Computer Science and Application 计算机科学与应用, 2017, 7(1), 74-87
Published Online January 2017 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2017.71010

Hans汉斯

Technology Development Analysis of Global Quantum Private Communication

Hongxin Li[1,2], Zhan Li[1], Bao Yan[1], Yu Han[1], Wei Wang[1], Ling Shan[3]

[1]Department of Language Engineering, PLA University of Foreign Languages, Luoyang Henan
[2]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Henan
[3]College of Animal Science and Technology, Henan University of Science and Technology, Luoyang Henan
Email: lihongxin830@163.com

Received: Jan. 6th, 2017; accepted: Jan. 21st, 2017; published: Jan. 24th, 2017

Abstract

With the rapid development of Information Technology (IT), people pay more attention to the confidentiality of network communications. As a result, higher safety requirement is in urgent need for encryption systems. The birth of quantum cryptography drawing great attention at home and abroad can tackle the problem perfectly, since the ideal quantum private communication possesses theoretically unconditional security. This paper mainly introduces the latest progress on quantum cryptography experiment, quantum cryptography network and quantum cryptography product, possessing important reference value.

Keywords

Quantum Private Communication, Quantum Key Distribution, Latest Development, Applications

全球量子保密通信技术进展研究

李宏欣[1,2]，李　瞻[1]，闫　宝[1]，韩　宇[1]，王　伟[1]，山　灵[3]

[1]解放军外国语学院语言工程系，河南　洛阳
[2]数学工程与先进计算国家重点实验室，河南　郑州
[3]河南科技大学动物科技学院，河南　洛阳
Email: lihongxin830@163.com

收稿日期：2017年1月6日；录用日期：2017年1月21日；发布日期：2017年1月24日

摘　要

随着互联网信息技术日新月异的发展，人们对于通信保密性的要求越来越高，从而对于加密体制的安全

文章引用: 李宏欣, 李瞻, 闫宝, 韩宇, 王伟, 山灵. 全球量子保密通信技术进展研究[J]. 计算机科学与应用, 2017, 7(1): 74-87. http://dx.doi.org/10.12677/csa.2017.71010

性提出了更高的要求。量子密码的诞生很好的解决了这一问题，目前最理想的量子保密通信，具有理论上的无条件安全性，国内外均引起了广泛关注。本文详细介绍了当前主要量子保密通信实验、量子保密通信网络以及量子保密通信产品三方面的国际最新进展，具有重要的参考价值。

关键词

量子保密通信，量子密钥分发，最新进展，产品应用

Copyright © 2017 by authors and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

量子保密通信技术的飞速发展，突破了许多经典信息技术的物理极限，展示了量子密码在安全通信和快速计算等方面的巨大应用前景。量子密码作为前沿科技在全球范围内成为了当今科研领域研究的热点。量子密码系统利用量子力学原理实现通信双方无条件安全的传输密钥而不被未经允许的第三方窃听，可以安全用于外交、军事、金融等需要高度保密的领域，并且有望成为下一代加密系统的主流方案。

在量子保密通信技术研究方面，美国、欧盟和日本等国家和地区的多家军方机构和科研院所，均制定了相应的发展计划，并取得了一系列研究成果。我国将以量子密码为核心的量子调控技术列入了《国家中长期科学和技术发展规划纲要(2006~2020)》中重大科学研究计划，并在多所高校和科研单位成立了相关的研究机构。2016 年 8 月 16 日，我们国家发射了全球首颗量子通信卫星，标志着量子密码的实用化进展迈出了重要一步。

近年来，量子通信已逐步从理论走向实验，并向实用化发展。加拿大 Rubenok 小组从理论上解决了量子通信网络中的量子中继问题，证明了 QKD 是现实条件下保障通信保密的有效技术；T. Silva 小组在两段 8.5 公里的光纤链路上，使用弱相干态和偏振编码对 MDI-QKD 协议进行原理性验证；Nicolas Gisin 小组进行了一项关于 MDI-QKD 实验工作，其传输距离成功达到了 307 公里；潘建伟小组通过研发高效低噪声单光子探测器，详细展示了能够抵抗所有针对探测器攻击的 MDI-QKD 实验；罗开广小组则通过 MDI-QKD 实验演示了一种可以抵抗所有探测器侧信道攻击的偏振编码方案。

随着量子保密通信相关创新理论的不断涌现，量子保密通信网络方向的成果不断涌现，世界各主要国家和组织均相继建成了各自的实地量子保密通信网络。比如，美国的伯特利量子通信网络(Battelle Quantum Network)、日本东京量子通信网络(Tokyo Network)、欧洲 SECOQC 量子通信网络以及中国京沪量子通信干线工程等。

本文重点从量子保密通信实验发展动态、网络发展现状和产品研制三个方面对国际量子保密通信技术的最新进展进行详细的介绍、对比和分析，全面总结了近年来量子保密通信技术发展的趋势和特点，具有一定的参考价值。

2. 量子保密通信概述

2.1. 量子保密通信定义

量子保密通信是一种新型的通信技术，它利用量子的物理特性来保证通信的无条件安全。量子保密

通信是量子物理、数学和计算机等学科相结合的新的研究领域，涉及的研究内容包括：量子密钥分发(Quantum Key Distribution，简称 QKD)、量子秘密共享(Quantum Secret Sharing，简称 QSS)、量子隐形传态(Quantum Teleportation)和量子安全直接通信(Quantum Secure Direct Communication，简称 QSDC)等。

2.2. 量子保密通信特点

利用量子的叠加态性质、量子纠缠以及量子不可克隆原理和测不准原理等性质，使得量子保密通信具有安全性强、效率高和传输距离远等特点。因此，量子通信技术的飞速发展不仅在军事、国防等领域能够发挥巨大的作用，而且可以在很大程度上促进社会经济的发展。

2.3. 量子保密通信关键技术

量子保密通信协议大部分采用诱骗态 QKD 方案，诱骗态协议具有抗分束攻击和提高传输距离的优势。诱骗态协议设计的初衷就是为了消除光子数分离攻击给量子保密通信带来的安全威胁。

诱骗态的思想最早由韩国学者 Hwang 在 2003 年提出，随后由我国学者清华大学王向斌教授和多伦多大学的 Lo 小组分别独立系统发展。诱骗态协议的基本原理为，在 PNS 攻击中，窃听者 Eve 需要阻断单光子信号，因此对于不同平均光子数的信号脉冲，信道将表现出不同的衰减率，这与信号的自然衰减是不同的。Alice 通过随机发送平均光子数不同的信号光子(分别称为信号态和诱骗态)，然后和 Bob 一起监测信道对于信号态和诱骗态的衰减来判断是否存在窃听者。在实际应用中，Alice 可以通过信道参数来估计出窃听者所获得的信息量，由此精确计算安全密钥率。

2.4. 量子保密通信安全问题

量子密码虽然在理论上保证了通信双方可以安全的建立共享密钥，但是在实际系统中，理想条件难以实现，这使得量子通信存在各种不完美特性，从而给实际通信系统的安全性和效率造成严重影响。针对这些漏洞，现今已经提出很多量子黑客攻击方法，比如分束攻击、时移攻击、致盲攻击以及特洛伊木马攻击等的。

针对这些问题，人们提出了各种改进方案和技术，来解决量子通信存在的安全性和效率问题，使得量子保密通信技术更加实用化。

3. 量子保密通信实验

在现代通信系统中，量子通信不仅只是一个单独独立的通信系统，它也可以作为安全链路或者密钥支撑系统而应用于经典通信中。21 世纪以来，在理论方面，量子通信研究取得了显著进展，与此同时，经过大量的实验探究，各种量子通信协议的安全性与有效性也得到了验证和提高。下面，我们具体介绍一下当前具有代表性的六个重要实验。

3.1. Yuan 小组“量子接入网”

首先介绍的新技术为 Yuan 小组的“量子接入网络(Quantum Access Network，简称 QAN)”[1]。近年来，QKD 以其理论上的无条件安全性，深得密码学界关注，人们普遍认为未来保密通信方式将因此掀起一场伟大的革命。然而，如何将 QKD 的应用扩展至专用高安全性网络中至今还没有人给出可以信服的解决方法。针对这一情况，Yuan 与 Fröhlich 等人设计了“量子接入网络”，该网络基于简单而且成本较低的长距通信，采用的技术为时分复用与波分多路复用技术，能够大大增加量子通信网络中用户的数量，可以同时实现“多对一”和“一对多”的量子通信，实验环境如图 1 所示。

Yuan 小组在随后在报告中介绍了该小组的另外一项工作：10 Gb/s 密集波分复用网络下的高速 QKD

实验[2]。

QKD 技术虽然是一项革命性的量子通信技术，但是要进行大规模应用，QKD 系统的运行环境必须与现有的经典数据通信环境相兼容，而利用波分复用技术，便可实现这一点。通过波分复用技术，可以将量子数据信号与经典数据信号联结在同一根光纤上进行传输，从而实现两者硬件设施的通用，因此，针对波分复用网络条件下的 QKD 研究，愈发成为当今量子保密通信界的焦点。以现有的技术与设备，在粗波分复用技术(Coarse Wavelength Division Multiplexing，简称 CWDM)和双向 1 Gb/s 数据光纤通信环境下，可以使 QKD 系统在超过 50 公里的光纤上以每秒 500kb 的速率进行密钥分发，在这样的基础上，Yuan 小组决定在密集波分复用技术(Dense Wavelength Division Multiplexing，简称 DWDM)以及双向 10 Gb/s 数据光纤通信环境下分发密钥，以期能提高波分复用环境下 QKD 系统的工作效率。

图 2 为 QKD 与 10 Gb/s 光纤信道复用原理图，其中光纤长度可以在 25 公里至 70 公里之间变化。

3.2. Rubenok 小组实验

最近，学术界有关人士相继发现单光子探测器存在一些漏洞，随即便有不法分子利用这些漏洞对 QKD 系统进行攻击，这对 QKD 系统的安全性造成了极大威胁。针对这一情况，Rubenok 小组经过深入研究，克服了单光子探测器缺陷带来的安全威胁，证明了 QKD 是现实条件下保障通信保密的有效技术，此外，他们还通过检测实际环境下受控双光子干涉的可行性，从理论上解决了量子通信网络中量子中继问题[3]，图 3 为 Rubenok 等人搭建的实验环境。

3.3. T. Silva 小组实验

T. Silva 小组的主要工作是在两段 8.5 公里的光纤链路上，使用弱相干态和偏振编码对 MDI-QKD 协议进行原理性验证[4]，图 4 和图 5 分别为该小组的实验方案和实验环境搭建示意图。

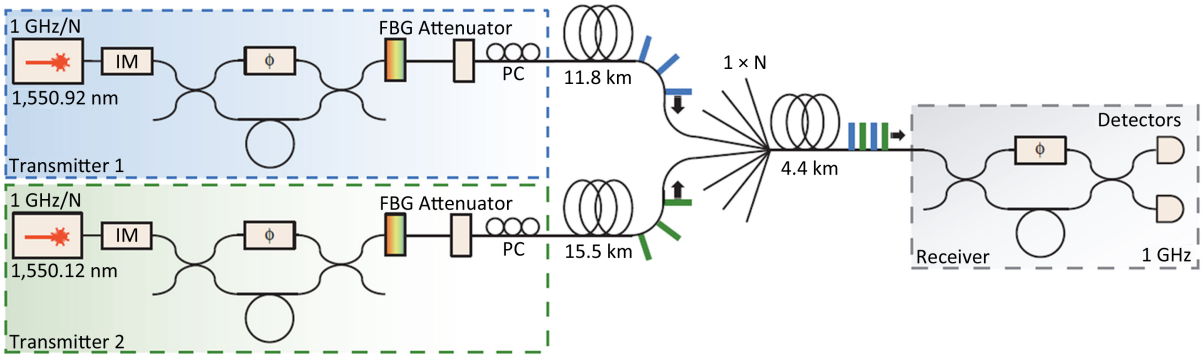


Figure 1. Setting up QAN experimental environment
图 1. QAN 实验环境搭建

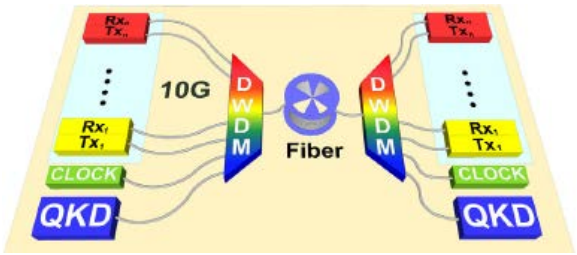


Figure 2. Combination schemes of QKD and 10 Gb/s data communication channel
图 2. QKD 和 10 Gb/s 数据信道通信组合示意图

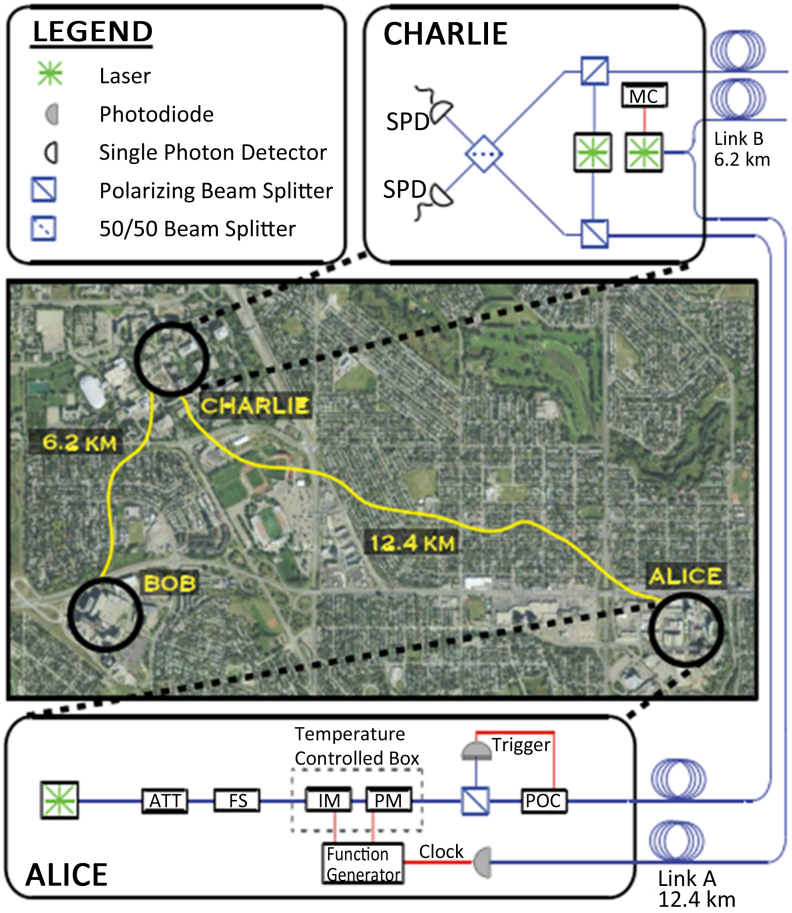


Figure 3. Experimental environment set up by Rubenok *et al*.
图 3. Rubenok 等人搭建的实验环境

T. FERREIRA DA SILVA *et al.*

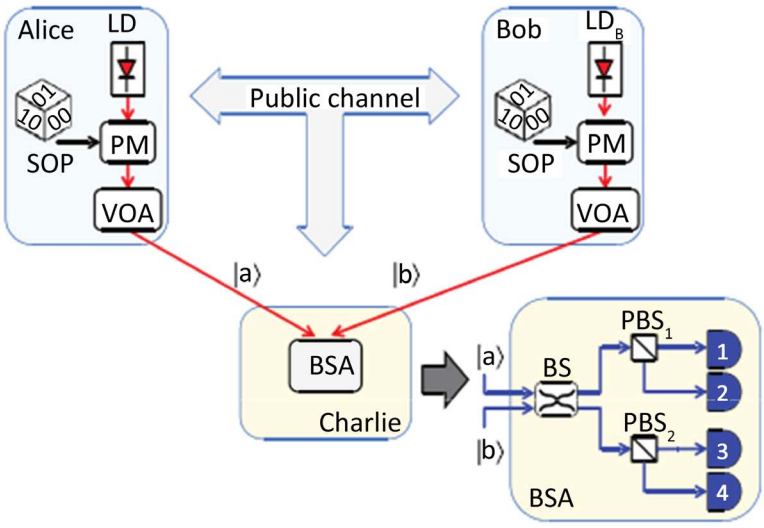


Figure 4. MDI-QKD scheme using part BSA based on linear optics
图 4. 基于线性光学使用部分 BSA (Bell-State Analyzer)的 MDI-QKD 方案

3.4. 罗开广小组实验

罗开广小组通过他们的一个 MDI-QKD 实验，演示了一种可以抵抗所有探测器侧信道攻击的偏振编码方案，即使用每个独立脉冲的主动相位随机化来保护不完美光源，防止其受到攻击。同时，他们通过优化诱饵态协议的参数，证明了使用现有的商用通信设备对 MDI-QKD 进行偏振加密的可行性，用户只需要拥有简单、价格低廉的状态制备设备便可以共享使用由不可信网络服务器所提供的复杂、昂贵的探测器[5]，图 6 和图 7 分别为实验装置和环境搭建示意图。

3.5. 潘建伟小组实验

虽然 QKD 系统已被证明具有理论上的无条件安全性，但是现实中完全理想的无条件安全设备是不会

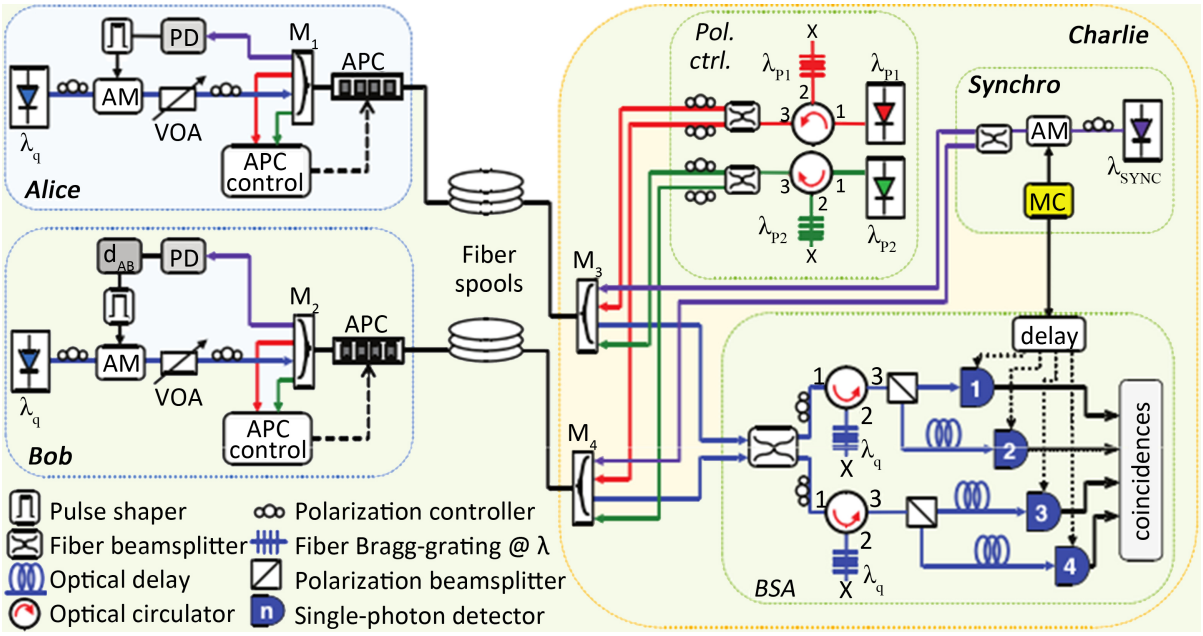


Figure 5. Setting up MDI experimental environment
图 5. MDI 实验环境搭建

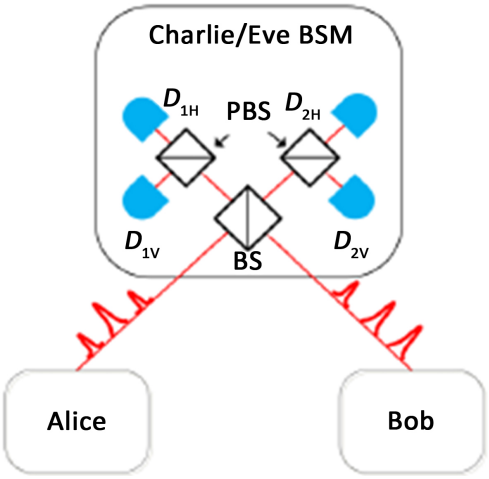


Figure 6. Typical MDI-QKD system
图 6. 典型的 MDI-QKD 装置

存在的，设备自身的各类缺陷已经逐渐成为各方攻击的首要目标。我国潘建伟院士团队的一项 MDI 实验工作振奋人心，潘建伟院士团队通过研发高效低噪声单光子探测器，忠实展示了能够抵抗所有针对探测器攻击的 MDI-QKD 实验，同时，利用诱骗态方法，该团队的实验抵抗了非完美光源攻击[6] [7]，图 8 为潘建伟院士团队 MDI-QKD 实验环境的搭建。

3.6. Gisin 小组实验

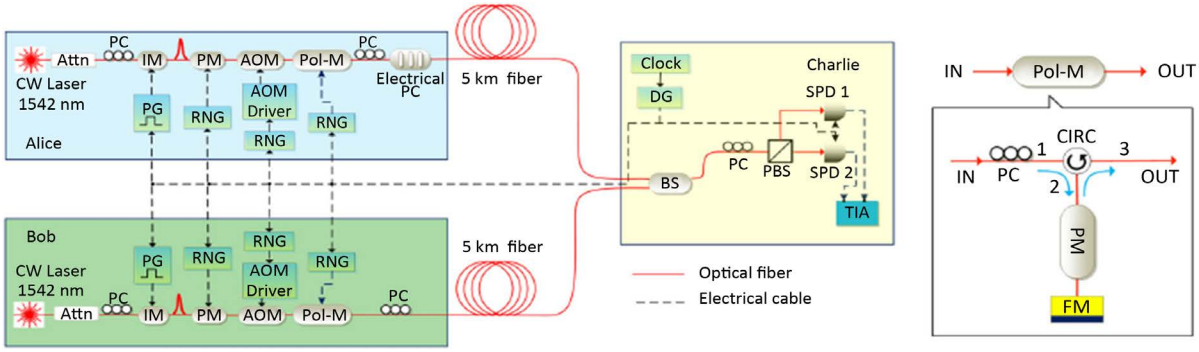
Gisin 小组关于 MDI-QKD 进行了一项实验工作，其传输距离达到 307 公里[8]，图 9 为 MDI-QKD 实验环境的搭建。

3.7. 详细试验参数比较

表 1 为各种著名 QKD 实验的具体参数数据对比。表 1 中列出了量子信道有关数据、探测器相关数据与安全性水平等数据。

4. 量子保密通信网络

理论是实践的方向，伴随着量子保密通信实验以及创新理论的不断涌现，与量子保密通信相关的产业也在飞速发展，这些产业中最具代表性的便是量子保密通信网络。量子保密通信网络方向的研究，最主要的工作为潘建伟院士小组的研究成果，包括近期所做的 MDI 相关实验和建立的三节点量子电话网与五节点全通型量子通信网络，美国的巴特尔量子网络(Battelle Quantum Network)以及日本的东京网络(Tokyo Network)。



(a) (b)

Figure 7. MDI-QKD experiment environment set up based on polarization encoding
图 7. 偏振编码 MDI-QKD 实验环境搭建

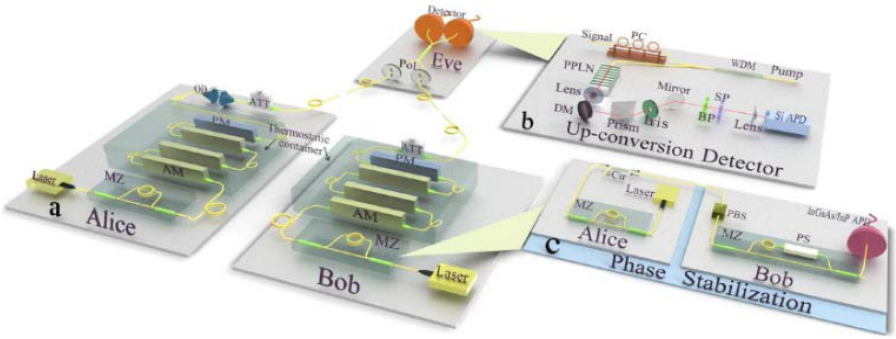


Figure 8. MDI-QKD experiment environment set up by Pan's team
图 8. 潘建伟院士团队 MDI-QKD 实验环境搭建

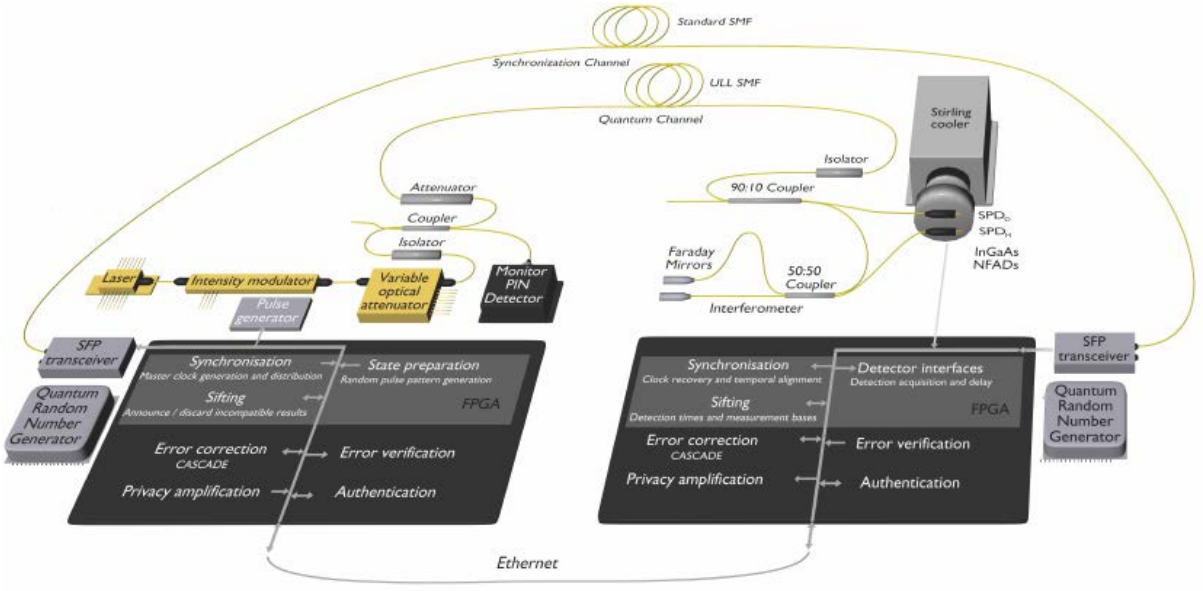


Figure 9. MDI-QKD experiment environment set up by Gisin's group
图 9. Gisin 小组 MDI-QKD 实验环境的搭建

Table 1. Comparison of all kinds of famous QKD experiment data
表 1. 各种著名 QKD 实验的数据对比

	量子信道有关数据		探测器相关数据			安全性水平			
	长度 (km)	衰减 (dB)	探测器类型	温度 (K)	所用协议	攻击方式	有限密钥大小	$\in_{qkd}$	T_{sec}
Gisin 2014	307	51.9	InGaAs	153	COW	Collective	6.6×10^5	4×10^{-9}	3.18
Wang 2012	260	52.9	SNSPD	1.7	DPS	Individual	---	---	1.85
Stucki 2009	250	42.9	SNSPD	2.5	COW	Collective	---	---	15
Takesue 2007	200	42.1	SNSPD	3	DPS	Individual	---	---	12.1
Liu 2010	200	---	SNSPD	2.4	BB84	Collective	---	---	15
Rosenberg 2009	135	27.8	SNSPD	3	BB84	Collective	---	---	0.2
Namekata 2011	160	33.6	InGaAs	193	DPS	Individual	---	---	490
Yuan 2009	100	20	InGaAs	243	BB84	Collective	---	---	1.01×10^4
Shimizu 2014	90	30	SNSPD	2.5	DPS	Individual	---	---	1100
Lucamarini 2013	80	16	InGaAs	243	BB84	Collective	$\sim 10^9$	$\sim 10^{-10}$	1.20×10^5
Walenta 2014	25	5.3	InGaAs	293	COW	Collective	10^6	4×10^{-9}	2.25×10^4

4.1. 潘建伟小组 MDI 量子网络

潘建伟院士团队基于诱骗态建立了一个“三节点量子安全通信网络系统”[9]，该系统以商业光纤网络为基础，可应用于现实环境中。在系统的三个节点中，任意两个相邻的节点均由长约 20 公里的商用光纤相连，实时进行全密钥交换与协议应用。系统所生成的量子密钥在通信中可被立即使用，实现了三节点中任意两个通信节点之间的实时语音保密通信，以及从一个节点至另外两个节点的“一次一密”实时网络对讲。

图 10 为三节点量子电话网的体系结构，两套诱骗态 QKD 系统分别安置在滨湖－中科大线路与中科大－

杏林线路上。QKD 系统已被大规模升级过一次，目的是为了能够与三节点之间具有实时音频通信功能的无缝集成设备相兼容，该实时音频通信过程经由一次一密加密方法进行加密。该系统为世界上首个三节点光量子电话网，真正实现了“电话一拨即通、语音实时加密、安全牢不可破”的量子保密电话，把我国的实用化量子通信研究推向了国际领先水平。

在成功研发三节点量子电话网之后，潘建伟院士团队又以三节点量子电话网为基础，利用自主研发的光量子程控开关，成功组建了“五节点全通型量子通信网络”[10]。五节点全通型量子通信网络包括四个全通节点以及一个中继附加节点，如图 11 所示。

与三节点量子电话网相比，五节点全通型量子通信网络是世界上首个成为现实的全通型量子通信网络，首次实现了任意两个用户之间的实时语音量子保密通信，互不影响，实用量子通信系统的有效通信距离与覆盖面积已达到城市范围。这一成果在世界同类产品中居于领先水平，标志着中国在城域量子网络技术方面已经位居世界前列。

4.2. 巴特尔量子网络

巴特尔(Battelle)量子网络由美国巴特尔公司与瑞士 ID Quantique 公司共同建设，作为美国境内的首个商用 QKD 系统，巴特尔量子网络于 2013 年 9 月开始运行。目前该公司正逐渐在俄亥俄州哥伦布市建立城市内的量子通信网络，其最终打算是建立更大的城际网络[11]。为了更好地保护巴特尔网络的所有设施，巴特尔公司计划于 2016 年实现俄亥俄州与华盛顿特区之间的量子保密通信，全程长达 650 公里。

4.3. 日本东京网络

由日本国家情报通信研究机构(NICT)主导，联合日本的多家公司与东芝欧洲研究中心、瑞士 ID Quantique 公司以及奥地利 All Vienna 研究组共同协作，集中当时欧洲和日本在量子通信技术上的最新研究技术，在东京正式建成了 4 节点城域量子通信网络“Tokyo QKD Network”。该网络最远通信距离为

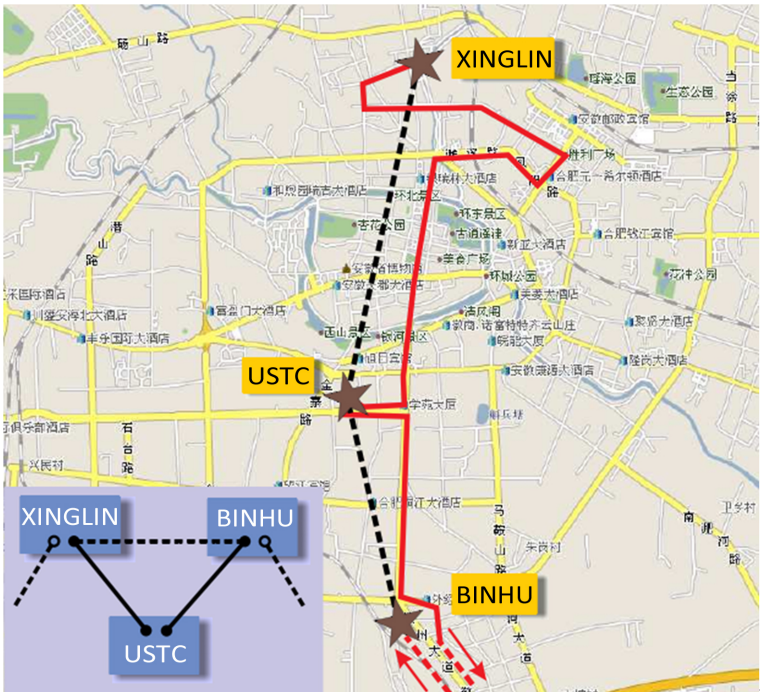


Figure 10. Three-node quantum network architecture
图 10. 三节点量子电话网的体系结构

90 公里，最快的节点间通信速率达到了每秒 304 kb，45 公里点对点通信速率可达每秒 60 kb，在全网络上可进行视频通话，如图 12 所示。

除了建立了东京网络之外，在量子保密通信技术领域，日本也提出了长期研究战略：日本邮政省将量子保密通信的相关研究确定为 21 世纪国家的战略项目，目前每年投入 2 亿美元，计划在 5 至 10 年之内建成全国性的高速量子通信网；日本国立信息通信研究院计划在 2020 年实现量子中继，到 2040 年建成极限容量、无条件安全的广域光纤与自由空间量子通信网络。

5. 量子保密通信产品

科学技术是第一生产力，随着量子保密通信理论的不断成熟，量子保密通信网络的不断应用，量子保密通信产品也如雨后春笋般涌现，为用户带来更加安全的通信体验。量子保密通信产品研究方面，最具代表性的有国内科大国盾量子技术股份有限公司的高速单光子探测器、皮秒脉冲激光器以及 QPC-E 偏

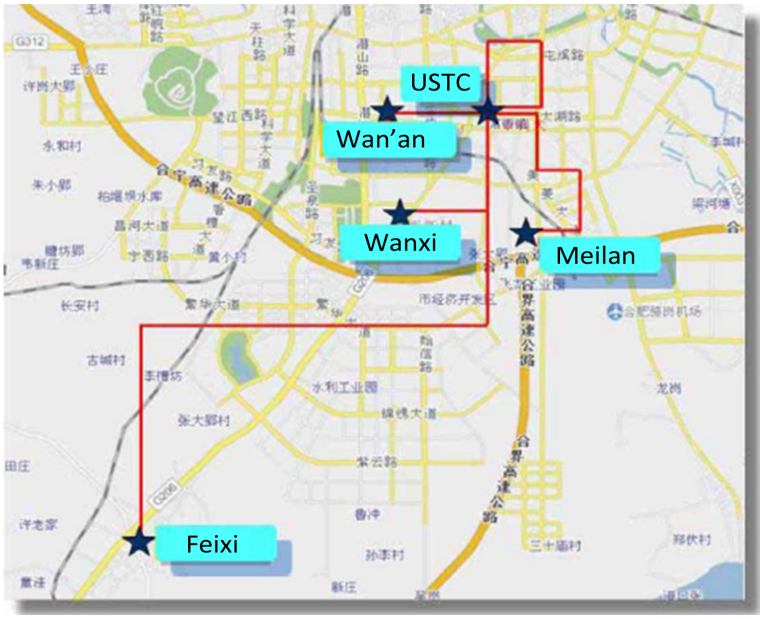


Figure 11. All-pass five-node type quantum communication network diagram
图 11. 五节点全通型量子通信网络示意图

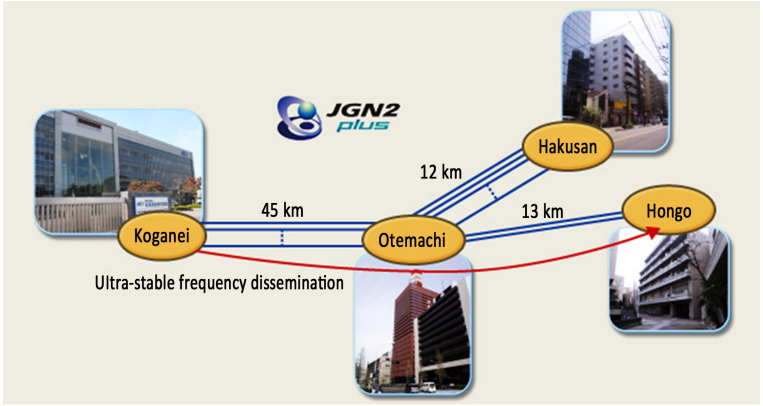


Figure 12. Future of Tokyo quantum network
图 12. 东京量子网络的未来展望

振控制器，国外俄罗斯 Scontel 公司的超导单光子探测器 SSPD 和瑞士 ID Quantique 公司的随机数发生器高速红外单光子探测器。

5.1. 国内量子通信产品

科大国盾量子技术股份有限公司(原安徽量子通信技术有限公司(源自中国科学技术大学，于 2009 年 5 月创立，是我国第一家从事量子通信产业的高新技术企业。该公司自主研发的 QCD-300 系列双通道低噪声近红外单光子探测器(图 13)、APCS-1250A 高速近红外单光子探测器(图 14)和 QCL-102 系列高速皮秒脉冲激光器(图 15)等产品。

5.2. 俄罗斯 Scontel 公司产品

国外方面，俄罗斯 Scontel 公司是世界著名的超导探测器制造商，以生产快速、高灵敏的超导探测器而闻名，其超导单光子探测器的频率覆盖范围从可见光范围至数兆赫不等。这里重点介绍该公司的代表性产品——超导单光子探测器(Superconducting Single Photon Detector，简称 SSPD)。

SSPD 基于超导单光子探测技术制成，多应用于量子相关型量子密码系统，包括实用型量子密码系统。其主要特点是使用简单，SSPD 记录的特征可在接收系统中完整实现。SSPD 具有单通道、双通道、多通

Figure 13. Dual channel low-noise near-infrared single-photon detector in QCD-300 series
图 13. QCD-300 系列双通道低噪声近红外单光子探测器

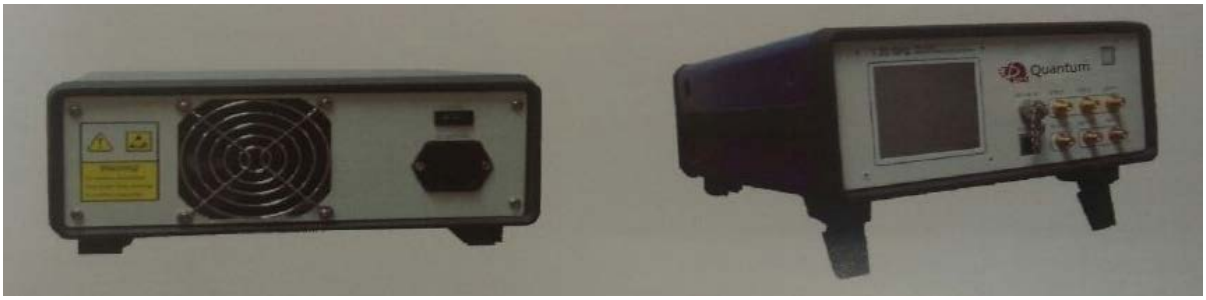


Figure 14. APCS-1250A high-speed near-infrared single-photon detector
图 14. APCS-1250A 高速近红外单光子探测器

道(最多 6 个通道)等配置可选，同时，SSPD 使用标准单模光纤，可由本地或远程控制，与 Labview 等其他软件集成方便。在运行过程中，SSPD 采用低温存储杜瓦瓶或闭环冷却系统控制操作环境温度，当采用低温液氮杜瓦瓶制冷时，工作温度为 4.2 K 或者 2 K (1、2、4 通道)，采用闭环低温制冷时，工作温度为 3 K。当 SSPD 运行时，光子吸收效应导致 SSPD 终端输出 1mV 的电压脉冲，该脉冲通过同轴电缆传递给位于控制单元内部的高频放大器，经高频放大器放大后，每一个大于 50dB 增益的通道产生大于 0.5 V 的信号，这一信号可以根据需要进一步传递到鉴别器(Discriminators)、计数器和示波器(Counter and Oscilloscope)或者其他电路。

5.3. 瑞士 ID Quantique 公司产品

瑞士 ID Quantique 公司成立于 2001 年，由四名日内瓦大学研究人员创办而成，原先为日内瓦大学的一部分，目前已成为独立公司，总部位于瑞士日内瓦。该公司的代表性产品为随机数生成器(Random Number Generation，简称 RNG) (图 16)以及 ID-210 高速红外单光子探测器(图 17)。

ID-210 是全新的高速红外单光子探测器，探测器类型为 InGaAs/InP APD，光谱范围是 900 至 1700 纳米，最大触发频率为 100 兆赫，新增自由运转模式(free-running mode)和自由门模式(free-gating mode)。该探测器主要应用于量子光学、量子密码以及光纤测量等领域。

Figure 15. High-speed picosecond pulse laser in QCL-102 series
图 15. QCL-102 系列高速皮秒脉冲激光器

Figure 16. Random number generator
图 16. 随机数发生器

Figure 17. ID-210 high-speed infrared single-photon detector
图 17. ID-210 高速红外单光子探测器

6. 总结与展望

本文详细总结了近年来国际量子保密通信技术的最新发展情况，结合国内外相关的研究小组和公司，重点从量子保密通信实验、量子保密通信网络以及量子保密通信产品研究三个方面进行了深入的分析。量子保密通信实验方面，选取了六个代表性知名实验进行了总结性介绍，分析了各个实验的特点；网络方面重点对潘建伟院士所在小组的研究成果、美国巴特尔量子网络和日本东京量子网络进行了研究；产品展示方面，主要选取了国内外三大公司的相关产品进行了介绍。

21 世纪是信息化、量子化和大数据的时代，保密通信技术将成为国际聚焦的制高点，而量子保密通信技术作为一种新兴的保密手段，必将会大有用武之地。

基金项目

国家高科技研究和发展项目(863 项目) (2011AA010803)；国家自然科学基金项目(U1204602)；数学工程与先进计算国家重点实验室开放课题项目(2013A14)。

参考文献 (References)

[1] Fröhlich, B., Yuan, Z.L., *et al*. (2013) A Quantum Access Network. *Nature*, **501**, 69-72. https://doi.org/10.1038/nature12493

[2] Yuan, Z.L., *et al*. (2014) QKD for 10Gb/s Dense Wavelength Division Multiplexing Networks. *Applied Physics Letters*, **104**, 051123. https://doi.org/10.1063/1.4864398

[3] Rubenok, A., *et al*. (2013) Real-World Two-Photon Interference and Proof-of-Principle QKD Immune to Detector Attacks. *Physical Review Letters*, **111**, 130501. https://doi.org/10.1103/PhysRevLett.111.130501

[4] Silva, T. *et al*. (2013) Proof-of-Principle Demonstration of MDI Quantum Key Distribution Using Polarization Qubits. *Physical Review A*, **88**, 052303. https://doi.org/10.1103/PhysRevA.88.052303

[5] Tang, Z., *et al*. (2014) Experimental Demonstration of Polarization Encoding MDI QKD. *Physical Review Letters*, **112**, 190503.

https://doi.org/10.1103/PhysRevLett.112.190503

[6] Liu, Y., *et al*. (2013) Experimental MDI QKD. *Physical Review Letters*, **111**, 130502. https://doi.org/10.1103/PhysRevLett.111.130502

[7] Tang, Y.L., *et al*. (2014) MDI QKD over 200 km. arXiv:1407.8012

[8] Korzh, B., *et al*. (2014) Provably Secure and Practical QKD over 307km of Optical FIBRE. arXiv:1407.7427

[9] Chen, T.Y., et al. (2009) Field Test of a Practical Secure Communication Network with Decoy-State Quantum cryptography. *Optics Express*, **17**, No. 8.

[10] Chen, T.Y., *et al*. (2010) Metropolitan All-Pass and Inter-City Quantum Communication Network. *Optics Express*, **18**, No. 26. https://doi.org/10.1364/OE.18.027217

[11] Morrow, A. *et al*. (2012) Battelle QKD Test Bed. *IEEE Conference on Technologies for Homeland Security*, 13-15 November 2012, 162-166. https://doi.org/10.1109/ths.2012.6459843

期刊投稿者将享受如下服务：

1. 投稿前咨询服务 (QQ、微信、邮箱皆可)
2. 为您匹配最合适的期刊
3. 24 小时以内解答您的所有疑问
4. 友好的在线投稿界面
5. 专业的同行评审
6. 知网检索
7. 全网络覆盖式推广您的研究

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org