基于量子密钥的移动终端保密通信方案研究

Research on Mobile Terminal Encryption Communication Based on Quantum Key Distribution

李路曼，旷　炜，侯玉华，李兴新，彭成智（中讯邮电咨询设计院有限公司，北京 100048）
Li Luman，Kuang Wei，Hou Yuhua，Li Xingxin，Peng Chengzhi（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
随着移动互联网的高速发展，移动终端已被广泛普及，与此同时，网络信息安全面临严峻挑战。为解决移动通信信息安全问题，满足移动终端高安全保密通信需求，基于量子密钥技术，利用量子制密系统和量子密钥管理系统，将量子密钥分发到每个移动终端，通过密钥中转加密的方式实现移动终端保密通信。该方案可以为政企和个人的移动终端保密通信提供安全保障。

关键词：
移动终端；信息安全；量子密钥；量子保密通信
doi：10.12045/j.issn.1007-3043.2023.11.008
文章编号：1007-3043（2023）11-0040-04
中图分类号：TN929.5
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
With the rapid development of mobile Internet，the use of mobile terminals has been widely popularized，and the network information security is facing severe challenges. In order to solve the security of mobile communication information and meet the safe secure communication requirements of mobile terminals，it uses the secret system and quantum key management system to distribute quantum keys to each mobile terminal based on Quantum Key Distribution technology，and realizes the secure communication of mobile terminal through the key transfer encryption method. This scheme can provide security guarantee for the mobile secure communication of government，enterprise and individual.

Keywords：
Mobile terminal；Information security；Quantum key distribution；Quantum secure communication

引用格式：李路曼，旷炜，侯玉华，等. 基于量子密钥的移动终端保密通信方案研究[J]. 邮电设计技术，2023（11）：40-43.

1 概述

随着移动通信产业的迅猛发展，移动终端逐渐转变为互联网业务的关键入口[1]。然而，随之而来的非法截听、信息窃取、诱骗欺诈等移动终端信息安全问题也开始让人担忧，国际国内发生的“飞马”事件、“窃听门”事件等网信安全事件层出不穷，不仅损害个人和企业合法权益，更是威胁到国家安全和发展利益[2]。因此，如何解决移动通信信息安全问题，为用户提供移动通信安全服务，是亟待解决的问题。

目前国内移动通信系统没有对语音业务提供端到端的安全措施，信息被非法截取的现象极易发生。传统的保密通信技术是通过经典加密算法对信息进行加密，但随着计算机运算能力的快速提高，尤其是云计算、大数据、量子计算的兴起，给依赖数学复杂度来保障安全的经典网络加密方法带来了巨大挑战[3]。

基于量子密钥技术实现的量子保密通信，是以量子力学为基础，利用量子的不确定性原理、不可克隆

收稿日期：2023-09-08

原理等物理特性[4]，使通信的双方能够产生并分享一个用来加密和解密消息的随机密钥，从而实现安全通信[5]。它具有密钥分发和生成后不会被破译或计算破解、信息不会泄密的优势，可以保证绝对的安全性。本文将量子密钥技术和传统移动通信相结合，利用量子制密系统和量子密钥管理系统，将量子通信密钥和量子通话密钥分发到移动终端，通过密钥中转加密的方式实现移动终端保密通信，为政企和个人的移动通信提供安全保障。

2 量子保密通信技术

2.1 量子密码学

在密码学中，无论是非对称加密算法，还是对称加密算法，其使用的密钥都是来源于随机数。传统密码技术中使用的随机数是由确定性算法产生，具有可预测性，因此，被广泛称为伪随机数[8]，其安全性依赖于算法的复杂度，但随着计算机技术的发展，计算能力、运行速度和应用范围均呈现指数增长，使得任何加密算法都存在被破译的风险[9]。基于经典物理过程所产生的随机数来源于自然界中的模拟信号[10]，但从理论上讲，这种随机过程属于经典物理范畴，并非绝对安全，只是安全系数较高，如果获取足够多的信息，计算能力强大的窃听者也是可以破解的[8]。

进入信息化时代，对于安全性的需求越来越高，由量子力学与密码学结合形成的量子密码学应运而生[11]。量子密码学的理论基础是量子力学，使用的随机数来源于量子随机数发生器（Quantum Random Number Generator，QRNG）产生的量子信号，其安全性由量子的不确定性原理和不可克隆原理保证，具备不可预测性、不可重复性和无偏性等特征，满足真随机性的所有条件[12]，从根本上保证了随机序列的不可预测性和不可再生性[17-18]。结合一次性密码（One Time Password，OTP）技术，可以有效抵抗任意的量子计算和非量子计算破译威胁，保障信息传输的“无条件”安全[19]，从而构建保密系统。其中：

a）不确定性原理[13]。由德国物理学家海森堡于1927年提出，即对于微观粒子的某些物理量，当确定其中一个量时，就无法同时确定另一个量，例如微观世界的一个粒子永远无法同时确定粒子的位置和其动量。当有人对量子系统进行偷窥时，一定会破坏这个系统。

b）不可克隆原理[13-14]。任意一个未知的量子态进行完全相同的复制过程是不可实现的，因为复制的前提是测量，而测量一般会改变该量子的状态。任何量子密码都不可能被第三方复制而被窃取信息。

基于以上2个原理，即使量子密钥不幸被截获，也会因为测量过程中对量子状态的改变使得攻击者只能得到一些毫无意义的数据[14]。因此，相较于传统密码技术，量子密码技术拥有无条件安全性的优势，能够有效避免信息被攻击破译，保障了信息传输的绝对安全[15]。

2.2 量子保密通信

随着信息技术的飞速发展和网络通信技术的广泛应用，信息安全日益成为事关国家安全和发展利益、企业合法权益和个人隐私的重要问题，在要求信息安全传送，不被第三方窃取、修改和伪造的基础上，还要求通信过程方便快捷。目前，我国量子保密通信技术已经达到了实用化、产业化的发展水平，在国家政策的大力支持下，在金融、政务、国防军事等领域得到了广泛的应用[6]，试点部署和示范应用最多的量子保密通信方案是结合量子密钥分发和对称密码技术的加密通信，也是通信领域研讨和标准化推进的重点方向。

根据量子密钥分发和使用方式的不同，量子保密通信主要分为2种模式，一种是量子密钥在线分发，通过量子密钥分发网络生成的量子密钥直接分发到移动终端。典型的行业应用包括政企保密专线或专网、高端安全会议、数据中心之间的数据灾备及数据安全传输等。这种模式的优势在于方案成熟、改造量小等，劣势在于量子密钥分发网络覆盖有限、部署成本高、支持的业务类型少等。另一种是量子密钥在线与离线结合分发，通过安全通信技术和手段将量子密钥分发到移动终端，典型的行业应用包括量子安全移动通信、量子安全物联网、量子安全远程办公等场景。这种模式支持的业务类型多样，使用方式便捷灵活，可与现有业务系统更好地结合，成本相对较低，因此，本文基于此模式进行移动终端保密通信方案设计。

3 基于量子密钥的移动终端保密通信

3.1 量子密钥获取及分发

为保证通信的无条件安全性，本文采用QRNG作为密钥源，分别与量子制密系统和量子密钥管理系统对接，将生成的量子密钥进行加密存储。量子密钥分发涉及QRNG、量子制密系统和量子密钥管理系统以

及移动终端，分发过程如图1所示。每部移动终端在初始状态下均需初始化和离线充注N组量子通信密钥，注入的量子通信密钥由量子制密系统分发。完成量子通信密钥分发后，量子制密系统与量子密钥管理系统在线同步更新量子密钥，使量子密钥管理系统与移动终端拥有完全一致的对称密钥，且每部移动终端中存储的量子通信密钥互不相同。当移动终端中的量子通信密钥小于一定阈值或使用期限到期时，移动终端自动向量子制密系统发起新的量子通信密钥充注请求。同时，量子制密系统需与量子密钥管理系统同步更新密钥。

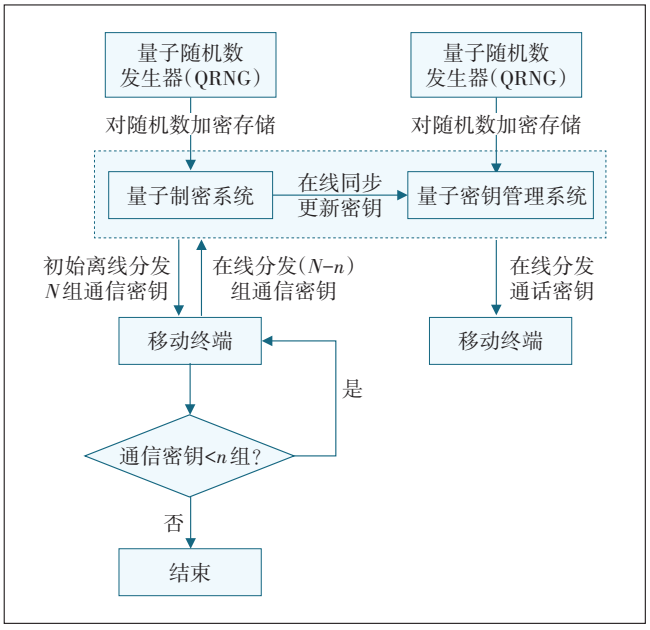

图1　量子密钥分发过程

3.2 移动终端保密通信

移动终端保密通信由移动终端和量子密钥管理系统构成，有以下3种通信机制。

方案1(见图2)：双方通信时，首先移动终端A向量子密钥管理系统发起与移动终端B之间的通信请求。然后，量子密钥管理系统随机产生一组用于此次安全通话的量子通话密钥，并分别在分配到各自的量子通信密钥组里随机选择一个量子通信密钥进行加密，分发给双方。最后，移动终端A和移动终端B分别使用各自的量子通信密钥解密得到量子通话密钥，并进行加密通话。通话结束后，立即销毁此次通话所使用的量子通信密钥和量子通话密钥，不重复使用。

方案2(见图3)：双方通信时，首先移动终端A向量子密钥管理系统发起与移动终端B之间的通信请求。然后，双方使用各自的量子通信密钥组进行密钥协商，获取量子通话密钥。最后，移动终端A和移动终端B使用量子通话密钥进行加密通话。通话结束后，立即销毁此次通话所使用的量子通信密钥和量子通话密钥，不重复使用。

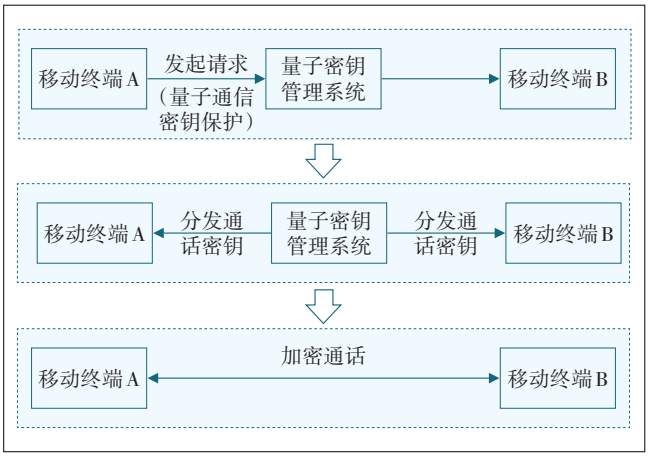

图2　保密通信机制(方案1)

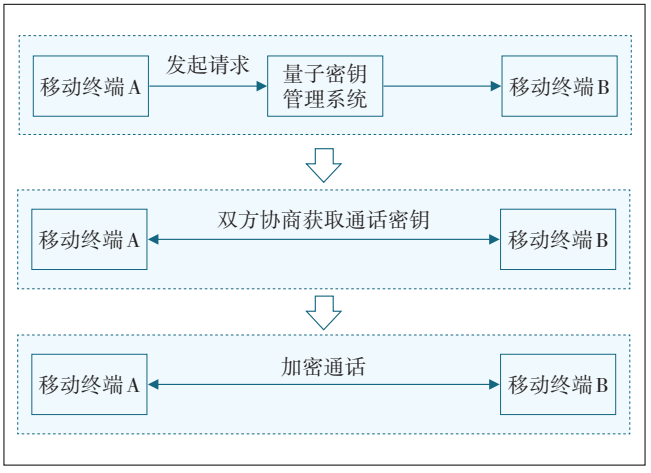

图3　保密通信机制(方案2)

方案3：假设移动终端未提前充注量子密钥，通话机制如图4所示，由移动终端与量子密钥管理系统通过传统公钥证书方式进行身份认证和密钥协商，获取通话密钥进行加密通话。通话结束后，立即销毁此次通话所使用的量子通信密钥和量子通话密钥，不重复使用。

3.3 量子密钥在线充注

当移动终端中存储的量子通信密钥小于一定阈值n或使用期限到期时，移动终端会自动向量子制密系统提交认证信息，发起新的量子通信密钥充注请求，量子制密系统对该终端提交的认证信息进行核

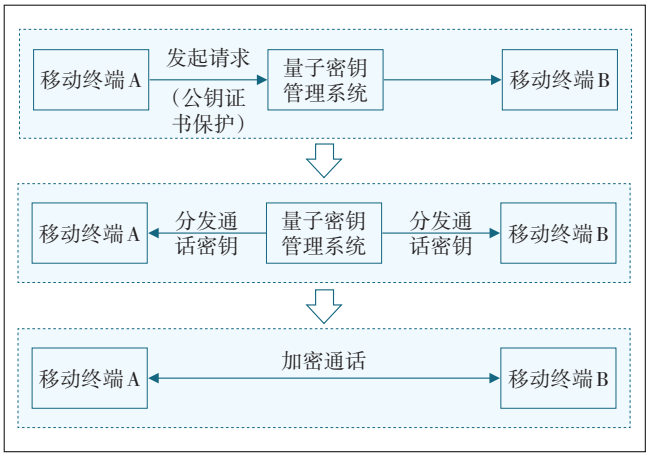

图4　保密通信机制（方案3）

验，核验成功后，向该终端在线分发（$N-n$）组新的量子通信密钥，以保证每部移动终端都能拥有源源不断的量子通信密钥以供使用，其在线分发流程如图5所示。

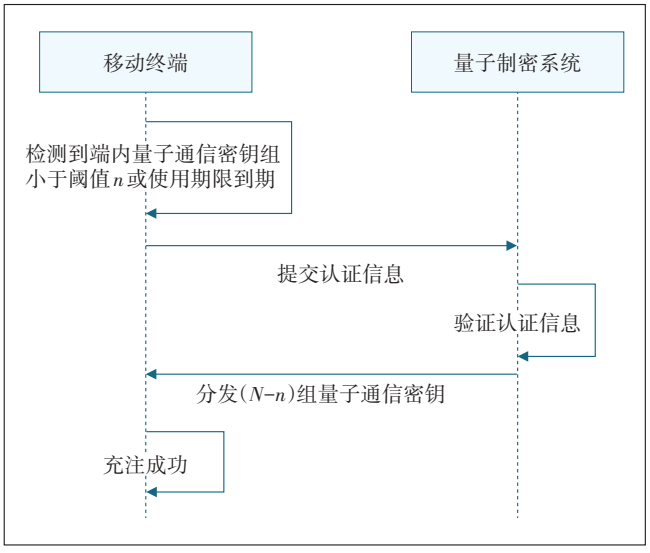

图5　量子密钥在线分发流程

4　结束语

数字经济时代，移动终端逐渐成为人们生活和工作中不可或缺的产品，其为人们带来智能化便利的同时，也导致了一系列日益凸显的移动通信信息安全问题，可靠的移动通信安全已经成为护航经济发展、保障社会安全的重要基石。因此，高安全的移动终端保密通信成为保障信息安全的核心需求。本文利用量子态的不确定性原理和不可克隆原理，将量子密钥技术、国密算法和传统移动通信相结合，开展了基于量子密钥的移动终端保密通信方案研究，为用户提供高可靠的端到端的移动通信安全保障。

参考文献：

[1] 赵晓松. 移动智能终端的安全威胁分析[J]. 济南职业学院学报，2020(3)：119-121.
[2] 李兴新，郭晓花，侯玉华，等. 新形势下移动终端安全需求和对策[J]. 邮电设计技术，2021(6)：88-92.
[3] 韩家伟. 量子密钥分发与经典加密方法融合关键技术研究[D]. 长春：吉林大学，2018.
[4] 宋安平，高新平，王静，等. 基于量子安全加密技术的5G通信创新应用[J]. 江苏通信，2022，38(4)：74-78.
[5] 赖俊森，吴冰冰，汤瑞，等. 量子通信应用现状及发展分析[J]. 电信科学，2016，32(3)：123-129.
[6] 许伟. 量子保密通信技术应用及未来发展分析[J]. 信息技术与信息化，2020(3)：92-94.
[7] 程明，张成良，唐建军. 量子保密通信应用与技术探讨[J]. 信息通信技术与政策，2022(7)：14-19.
[8] 唐光召. 量子随机数发生器的理论与实验研究[D]. 长沙：国防科学技术大学，2013.
[9] 孙刚. 关于网络安全技术中的量子密码通信分析[J]. 数字通信世界，2020(9)：97-98.
[10] 董俊，朱文，蒲秀英，等. 物理真随机数发生器的设计[J]. 电光与控制，2013，20(2)：93-96.
[11] 易运晖. 单光子量子安全通信技术研究[D]. 西安：西安电子科技大学，2013.
[12] 魏正军，廖常俊，王金东，等. 物理真随机码发生器随机性分析[J]. 光子学报，2006，35(7)：1086-1089.
[13] 谢小兵. 量子密码技术原理及应用前景初探[J]. 金融电子化，2021(7)：64-66.
[14] 陆炳旭. 量子密码技术发展概述[J]. 计算机光盘软件与应用，2014，17(24)：314-315.
[15] 杜忠岩，冷超，王题，等. 面向5G网络的量子加密在智慧城市中的应用[J]. 邮电设计技术，2022(5)：16-21.
[16] 冯凯锋. 量子密钥分发系统和量子随机数发生器[D]. 北京：中国科学院研究生院（电子学研究所），2002.
[17] 苗春华，王剑锋，魏书恒，等. 基于量子密钥的移动终端加密方案设计[J]. 网络安全技术与应用，2018(6)：38，44.
[18] 任杰，赵春旭，薛淼，等. 区块链在量子通信中的应用探讨[J]. 邮电设计技术，2022(11)：7-14.

作者简介：
李路曼，毕业于中国科学院大学，工程师，硕士，主要从事移动终端信息安全相关研究工作；旷炜，毕业于清华大学，工程师，硕士，主要从事安全平台相关研究工作；侯玉华，毕业于沈阳工业大学，高级工程师，硕士，主要研究方向为移动信息安全、终端操作系统；李兴新，高级工程师，硕士，主要从事移动终端信息安全、终端操作系统相关研究工作；彭成智，毕业于北京电子科技学院，工程师，学士，主要从事密码应用、数据安全、通信安全相关研究工作。