面向广域移动应用的信息论安全密钥共享

Guyue Li，*IEEE*会员，Hongyi Luo、Jiabao Yu、Aiqun Hu，*IEEE*高级会员和Jiangzhou Wang，*IEEE*会士

arXiv:2301.01453v1 [cs.IT] 4 Jan 2023

随着物联网网络中手持设备的快速增长，移动应用已遍布日常生活。随着技术的发展，与之相关的风险和威胁也随之增加，尤其是在即将到来的量子时代。然而，现有物联网网络缺乏能够满足广域移动应用机密消息传输需求的抗量子秘密密钥共享方案。为解决这一问题，本文提出一种新的方案——基于信道互易性（CR）的量子密钥分发（QKD），即 CR-QKD。该方案结合量子密钥分发和基于信道互易性的密钥生成（CRKG）等新兴技术，实现密钥共享。利用量子物理学定律和无线信道特性，即使面对计算能力无限的对手，该方案也能确保密钥的保密性。本文详细阐述了单用户场景下的基本机制，并通过重新设计多用户边缘转发策略将其扩展至多用户场景。此外，为了提高 CR-QKD 的实用性，本文还研究了一些增强策略，以安全地降低时延并提高密钥生成速率。本文在一个城域网中展示了 CR-QKD 原型，其中两个相距约十五公里的远程物联网设备实现了密钥共享。实验结果验证，CR-QKD 的密钥速率可达每秒 424 比特，重传率为 2.1%。

索引词—**密钥生成、物理层安全、量子密钥分发、广域移动应用、物联网**

一、引言

近年来，物联网（IoT）网络中的移动设备和应用程序数量不断增加，种类也日益丰富。然而，物联网的蓬勃发展导致大量私人消息通过公共信道进行交换，引起了人们的关注。不幸的是，物联网设备容易受到各种威胁和安全挑战的影响，这些问题阻碍了物联网在智能家居、无人驾驶车辆、电子健康和军事网络等敏感领域的发展 [1]。为了避免消息被第三方泄露，通信设备通常会使用共享密钥对消息进行加密。因此，实现物联网网络安全的一个关键前提是进行能够避免窃听者拦截的密钥共享 [2]。

在经典密码方案中，两个合法参与方 Alice 和 Bob 使用公钥密码系统（PKC）进行密钥分发。由于加密算法所采用的某些数学问题难以求解，第三方 Eve 在计算上极难推导出私钥或消息。然而，新兴的量子计算技术有可能使一些以往难以求解的问题变得可解 [3]。因此，随着未来几年量子计算取得重大进展，基于计算安全的密钥分发将不再安全，这就需要研究不依赖计算安全的替代方案。

在此背景下，新兴技术受到了广泛关注，例如量子密钥分发（QKD） [4] 和基于信道互易性的密钥生成（CRKG） [5], ，它们能够提供具备信息论安全性的密钥共享服务，这种安全性也称为无条件安全或物理安全。

- QKD 是一种众所周知的抗量子机制，它通过在量子信道中传输单光子，向相距遥远的各方分发密钥 [6]。利用量子物理学定律，QKD 能够在密钥生成过程中检测窃听者；在该过程中，未经授权地观测量子通信会导致错误率明显增加。这种对窃听的敏感性使 QKD 能够确保密钥的保密性，即使面对计算能力无限的对手也是如此。

- CRKG 建立在信道互易性的基础上，这意味着在时分双工（TDD）系统中，前向和反向通信链路的信道响应非常相似。此外，动态且复杂的无线通信环境会使信道响应随时间变化且难以预测。因此，合法用户可以根据无线电信道测量结果共享一对公共随机性。由于 CRKG 无需第三方协助或昂贵的基础设施，近年来已成为一种新范式，为去中心化或设备到设备传感器应用提供轻量级且信息论安全的密钥共享解决方案 [7]。

表 I 总结了这些典型的密钥分发

Guyue Li 和 Hongyi Luo 就职于中国南京 210096 东南大学网络空间科学与工程学院（电子邮箱：guyuelee@seu.edu.cn；hongyiluo@seu.edu.cn）。Jiabao Yu 就职于中国南京 210096 紫金山实验室（电子邮箱：yujiabao@pmlabs.com.cn）。Aiqun Hu 就职于中国南京 210096 东南大学国家移动通信研究实验室（电子邮箱：aqhu@seu.edu.cn）。Jiangzhou Wang 就职于英国坎特伯雷 CT2 7NT 肯特大学工程学院。电子邮箱：（电子邮箱：j.z.wang@kent.ac.uk）。Guyue Li 和 Aiqun Hu 也就职于中国南京 210096 紫金山实验室。

表 I 典型密钥分发方法的总结与比较

指标 / 方法	安全级别	移动性支持	分发距离	用户成本
PKC	计算安全	中间	**Long**	中间
QKD	**信息论安全**	Weak	**Long**	High
CRKG	**信息论安全**	**强**	短	**Low**
CR-QKD	**信息论安全**	**强**	**Long**	**Low**

方法，并从安全级别、移动性支持、分发距离和用户成本等角度分析其特征。我们发现，尽管可以在物理层分别构建量子密钥分发和 CRKG，但目前尚未针对远程移动设备的安全需求研究密钥共享方案。尽管点对点连接适合构建骨干量子核心网络以跨越长距离，但不太适合提供最后一公里服务，让众多用户接入这一量子密钥分发基础设施 [6]。同样，尽管 CRKG 领域已有大量研究，但收发器之间距离较短，遗憾的是阻碍了其广泛应用。随着手持设备迅速普及，远程环境监测和老年人监护等广域移动应用已成为物联网网络中不可或缺的一部分。我们需要开发一种新架构，将两个接入网络之间的终端用户连接到城域网，从而以更具成本效益且更灵活的方式实现无条件安全的密钥共享。

本文介绍并通过实验验证了基于简单且经济高效的电信技术的“信道互易辅助量子密钥分发（CR-QKD）”这一概念。该方案可将量子密钥分发的应用范围扩展至物联网网络，从而大幅提升其对用户的吸引力。本文的贡献主要有三方面：

- 我们提出了一种新型密钥共享架构，称为 CR-QKD。该架构利用 CRKG 技术提供最后一公里服务，从而连接骨干量子核心网络与物联网用户。CR-QKD 在信息论意义上是安全的，且物联网用户无需配备昂贵的量子基础设施即可交换密钥，因此硬件要求显著降低。

- 我们提出了一种多用户机制，通过精心设计密钥对齐方案来实现 CR-QKD 的构想。我们还分别从可行性和安全性的角度，指出 CR-QKD 混合架构所带来的挑战。为降低时延并以安全的方式提高密钥生成速率，我们研究了相应的对策。

- 我们在城域网中实现了一个CR-QKD原型系统，在该系统中，两个相距约15公里的远程物联网设备之间共享密钥。实验结果验证了CR-QKD能够以每秒424比特的密钥速率运行，重传率为2.1%。

II. CR-QKD 架构概述

本节首先介绍量子密钥分发和CRKG，然后讨论二者的组合模式，以实现在广域移动应用中的安全通信。

A. 量子密钥分发

量子密钥分发协议利用量子通信信道和经过认证的经典信道，使两个远程通信方能够以经证明的安全性交换密码密钥。自 [8],以来，量子密钥分发协议设计与分析蓬勃发展，形成了一个涵盖大量协议、安全性分析和实用实现方法的研究领域。尽管量子密钥分发研究取得了显著进展，但这些发展主要集中于保障大规模基础设施的安全，采用长距离光纤传输，以及在固定终端之间进行自由空间传输。也有一些研究利用光束转向模块，补偿发射端量子密钥分发模块的手部移动，以探索手持式自由空间量子密钥分发 [9, 10]。然而，这些方案的传输距离有限，且目前难以将量子密钥分发接收器小型化。换言之，这些方案无法实现双向传输，因此不适用于将量子密钥从核心网络分发给终端用户。本文利用量子密钥分发构建骨干量子核心网络，以实现远距离连接。

B. CRKG

CRKG 利用收发器之间的无线信道作为密钥生成的随机源；随着无线信道随时间变化，这些密钥也可以动态补充。在此类情况下，只要窃听者与合法用户相距几个波长，其所经历的物理信道就独立于合法用户的物理信道，而这在无线网络中通常成立。迄今为止，CRKG 领域在理论探索、建模、协议设计以及各种物联网平台上的原型实现等方面均取得了丰硕成果 [11]。然而，这些进展主要聚焦于短距离应用中的无线通信技术，例如 ZigBee、超宽带、蓝牙和 WiFi。当距离达到数公里时，信噪比较低，上行和下行数据包之间的时延也会增大。因此，远距离 CRKG 难以满足密钥生成对信道参数测量之间高相关性的要求 [11]。由于这些原因，CRKG 更适用于相距一公里以内的无线收发器之间的秘密密钥共享

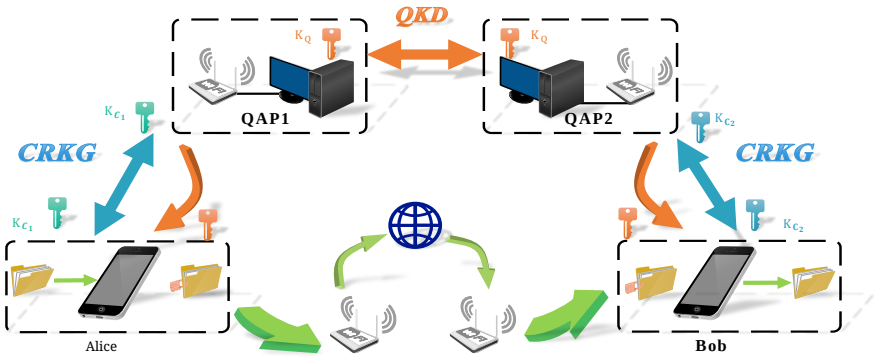

图1. 通过结合量子密钥分发与 CRKG，实现两名远距离用户之间安全通信的示意图。

因此，本文利用这一特性，完成从量子接入点（QAP）到物联网用户的最后一公里密钥分发任务。

C. 量子密钥分发与 *CRKG* 的组合模式

量子密钥分发和 PKG 均不适用于远距离物联网网络，因此，如何结合二者的优势以应用于这一新场景，是一个关键问题。图1描述了系统模型，并展示了一种可能的组合模式。Alice 和 Bob 是两名相距遥远的无线用户，彼此之间没有直接链路。QAP1 和 QAP2 是两个量子节点，它们通过长距离光纤或地面至卫星自由空间链路相连。QAP1 和 QAP2 分别通过无线链路连接 Alice 和 Bob。

为了完成 Alice 与 Bob 之间的密钥分发，首先在 Alice 与 QAP1（链路1）、QAP1 与 QAP2（链路2），以及 QAP2 与 Bob（链路3）之间分别共享三把密钥。利用 CRKG 技术，通过无线链路1和3生成信道密钥；而 QAP1 与 QAP2 之间则采用成熟的量子密钥分发技术分发量子密钥，也可以反向分发。接下来，使用信道密钥加密量子密钥，并将其安全地传送给 Alice 和 Bob。换言之，Alice 和 Bob 共享一把统一密钥，随后用于加密和解密数据传输中的消息。因此，这种模式也简称为统一密钥模式。值得注意的是，Alice 和 Bob 可以自由选择无线链路和互联网路由来传输消息。原因如下：首先，由于量子链路的速率有限，其消息传输速率相对较低。其次，由于 Alice 和 Bob 是移动设备，它们更可能采用与密钥分发过程中不同的通信路由。最后，统一密钥模式所需的消息传输时延更短，因为只需对消息进行一次加密和解密。获得统一量子密钥的核心过程称为 CR-QKD，下一节将对此进行详细阐述。

III. 协作中继量子密钥分发的概念设计

本节首先介绍 CR-QKD 的基本机制，然后研究 CR-QKD 中存在的密钥对齐、效率和安全性问题。

A. 机制描述

如图1所示，Alice 和 Bob 希望在 QAP1 和 QAP2 的帮助下共享量子密钥，同时防范窃听量子信道并监听经典信道上所有交互信息的恶意窃听者 Eve。与大多数现有的量子密钥分发和信道随机密钥生成协议类似，我们假设经典通信信道经过认证，通信各方的身份均已验证，且传输消息的完整性得到保证。

协作中继量子密钥分发协议包含三个主要阶段，即量子密钥分发[1]、CRKG 和边缘转发，下面将逐一进行阐述。

- **QKD阶段：** 首先，QAP1 通过量子信道以单光子信号的形式制备并向 QAP2 发送一组随机量子比特。这些量子比特选自一组由两个基矢构成的四种状态。对于每个来自 QAP1 的输入状态，QAP2 随机选择两个基矢之一进行测量并记录结果。量子通信结束后，QAP2 通过经典信道向 QAP1 公布检测到的比特位置及所用基矢，开始基矢协调。随后，QAP1 和 QAP2 保留基矢相同的比特，并丢弃其余比特。之后，QAP1 向 QAP2 公布其中一部分比特，用于窃听检测。如果 QAP2 检测到的结果与 QAP1 发送的比特之间的误码率较高，则判定存在窃听，这些共享比特将失效。否则，QAP1 和 QAP2 对其余未公开的比特进行信息协调和隐私放大。最后，QAP1 和 QAP2 通过密钥验证检查双方是否获得相同结果。如果是，则将这对比特保留为量子密钥 K_Q；否则，双方都将其丢弃。

- **CRKG阶段：** CRKG协议通常包含四个阶段，即信道探测、量化、信息协调和隐私放大。Alice和QAP1首先进行信道探测，即在一个信道相干时间内进行双向测量。随后，他们将模拟测量转换为数字

[1]我们的研究不局限于特定的量子密钥分发协议，因此选择 BB84协议作为代表来介绍 CR-QKD 机制。

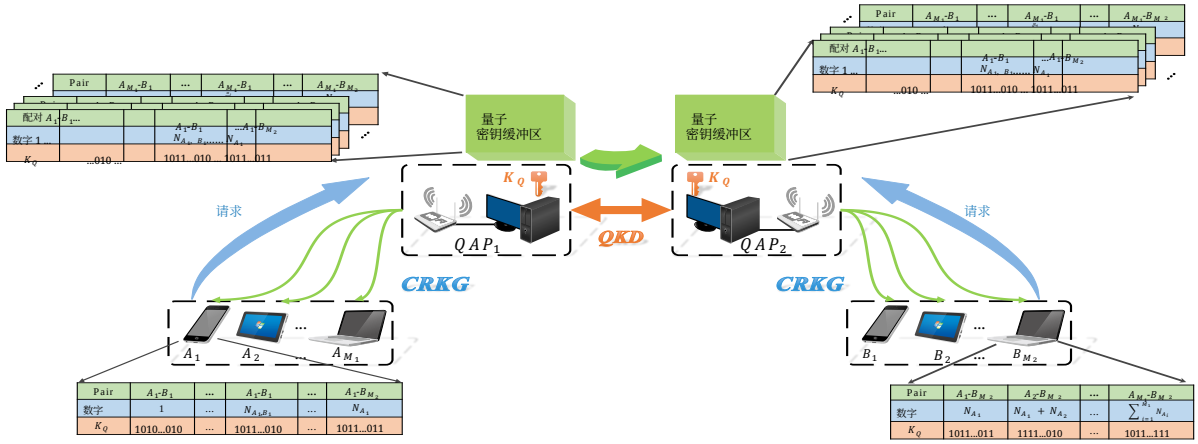

图 2. CR-QKD 的示意图，位于一个多用户场景：边缘节点根据用户的需求向其分发量子密钥，其中 N_{A_i}，B_j 表示 A_i –用户对所需的密钥组数量 B_j 用户对，N_{A_i} 表示用户 A_i所需的密钥组总数。

比特串。这些比特串可能存在不匹配，因此必须采用信息协调来纠正不匹配。为避免信息泄露，需要通过隐私放大从协调后的比特串中提取密钥。最后，经过密钥验证后，Alice和QAP1保留这一对比特作为信道密钥 K_{C1}，Bob和QAP2保留这一对比特作为信道密钥 K_{C2}。

- **边缘转发阶段：** 在最后阶段，将先前由 QAP1 和 QAP2 共享的量子密钥转发给 Alice 和 Bob，从而完成秘密密钥共享的最终任务。这里首要考虑的是安全性，因为窃听者不应通过这一转发过程获取有关量子密钥的任何信息。借助信道密钥，边缘节点可以使用一次一密（OTP）加密算法对量子密钥进行加密，然后将密文转发给用户。至此，秘密密钥共享任务完成。

尽管 CR-QKD 提供了一种潜在的解决方案，但在实际实施中仍面临一些挑战。我们将这些挑战分为三类，并在下文讨论相应的对策。

B. 密钥对齐

一次一密是一种著名的加密方案，可提供“完美保密”。然而，这里面临的一个挑战是，用于一次一密的信道密钥长度必须至少与待加密的量子密钥一样长。由于信道密钥 K_{C1} andK_{C2} 是由不同的无线信道生成的，其密钥生成速率很可能彼此不同，也可能不同于量子密钥 K_Q 的生成速率。因此，分发给 Alice 和 Bob 的量子密钥可能会出现错乱。

我们通过将量子密钥和信道密钥划分为若干组，并在边缘转发之前为各组编号，来解决密钥对齐问题。每组包含固定数量的 L_G 位。属于同一组的量子密钥位和信道密钥位通过二进制异或运算进行加密。随后，密文连同组号一起转发。Alice 和 Bob 最终获得量子密钥他们使用对应的信道密钥解密密文后，便可获得量子密钥。在选择组大小时，必须权衡通信开销与实时性。若组较小，组号所占字段长度将与密文长度相当，通信开销会显著增加。反之，若组较大，通信开销虽会降低，但需要较长时间才能积累足够的密钥用于转发。

接下来，我们将密钥对齐问题扩展到多用户场景，其中 $A = \{A_1, A_2, \cdots, A_{M_1}\}$ and $B = \{B_1, B_2, \cdots, B_{M_2}\}$ 分别是处于 QAP1 和 QAP2 服务范围内的两组物联网用户。 A 中的用户希望与 B 中的用户共享密钥。在这种情况下应用 CR-QKD 时，会出现一个新问题：如何将量子密钥从边缘分发给需求和信道条件各不相同的多个用户。本文介绍了一种多用户边缘转发策略，可根据每位用户的需求向其分发量子密钥。图 2 展示了采用该策略进行的一轮量子密钥分发过程。

首先， A 中的用户广播其密钥共享目标用户的名称以及所需密钥组的数量。收到这些请求后，QAP1 将相关信息发送给 QAP2。随后，QAP2 通过无线信道广播这些信息， B 中的相关用户将其记录在本地。接下来，QAP1 和 QAP2 通过上述 QKD 阶段共享量子密钥序列。这些量子密钥序列被划分为若干组并进行编号，每组包含 L_G位。QAP1 根据用户对的请求，为每个用户对分配量子密钥组。用户对与密钥组编号之间的映射关系会发送给 QAP2。此分配信息保存在量子密钥缓冲区中。这样一来，QAP1 和 QAP2 上的量子密钥便实现了同步。接下来，它们分别与提出需求的用户生成信道密钥。对于每位用户，CRKG 过程会重复执行多次，直到累积了足够数量的密钥组。最后，QAP1 和 QAP2 使用这些 CRKG 密钥对相应的量子密钥进行加密，并广播

密文以及用户对和组编号，发送给终端用户。每个终端用户使用自己的 CRKG 密钥解密相关密文，从而获得量子密钥。最后，这些量子密钥会分配给各用户对，用于消息加密，本轮量子密钥分发至此结束。

C. 效率提升

基本的 CR-QKD 机制耗时较长，因为在量子密钥分发和 CRKG阶段都需要大量交互才能获得相同的密钥。在多用户场景下，这一问题会更加严重。在时分多址（TDMA）系统中，每轮多用户密钥分发的时延等于生成量子密钥和信道密钥所用时间之和，再加上密钥转发所用的时间。生成量子密钥所用的时间，可用量子密钥比特数除以量子密钥生成速率计算。生成信道密钥所用的时间，等于 QAP1 和 QAP2 中耗时较长的一方。对于每个量子接入点，其时延等于它与所有用户之间生成信道密钥所用时间的总和。减少时延的一种方法是让量子密钥分发和 CRKG 过程并行进行。然而，由于转发时间为正值且存在取最大值操作，时延缩减比例不到 50%。

进一步减少时延的另一种方法是提高密钥生成速率。实际上，密钥生成率在很大程度上受信息协调造成的长时延影响。信息协调通过经典信道交换奇偶校验信息或伴随式，以检测和纠正初始密钥材料中的错误。根据使用不相同的密钥的一次一密 [12], , 我们提出一种简化的 CR-QKD 机制，在 CRKG阶段省去复杂的信息协调步骤，并使用未经协调的信道密钥转发量子密钥。面临的挑战是：当双方的未经协调的信道密钥不同时，尽管这些密钥高度相关，仍需正确解密量子密钥。我们将异或加解密模块与物理信道视为一个等效的级联信道。这样，密钥之间的微小差异就可以视为传输错误，因此可以通过具有更强纠错能力的现成信道编码予以纠正。图 3 展示了在典型 WiFi 场景中，简化的 CR-QKD 机制相较于并行 CR-QKD 机制在时延和密钥生成速率上限方面的性能提升比例。如图所示

左图显示，随着 L_G的增加，时延降低比例逐渐下降，但在 $L_G \leq 1024$时仍可实现超过 20%的降低比例。HT-Mixed 模式的降低效果比 Non-HT 模式更为显著，因为前者的时间开销大于后者。右图显示，随着量化信道测量值之间的比特不一致率增大，密钥生成速率上界的增长更加显著；而随着 L_G的增加，该上界略有下降。当 $L_G = 1024$ 和 $\epsilon_q = 0.1$时，时延降低比例和密钥速率上界增长比例分别约为 20%和 10%。这些仿真结果验证了所提出的简化的 CR-QKD 机制的有效性。

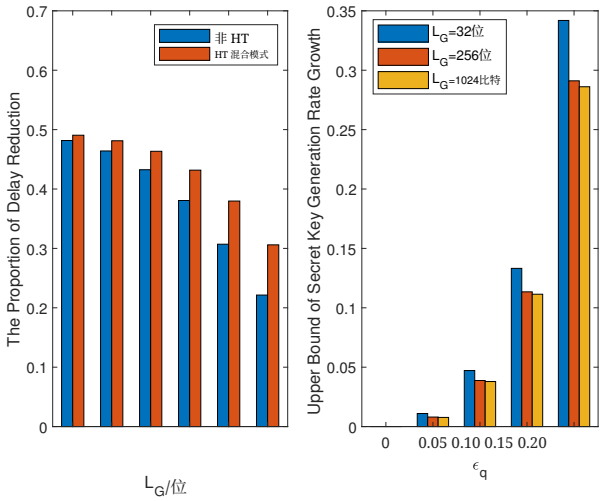

图 3. 典型 WiFi 场景下时延和密钥生成速率的性能改进：传输距离设为 150 米，带宽设为 20 MHz。WiFi 帧在 Non-HT（非高吞吐量）和 HT-Mixed 模式下的固定开销分别为 20 us 和 40 us。

D. 安全增强

CRKG 的另一项挑战在于其混合架构带来的安全风险增加，因为系统的安全性取决于其中最薄弱的一环。我们假设 QAP1 和 QAP2 的终端安全由可信计算等技术保障。与密钥相关的操作均在可信执行环境中运行，因此攻击者无法通过 QAP1 和 QAP2 上的混合接口读取量子密钥或信道密钥。由于边缘转发阶段采用 OTP 加密方案，其安全性取决于 OTP 所用的密钥。然而，现有 CRKG 方法的安全性高度依赖信道变化，因此在缓慢变化环境中容易受到攻击 [13]。当用户移动性较低时，例如在无线传感器网络中，相邻信道样本之间存在不可避免且未知的时间相关性，导致量化比特序列中有很大比例的比特片段重复。在缓慢变化环境中，可以采用若干方案来促进 CRKG 的实际应用。一种方案是引入辅助设备，例如中继器和可重构智能表面（RIS），以提高密钥生成速率和随机性 [14]。然而，该方案面临一些实际问题，例如缺乏可信中继器，以及 RIS 设备带来的额外硬件开销。另一种思路是通过置换或交织技术打乱这些比特片段。然而，如果置换信息公开，密钥的安全性可能会受到损害。 [15] 提出了一种采用信道混淆的全新物理层密钥生成方法，通过随机滤波和随机天线调度改善信道参数的动态特性；这两种技术具有相互补偿的参数，可用于隐藏混淆信息。

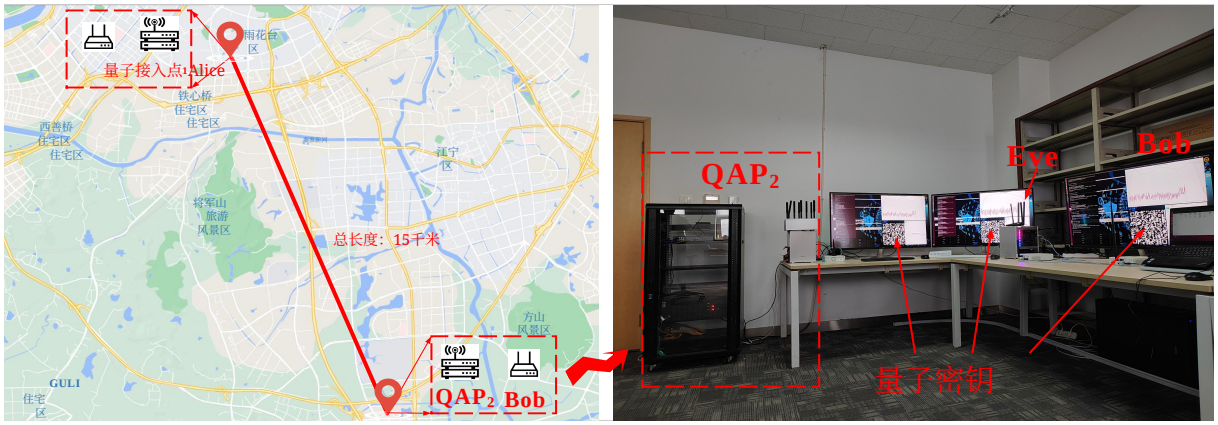

图4. 南京（中国中东部江苏省省会）城域网中CR-QKD原型平台示意图。其中一个位于雨花台区，另一个位于江宁区的中国网络谷。

IV. 案例研究：CR-QKD的实现

为实现 CR-QKD 的概念，我们在城域网中搭建了一个单用户保密传输原型系统。

A. 实验设置

如图4左图所示，QAP1和QAP2是相距十五公里的两个量子接入点。Alice和Bob分别是位于QAP1和QAP2无线服务范围内的两个远程物联网用户。为便于说明，我们不失一般性地聚焦于中国网络谷的无线接入网络，如图4右图所示。此处，QAP2由一台QKDM-POL40-S系列量子密钥分发终端（用于生成量子密钥）[2]、一台内置CBX子板的USRP N210软件无线电设备（用于提供无线连接服务）以及一台运行可信执行环境的计算机（用于生成无线信道密钥并分发量子密钥）组成。QAP2中的量子密钥分发终端和USRP N210均通过以太网电缆连接到计算机。终端用户Bob和被动窃听者Eve分别由两台USRP N210软件无线电设备实现。我们设计了一个用于信道探测的TDD帧，其中包含用于同步的正弦序列和用于信道估计的M序列。该信号工作在2.605 GHz频率和20 MHz带宽下，以避免与WiFi等普遍使用的2.4 GHz信号发生冲突。Bob收到来自AP2的信道探测信号后，会立即切换到TX模式并发送相同的信道探测信号。通过使用相同的信道探测信号进行信道估计，进一步对信道状态信息（CSI）的幅度部分进行预处理和量化，以生成无线信道密钥。

B. 性能结果

考虑到 QAP1 和 QAP2 的实验场景及结果具有可比性，我们仅以 QAP2 为例进行性能分析。

[2]量子密钥满足严格的密钥随机性要求，因为它们符合 GM/T 0005-2012 规范。

表 II 总结了在三种典型室内场景（办公室、大厅和走廊）中，从 QAP2 向 Bob 和 Eve 进行秘密密钥共享的结果。首先，在上述场景中，测得 QAP2 与 Bob 之间信道密钥的密钥生成率（KGR）分别为每秒 315.4、424.7 和 383.7 比特（bps）。这些速率足以支持传统对称加密算法（如 AES）每秒更新一次 256 位密钥，以实现安全通信。在随机性测试中，我们检查了一个长度为 340 万比特的比特序列，该序列在量化阶段输出后未经进一步处理。生成的信道密钥通过了 14 项 NIST 统计测试，表明其具有随机性。然而，尽管简化的 CR-QKD 机制带来了较高的密钥生成率和较强的随机性，但省去复杂的信息协调步骤也导致 QAP2 与 Bob 之间的密钥不一致率（KDR）相对较高，分别为 8.1%、4.7% 和 5.8%。人员数量、移动频率以及 USRP 的切换时间都会影响上行和下行信道的互易性，最终导致嘈杂的办公室、偶尔有人经过的走廊和空荡荡的大厅中出现不同的 KDR。同时，使用基于信道纠错编码的未经协调的信道密钥转发量子密钥时，若解码失败，就需要重传量子密钥。使用 Polar 码从 QAP2 向 Bob 传输时，相应的重传率（RR）分别为 11.6%、2.1% 和 6.7%，与 KDR 成正比。

为展示我们所提出方案的安全性，我们还根据密钥失效率（KDR）和破解率（CR），评估了近端窃听者 Eve 的量子密钥破解性能。在这三个场景下，QAP2 与 Eve 之间的密钥失效率均约为 50%；其中，直走廊中的视距会导致相对较低的密钥失效率，但仍高于 45%。此外，实验结果表明，Eve 在这三个场景下的破解率均为零，这意味着没有任何量子密钥被破解。

V. 结论与未来方向

将量子密钥分发集成到物联网网络中，有利于量子密钥分发的实际部署，并增强终端用户的安全性。

表 II 三种室内场景下的量子密钥无线分发性能

场景	QAP2 - Bob				QAP2 - Eve	
指标	密钥生成率/比特每秒	NIST	KDR	RR	KDR	CR
办公室	315.4	14	8.1%	11.6%	48.1%	0%
Hall	424.7	14	4.7%	2.1%	49.2%	0%
走廊	383.7	14	5.8%	6.7%	45.3%	0%

本文提出了一种面向物联网网络的CR-QKD框架。在CR-QKD中，分别采用量子密钥分发和CRKG组件，在骨干核心网络和最后一公里无线接入网络中共享秘密密钥。CR-QKD原型的演示标志着面向广域移动应用（如保密VoLTE和保密VoWiFi）的真实世界信息论安全迈出了重要一步。

以下列出未来研究中的一些开放问题。

- **设备认证**：考虑到 CR-QKD 的混合架构，它更容易受到来自用户端或量子接入点端的欺骗攻击。然而，量子密钥分发和 CRKG 都没有提供验证传输源的方法。因此，应进一步研究 CR-QKD 中的源认证，可采用非对称密码技术或新兴的物理层技术，例如射频指纹识别和物理不可克隆函数 [1]。

- **不可信量子接入点：**所提出的 CR-QKD 方案依赖于对中间量子接入点的信任。本文采用可信计算技术，确保存储在量子接入点中的信息免受外部软件攻击。当无法使用可信平台时，设计一种能够放宽这一假设的方案，也将是一个很有价值的未来研究方向。

- **性能优化**：本文提出了一种多用户边缘转发策略，按需分配量子密钥。然而，其性能指标（如时延、密钥生成速率和能效）受信道互易性较弱的用户对所限。如何通过在不同用户对之间分配功率或频谱资源来优化这些性能指标，是一个值得探讨并有待研究的课题。

- **系统集成与兼容性**：我们的原型基于USRP平台构建，与商用现货设备不同。目前尚不清楚这些性能能否在现有通信标准下实现，也不清楚CR-QKD是否会影响网络效率。还应进一步研究其系统集成与兼容性问题，包括帧格式设计、密钥管理方案，以及实际通信系统中的效率评估。

VI. 致谢

我们感谢彭林宁教授、丁延军先生、王东博士、SiyunWu先生和Xuyang Wang博士来自紫金山实验室的同事，感谢他们为实验平台提供帮助。本工作部分得到国家重点研发计划项目（批准号：2020YFE0200600和2022YFB2902202）、国家自然科学基金项目（批准号：62171121）、江苏省自然科学基金项目（批准号：BK20211160）以及江苏省网络与信息安全重点实验室项目（批准号：BM2003201）的资助。

参考文献

[1] K. Sood、S. Yu、D. D. N. Nguyen、Y. Xiang、B. Feng和X. Zhang，“关于下一代异构物联网网络与节点认证的教程”，*IEEE*物联网杂志，第4卷，第4期，第120–126页，2021年。[2] M. S. Hossain、G. Muhammad、S. M. M. Rahman、W. Abdul、A. Ale- laiwi和A. Alamri，“面向基于生物特征的物联网基础设施端到端安全”，*IEEE*无线通信，第23卷，第5期，第44–51页，2016年。[3] S. Imre，“量子通信：面向通信工程师的阐释”，*IEEE*通信杂志，第51卷，35，2013年8月，第28–69页。[4] C. Wang和A. Rahman，“量子赋能的6G无线网络：机遇与挑战”，*IEEE*无线通信，第29卷，第1期，第58–69页，2022年。[5] G. Li、C. Sun、J. Zhang、E. Jorswieck、B. Xiao和A. Hu，“5G及后续无线通信中的物理层密钥生成：挑战与机遇”，*Entropy*，第21卷，2019年。[6] B. Fr¨ohlich、J. F. Dynes、M. Lucamarini、A. W. Sharpe、Z. Yuan和A. J. Shields，“量子接入网络”，*Nature*，第501卷，第72页，2013年，第69–页。[7] U. M. Maurer，“利用共同信息通过公开讨论进行秘密密钥协商”，*IEEE*信息论汇刊，第39卷，第3期，第733–742页，1993年5月。[8] C. H. Bennett和G. Brassard，“量子密码学：公钥分发与抛币”，*IEEE*计算、系统与信号处理国际会议论文集，第175卷，第175–179页，1984年。[9] H. Chun、I. Choi、G. Faulkner、L. Clarke、B. Barber、G. George、C. Capon、A. Niskanen、J. Wabnig、D. O’Brien和D. Bitauld，“采用动态运动补偿的手持式自由空间量子密钥分发”，*Opt. Express*，第25卷，第6期，第6784–6795页，2017年3月。[10] Elmabrok、Osama、Razavi和Mohsen，“室内环境中的无线量子密钥分发”，美国光学学会*B*辑：光学物理，第35卷，第2期，第197–207页，2018年。[11] J. Zhang、G. Li、A. Marshall、A. Hu和L. Hanzo，“无线信道密钥生成历经三十年发展，为物联网安全开辟新前沿”，*IEEE Access*，第8卷，第138 406–138 446页，2020年。[12] G. Li、Z. Zhang、J. Zhang和A. Hu，“利用一次一密和密钥生成对无线通信进行实时加密”，*IEEE*物联网杂志，第8卷，第1期，第357–369页，2021年。[13] N. Aldaghri和H. Mahdavifar，“静态环境中的物理层秘密密钥生成”，*IEEE*信息取证与安全汇刊，第15卷，第2692–2705页，2020年2月。[14] G. Li、L. Hu、P. Staat、H. Elders-Boll、C. Zenger、C. Paar和A. Hu，“用于物理层密钥生成的可重构智能表面：建设性还是破坏性？”，*IEEE*无线通信，第1–12页，2022年。[15] G. Li、H. Yang、J. Zhang、H. Liu和A. Hu，“在缓慢变化环境中利用信道混淆快速、安全地生成密钥”，载于*IEEE INFOCOM*会议论文集，线上会议，2022年5月，第1–10页。