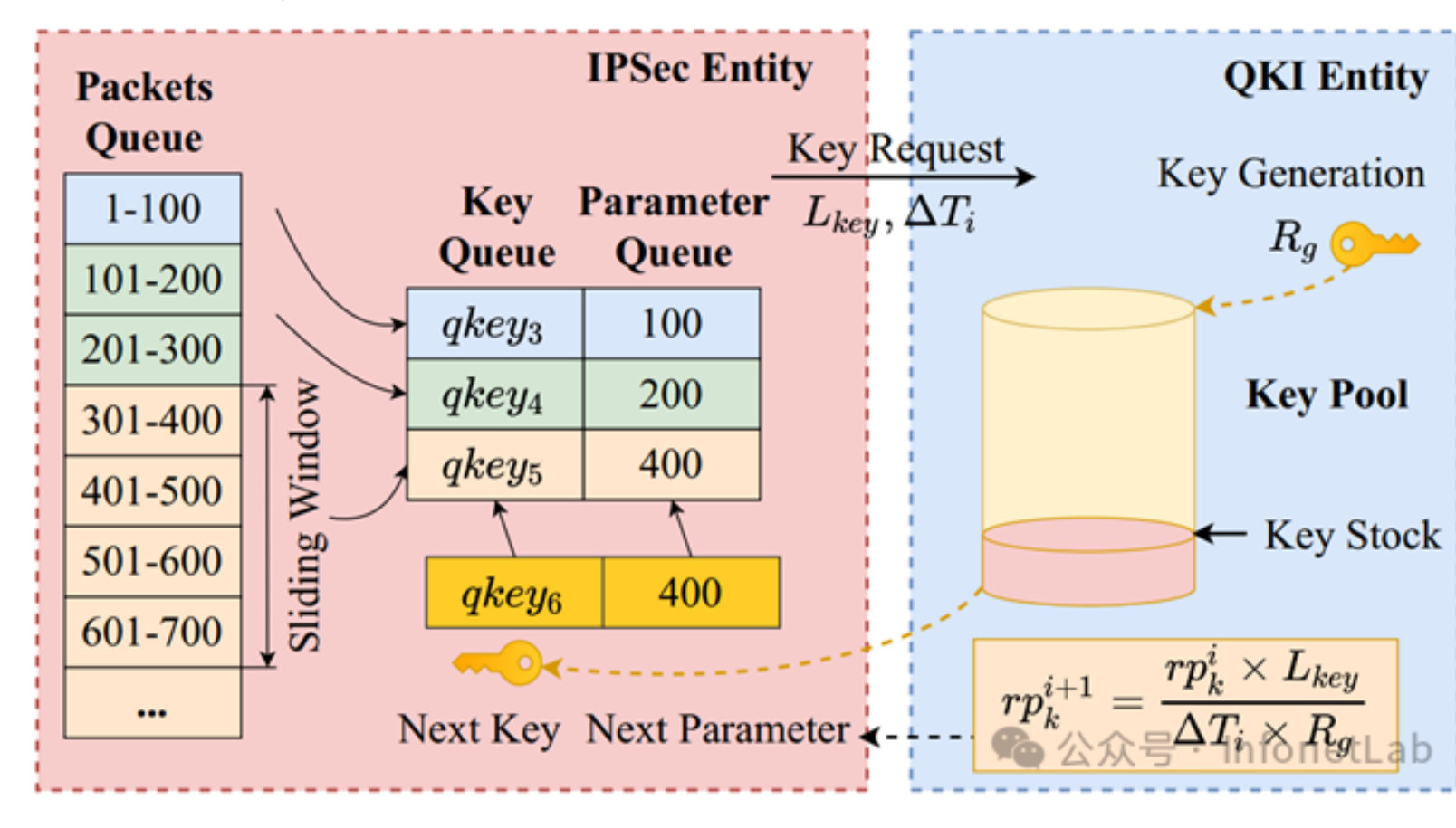


图2 动态密钥更新

首先要解决密钥同步问题，即通信双方不匹配的密钥将会使得数据包验证失败从而丢弃数据包，无法完成正常的数据传输。由于通信双方独立于QKI设备获取量子密钥，需要同步量子密钥流的起始位置。为了确保会话密钥快速更新期间加密和解密密钥之间的一致性，我们使用ESP数据包头包含的4字节序列号字段将数据包与其对应的量子密钥相关联。具体地，IPSec进程维护一个滑动窗口，每个窗口对应一个量子密钥的保护范围。在加密和解密过程中，对滑动窗口进行调整，确保数据包与其相应的量子密钥之间的无缝对齐。如图2所示，$qkey_3$保护序列号范围为1到100的数据包。此时，滑动窗口覆盖序列号1到100。随着量子密钥的每次变化，滑动窗口将转移到覆盖序列号101到300，随后是301到700。

然后要解决的是效率问题，通信双方之间的量子密钥生成率较低且动态波动，这不可避免地导致量子密钥低供应与互联网数据传输的高需求之间的差距。采用固定速率密钥更新机制要么耗尽密钥，要么积累大量未使用的密钥。为了解决这个问题，我们引入密钥重用参数$rp_k$来调节每个量子密钥的使用次数。鉴于量子密钥生成和数据传输需求都动态波动，通过实时调整$rp_k$来保持量子密钥生成和消耗间的平衡，具体设计可参照原文描述。

## 结果分析

### 一、实验设置

为了评估IPSeQ的性能，我们使用实际的QKD设备和网络平台搭建了IPSeQ原型系统。如图3所示，实验框架主要由量子密钥接口，IPSec进程，测试平台三部分组成。QKI为IPSec进程提供密钥接口，并接收QKD设备生成的密钥。我们修改并开发了开源软件strongSwan作为IPSec进程。认证加密方案设置为AES128-GCM16，使用用户态模式IPSec实现以方便更改和获取密钥。使用四台Ubuntu电脑主机，其中，两台作为网关保护子网，两台在每个子网内部。两台QKD设备为网关提供量子密钥，我们使用的是国盾量子公司的一对 QKD-PHA1250-S 高速时相编码 QKD 系统。

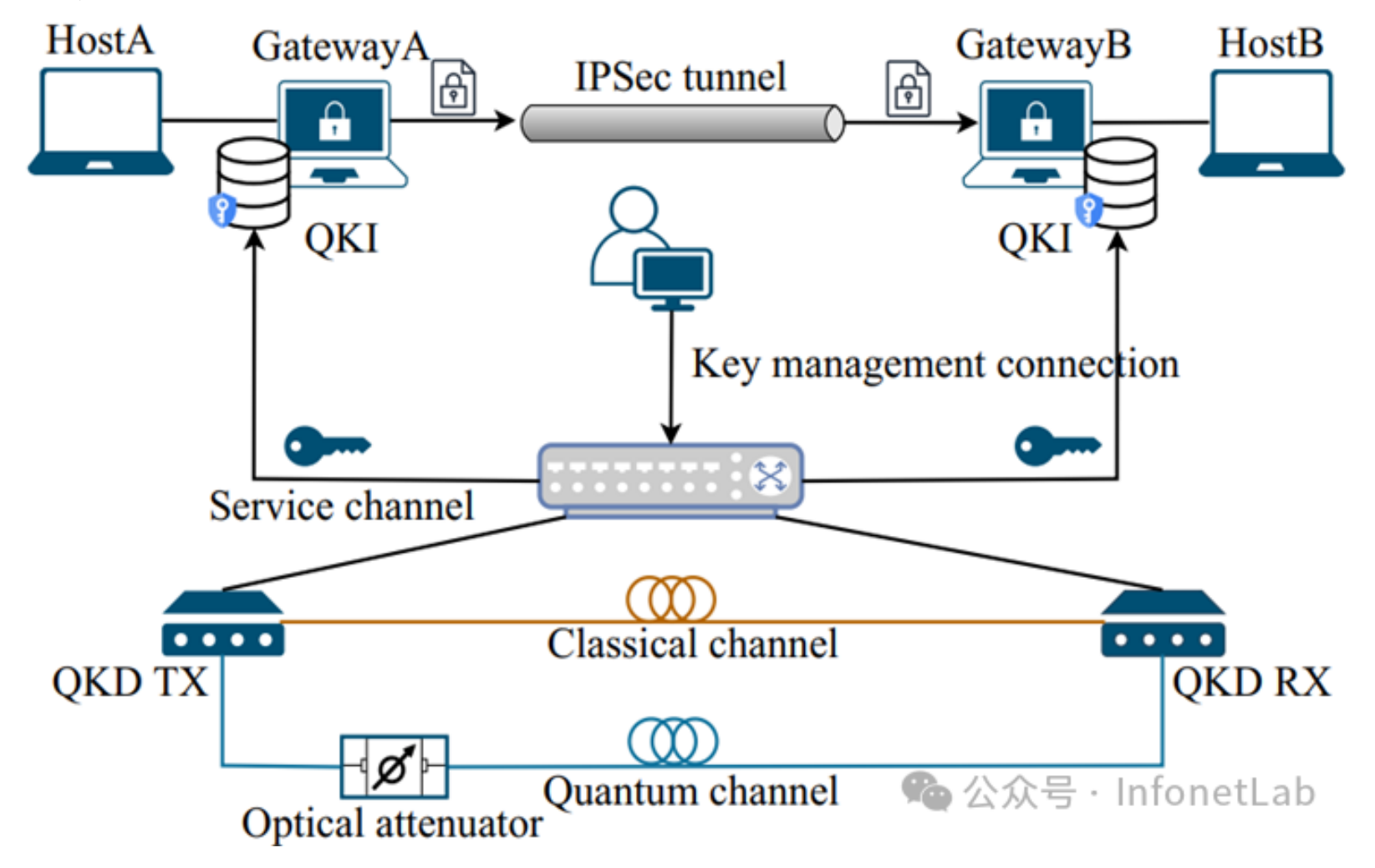


图3 IPSeQ原型系统

我们首先将IPSeQ与标准IPSec在处理延迟方面进行比较，使用ping命令记录每个数据包的延迟。随后，我们量化SA密钥替换的开销以及建立IPSec连接所需时间。为了证明IPSeQ可以实现快速密钥更新并保持密钥同步，我们使用iPerf工具评估两个IPSec网关间的传输性能，对所提出的动态密钥更新方案和标准密钥重新协商方案进行评估。最后，为了验证动态密钥更新机制的有效性及其在实际噪声量子信道中的可行性，我们评估了信道长度对密钥生成率和密钥重用参数的影响。

### 二、实验结果

图4显示IPSeQ的性能在RTT方面与标准方案相当，主机A和主机B之间的RTT约为2ms。我们还观察到：由于需要进行CREAT_CHILD_SA交换，标准方案产生了约7ms的密钥更换延时；相比之下，IPSeQ直接从密钥池获取密钥，通过QKD过程不断向密钥池补充密钥，通信延迟仅约1ms，显著降低开销。此外，标准握手延迟超过8ms，而IPSeQ在引入了两个量子密钥增强过程后的综合延迟小于10ms，两者之间的差异很小且可以接受，但IPSeQ提供了显著增强的安全性。

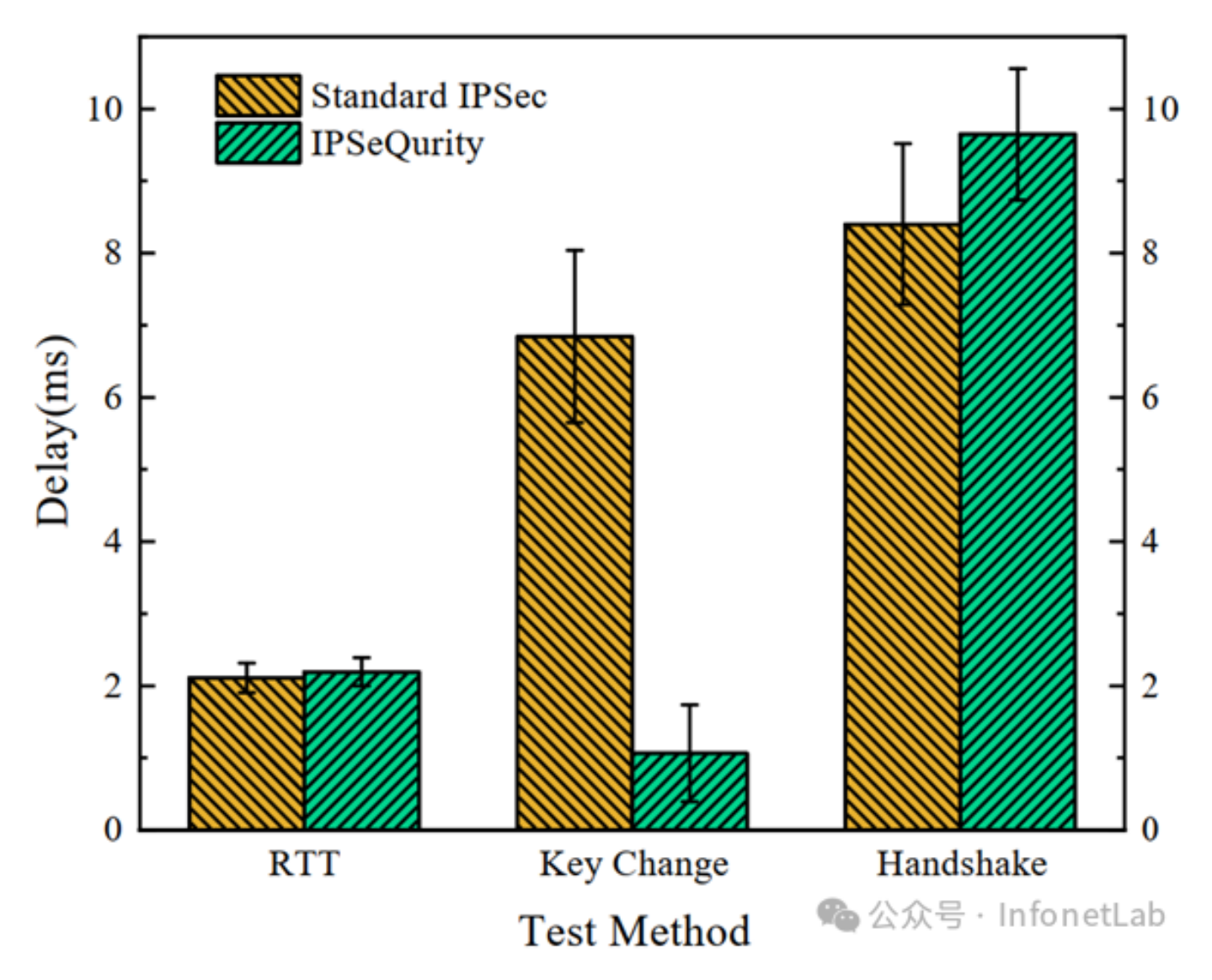


图4 IPSeQ时延测试

图5显示了不同密钥更新频率下IPSeQ与标准方法的吞吐量性能对比。标准方法依赖于CREATE_CHILD_SA交换。当应用程序发送一定数量的数据包时更新密钥，这种交换涉及多个数据包的交互，导致过多的开销。因此，当密钥更新频率较高时，吞吐量会急剧下降。相比之下，IPSeQ使用密钥重用参数来控制密钥更新并直接从QKI获取量子密钥，从而最大限度地减少交互开销。即使更新频率增加，吞吐量仍然相对不受影响并保持在较高水平。对于没有密钥更新的场景，即使存在QKI通信、密钥同步和其他相关进程相关的开销，IPSeQ也仅有约7%的性能下降。此外，在快速密钥更新的情况下，图5表明我们的协议在丢包方面性能明显优于标准方案。这是因为在IPSec SA的密钥重新协商过程中，标准方案可能会因密钥的变化而导致报文加解密的不一致问题。相比之下，IPSeQ通过滑动窗口机制保持数据包和密钥之间良好的同步，从而最大限度地减少数据包丢失。

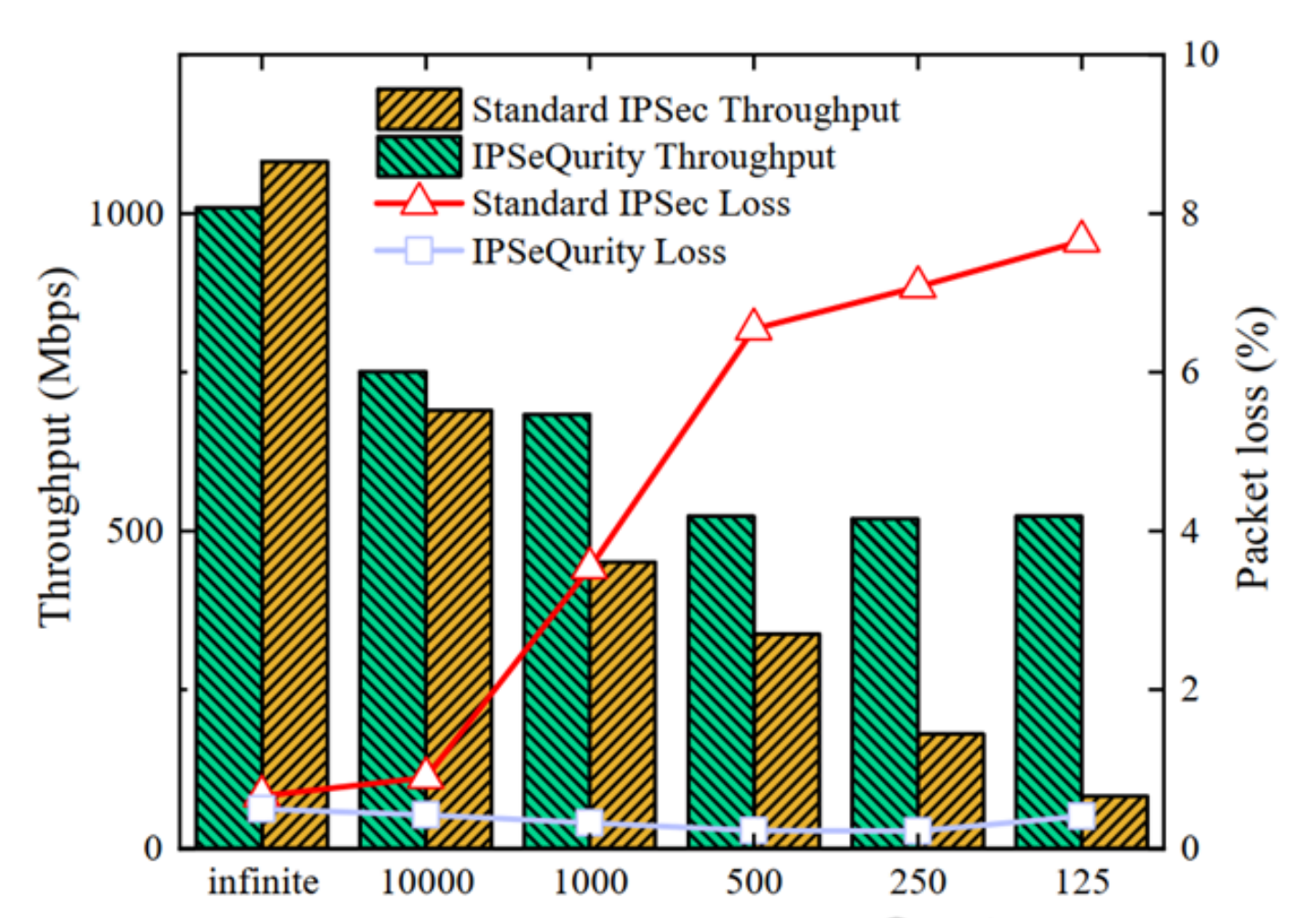


图5 不同密钥更新频率下传输性能比较

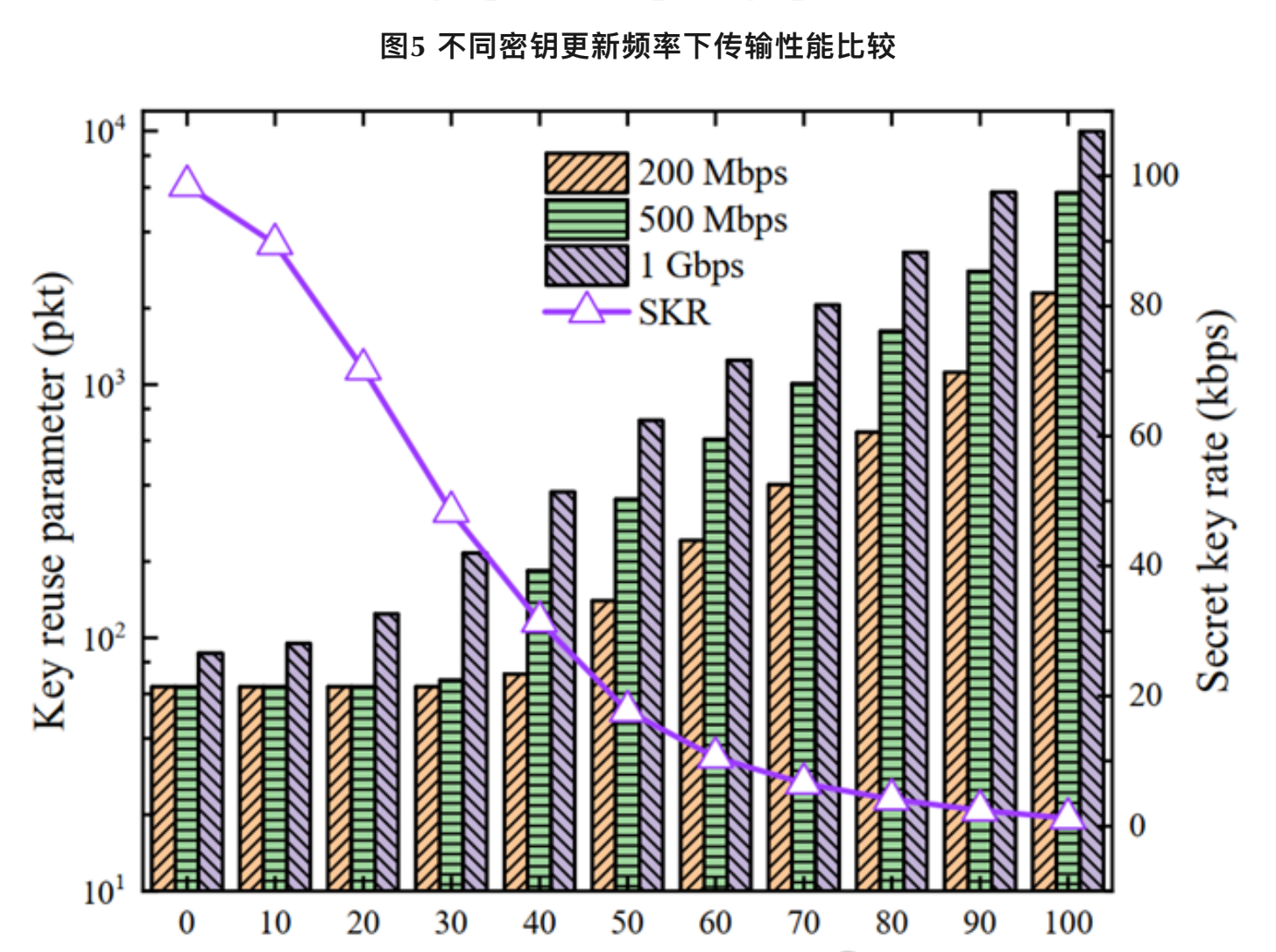


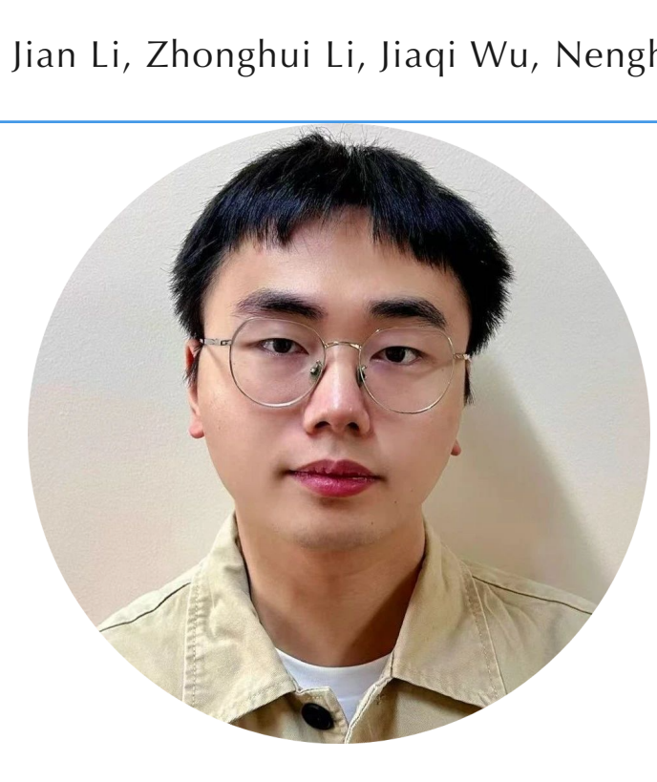
图6 不同信道长度下成码率及平均密钥复用参数变化

图6显示了测试过程中平均密钥生成率（成码率）和平均密钥重用参数随着光距离增加（对应0.2dB/km衰减）的变化。如图6所示，随着信道长度的增加，成码率呈指数下降，而平均密钥重用参数逐渐上升。与 200Mbps 的数据传输相比，500Mbps 带宽下的平均密钥重用参数更高，而1Gbps 时的平均密钥重用参数最高。这是因为，当密钥生成速率固定时，传输速率的增加也会增加密钥消耗，必须向上调整密钥重用参数，以保持密钥生成率和消耗率之间的平衡。此外，我们的协议即使在低密钥生成速率下也能保持高传输效率。

实验结果表明，IPSeQ协议安全性相比于传统IPSec协议有大幅度提升，同时对协议性能并不会产生很大影响。与此同时，IPSeQ在快速密钥更新场景下能够有效减小密钥更换开销，显著提高传输效率，并通过滑动窗口机制保持密钥同步。另外，通过采用动态调节机制，IPSeQ在密钥资源充足时能够通过减小密钥复用参数实现快速的密钥更新，在密钥稀缺的场景下也能够维持传输的稳定性。

题目：IPSeQ: A Security-Enhanced IPSec Protocol Integrated with Quantum Key Distribution

作者：Xumin Gao, Kaiping Xue, Jian Li, Zhonghui Li, Jiaqi Wu, Nenghai Yu, Qibin Sun, Jun Lu



论文第一作者高旭民是实验室2023级硕士研究生，本科毕业于中国科学技术大学，主要研究方向为量子网络。

供稿人：高旭民
编辑人：李忠辉

阅读原文