JIPET

Journal of Intelligent Procedures in Electrical Technology
Vol. 15/ No. 60/ Winter 2025
P-ISSN: 2322-3871, E-ISSN: 2345-5594, http://jipet.iaun.ac.ir/

https://dorl.net/dor/20.1001.1.23223871.1403.15.60.3.8
Review Article

A Review of the Quantum Key Distribution Network in Fiber Optics

Masoumeh Shirichian[1], *Ph.D. Student*, Reza Sabbaghi-Nadooshan[1], *Associate Professor*, Mahboobeh Houshmand[2], *Assistant Professor*, Monireh Houshmand[3], *Associate Professor*

[1]Department of Electrical Engineering- Central Tehran Branch, Islamic Azad University, Tehran, Iran
[2]Department of Computer Engineering- Mashhad Branch, Islamic Azad University, Mashhad, Iran
[3]Department of Electrical Engineering- Imam Reza International University, Mashhad, Iran
m.shirichian@itrc.ac.ir, r_sabbaghi@iauctb.ac.ir, houshmand@mshdiau.ac.ir, m.hooshmand@imamreza.ac.ir

Abstract

Telecommunication networks are certainly one of the cornerstones of the modern information society and one of the main drivers of the economy and provide a basis on which many daily activities can rely. Also, new technologies such as the Internet of Things, artificial intelligence, self-driving cars, 5G, etc. will not reach their full potential unless an infrastructure communication network meets their needs. Security is critical to their infrastructure and services. On the other hand, the development of quantum computing technology in recent years and the construction of quantum computers with very high processing power and solving very complex problems faster than current computers has made cybersecurity, computer security and communication devices a vital and important issue for governments. However, with the advancement of quantum technology, these threats can be prevented by using quantum methods to distribute keys, so quantum cryptography is considered as an alternative to classical methods against quantum computers and cyberattacks. Quantum key distribution is the most popular sub-branch of quantum cryptography, and commercial examples are now available in the market. However, the implementation of quantum key distribution networks in fiber optics, which is discussed in this paper, is one of the solutions that provide unconditional security through quantum cryptography to establish secure communication. The distinguishing point of this article is to provide an overview of the latest research in the field of implementation of quantum key distribution networks in fiber optics. In addition, the quantum key distribution networks implemented in the world are reviewed and compared and the approach of different countries in this field is studied.

Keywords: integration of the quantum key distribution network with software defined network, optical nodes network, quantum cryptography, quantum key distribution network, trusted relays network

Received: 4 April 2022
Revised: 26 May 2022
Accepted: 5 August 2022

Corresponding Author: Dr. Reza Sabbaghi-Nadooshan

Citation: M. Shirichian, R. Sabbaghi-Nadooshan, M. Houshmand, M. Houshmand, "A review of the quantum key distribution network in fiber optics", Journal of Intelligent Procedures in Electrical Technology, vol. 15, no. 60, pp. 41-70, March 2025 (in Persian).

https://dorl.net/dor/20.1001.1.23223871.1403.15.60.3.8
مقاله مروری

مروری بر شبکه توزیع کلید کوانتومی در فیبرنوری

معصومه شیریچیان[۱]، دانشجوی دکتری، رضا صباغی‌ندوشن[۱]، دانشیار، محبوبه هوشمند[۲]، استادیار، منیره هوشمند[۳]، دانشیار

۱- گروه مهندسی برق- واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران
۲- گروه مهندسی کامپیوتر- واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران
۳- گروه مهندسی برق- دانشگاه بین‌المللی امام رضا (ع)، مشهد، ایران
m.shirichian@itrc.ac.ir, r_sabbaghi@iauctb.ac.ir, houshmand@mshdiau.ac.ir, m.hooshmand@imamreza.ac.ir

چکیده: شبکه‌های مخابراتی، مسلماً یکی از سنگ بناهای جامعه اطلاعاتی مدرن و یکی از محرک‌های اصلی اقتصاد هستند و زمینه‌ای را فراهم می‌کنند که بسیاری از فعالیت‌های روزمره بر آن تکیه نماید. همچنین فناوری‌های جدید مانند اینترنت اشیا، هوش مصنوعی، خودروهای خودران، 5G و ... به پتانسیل کامل خود نمی‌رسند مگر این‌که یک شبکه ارتباطی زیربنایی نیازهای آن‌ها را برآورده کند که برای زیرساخت و خدمات آن‌ها امنیت موضوعی بسیار حیاتی است. از سوی دیگر پیشرفت فناوری محاسبات کوانتومی در سال‌های اخیر و ساخت رایانه‌های کوانتومی با توان پردازش بسیار بالا و حل مسائل بسیار پیچیده با سرعتی بیشتر از رایانه‌های فعلی باعث شده که امنیت سایبری، امنیت رایانه‌ها و وسایل ارتباطی به یک مسئله حیاتی و مورد توجه دولت‌ها تبدیل گردد. با این حال با پیشرفت فناوری کوانتومی می‌توان با استفاده از روش‌های کوانتومی برای توزیع کلیدها از این تهدیدات جلوگیری نمود، لذا رمزنگاری کوانتومی به‌عنوان جایگزین روش‌های کلاسیک در مقابل رایانه‌های کوانتومی و حملات سایبری در نظر گرفته شده است. توزیع کلید کوانتومی معروف‌ترین زیرشاخه رمزنگاری کوانتومی است که امروزه نمونه‌های تجاری آن نیز در بازار موجود است. استفاده از رمزنگاری کوانتومی در زیرساخت شبکه‌های کلاسیک کنونی منجر به برقراری امنیت بی‌قید و شرط در ارتباطات بلند برد گردیده که در این مقاله به آن پرداخته شده است. نقطه تمایز این مقاله ارائه مروری بر جدیدترین تحقیقات در زمینه پیاده‌سازی شبکه‌های توزیع کلید کوانتومی در فیبرنوری است. همچنین شبکه‌های توزیع کلید کوانتومی پیاده‌سازی شده در دنیا بررسی و مقایسه گردیده و رویکرد کشورهای مختلف در این زمینه را مورد مطالعه قرار می‌دهد.

کلمات کلیدی: ادغام شبکه توزیع کلید کوانتومی با شبکه مبتنی بر نرم‌افزار، رمزنگاری کوانتومی، شبکه توزیع کلید کوانتومی، شبکه گره‌ها قابل‌اعتماد، شبکه گره‌های نوری

تاریخ ارسال مقاله: ۱۴۰۱/۱/۱۵
تاریخ بازنگری مقاله: ۱۴۰۱/۳/۵
تاریخ پذیرش مقاله: ۱۴۰۱/۵/۱۴

نام نویسنده‌ی مسئول: دکتر رضا صباغی‌ندوشن
نشانی نویسنده‌ی مسئول: تهران- دانشگاه آزاد اسلامی واحد تهران مرکزی- دانشکده فنی مهندسی- گروه مهندسی برق

۱- مقدمه

فناوری‌های کوانتومی مانند مترولوژی[۱]/سنسورهای کوانتومی[۲]، شبیه‌سازی کوانتومی، محاسبات کوانتومی و ارتباطات و رمزنگاری کوانتومی[۳] بر مبنای قوانین و اصول بنیادین مکانیک کوانتومی همچون برهم‌نهی[۴]، درهم‌تنیدگی[۵]، اندازه‌گیری کوانتومی، کپی ممنوع و اصل عدم قطعیت هستند [۱]. با توجه به این‌که محاسبات کوانتومی توسط پردازنده‌ها یا رایانه‌های کوانتومی صورت می‌پذیرد و رایانه‌های کوانتومی به دلیل سرعت پردازش بالا، قادر خواهند بود مسائل دشوار ریاضی که در ارتباطات کلاسیک از آن استفاده شده است را در زمان بسیار کوتاهی حل و اکثر الگوریتم‌های رمزنگاری کلید عمومی را رمزگشایی نمایند، لذا تهدیدی جدی برای امنیت ارتباطات کلاسیک خواهند بود. ازاین‌رو می‌توان از برنامه‌های کاربردی مکانیک کوانتومی برای جلوگیری از این تهدیدات استفاده نمود. رمزنگاری کوانتومی این امکان را می‌دهد الگوریتم‌هایی طراحی گردد که از یک‌سو، بر محدودیت‌های فیزیک کلاسیک [۲] غلبه کنند و از سوی دیگر، در برابر حملات رایانه‌های کوانتومی آسیب‌پذیر نباشند [۳]. با این حال راه‌حل‌های مختلفی برای امن کردن ارتباطات ارائه شده که می‌توان به امنیت پساکوانتومی و ارتباطات کوانتومی برای حفظ امنیت ارتباطات در برابر رایانه‌های کوانتومی اشاره کرد. با توجه به این‌که افت و نویز از چالش‌های ارتباطات بلند برد است برای حل این مشکل در شبکه‌های کلاسیک از تکرارکننده‌های کلاسیک استفاده می‌شود. تکرارکننده‌های کلاسیکی پس از دریافت سیگنال ضعیف و نویزی با تقویت و تصحیح خطا، یک سیگنال قوی و تمیز را بازتولید می‌نمایند و به این طریق بر چالش افت و نویز کانال غلبه می‌کنند. حال آن‌که قوانین مکانیک کوانتومی مانند اصل کپی ممنوع مانع از اجرای مستقیم چنین اعمالی در شبکه‌های کوانتومی می‌شوند [۵،۴]، لذا برای حل این چالش تاکنون راه‌کارهای مختلفی ارائه شده که براساس پیشرفت فناوری می‌توان آن‌ها را در کوتاه‌مدت، میان‌مدت و بلندمدت پیاده‌سازی کرد. راه‌کار کوتاه‌مدت شبکه توزیع کلید کوانتومی[۶] نام دارد که این نوع شبکه‌ها دارای ادوات کلاسیکی و کوانتومی است به‌طوری که کاربران، سرویس رمزنگاری کوانتومی را بر بستر شبکه‌های مخابراتی کنونی دریافت می‌نمایند. راه‌کار میان‌مدت استفاده از شبکه‌های کوانتومی نسبتاً قابل اعتماد است که منظور از آن استفاده از فناوری‌های فضایی برای ایجاد ارتباطات ماهواره‌ای است. از آنجا که رمزنگاری کوانتومی در فضای آزاد انتقال فوتون‌ها را در مسافت طولانی ممکن می‌سازد، پتانسیل ایجاد یک شبکه ارتباطات کوانتومی جهانی وجود دارد. راه‌کار بلندمدت شبکه‌های کوانتومی غیرقابل اعتماد است. این نوع شبکه‌ها امکان تبادل اطلاعات کوانتومی بین رایانه‌های کوانتومی را فراهم می‌کنند. ارتباطات بلندبرد در این نوع شبکه توسط تکرارکننده‌های کوانتومی برقرار می‌شود که اساس کار آن‌ها درهم‌تنیدگی است. به همین دلیل در متون علمی از این شبکه‌ها تحت عنوان شبکه تکرارکننده‌های کوانتومی یا شبکه‌های مبتنی بر درهم‌تنیدگی یا اینترنت کوانتومی نیز یاد می‌شود [۵].

در این مقاله قصد داریم نحوه پیاده‌سازی شبکه‌های توزیع کلید کوانتومی در فیبرنوری را شرح داده و انواع شبکه‌های توزیع کلید کوانتومی که بر روی فیبرنوری طراحی و پیاده‌سازی شده‌اند و در کشورهای مختلف توسط نهادهای دولتی و خصوصی مورد استفاده قرار گرفته‌اند را معرفی نمائیم. از این‌رو در قسمت ۲ مقدماتی مربوط به انواع رمزنگاری کوانتومی و نحوه ایجاد پیام‌های رمزنگاری شده با استفاده از کلیدهای کوانتومی بیان گردیده است. در قسمت ۳ نحوه عملکرد شبکه‌های توزیع کلید کوانتومی در فیبرنوری توضیح داده شده است. انواع شبکه‌های توزیع کلید کوانتومی که تاکنون در دنیا طراحی و پیاده‌سازی شده‌اند، در قسمت ۴ و فرصت‌ها و چالش‌های این نوع شبکه‌ها در قسمت ۵ مورد بررسی قرار گرفته است. در انتها رویکرد کشورهای مختلف در زمینه ارتباطات کوانتومی در قسمت ۶ جمع‌بندی گردیده است.

۲- مقدمات

۲-۱- رمزنگاری کوانتومی

هدف از رمزنگاری کوانتومی ایجاد پروتکل‌هایی است که با وجود استراق سمع‌کننده بر روی کانال ارتباطی ناامن، داده‌ها به‌صورت امن مخابره گردند. در عملیاتی‌کردن هر نوع پروتکل ارتباطات کوانتومی وجود نویز گریزناپذیر است از این‌رو لحاظ کردن آن در طراحی انواع پروتکل‌های ارتباطات کوانتومی ضروری است. بر همین اساس، بسته به منشأ نویز، دو نوع سناریوی توزیع کلید کوانتومی قابل تعریف است. در سناریوی موسوم به پروتکل‌های وابسته به دستگاه[۷] توزیع کلید کوانتومی، نویزی که

دستگاه‌های آلیس[۸] (فرستنده) و باب[۹] (گیرنده) را تحت تأثیر قرار می‌دهد، یک نویز مطمئن به حساب می‌آید، به این معنی که این نویز ناشی از حمله‌ی استراق سمع‌کننده نیست، بلکه ناشی از محیط واقعی آزمایشگاه‌های آلیس و باب است. این نویز می‌تواند نویز مرحله‌ی آماده‌سازی حالت‌ها در آزمایشگاه آلیس، نویز برآمده از نقص مدولاتورها، نویز گرمایی محیط و نویز برآمده از نقص آشکارسازها باشد که برای اولین بار در سال ۱۹۸۴ توسط چارلز بنت[۱۰] و جیل براسارد[۱۱] مطرح شد [۶]. بعد از سال ۱۹۸۴ تلاش برای پیاده‌سازی پروتکل‌های توزیع کلید کوانتومی دیگری که در مقابل حملات مقاوم باشند صورت پذیرفت که از جمله آن‌ها می‌توان روش حالت طعمه[۱۲] را نام برد که در این روش پالس‌های همدوس ضعیف با استفاده از لیزرهای تضعیف شده تولید می‌گردند [۵]. فهرستی از آزمایش‌های پروتکل توزیع کلید کوانتومی حالت طعمه در جدول (۱) آمده است که اغلب آن‌ها با هدف بهبود نرخ تولید کلید کوانتومی در فاصله دور مطرح شده‌اند. همچنین در سال ۲۰۲۲ در مرجع [۷] ثابت گردید که حداکثر فاصله پروتکل‌های توزیع کلید کوانتومی وابسته به دستگاه چهار حالته و شش حالته را می‌توان به ترتیب از ۱۴۲ کیلومتر به ۱۸۰ کیلومتر و از ۱۴۶ کیلومتر به ۱۸۷ کیلومتر افزایش داد. با وجود این‌که امنیت یک پروتکل‌های وابسته به دستگاه توزیع کلید کوانتومی می‌تواند به‌طور دقیق اثبات شود، اما پیاده‌سازی آن در دنیای واقعی اغلب با نقص‌های تجربی ناشی از حملات مختلف به چشمه یا آشکارساز همراه است که برای فائق آمدن بر این مشکلات سناریوی دیگری که به پروتکل‌های مستقل از دستگاه اندازه‌گیری[۱۳] موسوم است، به توزیع امن کلید کوانتومی در شرایطی که همه منابع نویز به استراق سمع‌کننده نسبت داده می‌شوند، پرداخته می‌شود.

Table (1): List of decoy-state QKD protocol experiments and their performance

جدول (۱): فهرستی از آزمایش‌های پروتکل توزیع کلید کوانتومی حالت طعمه و عملکرد آن‌ها

مرجع	کدگذاری	کانال	حداکثر فاصله	نرخ کلید (بیت بر ثانیه)	سال
[۸]	فاز	فیبر	۶۰ کیلومتر	۴۴۲/۵	۲۰۰۶
[۹]	پلاریزاسیون	فیبر	۱۰۲ کیلومتر	۸/۱	۲۰۰۷
[۱۰]	فاز	فیبر	۱۰۷ کیلومتر	۱۴/۵	۲۰۰۷
[۱۱]	پلاریزاسیون	فضای آزاد	۱۴۴ کیلومتر	۱۲/۸	۲۰۰۷
[۱۲]	فاز	فیبر	۲۵/۳ کیلومتر	۵/۵ K	۲۰۰۷
[۱۳]	فاز	فیبر	۱۲۳ /۶ کیلومتر	۱	۲۰۰۷
[۱۴]	فاز	فیبر	۲۵ کیلومتر	۰/۹	۲۰۰۸
[۱۵]	فاز	فیبر	۱۰۰/۸ کیلومتر	۱۰/۱K	۲۰۰۸
[۱۶]	فاز	فیبر	۳۳ کیلومتر	۳/۱K	۲۰۰۹
[۱۷]	فاز	فیبر	۱۳۵ کیلومتر	۰/۲	۲۰۰۹
[۱۸]	فاز	فیبر	۱۰۰ کیلومتر	۱۰/۱K	۲۰۰۹
[۱۹]	فاز	فیبر	۲۰ کیلومتر	۱/۵K	۲۰۱۰
[۲۰]	پلاریزاسیون	فیبر	۲۰۰ کیلومتر	۱۵	۲۰۱۰
[۲۱]	پلاریزاسیون	فیبر	۱۳۰ کیلومتر	۰/۲K	۲۰۱۰
[۲۲]	فاز	فیبر	۴۵ کیلومتر	۳۰۴ K	۲۰۱۱
[۲۳]	پلاریزاسیون	فضای آزاد	۹۶ کیلومتر	۴۸	۲۰۱۳
[۲۴]	فاز	فیبر	۱۹/۹ کیلومتر	۴۳/۱K	۲۰۱۳
[۲۵]	فاز	فیبر	۸۰ کیلومتر	۱۲۰	۲۰۱۳
[۲۶]	فاز	فیبر	۲۴۰ کیلومتر	۸/۴	۲۰۱۷
[۲۷]	پلاریزاسیون	فضای آزاد	۱۲۰۰ کیلومتر	۱/۱K	۲۰۱۷
[۲۸]	فاز	فیبر	۲ دسیبل	۱۳/۷M	۲۰۱۸
[۲۹]	زمان	فیبر	۴۲۱ کیلومتر	۶/۵	۲۰۱۸
[۳۰]	فاز	فیبر	۵۰ کیلومتر	۶۰K	۲۰۲۰
[۳۱]	پلاریزاسیون	فضای آزاد، آب‌وهوا	۳۰ متر	۲۲۰/۵	۲۰۲۱

سناریوی مستقل از دستگاه اندازه‌گیری، از پروتکل توزیع کلید کوانتومی مبتنی بر درهم تنیدگی [۳۲] الهام گرفته شده است. به این‌صورت که آلیس و باب پالس‌های همدوس ضعیف[۱۴] تصادفی را در چهار حالت قطبش آماده می‌کنند و آن‌ها را به گره میانی غیرقابل اعتماد (چارلی) که دستگاه اندازه‌گیری در آن قرار دارد می‌فرستند. در گره میانی با اندازه‌گیری حالت بل بر روی حالت قطبش چهار حالت بل ایجاد می‌شود. در این زمان چارلی با استفاده از فیبرنوری (کانال عمومی کلاسیک) نتیجه اندازه‌گیری خود را برای آلیس و باب ارسال می‌کند. سپس آلیس و باب پایه‌هایی را که با نتایج مطابقت دارند را نگه داشته و بقیه را دور می‌اندازند. سرانجام از پایه‌های باقی‌مانده برای تولید کلید خام استفاده می‌کنند که پس از تصحیح خطا و تقویت حریم خصوصی یک کلید امن تولید می‌شود [۳۳]. جدول (۲) خلاصه آزمایش‌های پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری پس از اختراع آن را نشان می‌دهد. در سال ۲۰۲۲ در مرجع [۷] اثبات گردید که حداکثر فاصله انتقال پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری چهار حالته و شش حالته می‌تواند به ترتیب از ۱۹۵ کیلومتر به ۲۷۳ کیلومتر و از ۲۰۰ کیلومتر به ۲۸۲ کیلومتر افزایش یابد. در سال ۲۰۱۸ در مرجع [۳۴] یک پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری به نام توزیع کلید کوانتومی میدان دوقلو[۱۵] معرفی گردید که بر اساس آن پالس‌های نوری ضعیف توسط دو منبع نوری تولید می‌شوند که فازهای آن تصادفی بوده و سپس این فازها با بیت‌ها و پایه‌های امن کدگذاری فاز می‌شوند که در جدول (۳) خلاصه آزمایش‌های اخیر این پروتکل نشان داده شده است. آزمایش‌ها نشان می‌دهد پروتکل و فناوری‌های استفاده شده در توزیع کلید کوانتومی میدان دوقلو نرخ کلید امن بالایی را در یک فاصله توزیع طولانی ایجاد می‌نماید بنابراین عملاً برای پیاده‌سازی میدانی درون‌شهری مفید است [۳۵].

۲-۲- پد یکبار مصرف[۱۶]

کلیدهای امن کوانتومی ایجاد شده توسط پروتکل‌های رمزنگاری مذکور برای ارسال اطلاعات به‌صورت امن به‌کار می‌رود. به‌منظور انتقال پیام به‌صورت رمز، فرستنده بیت‌های پیام خود را یکی‌یکی با بیت‌های کلید امن مشترک یای انحصاری[۱۷] می‌کند به‌طوری‌که هر بیت کلید امن تنها برای یک بیت پیام به‌کار رود سپس نتایج از طریق یک کانال عمومی به گیرنده ارسال می‌گردد. گیرنده، پیام رمز شده دریافتی را با کلید امن مشترک یای انحصاری می‌نماید؛ به این ترتیب بیت‌های کلید حذف شده و پیام اصلی توسط گیرنده دریافت می‌شود که این روش به روش پد یکبار مصرف معروف است [۵۴]. امنیت بی‌قید و شرط در این تکنیک مستلزم آن است که طول کلید کوانتومی با طول پیام مخابره شونده یکی باشد اما در اغلب کاربردها به چنین امنیت مطلقی نیاز نیست لذا می‌توان کلیدهایی با طول کمتر نسبت به پیام را با الگوریتم‌هایی از جمله استاندارد رمزنگاری پیشرفته[۱۸] و الگوریتم استاندارد رمزنگاری داده[۱۹] ترکیب کرد.

۳- عملکرد شبکه توزیع کلید کوانتومی در فیبرنوری

در حال حاضر تجاری‌ترین بخش ارتباطات کوانتومی شبکه توزیع کلید کوانتومی است که با تجهیز نمودن زیرساخت‌های شبکه کلاسیک به ادوات کوانتومی مانند چشمه‌های نور کوانتومی، آشکارسازهای کوانتومی و مولد اعداد تصادفی کوانتومی به سه روش شبکه توزیع کلید کوانتومی گره‌ها (رله‌های) قابل اعتماد و غیرقابل اعتماد[۲۰]، شبکه گره‌های نوری[۲۱] و ادغام شبکه توزیع کلید کوانتومی با سایر شبکه‌های مخابراتی گسترش یافته است.

۳-۱- شبکه توزیع کلید کوانتومی گره‌ها (رله‌های) قابل اعتماد و غیرقابل اعتماد

برای پیاده‌سازی شبکه توزیع کلید کوانتومی میان دو گره فرستنده و گیرنده از دو لینک متمایز ازجمله اینترنت برای ترافیک پیام و فیبرنوری برای توزیع کلید کوانتومی استفاده می‌کنند. در شبکه توزیع کلید کوانتومی نقطه به نقطه که در شکل (۱) نشان داده شده است از یک سیستم کنترل فرایند نوری[۲۲] جهت مدیریت دستگاه‌های نوری و الکترونیکی که شامل مجموعه منبع لیزر[۲۳] در فرستنده و مجموعه آشکارسازها در گیرنده استفاده می‌شود.

Table (2): List of MDI-QKD protocol experiments and their performance [33]

جدول (۲): فهرستی از آزمایش‌های پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری و عملکرد آن‌ها [۳۳]

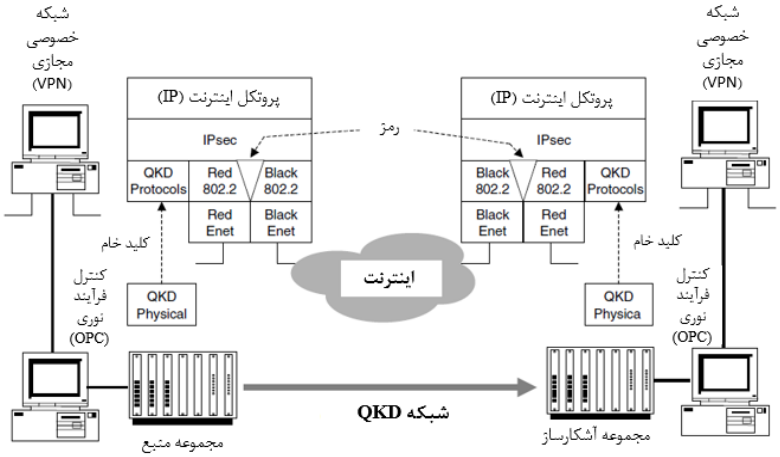
مرجع	کدگذاری	فاصله یا تلفات	نرخ کلید (بیت بر ثانیه)	سال
[۳۶]	پنجره زمانی	۸۱/۶ کیلومتر	۰/۲۴	۲۰۱۳
[۳۷]	پنجره زمانی	۵۰ کیلومتر	۰/۱۲	۲۰۱۳
[۳۸]	پلاریزاسیون	۱۷ کیلومتر	۱/۰۴	۲۰۱۳
[۳۹]	پلاریزاسیون	۱۰ کیلومتر	$۴/۷ \times ۱۰^{-۳}$	۲۰۱۴
[۴۰]	پنجره زمانی	۲۰۰ کیلومتر	۰/۰۲	۲۰۱۴
[۴۱]	پنجره زمانی	۲۰ کیلومتر	۸/۳	۲۰۱۵
[۴۲]	پنجره زمانی	۶۰ کیلومتر	۵×۱۰^{-۲}	۲۰۱۵
[۴۳]	فاز	۴ دسیبل	۰/۱	۲۰۱۵
[۴۴]	پنجره زمانی	۵۵ کیلومتر	۱۶/۵	۲۰۱۶
[۴۵]	پنجره زمانی	۴۰۴ کیلومتر	$۳/۲ \times ۱۰^{-۴}$	۲۰۱۶
[۴۶]	پلاریزاسیون	۴۰ کیلومتر	۱۰	۲۰۱۶
[۴۷]	پلاریزاسیون	۱۰۲ کیلومتر	۴/۶ K	۲۰۱۶
[۴۸]	پنجره زمانی	۱۴ دسیبل	۰/۸۵	۲۰۱۷
[۴۹]	پنجره زمانی	۲۰ کیلومتر	$۶/۳ \times ۱۰^{-۳}$	۲۰۱۷
[۵۰]	پنجره زمانی	۸۰ کیلومتر	۱۰۰	۲۰۱۷
[۵۱]	پنجره زمانی	۱۶۰ کیلومتر	۲/۶	۲۰۱۸
[۵۲]	پنجره زمانی	۱۰۰ کیلومتر	۱۴/۵	۲۰۱۹
[۵۳]	پلاریزاسیون	۲۰/۴ دسیبل	۶/۲ K	۲۰۱۹

Table (3): List of Twin field QKD protocol experiments and their performance [33]

جدول (۳): فهرستی از آزمایش‌های پروتکل توزیع کلید کوانتومی دوقلو و عملکرد آن‌ها [۳۳]

مرجع	فاصله یا تلفات	نرخ کلید (بیت بر ثانیه)	سال
[۵۵]	۹۰/۸ دسیبل	۰/۰۴۵	۲۰۱۹
[۵۶]	۳۰۰ کیلومتر	$۲/۰۱ \times ۱۰^{۳}$	۲۰۱۹
[۵۷]	۳۰۰ کیلومتر	۳۹/۲	۲۰۱۹
[۵۸]	۵۵/۱ کیلومتر	۲۵/۶	۲۰۱۹
[۵۹]	۵۰۲ کیلومتر	۰/۱۱۸	۲۰۱۹
[۳۵]	۵۰۹ کیلومتر	۰/۲۶۹	۲۰۲۰
[۶۰]	۶۰۰ کیلومتر	۱	۲۰۲۱

این سیستم از طریق یک اترنت خصوصی[۲۴] به رایانه‌ی وی‌پی‌ان[۲۵] که پروتکل‌های توزیع کلید کوانتومی و مجموعه پروتکل‌های اینترنت[۲۶] را اجرا می‌کنند، متصل است. پس از تولید کلید خام[۲۷] و ارسال آن از طریق کانال فیبرنوری این کلید از طریق سیستم کنترل فرایند نوری به رایانه‌ی وی‌پی‌ان منتقل می‌شود. با توجه به این‌که پروتکل‌های توزیع کلید کوانتومی در رایانه‌ی وی‌پی‌ان قرار دارند پس از عمل غربال‌گری، تشخیص و تصحیح خطا، تقویت حریم خصوصی و شناسایی استراق سمع‌کننده بر روی کلید خام، کلید امن[۲۸] تولید می‌گردد که این کلیدها به‌طور پیوسته در مخزن کلید مشترک قرار می‌گیرند. حال آن‌که برای محافظت از جریان ترافیک پیام، اصلاحاتی بر روی پروتکل تبادل کلید اینترنت[۲۹] صورت پذیرفته که باعث می‌شود از کلیدهای امن انباشته در مخزن کلید به‌جای الگوریتم استاندارد رمزنگاری پیشرفته، الگوریتم استاندارد رمزنگاری داده سه گانه[۳۰] و غیره استفاده گردد [۶۳-۶۱]. در شبکه گره قابل اعتماد برای افزایش بعد مسافت و ایجاد ارتباطات بلند برد لازم است میان مبدأ و مقصد از گره‌های میانی که به رله کلید معروف هستند استفاده شود.



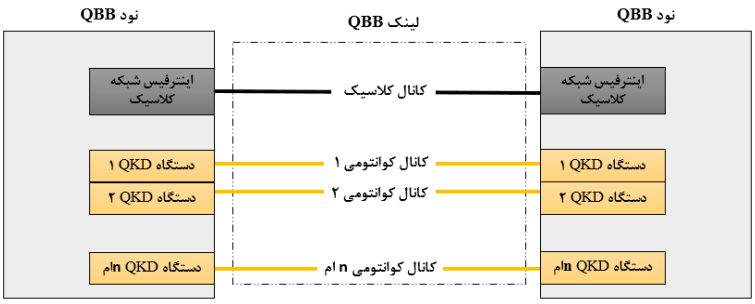
شکل (۱): معماری سیستم برای یک لینک توزیع کلید کوانتومی نقطه‌به‌نقطه [۶۳]

Figure (1): System architecture for a point-to-point QKD link [63]

از آنجا که لازم است رله کلیدها در مکان‌های ایمن و کاملاً محافظت شده جاسازی شوند، این شبکه به نام گره‌های قابل‌اعتماد[۳۱] و یا رله کلید[۳۲] معروف است. شبکه توزیع کلید کوانتومی با رله‌های قابل اطمینان به دو صورت برای انتقال پیام به‌کار می‌رود:

۱- در روش اول از رله‌های قابل انتقال برای انتقال کلید استفاده می‌گردد به این‌صورت که کلید مورد توافق میان مبدأ و مقصد توسط کلید کوانتومی میان فرستنده و رله میانی با تکنیک پد یکبار مصرف رمزگذاری شده سپس درون حافظه رله ذخیره می‌شود و در رله میانی با روش پد یکبار مصرف رمزگشایی می‌شود. در ادامه کلید مورد توافق با کلید کوانتومی دیگر و با همان روش رمزگذاری و رمزگشایی شود تا از رله‌های میانی به مقصد مورد نظر برسد. به این‌صورت کلید مورد توافق میان مبدأ و مقصد به اشتراک گذاشته می‌شود و از این کلید برای انتقال پیام امن استفاده می‌گردد.

۲- در روش دوم از رله‌های قابل‌اعتماد برای انتقال پیام امن استفاده می‌گردد. در این حالت میان فرستنده و رله میانی توزیع کلید کوانتومی صورت می‌پذیرد سپس پیام مورد نظر با روش پد یک‌بار مصرف توسط کلید کوانتومی رمزگذاری شده و درون حافظه رله میانی ذخیره می‌شود سپس در همان رله با روش پد یک‌بار مصرف رمزگشایی می‌گردد و با ادامه رمزگذاری و رمزگشایی در رله‌های میانی پیام مورد نظر از مبدأ به مقصد خواهد رسید [۶۵،۶۴،۵]. در کشورهای چین، ایالات‌متحده آمریکا، اسپانیا و ژاپن این نوع شبکه پیاده‌سازی شده و مورد استفاده قرار گرفته است. با توجه به این‌که در شبکه رله قابل‌اعتماد نرخ تولید کلید کوانتومی پایین است جهت افزایش آن شبکه ستون فقرات کوانتومی[۳۳] با چندین کانال کوانتومی به‌صورت موازی پیشنهاد داده شده است. شبکه ستون فقرات کوانتومی نوعی شبکه توزیع کلید کوانتومی است که شامل گره‌ها و لینک‌های ستون فقرات کوانتومی است. یک لینک ستون فقرات کوانتومی دو گره ستون فقرات کوانتومی را به یکدیگر متصل می‌کند. همان‌طور که در شکل (۲) نشان داده شده است، یک لینک ستون فقرات کوانتومی شامل تعداد دلخواهی کانال‌های کوانتومی برای ارسال سیگنال‌های کوانتومی و یک کانال کلاسیک برای ارسال سیگنال‌های کلاسیک و کلیدهای امن کوانتومی است. هر گره ستون فقرات کوانتومی شامل چندین دستگاه توزیع کلید کوانتومی برای ارسال کلیدهای خام تولیدشده از طریق لینک‌های ستون فقرات کوانتومی موازی و یک کانال کلاسیک است همچنین این گره دارای رایانه مخصوصی با چندین درگاه رابط ستون فقرات کوانتومی است که امکان اتصال به لینک ستون فقرات کوانتومی را فراهم می‌نماید. هدف از ایجاد چنین شبکه‌ای افزایش نرخ تولید کلید کوانتومی با وجود چندین کانال کوانتومی به صورت موازی است. این نوع شبکه در سال ۲۰۰۴ در اروپا پیاده‌سازی شده است [۶۶]. در سال ۲۰۱۷ آزمایش‌های موفق متعددی در ارتباطات کوانتومی برای ارسال کلیدها در فواصل بیش از ۱۰۰ کیلومتر با استفاده از کانال‌های فیبرنوری مانند آنچه در مرجع [۶۷] مطرح شده است، انجام گردید. در این مقاله نشان داده شده است که پروتکل بی‌بی ۸۴ [۳۴] می‌تواند نرخ‌های کلید مثبت را برای مسافت‌های ۲۴۰ کیلومتری بدون مالتی پلکس شدن سیگنال‌های معمولی و تا ۲۰۰ کیلومتری با مالتی پلکس شدن آن فراهم نماید.



شکل (۲): گره‌ها و لینک ستون فقرات کوانتومی [۶۶]

Figure (2): Quantum Back Bone nodes and link [66]

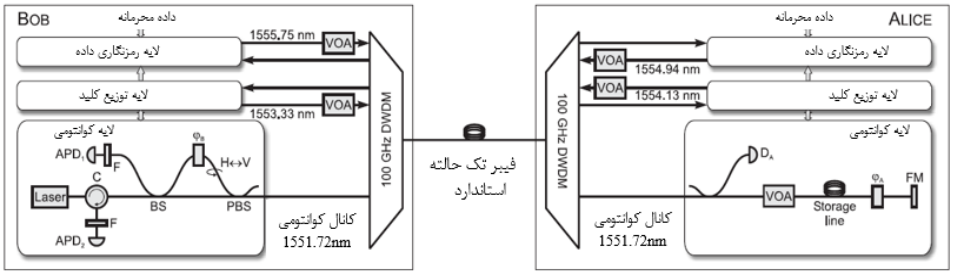
همچنین در همان سال توشیبا به یک راه‌حل تجاری برای توزیع کلیدهای کوانتومی با سرعت ۱۳/۷ مگابیت بر ثانیه دست یافت [۶۸] به‌طوری که بهبود سرعت هفت برابر قدرتمندتر از سیستم‌های ۱/۹ مگابیت بر ثانیه توسعه یافته در سال ۲۰۱۶ است. با عنایت به این‌که در شبکه‌های رله قابل‌اعتماد به گره‌های میانی اجازه داده می‌شود کلیدها را مسیریابی نمایند لذا در سال ۲۰۲۱ در مرجع [۶۹] رویکرد اتوماتیک‌سازی طراحی شبکه مطرح شده است. در این مقاله نویسندگان از روش‌های خوشه‌بندی مبتنی بر مدوید[۳۵] برای طراحی شبکه‌های توزیع کلید کوانتومی بر روی فیبرنوری استفاده می‌کنند که با انتخاب گره‌های شبکه به‌عنوان تکرارکننده و بهینه‌سازی تعداد تکرارکننده‌ها قصد دارند تعداد گره‌های شبکه را از ۱۰ نود به شبکه‌هایی با بیش از ۲۰۰ نود گسترش دهند. برای این‌منظور کار خود را بر روی شبکه فیبر نوری یک اپراتور تجاری در اسپانیا آزمایش نموده‌اند. همان‌طور که بررسی گردید زیرساخت شبکه گره‌های قابل‌اعتماد، می‌تواند شبکه آی‌پی[۳۶] و یا اینترنت موجود باشد که با توزیع کلید کوانتومی در گره‌های قابل‌اعتماد با قابلیت مسیریابی در آن گره‌ها، ارتباطات بلند برد امن میان مبدأ و مقصد ایجاد گردد. با پیاده‌سازی پروتکل‌های مبتنی بر درهم‌تنیدگی همانند پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری، ایجاد شبکه‌های توزیع کلید کوانتومی مبتنی بر رله‌های غیرقابل‌اعتماد نیز گسترش یافته است. پروتکل-های مبتنی بر رله غیرقابل‌اعتماد معمولاً از امنیت بیشتری نسبت به پروتکل‌های مبتنی بر رله قابل‌اعتماد برخوردار است، زیرا می‌تواند تمام حفره‌های امنیتی در سمت دستگاه اندازه‌گیری را حذف کند. حتی رله غیرقابل‌اعتماد می‌تواند توسط یک استراق سمع‌کننده کنترل شود بدون اینکه بر امنیت شبکه تأثیر بگذارد. همچنین پروتکل‌های استفاده شده در رله غیرقابل‌اعتماد می‌توانند فاصله توزیع کلید کوانتومی را به میزان قابل توجهی افزایش دهند. به عنوان مثال، در مرجع‌های [۳۵] و [۶۰] فاصله قابل دستیابی یک رله غیرقابل‌اعتماد با استفاده از پروتکل‌های توزیع کلید کوانتومی میدان دوقلو به ترتیب به ۵۰۹ کیلومتر و ۶۰۰ کیلومتر رسیده است. از آنجا که پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری اجازه اتصال دو رله غیرقابل‌اعتماد را نمی‌دهند ازاین‌رو با این روش نمی‌توان شبکه توزیع کلید کوانتومی را به فاصله دلخواه گسترش داد لذا این شبکه‌ها برای دسترسی با برد محدود و شبکه‌های شهری مناسب‌تر است، در حالی که جهت گسترش ارتباطات بلند برد نیاز به یکپارچه‌سازی آن با رله‌های قابل‌اعتماد است. حال آن‌که استفاده از این نوع شبکه‌های کوانتومی امن برای تعداد بیشتری از کاربران موضوع مهم دیگری است که مورد توجه پژوهشگران قرار گرفته و تحقیقات جهت استفاده از شبکه‌های نوری مطرح شده است.

۳-۲- شبکه گره‌های نوری

در سال‌های اخیر، شبکه‌های نوری مانند شبکه‌های نوری فعال[۳۷] [۷۰]، شبکه‌های نوری الاستیک[۳۸] [۷۱]، شبکه‌های نوری غیرفعال[۳۹] و شبکه تمام نوری[۴۰] به‌عنوان یک زیرساخت مهم شبکه به‌طور گسترده گسترش یافته است که در حوزه‌های دولتی، مالی و نظامی، امنیت این شبکه‌ها اهمیت بیشتری پیدا می‌کند [۷۲]. این نوع شبکه‌ها در برابر بسیاری از حملات سایبری آسیب‌پذیر هستند که ممکن است منجر به خسارات مالی عظیم یا حتی تلفات شود [۷۳] لذا جهت ایجاد امنیت و افزایش

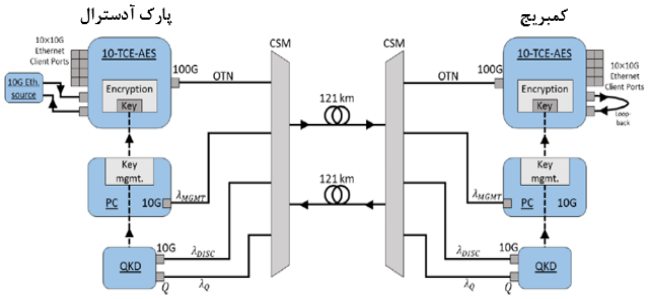
تعداد کاربران و فواصل میان گره‌ها موضوع استفاده از رمزنگاری کوانتومی در شبکه‌های نوری مطرح گردیده که در ذیل نحوه پیاده‌سازی و عملکرد این شبکه‌ها توضیح داده شده است.

الف- شبکه‌های نوری فعال: منظور از شبکه‌های نوری فعال استفاده بهینه از ظرفیت کانال فیبر نوری با استفاده از مالتی-پلکسینگ تسهیم طول موج و زمان است که برای امن‌سازی این نوع شبکه با استفاده از رمزنگاری کوانتومی باید یک سیستم کامل توزیع کلید کوانتومی برای هر کاربر نصب گردد. همان‌طور که در معماری شبکه توزیع کلید کوانتومی شکل (۳) نشان داده شده است با استفاده از ماژول‌های مالتی‌پلکسینگ تسهیم طول‌موج متراکم[۴۱] ۱۰۰ گیگاهرتزی چهار کانال کلاسیک و یک کانال کوانتومی تسهیم گردیده که برای کاهش ۱۰ درصد نویز رامان کانال‌های کلاسیک در طول‌موج‌های بالاتر و کانال کوانتومی در طول‌موج پایین‌تر یعنی ۱۵۵۱/۷۲ نانومتر قرار گرفته است. همچنین تجهیزات اپتیکی برای تولید کلید کوانتومی موردنظر در لایه کوانتومی پیاده‌سازی شده است. کلید کوانتومی تولید شده در این لایه برای اعمال فرآیند غربال‌گری، تصحیح خطای کوانتومی و تقویت حریم خصوصی به لایه توزیع کلید فرستاده می‌شود که در این لایه فرستنده و گیرنده کلید امن را با استفاده از دو کانال اصالت‌سنجی شده به اشتراک می‌گذارند. در لایه رمزگذاری داده‌ها، داده‌های مورد نظر توسط کلید امن تولید شده رمزگذاری شده سپس توسط دو کانال دوطرفه منتقل می‌یابد [۷۴]. با توجه به این‌که استفاده از پروتکل‌های توزیع کلید کوانتومی در شبکه‌های فعال نوری به روشی جذاب برای سازگاری انتقال سیگنال کوانتومی و سیگنال نوری کلاسیک توسط فناوری مالتی پلکسینگ تقسیم طول‌موج در یک فیبر مشترک تبدیل شده [۷۵]، در کشور چین مورد استفاده قرار گرفته است. در مقاله [۷۶] تخصیص طول موج بهینه در شبکه‌های ترکیبی کوانتومی کلاسیک که با استفاده از مالتی‌پلکسینگ تسهیم طول‌موج متراکم پیاده‌سازی شده مورد مطالعه قرار گرفته تا نرخ تولید کلید امن لینک‌های توزیع کلید کوانتومی را با در نظر گرفتن تداخل کانال مجاور و پراکندگی رامان به‌عنوان منابع نویز پس‌زمینه تحلیل شود. همچنین نویسندگان در سال ۲۰۲۰ در مقاله [۷۷] فناوری مالتی پلکسینگ تسهیم فضا[۴۲] را در فیبرهای‌نوری بررسی کردند و پیاده‌سازی توزیع کلید کوانتومی را بر روی فیبرهای چندهسته‌ای و همچنین سازگاری سیستم‌های کوانتومی با نسل بعدی شبکه‌های نوری مجهز به مالتی پلکسینگ تسهیم فضا را مطالعه نمودند. با توجه به این‌که شبکه‌های ۵G دارای لینک‌های مهم طبقه‌بندی شده هستند که ممکن است مقدار زیادی از ترافیک برنامه‌ها از آن جریان یابند، این لینک‌های حیاتی می‌تواند اهداف بسیار جذابی برای استراق سمع‌کنندگان باشند. از سوی دیگر در شبکه ۵G معمولاً رمزگذاری ترافیک داده فراهم نمی‌گردد از این‌رو همان‌طور که در شکل (۴) مشاهده می‌شود در انگلستان از زیرساخت شبکه یوکی‌کیوتل[۴۳] که بخشی از شبکه کوانتومی این کشور با گره‌های قابل‌اعتماد محافظت شده است، برای اتصال آزمایشگاه‌های تحقیقاتی بی‌تی[۴۴] در ایپسویچ (پارک آدسترال) به دانشگاه کمبریج به طول ۱۲۱ کیلومتر استفاده گردیده است به‌طوری‌که برای اتصال آن‌ها از ۵ کانال ۱۰۰G در یک سیستم مالتی‌پلکسینگ تسهیم طول‌موج متراکم استفاده شده است. در این شبکه در بازه زمانی ۳ ثانیه در هر کانال ۱۰۰G یک کلید رمزگذاری با استفاده از الگوریتم‌های توزیع کلید کوانتومی تولید می‌شود که این کلیدها در قسمت مدیریت کلید نگهداری می‌گردد سپس از این کلیدها برای امن کردن اطلاعات کلاینت‌ها استفاده خواهد شد به این ترتیب امنیت ارتباطات را در شبکه ۵G فراهم نموده‌اند [۷۸].



شکل (۳): نمای آزمایش توزیع کلید کوانتومی با مالتی‌پلکسینگ تسهیم طول‌موج متراکم [۷۴]

Figure (3): The view of quantum key distribution experiment with dense wavelength-division multiplexing [74]



شکل (۴): دیاگرام شبکه برای نشان دادن اتصال گره‌های شبکه پارک آدسترال و دانشگاه کمبریج با استفاده از الگوریتم‌های رمزنگاری کوانتومی [۷۸]

Figure (4): Network diagram to show the connection of Park Adstral and Cambridge university nodes using quantum cryptographic algorithms [78]

ب- شبکه‌های نوری الاستیک: در سال‌های اخیر، محبوبیت محاسبات ابری/مه‌آلود، اینترنت اشیا، سرویس‌های توزیع محتوا و سرویس چندرسانه‌ای به طور قابل توجه افزایش یافته است [۸۰،۷۹]. این برنامه‌ها عمدتاً پهنای باند دارند و منجر به افزایش سریع ترافیک در شبکه اصلی می‌شوند. شبکه‌های مالتی پلکسینگ تسهیم طول‌موج برای کاربردهای جدید کافی نیستند [۸۱]. لذا جهت دستیابی به ظرفیت بالا، تأخیر کم و الزامات شبکه نسل پنجم 5G شبکه‌های نوری الاستیک به‌عنوان راه‌حلی مقیاس‌پذیر، انعطاف‌پذیر و کارآمد برای نسل بعدی شبکه‌های هسته نوری با سرعت بالا پیشنهاد شده‌اند [۸۳،۸۲]. این شبکه‌ها از فناوری‌های توانمندی مانند مالتی پلکسینگ تسهیم فرکانس متعامد و مالتی پلکسینگ تسهیم طول موج نایکوئیست استفاده می‌کنند که با تقسیم طیف موجود به بخش‌های هم‌اندازه (۱۲/۵ گیگاهرتز یا ۶/۲۵ گیگاهرتز) به نام اسلایس[۴۵] ظاهر می‌شود [۸۵،۸۴]. نویسندگان در سال ۲۰۲۱ در مقاله [۸۶] عملکرد توزیع کلید کوانتومی را بر روی شبکه نوری آلاستیک با فیبرهای چند هسته‌ای مورد مطالعه قرار داده و راه‌حل‌هایی برای مشکل تخصیص منابع ترکیبی کوانتومی-کلاسیک پیشنهاد نموده‌اند.

ج- شبکه نوری غیرفعال: شبکه نوری غیرفعال فناوری ارتباطی دیگری است که امکان پیاده‌سازی یک نقطه به چند نقطه را فراهم می‌سازد. در حال حاضر استفاده از شبکه‌های نوری غیرفعال که به شبکه‌های دسترسی نوری نیز معروف هستند به دلیل هزینه پایین توسعه فیبرنوری افزایش یافته است که از جمله شبکه‌های دسترسی نوری می‌توان شبکه نوری غیرفعال با سرعت گیگابیت[۴۶] و شبکه نوری غیرفعال اترنت[۴۷] را نام برد. شبکه نوری غیرفعال از یک ترمینال خط نوری[۴۸] در مرکز مخابراتی تشکیل شده که از طریق تقسیم‌کننده‌های نوری[۴۹] که جهت توزیع سیگنال به کاربران در این شبکه استفاده می‌شوند به تعدادی واحد شبکه نوری[۵۰] در نزدیکی کاربران متصل شده است. در شبکه دسترسی کوانتومی، تجهیزات کوانتومی در ترمینال خط نوری و واحد شبکه نوری قرار می‌گیرند [۵]. در این نوع شبکه‌ها از شبکه دسترسی کوانتومی بالارو[۵۱] استفاده می‌شود. در این حالت فرستنده‌های کوانتومی با اطمینان از این‌که تنها فوتون‌های یک فرستنده در یک‌زمان به گیرنده می‌رسد، در طرف گیرنده تنها از یک آشکارساز به‌صورت اشتراکی استفاده می‌کنند به این ترتیب کلید کوانتومی میان فرستنده و گیرنده به اشتراک گذاشته می‌شود و اطلاعات از طریق این کلیدها به‌صورت امن منتقل می‌گردد [۲۴]. در حال حاضر شبکه دسترسی کوانتومی در اسپانیا و چین مورد بهره‌برداری قرار گرفته است.

د- شبکه تمام نوری: شبکه تمام نوری به معنی ارتباطی است که برای انتقال اطلاعات بین گره‌های مختلف شبکه مخابراتی از تجهیزات نوری استفاده می‌کند. زیرساخت مورد استفاده در این نوع شبکه‌ها فیبرنوری و یا فیبر تاریک است. محدوده استفاده شبکه‌های تمام نوری می‌تواند شبکه محلی[۵۲] و یا شبکه گسترده[۵۳] باشد. از دستگاه‌های تمام اپتیکی مورد استفاده در این نوع شبکه می‌توان سوئیچ، مسیریاب نوری، مالتی‌پلکسر فزود-فرود نوری قابل تنظیم[۵۴] و چرخاننده[۵۵] را نام برد. این شبکه‌ها به گره‌های میانی قابل‌اعتماد نیازی ندارند. بااین‌وجود، در این نوع از شبکه‌های توزیع کلید کوانتومی، حداکثر فاصله و نرخ کلید امن با تضعیف فیبرها محدود می‌شوند [۸۷،۸۸]. اولین بار این نوع شبکه در ایالات متحده آمریکا پیاده‌سازی شده است.

مالتی‌پلکسرهای فزود-فرود نوری قابل تنظیم معمولی که برای سوئیچینگ کانال‌های داده کلاسیک طراحی شده‌اند معمولاً اتلاف ۱۲-۲۰ دسی‌بل دارند [۸۹] که برای مسیریابی و سوئیچینگ سیگنال توزیع کلید کوانتومی مناسب نیستند. جدا از تلفات زیاد آن، نویزهای تولید شده از پیش تقویت‌کننده‌ها و پس تقویت‌کننده‌های این مالتی‌پلکسرها در کانال کوانتومی چالش قابل‌توجهی برای گیرنده [۹۰] ایجاد می‌نماید. برای غلبه بر ایرادات مطروحه در سال ۲۰۱۹ در مرجع [۹۱] یک معماری مالتی پلکسر فزود-فرود نوری قابل تنظیم بدون رنگ و بدون جهت پیشنهاد شده است که با نام مالتی پلکسر فزود-فرود نوری قابل تنظیم کوانتومی[۵۶] شناخته می‌شود که یک معماری جدید برای فعال کردن سوئیچینگ کانال‌های داده کلاسیک و سوئیچینگ کلید کوانتومی به طور همزمان است. همان‌طور که بررسی گردید زیرساخت شبکه‌های نوری، شبکه نوری فعال، شبکه نوری الاستیک، شبکه نوری غیرفعال و شبکه تمام نوری هستند که با توزیع کلید کوانتومی بر روی این شبکه‌ها علاوه بر ایجاد امنیت، تعداد کاربران شبکه افزایش یافته است. علاوه بر این در سال‌های اخیر موضوع کنترل اتوماتیک شبکه‌ها مطرح گردیده است که با پیشرفت تکنولوژی شبکه‌های کوانتومی کنترل اتوماتیک این نوع شبکه‌ها نیز مورد توجه قرار گرفته است.

۳-۳- ادغام توزیع کلید کوانتومی در سایر شبکه‌های مخابراتی

یک‌پارچه‌سازی (ادغام) شبکه توزیع کلید کوانتومی با شبکه‌های مخابرات کنونی از دو منظر دیگر نیز قابل بررسی است:

الف- زیرساخت شبکه نوری مشترک: شرط موفقیت تجاری سیستم‌های توزیع کلید کوانتومی استفاده از هر دو کانال ارتباطی کلاسیک و کوانتومی در یک زیرساخت شبکه نوری مشترک و قابل تنظیم است که این امر به همزیستی کانال‌های نوری کوانتومی و کلاسیک روی یک فیبر نیاز دارد. این هم‌زیستی ارتباطات کوانتومی و کلاسیک روی یک بستر مخابراتی دارای مضراتی است: اولاً اگر از رشته فیبری که محل عبور پالس‌های نوری ضعیف کوانتومی است برای ردوبدل کردن پالس‌های نسبتاً قوی کلاسیک استفاده شود، نویز تحمیلی به سیگنال‌های حساس کوانتومی زیاد و حتی غیرقابل‌تحمل می‌شود؛ دوما معماری شبکه‌های کلاسیک موجود لزوماً بهترین معماری ممکن برای یک شبکه کوانتومی نیست. با این حال کنترل و مهندسی مضرات این همزیستی به دلیل این‌که بسیاری از پروتکل‌های توزیع کلید کوانتومی و به‌طورکلی ارتباطات کوانتومی بر پایه‌ی تبادل پالس‌های نوری پیاده‌سازی می‌شوند و فیبر یکی از بهترین کانال‌های شناخته شده در این زمینه است لذا بهره‌گیری از آن برای انجام ارتباطات کوانتومی (در کنار ارتباطات کلاسیک در حال انجام) به لحاظ اقتصادی ضروری است که در مرجع‌های [۹۲]، [۹۳] و [۹۴] به آن پرداخته شده است. همچنین نویسندگان در سال ۲۰۲۰ در مرجع [۹۵] به‌طور تجربی امکان همزیستی کانال‌های توزیع کلید کوانتومی و کانال‌های نوری کلاسیک را بر روی فیبرهای چندهسته‌ای برحسب نرخ خطای بیت کوانتومی[۵۷] و نرخ کلید امن[۵۸] بررسی کرده‌اند؛ بنابراین همزیستی سیگنال‌های کلاسیک و کوانتومی نوعی شبکه کوانتومی در آینده‌ی دور و نزدیک خواهد بود به‌طوری‌که پروژه‌هایی در این زمینه از سال ۱۹۹۷ تاکنون در چین و انگلیس و سوئد انجام شده است.

ب- ادغام شبکه توزیع کلید کوانتومی با شبکه‌های مبتنی بر نرم‌افزار[۵۹]: در چند سال اخیر تلاش‌های زیادی جهت پیاده‌سازی شبکه‌های توزیع کلید کوانتومی بر روی شبکه آی‌پی صورت پذیرفته که با توجه به محدودیت‌ها، ادغام و یکپارچگی کامل آن با مشکلاتی همراه بوده است که ازجمله آن‌ها می‌توان گفت پارامترهای سیستم‌های ارتباطات کوانتومی[۶۰] که در بخش‌های اول و دوم قسمت ۳ اشاره شده است اغلب در طول نصب دستگاه تنظیم می‌شوند و در جریان عملیات ثابت باقی می‌ماند و هر تغییری در وضعیت پروتکل یا لینک نیاز به عملیات دستی توسط مدیر شبکه دارد. برای حل این مشکل روش‌های جدیدی مانند ادغام شبکه‌های کوانتومی با شبکه‌های مبتنی بر نرم‌افزار پیشنهاد شده است تا به این صورت انعطاف‌پذیری و کارایی این شبکه‌ها افزایش یابد [۹۶]. پارادایم شبکه‌های مبتنی بر نرم‌افزار معماری جدیدی است که با شکستن تجمیع عمودی و جداسازی فیزیکی سطح کنترل شبکه از سطح روترها و سوئیچ‌ها، از پیچیدگی مدیریت شبکه کاسته است و کنترل شبکه را در یک نقطه متمرکز می‌نماید. به‌طوری که کنترل چندین دستگاه شبکه در یک نقطه به‌صورت نرم‌افزاری صورت می‌پذیرد. در واقع شبکه‌های مبتنی بر نرم‌افزار با تغییراتی که در معماری شبکه ایجاد کرده توانسته است کنترل شبکه را با نرم‌افزار و به‌صورت یکپارچه فراهم نماید و مستقل از تولیدکننده تجهیزات عمل نماید. بدین‌صورت که دستورالعمل‌ها به‌جای این‌که از

سمت دستگاه‌ها و پروتکل‌های شرکت‌های تولیدکننده متفاوت صادر شوند، توسط کنترلرهای شبکه‌های مبتنی بر نرم‌افزار ایجاد می‌شوند. معماری این شبکه از سه لایه تشکیل شده است که عبارتند از: لایه کاربرد (برنامه‌ها و نرم‌افزارهای تحت شبکه در این لایه قرار می‌گیرند)، لایه کنترل (سرویس‌های شبکه در این لایه قرار دارند) و لایه زیرساخت (تجهیزات و زیرساخت شبکه در این لایه قرار می‌گیرند).

از آن‌جاکه پیاده‌سازی عملی فناوری ارتباطات کوانتومی امن در یک محیط چند کاربره، نیاز به نظارت خودکار بر وضعیت اتصال لینک‌ها، پارامترهای سیستم‌های کوانتومی و همچنین تنظیم آن‌ها به‌صورت همزمان با توجه به محدودیت‌های پروتکل دارد لذا می‌توان جهت پیاده‌سازی شبکه‌های توزیع کلید کوانتومی بر روی شبکه آی‌پی از پارادایم شبکه‌های مبتنی بر نرم‌افزار و جهت امنیت ارتباطات و مسیریابی شبکه‌های کوانتومی پویا از شبکه‌های مبتنی بر نرم‌افزار مبتنی بر پروتکل اوپن‌فلو[۶۱] استفاده نمود. ازاین‌رو تجهیزات و دستگاه‌های توزیع کلید کوانتومی در لایه زیرساخت نصب خواهد شد. یک لایه کنترل/مدیریت، لایه زیرساخت را با استفاده از یک مجموعه از پروتکل‌ها نظارت خواهد کرد. برنامه‌ها و نرم‌افزارهای مدیریتی و هماهنگی در لایه کاربرد قرار دارد که این جداسازی اجازه می‌دهد کنترل اتوماتیک شبکه توزیع کلید کوانتومی با موفقیت صورت پذیرد [۹۷]. همان‌طور که در بخش اول قسمت سوم توضیح داده شد در طول دهه گذشته تلاش‌های زیادی برای تبدیل لینک‌های ارتباطات کوانتومی نقطه‌به‌نقطه به شبکه‌های کوانتومی چند کاربره که در محیط واقعی عمل می‌کنند، صورت پذیرفته است. در نتیجه، شبکه‌های کوانتومی با موفقیت در سراسر جهان راه‌اندازی شده است و انواع جدیدی از دستگاه‌های ارتباطات کوانتومی توسعه‌یافته است. در میان آن‌ها سیستم‌های ارتباطات کوانتومی موج زیر حامل ساکن[۶۲] [۱۰۱-۹۸] وجود دارد که یکی از ویژگی‌های ارزشمند آن استفاده کارآمد از پهنای باند کانال کوانتومی و ظرفیت مالتی پلکسینگ سیگنال با اضافه کردن مجموعه‌های مستقل زیر حامل‌های کوانتومی به موج حامل [۱۰۱،۱۰۰] است. در اصل این روش اجازه می‌دهد تا بهره طیفی کانال‌های کوانتومی افزایش یابد. سیستم ارتباطات کوانتومی موج زیر حامل ساکن کاندید ستون فقرات شبکه‌های کوانتومی چند کاربره است. شکل (۵) طرح اصلی سیستم ارتباطات کوانتومی موج زیر حامل ساکن را نشان می‌دهد که شامل ماژول آرایه دریچه‌ای برنامه‌پذیر میدانی[۶۳] برای برقراری تعامل با کنترل‌کننده شبکه مبتنی بر نرم‌افزار و اجزای نوری به‌کار می‌رود. ماژول فرستنده (آلیس) شامل یک لیزر به‌عنوان منبع نوری، یک مدولاتور فاز جهت کدگذاری اطلاعات در فوتون‌ها و یک تضعیف‌کننده متغیر است که تعداد فوتون‌ها را در کانال کوانتومی کنترل می‌نماید [۱۰۲]. در این قسمت با چند مثال نشان داده می‌شود که کنترل سیستم‌های ارتباطات کوانتومی توسط شبکه مبتنی بر نرم‌افزار چگونه انجام می‌شود.

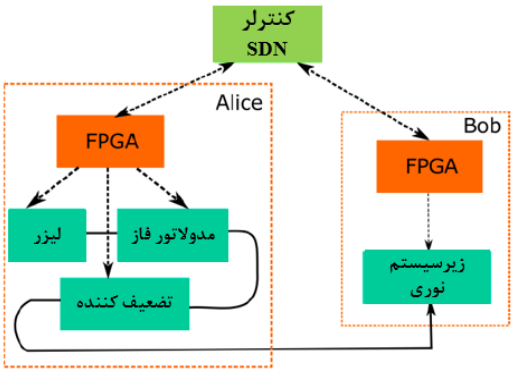
۱- در نمونه‌های پیاده‌سازی شده تلفات کانال نوری به علت گرما، خم شدن، ارتعاش و دیگر عوامل خارجی افزایش می‌یابد؛ بنابراین، تلفات لینک باید تحت نظارت قرار گیرد و به‌طور مرتب اندازه‌گیری شود و این داده‌ها در آرایه دریچه ای برنامه پذیر میدانی بارگذاری گردد و سپس این داده‌ها با مقادیر آستانه تلفات تعیین‌شده توسط مدیر مقایسه شود. اگر تلفات بیش از مقدار بحرانی باشد، آرایه دریچه ای برنامه پذیر میدانی یک سیگنال برای کنترل‌کننده شبکه مبتنی بر نرم‌افزار ارسال می‌کند و خواهان به‌روزرسانی وضعیت ماژول‌های فرستنده تمام سیستم‌های ارتباطات کوانتومی که از فیبر فعلی استفاده می‌کنند می‌شود [۱۰۲].

۲- یکی دیگر از ویژگی‌های ارزشمندی که مخصوص روش سیستم ارتباطات کوانتومی موج زیر حامل ساکن است، امکان افزودن یا رها کردن کانال‌های کوانتومی مستقل بر روی باندهای نوری [۹۹] مطابق با سیاست‌های شبکه و بدون متوقف کردن سیستم است [۱۰۲].

۳- طرح اصلی ساختار گره سیستم‌های ارتباطات کوانتومی با استفاده از پروتکل اپن‌فلو در لایه‌های مختلف شبکه در شکل (۶) نشان داده شده است. لایه کوانتومی از سیستم ارتباطات کوانتومی موج زیر حامل ساکن تشکیل شده است که مسئول تبادل اطلاعات کوانتومی، پردازش کلیدهای کوانتومی (غربال‌گری، تصحیح خطا و غیره) در داخل ماژول‌های ارتباطات کوانتومی و همزمانی نوری ماژول‌های آلیس و باب است. لایه مدیریت شبکه، توسط یک کنترل‌کننده شبکه مبتنی بر نرم‌افزار نشان داده شده که دستگاه‌های مسیریابی، سوئیچ‌های نوری، دستگاه‌های ارتباطات کوانتومی و وضعیت لینک‌ها را نظارت و کنترل می‌کند و مسیرها را برای سیگنال بهینه مشخص می‌نماید. لایه انتقال با استفاده از سوئیچ شبکه مبتنی بر نرم‌افزار که با پروتکل اوپن-

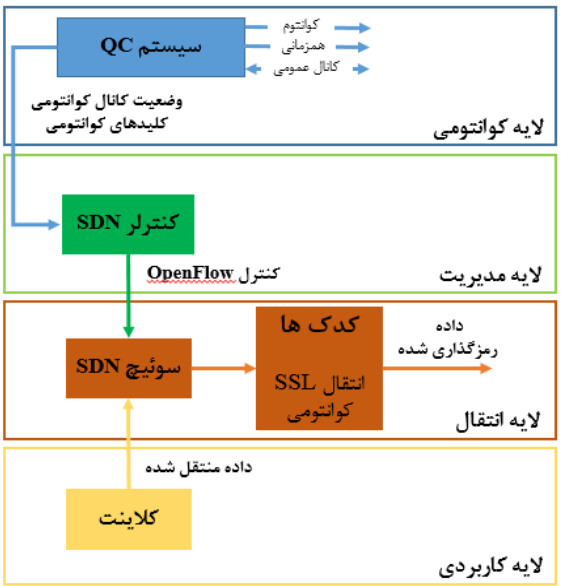
فلو سازگار است، مسیریابی فیزیکی شبکه و تبادل داده را انجام می‌دهد. این سوئیچ همچنین به‌عنوان یک رابط برای رمزگذاری داده‌ها با استفاده از کلیدهای کوانتومی یا کلاسیک بر اساس دستورات کنترلی عمل می‌کند. درنهایت لایه برنامه کاربری نشان دهنده رابط کاربر نهایی و نرم‌افزارهای ارتباطات شبکه است [۱۰۲].

کنترل‌کننده شبکه مبتنی بر نرم‌افزار با سوئیچ از طریق پروتکل اوپن‌فلو و با سایر دستگاه‌های متصل (سیستم‌های ارتباطات کوانتومی) از طریق نرم‌افزار تخصصی به‌منظور دریافت اطلاعات برای به‌روزرسانی وضعیت خود، مسائل مربوط به دستورات مسیریابی و تنظیم روش رمزنگاری ارتباط برقرار می‌کند. کلیدهای کوانتومی توسط سیستم ارتباطات کوانتومی به کنترل‌کننده شبکه مبتنی بر نرم‌افزار عرضه می‌شود که کنترل‌کننده شبکه مبتنی بر نرم‌افزار آن‌ها را به کدک می‌فرستد. در کدک براساس ترافیک داده‌ها از رمزگذاری کوانتومی و کلاسیک استفاده می‌شود. داده‌های کاربران که در لایه کاربردی تولید می‌شود به سوئیچ شبکه مبتنی بر نرم‌افزار ارسال می‌گردد و درنهایت، داده‌های رمز شده از طریق یک کانال نوری به گره هدف ارسال می‌شود. کلیدهای کوانتومی همچنین می‌توانند توسط کنترل‌کننده شبکه مبتنی بر نرم‌افزار برای رمزگذاری دستورات نیز مورد استفاده قرار گیرند، درنتیجه استحکام شبکه مبتنی بر نرم‌افزار در برابر تداخلات خارجی افزایش می‌یابد. یکی دیگر از برنامه‌های کنترل شبکه مبتنی بر نرم‌افزار در یک گره ارتباطات کوانتومی، مدیریت کلید است به‌طوری‌که مشتری می‌تواند برای امنیت بالاتر و سرعت کمتر، کلیدهای کوانتومی و برای امنیت کمتر و سرعت بالاتر، کلیدهای کلاسیک لایه سوکت ایمن[۶۴] و یا سایر کدک‌ها را انتخاب نماید [۱۰۲].



شکل (۵): طرح اصلی سیستم ارتباطات کوانتومی موج زیر حامل ساکن کنترل‌شده با شبکه مبتنی بر نرم‌افزار [۱۰۲]

Figure (5): Principal scheme of SDN-controlled SCW QC system [102]



شکل (۶): طرح اصلی ساختار گره سیستم ارتباطات کوانتومی با استفاده از پروتکل اوپن فلو [۱۰۲]

Figure (6): Principal scheme of OpenFlow-managed QC network node [102]

نوع دیگری از معماری شبکه نوری امن ترکیبی از نظارت مجازی‌سازی توابع شبکه[۶۵] و کنترل شبکه مبتنی بر نرم‌افزار با تکنولوژی توزیع کلید کوانتومی است که در سال ۲۰۱۶ در مرجع [۱۰۳] به آن پرداخته شده است. مجازی‌سازی توابع شبکه حوزه‌ی جدیدی در شبکه است که با کمک آن می‌توان دستگاه‌های سخت‌افزاری را به‌صورت مجازی و نرم‌افزاری پیاده‌سازی کرد. خرید و پیاده‌سازی تجهیزات سخت‌افزاری هزینه‌بر، زمان‌بر و نیازمند به نیروی متخصص است به همین دلیل مجازی‌سازی توابع شبکه به کمک مدیران شبکه آمده تا هزینه و پیچیدگی‌های آن را کاهش دهد. مجازی‌سازی توابع شبکه توسط شبکه‌های مبتنی بر نرم‌افزار تکمیل‌شده است. با این وجود استقرار آن دارای خطرات امنیتی است که توزیع کلید کوانتومی برای حل این مشکلات معرفی شده است. برای حل مشکل امنیتی شبکه‌های نوری، کائو و همکاران در سال‌های ۲۰۱۷ و ۲۰۱۸ در مرجع‌های [۱۰۴] و [۱۰۵] توزیع کلید کوانتومی را بر روی معماری شبکه نوری مبتنی بر نرم‌افزار پیشنهاد نموده‌اند. کائو و همکاران همچنین در سال ۲۰۱۷ یک طرح تخصیص منبع برای کلیدهای کوانتومی در شبکه‌های نوری ادغام شده با توزیع کلید کوانتومی را در مرجع [۱۰۶] طراحی کرده‌اند. علاوه بر این، در همان سال در مرجع [۱۰۷] برای اولین بار یک معماری امن جهت توزیع توابع شبکه مجازی‌سازی[۶۶] با ترکیبی از مجازی‌سازی توابع شبکه و فناوری توزیع کلید کوانتومی با برنامه‌ریزی بر روی یک شبکه نوری با استفاده از شبکه مبتنی بر نرم‌افزار پیشنهاد شده است. همچنین رویکردهای ادغام توزیع کلید کوانتومی و شبکه مبتنی بر نرم‌افزار در مرجع [۹۶] و مرجع‌های [۱۰۷]، [۱۰۸] و [۱۰۹] گزارش شده است. در این تحقیقات ثابت شده است که استفاده از شبکه مبتنی بر نرم‌افزار در شبکه‌های نوری توزیع کلید کوانتومی برای بهینه‌سازی عملکرد لینک‌های توزیع کلید کوانتومی مفید است. به‌عنوان‌مثال در مرجع [۱۰۹] نشان داده شده است که نظارت بر زمان واقعی پارامترهای کوانتومی، اطلاعاتی را به کنترل‌کننده شبکه مبتنی بر نرم‌افزار برای امن کردن مسیرهای نوری در شبکه نوری با تنظیمات مسیر نوری انعطاف‌پذیر برای اطمینان از توزیع بی‌وقفه کلیدهای کوانتومی در صورت حملات به لایه فیزیکی، ارائه می‌دهد. علاوه بر این، در مرجع‌های [۱۰۷] و [۱۱۰] استفاده از توزیع کلید کوانتومی برای مجازی‌سازی توابع شبکه مورد مطالعه قرار گرفته است و در چندین آزمایش کاربردی با استفاده از استاندارد رمزنگاری پیشرفته و کلیدهای کوانتومی بر امن کردن عملکرد مجازی‌سازی توابع شبکه تأکید نمودند. در سال ۲۰۱۷ در مرجع [۱۱۱]، نویسندگان کلیدهای امن را در شبکه‌های نوری ادغام شده با توزیع کلید کوانتومی مجازی‌سازی کردند تا شبکه‌های نوری مجازی[۶۷] ایمن بسازند. بر اساس پیشرفت‌های اتفاق افتاده در فناوری‌های توزیع کلید کوانتومی و آزمایش‌های میدانی و ترکیب آن‌ها با شبکه مبتنی بر نرم‌افزار و مجازی‌سازی توابع شبکه، توزیع کلید کوانتومی همچنین می‌تواند برای اتصالات امن توابع شبکه مجازی‌سازی توزیع‌شده در شبکه 5G نیز استفاده شود [۹۱]. علاوه بر این در سال ۲۰۱۹ در مرجع [۹۱] برای اولین بار سرویس شبکه امن کوانتومی با زنجیره توابع شبکه مجازی‌سازی توزیع شده روی یک شبکه نوری با استفاده از مالتی پلکسر فزود-فرود نوری قابل تنظیم کوانتومی نشان داده شده است. در سال ۲۰۲۰ در مرجع [۱۱۲]، نویسندگان طرحی را برای توزیع کلید کوانتومی بسیار کارآمد بر روی شبکه‌های نوری کوانتومی مترو[۶۸] پیشنهاد کرده‌اند که از استراتژی بای‌پس، زمانی که لینک‌های درونی و بیرونی یک گره در یک مسیر کوتاه هستند، استفاده می‌کند؛ بنابراین، گره می‌تواند به عنوان یک سوئیچ به جای یک رله قابل‌اعتماد عمل نماید. رشد انفجاری نیازهای کاربران، توسعه مجازی‌سازی عملکرد شبکه نوری[۶۹] را بر روی شبکه‌های الاستیک نوری الزامی می‌داند به‌طوری که از طریق مجازی‌سازی شبکه نوری، سرویس‌های شبکه را می‌توان با اشتراک گذاشتن منابع فیزیکی از نظر شبکه نوری مجازی ارائه کرد که بدین صورت مدیریت منابع نوری را ساده‌تر و انعطاف‌پذیری تخصیص منابع ارتقا می‌یابد. استراق سمع علیه شبکه نوری مجازی نه‌تنها خدمات مجازی، بلکه کل زیرساخت شبکه را به خطر می‌اندازد. توزیع کلید کوانتومی ادغام شده با شبکه‌های نوری سنتی یک فناوری امیدوارکننده برای حل این مشکل است که در سال ۲۰۲۱ در مقاله [۱۱۳]، ابتدا مفهوم جاسازی شبکه نوری مجازی را در شبکه نوری آلاستیک ادغام شده با توزیع کلید کوانتومی نشان داده سپس بر اساس این مفهوم، یک الگوریتم وون[۷۰] پویا برای تخصیص منابع فیزیکی شبکه به درخواست‌های شبکه نوری مجازی پیشنهاد نموده است که نه‌تنها نیازمندی‌های پهنای باند، بلکه خواسته‌های کلیدی را نیز در نظر می‌گیرد. همان‌طور که بررسی گردید با استفاده از زیرساخت شبکه‌های آی‌پی و شبکه‌های نوری و با کمک تکنولوژی شبکه مبتنی بر نرم‌افزار و مجازی‌سازی

توابع شبکه و با استفاده از پروتکل‌های توزیع کلید کوانتومی علاوه بر ایجاد امنیت بی‌قیدوشرط، بهینه‌سازی و اتوماتیک‌سازی شبکه‌های کوانتومی افزایش یافته است.

۴- شبکه‌های توزیع کلید کوانتومی پیاده‌سازی شده در فیبرنوری در جهان

همان‌طور که توضیح داده شد پس از ارائه‌ی اولین پروتکل توزیع کلید کوانتومی در سال ۱۹۸۴ دیگر پروتکل‌های متغیر گسسته توزیع کلید کوانتومی[۷۱] انتخاب‌های وسیعی را، متناسب با شرایط متنوع محیطی، برای طراحی سیستم‌های توزیع کلید کوانتومی فراهم آوردند. همچنین ارائه‌ی انواع روش‌های کدگذاری و پیاده‌سازی این پروتکل‌ها به بلوغ فناورانه‌ی این سیستم‌ها منجر شد، به‌گونه‌ای که روش‌های کدگذاری فاز (سال ۱۹۹۷) و روش‌های کدگذاری قطبش (سال ۱۹۹۵)، به‌ترتیب به‌عنوان روش‌های استاندارد پیاده‌سازی در فیبرهای نوری و فضای آزاد مطرح شدند. در طول زمان، تلاش‌های تئوری برای بهبود کارکرد پروتکل‌های توزیع کلید کوانتومی با در نظرگرفتن پیاده‌سازی‌های نزدیک به شرایط محیط واقعی آن منجر به ابداع انواع جدیدی از پروتکل‌های توزیع کلید کوانتومی موسوم به پروتکل‌های متغیر پیوسته توزیع کلید کوانتومی[۷۲] گردید که به جای استفاده از آشکارسازهای کوانتومی از روش‌های کلاسیک آشکارسازی که سریع‌تر و پربازده‌تر هستند استفاده می‌نمایند و در بستر شبکه‌های مخابراتی کنونی قابل پیاده‌سازی هستند. ابداع پروتکل‌های موسوم به مرجع فاز توزیع شده که ایده‌ای بین پروتکل‌های گسسته و پیوسته هستند، در فاصله نسبتاً اندکی بعد از ارائه پروتکل‌های پیوسته، توسط فیزیکدانان تجربی و با هدف به دست آوردن نرخ‌های بالاتر توزیع کلید طراحی شدند. ماحصل همه این تلاش‌ها، ارائه نمونه‌های تجاری‌سازی شده از سیستم‌های رمزنگاری کوانتومی است که اولین بار در سال‌های ۲۰۰۳ و ۲۰۰۴ توسط شرکت‌های فناوری‌های مجیک[۷۳] (نیویورک) و آیدی‌کوانتیک[۷۴] (ژنو) ارائه و بعد از آن شرکت‌های کوئنتسنس‌لبز[۷۵] (استرالیا)، سکیورنت[۷۶] (پاریس) وارد فاز تجاری‌سازی محصولات توزیع کلید کوانتومی شدند و بسیاری دیگری از شرکت‌ها همانند توشیبا[۷۷]، اچ‌پی[۷۸]، آی‌بی‌ام[۷۹]، میتسوپیشی[۸۰]، ان‌ای‌سی[۸۱] و ان‌تی‌تی[۸۲] فعالیت خود را در این زمینه آغاز نمودند. همزمان با این تلاش‌ها، پیشرفت‌های خیره‌کننده در طراحی ادوات مورد نیاز سیستم‌های توزیع کلید کوانتومی، همچون طراحی آشکارسازهای تک‌فوتونی ابررسانا با بازده نزدیک به یک و نویز نزدیک به صفر، انواع چشمه‌های تک‌فوتونی مبتنی بر بسترهایی همچون مراکز خلأ نیتروژن و نقاط کوانتومی، انواع مولدهای کوانتومی اعداد تصادفی صورت گرفت. علاوه بر این، کوچک‌سازی این ادوات و پیاده‌سازی آن‌ها در مقیاس‌های تراشه‌ای، نویدبخش ساخت دستگاه‌های رمزنگاری کوانتومی کاراتر و پربازده‌تر خواهد بود [۵]. به موازات فناوری توزیع کلید کوانتومی که پیاده‌سازی‌های آزمایشگاهی و میدانی آن از حدود سال ۱۹۹۵ تاکنون به دفعات انجام شده و طرح‌های موفق آن هم‌اکنون در مرحله‌ی تجاری‌سازی و پیاده‌سازی کاربردی می‌باشند، تحقیقات قابل‌توجه در زمینه توزیع کلید کوانتومی بر روی فیبرنوری از طریق شبکه‌های مخابراتی صورت پذیرفته است که در قسمت ۳ به‌طور کامل به آن پرداخته شد اما نکته اساسی اینجاست که پیاده‌سازی و عملیاتی‌کردن نتایج تحقیقات علمی با چالش‌های متعددی مواجه است که کشورهای توسعه‌یافته با تدوین نقشه راه فناوری ارتباطات کوانتومی، اختصاص بودجه‌های عظیم تحقیقاتی، عرضه نمونه‌های تجاری سیستم‌های رمزنگاری کوانتومی، اجرای موفق پروژه‌های رمزنگاری کوانتومی در مراکز مهم سیاسی و نظامی خود و سرمایه‌گذاری برای اجرای پروژه‌های مشابه در سطح ارتباطات شهری و بین‌شهری سعی در برپایی شبکه‌ای امن برای انتقال اطلاعات خود نموده‌اند ازاین‌رو همان‌طور که در جدول (۴) مشاهده می‌شود از سال ۲۰۰۱، کار روی اولین شبکه توزیع کلید کوانتومی در آمریکا و با حمایت و مشارکت دارپا[۸۳] آغاز گردید و اولین بخش آن در سال ۲۰۰۳ در یکی از آزمایشگاه‌های فناوری های بی‌بی‌ان[۸۴] راه‌اندازی شد. پس از آن، شبکه‌های کوانتومی متعددی در کشورهای مختلف جهان توسعه پیدا کرده‌اند. شبکه توزیع کلید کوانتومی چین امروزه بیش از ۱۰۰ گره دارد و حداکثر فاصله بین دو کاربر در این شبکه بیش از ۲۰۰۰ کیلومتر است که امکان ارتباط امن درون-شهری و بین-شهری را فراهم آورده است. در تمامی شبکه‌های پیاده‌سازی شده امنیت اطلاعات برای تمامی کاربران آن از جمله حکومت‌ها، مراکز سیاسی، مراکز تحقیقاتی، بانک‌ها، شبکه‌های برق و ... از اهمیت ویژه‌ای برخوردار است. همچنین در این سال‌ها دانشمندان این حوزه سعی در افزایش نرخ تولید کلید کوانتومی و مسافت میان کاربران به‌صورت همزمان نموده‌اند. در جدول (۴) مقایسه‌ای میان شبکه‌های درون-شهری و بین-شهری که

تاکنون در سراسر جهان پیاده‌سازی شده‌اند صورت پذیرفته است و برخی از جزئیات و اهداف آن شبکه‌ها در زیر بیان شده است.

۱- شبکه توزیع کلید کوانتومی دارپا اولین شبکه توزیع کلید کوانتومی در جهان است که در آزمایشگاه بی‌بی‌ان، دانشگاه بوستون و هاروارد نصب و در اکتبر ۲۰۰۳ مورد بهره‌برداری قرار گرفت. هدف از این پروژه توزیع کلیدهای امن از یک گره به گره دیگر با استفاده از توزیع کلید کوانتومی و همچنین محافظت از پیام‌ها در میان گره‌های ارتباطی با استفاده از رله‌های قابل‌اعتماد و سوئیچ‌های نوری است.

۲- پروژه اروپایی سیکوکیوسی[۸۵] یک شبکه شهری توزیع کلید کوانتومی مبتنی بر رله‌های قابل‌اعتماد است که از ۶ گره تشکیل و با تلاش چهل و یک گروه پژوهشی از اتحادیه اروپا، سوئیس و روسیه در شهر وین پیاده‌سازی شده است. با کمک این شبکه ارتباط تلفنی رمزگذاری شده با پد یکبار مصرف، یک کنفرانس ویدیویی امن با کلیه گره‌های مستقرشده انجام گردیده است.

۳- اولین شبکه توزیع کلید کوانتومی بدون رله‌های قابل‌اعتماد، با استفاده از توپولوژی ستاره بر اساس مالتی پلکسینگ تسهیم طول‌موج با چهار کاربر در شبکه فیبر مخابراتی پکن پیاده‌سازی شده است.

۴- در شبکه شهرکوانتوم[۸۶] دوربان از تجهیزات تجاری ای‌دی‌کوانتیک[۸۷] برای رمزگذاری داده‌ها استفاده شده است.

۵- شبکه توزیع کلید کوانتومی سوئیس مبتنی بر گره قابل‌اطمینان در منطقه شهری ژنو و فرانسه نصب و پیاده‌سازی شده است. از ویژگی‌های این شبکه مالتی‌پلکسینگ کانال‌های کوانتومی با کانال‌های کلاسیکی روی یک فیبر نوری است. این شبکه در بازه زمانی سال ۲۰۰۹ تا ۲۰۱۱ فعالیت کرده است.

۶- اولین شبکه منطقه شهری اسپانیا، در سال ۲۰۰۹ در مادرید پیاده‌سازی شده است.

۷- در شبکه توزیع کلید کوانتومی توکیو شش سیستم توزیع کلید کوانتومی متفاوت با توپولوژی مش دیده می‌شود. در این پروژه، عملیات شبکه شامل انتقال ویدئو کنفرانس امن، تشخیص شنود غیرمجاز، تغییر مسیر به لینک‌های ثانویه امن و تلفن همراه امن، توسط تیم‌های ژاپنی متعلق به موسسه ملی فناوری اطلاعات و ارتباطات آن کشور و شرکت‌های خصوصی مانند آن‌ای‌سی، آتی‌تی، میتسوپیشی اجرا شده است.

۸- شبکه سلسله مراتبی شهری هفت کاربره حاوی یک شبکه ستون فقرات چهار کاربره با توپولوژی مش، یک زیر شبکه دو کاربره و یک لینک دسترسی تک فیبر به یک کاربر است که پنج گره از آن در ادارات دولتی شهر ووهو قرار دارد. کلیدهای کوانتومی امن تولیدشده توسط این شبکه برای رمزگذاری ویدیو، صدا، پیام‌های متنی و فایل‌های محرمانه بین این دفاتر مورد استفاده قرار گرفتند.

۹- در سال ۲۰۱۱ شبکه بلندبردی شامل ۹ گره در اطراف ۳ شهر هیفای، چاهو و ووهو با پوشش ۲۰۰ کیلومتری طراحی شده است. شبکه توزیع کلید کوانتومی شهری هیفای شبکه‌ای با توپولوژی مش و بر اساس ترکیبی از عناصر فعال و غیرفعال و شبکه توزیع کلید کوانتومی شهری ووهو یک شبکه دسترسی کوانتومی با پیکربندی یک نقطه به چند نقطه است که بر اساس سوئیچ نوری پیاده‌سازی شده است.

۱۰- شبکه ارتباطات کوانتومی شهر جینان دارای ۵۶ گره است این شبکه بیش از ۲۰۰ کاربر رسمی دولتی دارد. گفته می‌شود که برای شبکه جینان ۱۹,۵ میلیون دلار سرمایه‌گذاری انجام شده است و برخی از مؤسسات مانند بانک صنعتی و تجاری چین، خبرگزاری شین هوا، کمیسیون تنظیم مقررات بانکی چین و دفاتر مختلف دولتی را به هم متصل نموده است.

۱۱- شرکت باتل با استفاده از تجهیزات شرکت ای‌دی‌کوانتیک، شبکه توزیع کلید کوانتومی را برای مصارف داخلی خود پیاده‌سازی نموده است. این شرکت دفتر مرکزی خود را در کلمبوس به یک مرکز تولیدی در دوبلین (اوهایو) متصل نموده است.

۱۲- شبکه‌های شهری پکن، جنیان، هیفای و شانگهای با فاصله دو هزار کیلومتر از طریق ۳۲ گره قابل‌اطمینان به هم متصل شده است بدین ترتیب طولانی‌ترین شبکه ارتباطات کوانتومی امن جهان پیاده‌سازی گردیده است. برنامه‌های کاربردی متعددی در زمینه مالی و دولتی با استفاده از این شبکه ایمن مورد استفاده قرار گرفته است.

Table (4): A comparison of the quantum key distribution networks implemented in the world

جدول (۴). مقایسه‌ای بر شبکه‌های توزیع کلید کوانتومی پیاده‌سازی شده در جهان

ردیف	مرجع	کشور	نام شبکه یا نام پروژه	سال استقرار	حداکثر فاصله دو کاربر (کیلومتر)	بیشترین نرخ کلید (کیلوبیت بر ثانیه)	نوع کلید	تعداد نود
۱	[۶۴]، [۱۱۴]	آمریکا	شبکه دارپا	۲۰۰۳	۲۹/۸	۱۰	متغیرگسسته	۱۰
۲	[۱۶]، [۱۱۵]، [۱۱۶]، [۱۱۷]	اروپا	پروژه اروپایی سیکوکیوسی	۲۰۰۴	۸۲	۱۷	متغیر گسسته متغیر پیوسته درهم‌تنیدگی	۶
۳	[۱۱۸]	چین	شبکه کوانتومی شهری نوع ستاره پکن	۲۰۰۷	۴۲/۶۸	۵۳	متغیر گسسته	۴
۴	[۱۱۹]	آفریقای جنوبی	پروژه شهر کوانتوم[۸۸] دوربان	۲۰۰۹	۲۷	۰/۸۹	متغیر گسسته	۴
۵	[۱۲۰]	سوئیس	شبکه کوانتومی سوئیس	۲۰۰۹	۱۷/۱	۲/۴	متغیر گسسته	۳
۶	[۱۲۱]	اسپانیا	شبکه ستون فقرات مادرید	۲۰۰۹	۶	-	متغیر گسسته	۳
۷	[۲۲]	ژاپن	شبکه کوانتومی توکیو	۲۰۱۰	۹۰	۳۰۰	متغیر گسسته درهم‌تنیدگی	۶
۸	[۱۲۲]	چین	شبکه کوانتومی ووهو یا وهان	۲۰۱۰	۱۴/۳	۴/۹۱	متغیر گسسته	۷
۹	[۱۲۳]	چین	شبکه بلند برد هیفای، چاهو، ووهو	۲۰۱۱	۱۹۹	۰/۸	متغیر گسسته	۹
۱۰	[۱۲۴]	چین	شبکه کوانتومی جینان	۲۰۱۲	۶۶	۳	متغیر گسسته	۵۶
۱۱	[۱۲۴]	آمریکا	شرکت خصوصی باتل[۸۹]	۲۰۱۳	۲۵	۱	متغیر گسسته	۲
۱۲	[۱۲۵]، [۱۲۶]	چین	شبکه دو هزار کیلومتری چین	۲۰۱۳	۲۰۰۰	۲۰-۳۰	متغیر گسسته	۳۲
۱۳	[۱۲۷]	اسپانیا	شبکه نوری غیرفعال مادرید با سرعت گیگابیت	۲۰۱۴	۱۶	-	متغیر گسسته	۳
۱۴	[۱۲۸]	چین	شبکه توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری هیفای	۲۰۱۶	۳۰	۰/۰۳۸۸	پروتکل مستقل از دستگاه اندازه‌گیری	۴
۱۵	[۱۲۹]	ژاپن	تغییرات در شبکه توزیع کلید کوانتومی توکیو	۲۰۱۷	۱۰	۵۰	متغیر پیوسته	-
۱۶	[۱۲۴]	آمریکا	شرکت کوانتوم اکسچنج[۹۰]	۲۰۱۸	۸۰۰	-	متغیر گسسته	۲
۱۷	[۱۲۴]	انگلیس	شبکه کوانتومی انگلیس	۲۰۱۸	۶۶	۸۰	متغیر گسسته	
۱۸	[۱۳۰]	اسپانیا	شبکه توزیع کلید کوانتومی مبتنی بر نرم‌افزار در مادرید	۲۰۱۸	۲۶/۴	۷۰	متغیر پیوسته	۳
۱۹	[۱۲۴]	روسیه	مرکز کوانتومی روسیه	۲۰۱۹	۳۰	۰/۱	متغیر گسسته	۲
۲۰	[۱۳۱]	چین	شبکه کوانتومی در دانشگاه شانگهای	۲۰۱۹	۲-۵۰	۰-۱۰/۲۵	متغیر پیوسته	-
۲۱	[۱۳۲]	انگلیس	شبکه کوانتومی کمبریج	۲۰۱۹	۱۰/۶	۲۵۸۰	متغیر گسسته	۳
۲۲	[۱۳۳]	انگلیس	شبکه کوانتومی کمبریج- ایپسوئیچ	۲۰۱۹	۱۲۱		متغیر گسسته	۵
۲۳	[۱۳۴]	چین	شبکه کوانتومی هیفای	۲۰۲۱	۱۸	۶۰	متغیر گسسته	۴۶

۱۳- شبکه نوری غیرفعال شهر مادرید با سرعت ۲/۴ گیگابیت بر ثانیه، بدون استفاده از گره‌های قابل‌اعتماد با همکاری دانشگاه پلی‌تکنیک مادرید، تلفنیکای اسپانیا[۹۱] و هواوی در سال ۲۰۱۴ پیاده‌سازی شده است.
۱۴- شبکه توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری در یک توپولوژی ستاره‌ای به مساحت ۲۰۰ کیلومترمربع در هیفای پیاده‌سازی شده است.
۱۵- با همکاری میتسوبیشی، دانشگاه گاکوشوین یک سیستم متغیر پیوسته تولید شد که این سیستم در تأسیسات موسسه ملی فناوری اطلاعات و ارتباطات کشور ژاپن نصب و به شبکه توزیع کلید کوانتومی توکیو متصل گردیده است.
۱۶- شرکت کوانتوم اکسچنج از طریق گره‌های قابل‌اطمینان با کمک فیبر تاریک شهر بوستون را به واشنگتن متصل نموده است که توسط شرکت زایو[۹۲] زیرساخت‌های ارتباطی آن تهیه‌شده است. برای تکمیل این پروژه ۱۰ میلیون دلار سرمایه‌گذاری شده است. مدیر این شرکت گفته است سرویس توزیع کلید کوانتومی طراحی‌شده در این شبکه برای بانک‌ها و سایر مؤسسات مالی که نیاز به اطمینان از امنیت داده‌های خود دارند، تدارک دیده شده است.
۱۷- ساخت شبکه کوانتومی بریتانیا، یک شبکه مبتنی بر فیبر در جنوب انگلستان، پروژه اصلی مرکز ارتباطات کوانتومی در برنامه ملی بریتانیا در فناوری‌های کوانتومی است. در بخش کمبریج - آکسفورد یک آزمایش سه‌هفته‌ای در فیبری با طول ۶۶ کیلومتر با تلفات ۱۶ دسی‌بل انجام شده است. ۲۰۰ گیگابیت بر ثانیه از ترافیک کلاسیک همزمان با استفاده از ترکیب الگوریتم استاندارد رمزنگاری پیشرفته و کلیدهای کوانتومی تولید شده توسط یک سیستم توزیع کلید کوانتومی روی یک فیبر در باند ۱۵۵۰ نانومتری اجرا و رمزگذاری شده است.
۱۸- در سال ۲۰۱۸ در شبکه مادرید توزیع کلید کوانتومی بر روی پارادایم شبکه‌های مبتنی بر نرم‌افزار انجام شده است.
۱۹- در مسکو، مرکز کوانتومی روسیه تولید چندین سیستم توزیع کلید کوانتومی را آغاز کرده است و توانسته است با استفاده از لینک‌های امن، یک شبکه کوانتومی را راه‌اندازی نماید به‌طوری‌که دفاتر بانک گازپروم[۹۳] را به هم متصل کرده سپس یک ارتباط کوانتومی بین دفاتر بانک اسبر[۹۴] را نیز برقرار نموده است.
۲۰- شبکه توزیع کلید کوانتومی متغیر پیوسته در محوطه دانشگاه شانگهای مستقر شده است. سیگنال کوانتومی و کلاسیک در این شبکه توسط مالتی پلکسینگ تسهیم طول‌موج که هر دو در باند تقریبا ۱۵۵۰ نانومتر حرکت می‌کنند پیاده‌سازی شده است.
۲۱- در شبکه شهری کمبریج کانال‌های کلاسیک و کوانتومی در یک فیبر با کمک ماژول‌های مالتی‌پلکسینگ تسهیم طول‌موج متراکم مالتی‌پلکس شده‌اند. همچنین در این شبکه کلیدهای امن با نرخ بالای ۲ تا ۳ مگابیت بر ثانیه تولید شده‌اند که از آن‌ها برای انتقال داده‌های رمزگذاری شده استفاده می‌شود.
۲۲- شبکه توزیع کلید کوانتومی کمبریج و ایپسویچ، در سال ۲۰۱۹ با پنج گره راه‌اندازی شد. در این شبکه سیگنال‌های کوانتومی و کلاسیک از طریق یک فیبر با طول کل ۱۲۱ کیلومتر منتقل می‌شوند.
۲۳- شبکه ارتباطات کوانتومی شهر هیفای دارای ۴۶ گره است که در ادارات دولتی، واحدهای نظامی، مؤسسات مالی و دفاتر بهداشت و درمان قرار دارد.

۵- فرصت‌ها و چالش‌های شبکه توزیع کلید کوانتومی

تاکنون نسل اول شبکه‌های کوانتومی که به شبکه توزیع کلید کوانتومی معروف است مورد بررسی قرار گرفته است. پیاده‌سازی شبکه‌های توزیع کلید کوانتومی در فیبرنوری به‌عنوان راه‌حلی است که امنیت غیرقابل حک را از طریق رمزنگاری کوانتومی فراهم نموده است. ارتباطات امن کوانتومی مبتنی بر توزیع کلید کوانتومی پتانسیل بالایی در ارتباطات مدرن دارند [۱۳۵]. اگرچه شبکه‌های توزیع کلید کوانتومی دستاوردهای بزرگ و پیشرفت قابل‌توجهی داشته است اما تضعیف سیگنال و حفظ قطبش باعث می‌شود طول چنین ارتباطاتی به چند صد کیلومتر محدود شود. همچنین ضریب تلفات فیبرنوری باعث می‌گردد تک‌فوتون‌ها با احتمال بسیار کمی به گیرنده برسند. این یک مسئله اساسی است که منجر به افت نرخ تولید کلید امن در فاصله طولانی می‌شود. راه‌حل‌های متعددی برای این مشکل وجود دارد که از جمله آن رله‌های قابل‌اعتماد یا تکرارکننده‌های

کوانتومی را می‌توان نام برد. در شبکه‌های توزیع کلید کوانتومی مبتنی بر رله‌های قابل‌اعتماد، اعتماد به رله‌ها مسئله اساسی است. از این‌رو لازم است رله‌ها در مکان‌های ایمن جاسازی و کاملاً محافظت شده باشند تا محتویات کلید و ترافیک پیام که در حافظه رله‌ها موجود است قابل‌دسترس نباشند. راه‌حل دیگر تغییر در طرح اجرای توزیع کلید کوانتومی است. عمدتاً دو طرح در اجرای آزمایشی توزیع کلید کوانتومی وجود دارد که عبارت‌اند از طرح آماده‌سازی و اندازه‌گیری [۱۳۶،۱۳۷] و طرح مبتنی بر درهم تنیدگی [۱۴۰-۱۳۸]. طرح توزیع کلید کوانتومی مبتنی بر درهم تنیدگی به‌طور طبیعی ارتباطات شبکه‌ای را بین کاربران برقرار می‌کند و مزایایی را در اجرای شبکه‌های کوانتومی نشان می‌دهد [۱۴۳-۱۴۱]. جفت فوتون‌های درهم‌تنیده توسط چشمه نور کوانتومی به‌ترتیب بین آلیس و باب توزیع می‌شوند؛ و رویدادهای تصادفی بین دو کاربر منجر به تولید کلیدهای رمزنگاری می‌شود [۱۴۴،۱۴۵]. توزیع کلید کوانتومی نوری پراکنده[۹۵] یک پروتکل توزیع کلید کوانتومی است که اخیراً پیشنهاد شده است [۱۴۸]. در این پروتکل زمان رسیدن فوتون‌ها به پایه زمانی بیشتر، برای تولید کلید استفاده می‌شود. فرآیند رمزگذاری با ابعاد بالا در مرحله پیش پردازش[۹۶] معرفی شده است تا نرخ تولید کلید را به حداکثر برساند [۱۴۰،۱۴۶،۱۴۷]. با این‌حال، پراکندگی رنگی فیبرهای نوری بر تولید کلیدهای امن تأثیر می‌گذارد. اخیراً توزیع کلید کوانتومی نوری پراکنده مبتنی بر درهم تنیدگی برای تحقق شبکه توزیع کلید کوانتومی از طریق توزیع درهم تنیدگی بر اساس تقسیم-کننده پرتو غیرفعال و مالتی پلکسینگ تسهیم طول موج [۱۴۱،۱۴۸] استفاده شده است. ازآنجایی‌که لینک‌های فیبر در این آزمایش بسیار کوتاه بودند، جبران پراکندگی اعمال نشده است. با این‌حال، می‌توان انتظار داشت که پراکندگی و تضعیف فیبر یک مشکل جدی در یک شبکه در مقیاس بزرگ باشد و اثرات جبران پراکندگی باید به‌طورجدی مورد توجه قرار گیرد [۱۴۹].

از دیگر اشکالات شبکه‌های توزیع کلید کوانتومی استفاده از سوئیچ‌های غیرقابل اعتماد برای افزایش تعداد کاربران شبکه است. از آنجاکه هر سوئیچ حداقل چند دسیبل تلفات به مسیر فوتونی اضافه می‌کند؛ بنابراین تنها در مناطق شهری مورداستفاده قرار می‌گیرد [۵]. در شبکه‌های نوری غیرفعال با توانایی گیگابیت فاصله انتقال و عملکرد توزیع کلید کوانتومی توسط تقسیم‌کننده‌های نوری محدود می‌گردد. برای حل این مشکل در تقسیم‌کننده نوری، فیلترهایی برای جداسازی سیگنال‌های کوانتومی استفاده شده است که از تلفات تولیدشده توسط تقسیم‌کننده‌های نوری جلوگیری می‌نماید، نرخ سیگنال‌های حالت کوانتومی را افزایش و نسبت سیگنال به نویز را بهبود می‌دهد. به این ترتیب نرخ تولید کلید بیشتر و فاصله انتقال طولانی‌تر می‌شود [۵]. پارادایم شبکه‌های مبتنی بر نرم‌افزار نیز با شکستن مسئله کنترل شبکه به قطعات قابل ردگیری، ایجاد انتزاع جدید در شبکه‌بندی، ساده‌سازی مدیریت شبکه و تسهیل تکامل شبکه را ساده‌تر کرده است.

به‌طورکلی باید گفت اگرچه پیشرفت‌های زیادی در اجرای عملی شبکه‌های توزیع کلید کوانتومی در فیبرنوری و در محیط واقعی صورت پذیرفته است اما همچنان نرخ پایین تولید کلید کوانتومی، برد محدود، نویز تحمیلی به سیگنال‌های کوانتومی در هم‌زیستی کانال ارتباطی کلاسیک و کوانتومی، تضعیف و پراکندگی فیبرهای نوری، تنظیمات زیرساخت شبکه، طراحی معماری شبکه، هزینه بالای تجهیزات کوانتومی و عدم وجود استانداردهای لازم و... برای این نوع شبکه‌ها موجب عدم پیاده-سازی یک شبکه ارتباطات کوانتومی جهانی با استفاده از شبکه‌های توزیع کلید کوانتومی در فیبرنوری شده است.

۶- جمع‌بندی و پیشنهاد برای جهت‌گیری‌های آتی

پیاده‌سازی شبکه‌های توزیع کلید کوانتومی در فیبرنوری به‌عنوان راه‌حلی است که امنیت بی‌قید و شرط را از طریق رمزنگاری کوانتومی فراهم نموده است لذا در این مقاله تعداد زیادی از مقاله‌های مرتبط با شبکه‌های توزیع کلید کوانتومی جمع‌آوری و براساس توزیع کلید کوانتومی بر روی زیرساخت انواع مختلف شبکه‌های کلاسیک کنونی به ۳ دسته تقسیم شده‌اند:

۱- زیرساخت شبکه گره‌های قابل‌اعتماد و غیر قابل‌اعتماد، شبکه آی‌پی موجود است که برای افزایش بعد مسافت و ایجاد ارتباطات بلند برد میان مبدأ و مقصد از گره‌های میانی که به رله کلید معروف هستند استفاده می‌نماید.

۲- زیرساخت شبکه‌های نوری، شبکه نوری فعال، شبکه نوری الاستیک، شبکه نوری غیرفعال و شبکه تمام نوری است که با توزیع کلید کوانتومی بر روی این شبکه‌ها علاوه بر ایجاد امنیت، تعداد کاربران شبکه افزایش یافته است.

۳- چندین سال است که برای کنترل اتوماتیک شبکه‌های آی‌پی و نوری پارادایم شبکه‌های مبتنی بر نرم‌افزار مطرح شده است. همچنین مجازی‌سازی توابع شبکه حوزه جدیدی در شبکه است که با کمک آن می‌توان دستگاه‌های سخت‌افزاری را به‌صورت مجازی و نرم‌افزاری پیاده‌سازی کرد تا هزینه و پیچیدگی‌های شبکه کاهش یابد. مجازی‌سازی توابع شبکه توسط شبکه‌های مبتنی بر نرم‌افزار تکمیل شده است. با این وجود، خطرات امنیتی جهت استقرار آن وجود دارد که توزیع کلید کوانتومی برای حل این مشکلات معرفی شده است.

با توجه به این‌که فناوری کوانتومی یک فناوری جذاب بر مبنای اصول مکانیک کوانتومی است که رایانش کوانتومی، رمزنگاری کوانتومی، ارتباطات کوانتومی، حسگرهای کوانتومی، شبیه‌سازی کوانتومی، اندازه‌شناسی کوانتومی و تصویر کوانتومی نمونه‌هایی از این فناوری هستند و با عنایت به این‌که تلفیق این فناوری با فناوری نانو حوزه جدیدی مانند اتوماتای سلولی کوانتومی را مطرح نموده است که فناوری نوظهور و بسیار جذابی برای پیاده‌سازی گیت‌های منطقی و مدارهای دیجیتال در مقیاس نانو است [۱۵۳-۱۵۰]، استفاده از این فناوری برای ساخت تجهیزات مورد نیاز در ارتباطات کوانتومی و کامپیوترهای کوانتومی پیشنهاد می‌شود. با این وجود قابلیت‌های فوق‌العاده فناوری کوانتومی سبب شده است در سال‌های اخیر دولت‌ها سرمایه-گذاری‌های زیادی بر روی برنامه‌های تحقیقاتی فناوری کوانتومی از جمله ارتباطات و رمزنگاری کوانتومی انجام دهند. اتحادیه اروپا در سال ۲۰۱۸ یک پروژه ۱ میلیارد یورویی تعریف کرده که به شرکت‌های نوپای اروپایی در ارتباطات و محاسبات کوانتومی کمک مالی می‌کند. همچنین بنا به برنامه تحقیق استراتژیک اعلامی از سوی پرچم‌دار کوانتوم اروپا مقرر است در طی ۳ سال توسعه مدل‌های تجاری سیستم‌های مقرون به‌صرفه برای ارتباطات درون-شهری و برون-شهری، استانداردها و صدور گواهینامه برای سیستم مولد اعداد تصادفی کوانتومی و بهره‌برداری از روش‌های رمزنگاری کوانتومی برای امنیت سیستم‌های حیاتی صورت پذیرد و در طی ۶ الی ۱۰ سال آینده سیستم‌های پیشرفته توزیع کلید کوانتومی و مولد اعداد تصادفی کوانتومی برای زیرساخت‌های حیاتی، اینترنت اشیا و 5G توسعه یابد. همچنین شبکه‌های توزیع کلید کوانتومی در فیبر، فضای آزاد و ماهواره‌های کوانتومی و تولید کلید کوانتومی در بیش از ۵۰۰ کیلومتر توسعه یابد. با توجه به سطح بالای سرمایه‌گذاری در فناوری‌های کوانتوم، اروپا می‌تواند با تمرکز بالای مؤسسات مالی که از توزیع کلید کوانتومی در شبکه استفاده می‌کنند یک بازار قابل‌توجهی ایجاد نماید. اروپا در رتبه دوم بزرگ‌ترین بازار جهانی رمزنگاری کوانتومی قرار دارد و پیش‌بینی می‌شود بازار رمزنگاری کوانتومی در اروپا از ۹۰ میلیون دلار در سال ۲۰۱۶ به ۵۱۸/۲ میلیون دلار در سال ۲۰۲۴ برسد. همچنین زیرساخت ارتباطات کوانتومی مبتنی بر شبکه‌های توزیع کلید کوانتومی زمینی-ماهواره‌ای به صورت یکپارچه در سراسر اتحادیه اروپا در حال بررسی است. در ژوئن ۲۰۲۱، هفت کشور از جمله بریتانیا، ایالات‌متحده آمریکا، ژاپن، کانادا، ایتالیا، بلژیک و اتریش، همکاری خود را برای توسعه یک شبکه رمزگذاری کوانتومی مبتنی بر ماهواره اعلام کردند [۱۵۴]. انگلستان از کشورهای پیشرو در فناوری کوانتومی اروپا است. دولت انگلیس با ۲۷۰ میلیون پوند برنامه ملی فناوری‌های کوانتومی انگلیس[۹۷] ایجاد کرده است. از جمله شرکت‌هایی که از این برنامه بهره‌مند می‌شوند می‌توان به ایرباس[۹۸]، بی‌تی[۹۹]، گوگل[۱۰۰]، لاکهید مارتین[۱۰۱] و ریتون[۱۰۲] و تعداد زیادی شرکت کوچک اشاره کرد. سپس با سرمایه‌گذاری ۱۵۳ میلیون پوندی در سال ۲۰۱۹ تجاری‌سازی محصولات و خدمات کوانتومی را گسترش داده است. همچنین دولت انگلیس با کمک کشورهای دارای توانایی سرمایه‌گذاری بزرگ مانند چین و ایالات‌متحده بر کاهش ۱۰ برابری هزینه فناوری‌های ارتباطات کوانتومی ظرف ۱۵ سال آینده اقدام نموده است. در حال حاضر در چین پروژه‌ای به نام صنعت فناوری کوانتومی ملی تعریف شده است که بخشی از آن به پیاده‌سازی شبکه ملی کوانتومی با ایجاد ارتباطات امن برای ارتش و دولت چین می‌پردازد، همچنین مشخص شده است که استقرار ماهواره کوانتومی چین علاوه بر ایجاد ارتباطات بین‌قاره‌ای، پاسخگوی نیازهای نیروی دریایی چین نیز است ازاین‌رو طی برنامه‌ریزی‌های صورت گرفته مقرر شده است که در طول سال‌های ۲۰۱۷ تا ۲۰۲۵ شبکه جهانی توزیع کلید کوانتومی مبتنی بر ماهواره را ایجاد نماید. ایالات‌متحده آمریکا سرمایه‌گذاری عظیمی در زمینه ساخت کامپیوترهای کوانتومی انجام داده و در مورد توسعه بازار شبکه‌های کوانتومی چند پروژه در حال انجام دارد بااین‌حال از نظر شبکه‌های کوانتومی از بقیه جهان عقب است لذا مقرر گردیده است که یک شبکه توزیع کلید کوانتومی ۸۰۰ کیلومتری با استفاده از فیبر نوری از بوستون تا واشنگتن دی سی مستقر شود [۱۵۴].

کره جنوبی کشور دیگری است که در حال ایجاد یک شبکه کوانتومی ملی است به‌طوری‌که شبکه ستون فقرات کوانتومی ۲۵۰ کیلومتری را به شبکه‌های کوانتومی شهری موجود متصل نماید. بنابر گزارش آی‌کیوتی[۱۰۳] پیش‌بینی می‌شود بازار شبکه‌های کوانتومی در سال ۲۰۲۶ به بیش از ۱۷ میلیارد دلار برسد که بیشترین سهم آن مربوط به تجهیزات توزیع کلید کوانتومی است [۱۵۵]. همچنین مراحل مختلف ساخت یک شبکه توزیع کلید کوانتومی در سراسر آن کشور مورد بحث قرار گرفته است. پیش‌بینی می‌شود در ژاپن نیز، شبکه‌ای در مقیاس بزرگ با بیش از ۱۰۰ دستگاه رمزنگاری کوانتومی و ۱۰۰۰۰ کاربر تا سال ۲۰۲۴ توسعه یابد [۱۵۴]. در راستای هدف توسعه شبکه‌های توزیع کلید کوانتومی مسائل و مشکلات بسیار گسترده و متنوعی وجود دارد که باید به نحوی حل شود تا بتوان یک ارتباط مطمئن و قابل‌اعتماد بین دو طرف ارتباط در شبکه برقرار کرد. این مسائل و مشکلات همگی از یک سنخ نیستند و منشأ و راه‌حل مشابه نیز ندارند و بخشی از آن‌ها توسط سخت‌افزار و بخش دیگر با روش‌های نرم‌افزاری قابل‌حل هستند لذا ضروری است در کارهای آتی راه‌حل‌های لازم برای چالش‌های مطروحه در این شبکه‌ها مانند نرخ پایین تولید کلید کوانتومی، برد محدود، تضعیف و پراکندگی فیبرهای نوری در شبکه‌های مورداشاره در مقاله و عدم وجود استانداردهای تجاری لازم و ... پیشنهاد گردد. برای پیاده‌سازی شبکه‌های کوانتومی میان‌مدت استفاده از فناوری‌های فضایی برای ایجاد ارتباطات ماهواره‌ای مطرح شده است که طراحی راه‌کارهای عملی جهت افزایش نرخ تولید کلید کوانتومی در این شبکه‌ها به‌عنوان کارهای آتی پیشنهاد می‌گردد. برای پیاده‌سازی شبکه‌های اینترنت کوانتومی استفاده از تکرارکننده‌های کوانتومی مطرح است که تاکنون تجاری‌سازی نشده‌اند لذا راه‌کار عملی جهت استفاده از تکرارکننده‌های کوانتومی در شبکه‌های توزیع کلید کوانتومی و اینترنت کوانتومی می‌تواند به‌عنوان کارهای آتی پیشنهاد گردد. همچنین ادغام شبکه‌های توزیع کلید کوانتومی با سایر فناوری‌های پیشرفته مانند بلاک چین، اینترنت اشیا، شبکه‌های بی‌سیم و ... جهت ایجاد پلتفرم‌های بسیار ایمن نیز از موضوعات تحقیقات آتی می‌تواند باشد.

References
مراجع

[1] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S.J. Glaser, F. Jelezko, S. Kuhr, "The quantum technologies roadmap: a European community view", New Journal of Physics, vol. 20, no. 8, Article Number: 080201, Aug. 2018 (doi: 10.1088/1367-2630/aad1ea).

[2] National Academies of Sciences, Engineering, Medicine, "Quantum computing: Progress and prospects", National Academies Press, April 2019 (ISBN: 978-0-309-47969-1).

[3] D. Gottesman, H.K. Lo, N. Lutkenhaus, J. Preskill, "Security of quantum key distribution with imperfect devices", Proceeding of the IEEE/ISIT, Chicago, IL, USA, June/July 2004 (doi: 10.48550/arXiv.quant-ph/0212066).

[4] M. Shirichian, S. Tofighi, "Protocol for routing entanglement in the quantum ring network", Proceeding of the IEEE/IST, pp. 658-663, Tehran, Iran, Dec. 2018 (doi: 10.1109/ISTEL.2018.8661126).

[5] A. Ahmadian, M. Ashrafi, M. Afsari, M. Bathayi, N.T. Bordbar, S. Tofighi, L. Chehreghani,S. Khademi, M. Shirichian, F. Farman, A. Mani, M. Nikayeen, M. Hashemi, M. Houshmand, "An Introduction of quantum communication", Atinegar (first Edition), 2020 (https://ketab.ir/book/294ae030-5b0f-4ac5-83ea-af77f85a-79e5) (ISBN: 978-622-7571-29-5) (in Persian).

[6] C.H. Bennett, G. Brassard, "An update on quantum cryptography", Proceeding of the Springer/TACT, pp. 475-480, Berlin, Heidelberg, Aug. 1984 (doi: 10.1007/3-540-39568-7_39).

[7] H.W. Li, C.M. Zhang, M.S. Jiang, Q.Y. Cai. "Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology", Communications Physics, vol. 5, Article Number: 53, Mar. 2022 (doi: 10.1038/s42005-022-00831-4).

[8] Y. Zhao, B. Qi, X. Ma, H.K. Lo, L. Qian "Experimental quantum key distribution with decoy states", Physical Review Letters, vol. 96, no. 7, pp. 2094-2098, Feb. 2006 (doi: 10.48550/ARXIV.QUANT-PH/050-3192).

[9] C.Z. Peng, J. Zhang, D. Yang, W.B. Gao, H.X. Ma, H. Yin, H.P. Zeng, T. Yang, X.B. Wang, J.W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding", Physical Review Letters, vol. 98, no. 1, Article Number: 010505, Jan. 2007 (doi: 10.48550/arXiv.q-uant-ph/0607129).

[10] D. Rosenberg, J.W. Harrington, P.R. Rice, P.A. Hiskett, C.G. Peterson, R.J. Hughes, A.E. Lita, S.W. Nam, J.E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber", Physical Review Letters, vol. 98, no. 1, Article Number: 010503, Jan. 2007 (doi: 10.1103/PhysRevLett.98.010503).

[11] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J.G. Rarity, A. Zeilinger, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km", Physical Review Letters, vol. 98, no. 1, Article Number: 010504, Jan. 2007 (doi: 10.1103/PhysRevLett.98.010504).

[12] Z.L. Yuan, A.W. Sharpe, A.J. Shields, "Unconditionally secure one-way quantum key distribution using decoy pulses", Applied Physics Letters, vol. 90, no.1, Article Number: 011118, Jan. 2007 (doi: 10.1063/1.2-430685).

[13] Z.Q. Yin, Z.F. Han, W. Chen, F.X. Xu, Q.L. Wu, G.C. Guo, "Experimental decoy quantum key distribution up to 130km fiber", arXiv preprint arXiv:0704.2941, April 2007 (doi:10.1088/0256-307X/25/10/008)

[14] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.F. Han, G.C. Guo, A. Karlsson, "Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source", Physical Review Letters, vol. 100, no. 9, Article Number: 090501, Mar. 2008 (doi: 10.1103/PhysRevLett.100.090501)

[15] A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe, A.J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate", Optics Express, vol. 16, no. 23, pp. 18790-18797, Nov. 2008 (doi: 10.13-64/OE.16.018790).

[16] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, S. Fasel, "The SECOQC quantum key distribution network in Vienna", New Journal of Physics, vol. 11, no. 7, Article Number: 075001, July 2009 (doi: 10.1364/OFC.2009.OThL2).

[17] D. Rosenberg, C.G. Peterson, J.W. Harrington, P.R. Rice, N. Dallmann, K.T. Tyagi, K.P. McCabe, S. Nam, B. Baek, R.H. Hadfield, R.J. Hughes, "Practical long-distance quantum key distribution system using decoy levels", New Journal of Physics, vol. 11, no. 4, Article Number: 045009, April 2009 (doi: 10.48550/arXiv.0-806.3085).

[18] Z.L. Yuan, A.R. Dixon, J.F. Dynes, A.W. Sharpe, A.J. Shields, "Practical gigahertz quantum key distribution based on avalanche photodiodes", New Journal of Physics, vol. 11, no. 4, Article Number: 045019, April 2009 (doi: 10.1088/1367-2630/11/4/045019).

[19] T.Y. Chen, H. Liang, Y. Liu, W.Q. Cai, L. Ju, W.Y. Liu, J. Wang, H. Yin, K. Chen, Z.B. Chen, C.Z. Peng, "Field test of a practical secure communication network with decoy-state quantum cryptography", Optics Express, vol. 17, no. 8, pp. 6540-6549, April 2009 (doi: 10.1364/OE.17.006540).

[20] Y. Liu, T.Y. Chen, J. Wang, W.Q. Cai, X. Wan, L.K. Chen, J.H. Wang, S.B. Liu, H. Liang, L. Yang, C.Z. Peng, "Decoy-state quantum key distribution with polarized photons over 200 km", Optics Express, vol. 18, no. 8. pp. 8587-8594, April 2010 (doi: 10.1364/OE.18.008587).

[21] T.Y. Chen, J. Wang, H. Liang, W.Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.Q. Cai, L. Ju, L.K. Chen, "Metropolitan all-pass and inter-city quantum communication network", Optics Express, vol. 18, no. 26, pp. 27217-27225, Dec. 2010 (doi: 10.1364/OE.18.027217).

[22] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, "Field test of quantum key distribution in the Tokyo QKD network", Optics Express, vol. 19, no.11, pp. 10387-10409, May 2011 (doi: 10.1364/OE.19.010387).

[23] J.Y. Wang, B. Yang, S.K. Liao, L. Zhang, Q. Shen, X.F. Hu, J.C. Wu, S.J. Yang, H. Jiang, Y.L. Tang, B. Zhong, "Direct and full-scale experimental verifications towards ground–satellite quantum key distribution", Nature Photonics, vol. 7, no. 5, pp. 387-393, April 2013 (doi: 10.1038/nphoton.2013.89).

[24] B. Fröhlich, J.F. Dynes, M. Lucamarini, A.W. Sharpe, Z. Yuan, A.J. Shields, "A quantum access network", Nature, vol. 501, no. 7465, pp. 69-72, Sept. 2013 (doi: 10.48550/arXiv.1309.6431).

[25] M. Lucamarini, K.A. Patel, J.F. Dynes, B. Fröhlich, A.W. Sharpe, A.R. Dixon, Z.L. Yuan, R.V. Penty, A.J. Shields, "Efficient decoy-state quantum key distribution with quantified security", Optics Express, vol. 21, no. 21, pp. 24550-24565, Oct. 2013 (doi: 10.1364/OE.21.024550)

[26] B. Fröhlich, M. Lucamarini, J.F. Dynes, L.C. Comandar, W.W. Tam, A. Plews, A.W. Sharpe, Z. Yuan, A.J. Shields, "Long-distance quantum key distribution secure against coherent attacks", Optica, vol. 4, no. 1 pp.163-167, Jan. 2017 (doi: 10.1364/OPTICA.4.000163).

[27] S.K. Liao, W.Q. Cai, W.Y. Liu, L. Zhang, Y. Li, J.G. Ren, J. Yin, Q. Shen, Y. Cao, Z.P. Li, F.Z. Li, "Satellite-to-ground quantum key distribution", Nature, vol. 549, no. 7670, pp. 43-47, Aug. 2017 (doi: 10.4-8550/arXiv.1707.00542).

[28] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A.W. Sharpe, A.R. Dixon, E. Lavelle, J.F. Dynes, A. Murakami, M. Kujiraoka, "10-Mb/s quantum key distribution", Journal of Lightwave Technology, vol. 36, no. 16, pp. 3427-3433, July 2018 (doi: 10.1109/JLT.2018.2843136).

[29] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.J. Li, D. Nolan, "Secure quantum key distribution over 421 km of optical fiber", Physical Review Letters, vol. 121, no. 19, Nov. 2018 (doi: 10.1103/PhysRevLett.121.190502).

[30] H.L. Yin, P. Liu, W.W. Dai, Z.H. Ci, J. Gu, T. Gao, Q.W. Wang, Z.Y. Shen. "Experimental composable security decoy-state quantum key distribution using time-phase encoding", Optics Express, vol. 28, no. 20, pp. 29479-29485, Sept. 2020 (doi:10.1364/OE.401829).
[31] C.Q. Hu, Z.Q. Yan, J. Gao, Z.M. Li, H. Zhou, J.P. Dou, X.M. Jin. "Decoy-state quantum key distribution over a long-distance high-loss air-water channel", Physical Review Applied, vol. 15, no. 2, Article Number: 024060, Feb. 2021 (doi: 10.48550/arXiv.2004.06708).
[32] A.K. Ekert, "Quantum cryptography based on Bell's theorem", Physical Review Letters, vol. 67, no. 6, pp. 661-663, Aug. 1991 (doi:10.1103/PhysRevLett.67.661).
[33] F. Xu, X. Ma, Q. Zhang, H.K. Lo, J.W. Pan,"Secure quantum key distribution with realistic devices", Reviews of Modern Physics, vol. 92, no. 2, Article Number: 025002, May 2020 (doi: 10.1103/RevModPhys.92.025002).
[34] M. Lucamarini, Z.L. Yuan, J.F. Dynes, A.J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters", Nature, vol. 557, no. 7705, pp. 400-403, May 2018 (doi: 10.1038/s41586-018-0066-6).
[35] J.P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.L. Hu, J.Y. Guan, Z.W. Yu, H. Xu, J. Lin, M.J. Li, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km", Physical Review Letters, vol. 124, no. 7, Article Number: 070501, Feb. 2020 (doi: 10.1103/PhysRevLett.124.070501).
[36] A. Rubenok, J.A. Slater, P. Chan, I. Lucio-Martinez, W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks", Physical Review Letters, vol. 111, no. 13, Article Number: 130501, Sept. 2013 (doi:10.1103/PhysRevLett.111.130501).
[37] Y. Liu, T.Y. Chen, L.J. Wang, H. Liang, G.L. Shentu, J. Wang, K. Cui, H.L. Yin, N.L. Liu, L. Li, X. Ma, "Experimental measurement-device-independent quantum key distribution", Physical Review Letters, vol. 111, no.13, Article Number: 130502, Sept. 2013 (doi:10.1103/PhysRevLett.111.130502).
[38] T.F. Da Silva, D. Vitoreti, G.B. Xavier, G.C. Do Amaral, G.P. Temporão, J.P. Von Der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits", Physical Review A, vol. 88, no. 5, Article Number: 052303, Nov. 2013 (doi: 10.1103/PhysRevA-.88.052303).
[39] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution", Physical Review Letters, vol. 112, no.19, Article Number: 190503, May 2014 (doi: 10.1103/PhysRevLett.112.190503).
[40] Y.L. Tang, H.L. Yin, S.J. Chen, Y. Liu, W.J. Zhang, X. Jiang, L. Zhang, J. Wang, L.X. You, J.Y. Guan, D.X. Yang, "Measurement-device-independent quantum key distribution over 200 km", Physical Review Letters, vol. 113, no. 19, Article Number: 190501, Nov. 2014 (doi: 10.1103/PhysRevLett.113.190501).
[41] C. Wang, X.T. Song, Z.Q. Yin, S. Wang, W. Chen, C.M. Zhang, G.C. Guo, Z.F. Han, "Phase-reference-free experiment of measurement-device-independent quantum key distribution", Physical Review Letters, vol. 115, no. 16, Article Number: 160502, Oct. 2015 (doi: 10.1103/PhysRevLett.115.160502).
[42] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, D. Korchinski, C. Duffin, F. Marsili, V. Verma, M.D. Shaw, J.A. Stern, "Measurement-device-independent quantum key distribution: from idea towards application", Journal of Modern Optics, vol. 62, no. 14, pp. 1141-1150, Aug. 2015 (doi: 10.48550/arXiv.1501.07307).
[43] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S.L. Braunstein, S. Lloyd, T. Gehring, C.S. Jacobsen, U.L. Andersen, "High-rate measurement-device-independent quantum cryptography", Nature Photonics, vol. 9, no. 6, pp. 397-402, June 2015 (doi: 10.1038/nphoton.2015.83).
[44] Y.L. Tang, H.L. Yin, Q. Zhao, H. Liu, X.X. Sun, M.Q. Huang, W.J. Zhang, S.J. Chen, L. Zhang, L.X. You, Z. Wang, "Measurement-device-independent quantum key distribution over untrustful metropolitan network", Physical Review X, vol. 6, no. 1, Article Number: 011024, Mar. 2016 (doi: 10.1103/PhysRevX.6.011024).
[45] H.L. Yin, T.Y. Chen, Z.W. Yu, H. Liu, L.X. You, Y.H. Zhou, S.J. Chen, Y. Mao, M.Q. Huang, W.J. Zhang, H. Chen, "Measurement-device-independent quantum key distribution over a 404 km optical fiber", Physical Review Letters, vol. 117, no. 19, Article Number: 190501, Nov. 2016 (doi: 10.1103/PhysRevLett.117.190501).
[46] G.Z. Tang, S.H. Sun, F Xu, H Chen, C.Y. Li, L.M. Liang, "Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution", Physical Review A, vol. 94, no. 3, Article Number: 032326, Sept. 2016 (doi: 10.1103/PhysRevA.94.032326).
[47] L.C. Comandar, M. Lucamarini, B. Fröhlich, J.F. Dynes, A.W. Sharpe, S.B. Tam, Z.L. Yuan, R.V. Penty, A.J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers", Nature Photonics, vol. 10, no. 5, Article Number: 312, May 2016 (doi: 10.1038/nphoton.2016.50).

[48] F. Kaneda, F. Xu, J. Chapman, P.G. Kwiat, "Quantum-memory-assisted multi-photon generation for efficient quantum information processing", Optica, vol. 4, no. 9, pp. 1034-1037, Sept. 2017 (doi: 10.1364/OPTICA.4.001034).
[49] C. Wang, Z.Q. Yin, S. Wang, W. Chen, G.C. Guo, Z.F. Han, "Measurement-device-independent quantum key distribution robust against environmental disturbances", Optica, vol. 4, no. 9, pp. 1016-1023, Sept. 2017 (doi: 10.1364/OPTICA.4.001016).
[50] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V.B. Verma, M.D. Shaw, S.W. Nam, D. Oblak, W. Tittel, "A cost-effective measurement-device-independent quantum key distribution system for quantum networks", Quantum Science and Technology, vol. 2, no. 4, Article Number: 04LT01, Sept. 2017 (doi: 10.48550/arXiv.1702.05155).
[51] Y. Liu, Q. Zhao, M.H. Li, J.Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.Z. Liu, C. Wu, X. Yuan, H. Li, "Device-independent quantum random-number generation", Nature, vol. 562, no. 7728, pp. 548-551, Oct. 2018 (doi: 10.1038/s41586-018-0559-3).
[52] H. Liu, W. Wang, K. Wei, X.T. Fang, L. Li, N.L. Liu, H. Liang, S.J. Zhang, W. Zhang, H. Li, L. You, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels", Physical Review Letters, vol. 122, no. 16, Article Number: 160501, April 2019 (doi: 10.1103/PhysRevLett.122.160501).
[53] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.Y. Chen, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics", Physical Review X, vol. 10, no. 3, Article Number: 031030, Aug. 2020 (doi: 10.1103/PhysRevX.10.031030).
[54] M. Razavi, "An introduction to quantum communications networks", Morgan & Claypool Publishers, May 2018 (ISBN: 978-1-6817-4652-4).
[55] M. Minder, M. Pittaluga, G.L. Roberts, M. Lucamarini, J.F. Dynes, Z.L. Yuan, A.J. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity", Nature Photonics, vol. 13, no. 5, pp. 334-338, May 2019 (doi: 10.1038/s41566-019-0377-7).
[56] S. Wang, D.Y. He, Z.Q. Yin, F.Y. Lu, C.H. Cui, W. Chen, Z. Zhou, G.C. Guo, Z.F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system", Physical Review X, vol. 9, no. 2, Article Number: 021046, June 2019 (doi: 10.1103/PhysRevX.9.021046).
[57] Y. Liu, Z.W. Yu, W. Zhang, J.Y. Guan, J.P. Chen, C. Zhang, X.L. Hu, H. Li, C. Jiang, J. Lin, T.Y. Chen, "Experimental twin-field quantum key distribution through sending or not sending", Physical Review Letters, vol. 123, no. 10, Article Number: 100505, Sept. 2019 (doi: 10.1103/PhysRevLett.123.100505).
[58] X. Zhong, J. Hu, M. Curty, L. Qian, H.K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution", Physical Review Letters, vol. 123, no. 10, Article Number: 100506, Sept. 2019 (doi: 10.1103/PhysRevLett.123.100506).
[59] X.T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.L. Tang, Y.J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound", Nature Photonics, vol. 14, no. 7, pp. 422-425, July 2020 (doi: 10.1038/s41566-020-0599-8).
[60] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R.I. Woodward, M.J. Li, Z. Yuan, A.J. Shields, "600-km repeater-like quantum communications with dual-band stabilization", Nature Photonics, vol. 15, no. 7, pp. 530–535, July 2021 (doi: 10.48550/arXiv.2012.15099)
[61] S. Kent, R. Atkinson, "RFC2401: Security architecture for the internet protocol", Browse RFC, 1998 (doi: 10.17487/RFC2401).
[62] D. Harkins, D. Carrel. "The internet key exchange (IKE)", RFC 2409, Nov. 1998 (doi: 10.17487/RFC2409).
[63] C. Elliott, "Building the quantum network", New Journal of Physics, vol. 4, no.1, Article Number: 46, July 2002 (doi: 10.1088/1367-2630/4/1/346).
[64] C. Elliott, D. Pearson, G. Troxel, "Quantum cryptography in practice", Proceedings of the ATAPCC, pp. 227-238, Karlsruhe Germany, Aug. 2003 (doi: 10.1145/863955.863982).
[65] A. Herman, I. Friedson, "Quantum Computing: How to address the national security risk", Hudson Institute, Aug. 2018.
[66] M. Dianati, R. Alléaume, M. Gagnaire, X. Shen."Architecture and protocols of the future European quantum key distribution network", Security and Communication Networks, vol. 1, no.1, pp. 57-74, Jan. 2008 (doi: 10.1002/sec.13).
[67] B. Fröhlich, M. Lucamarini, J.F. Dynes, L.C. Comandar, W.W. Tam, A. Plews, A.W. Sharpe, Z. Yuan, A.J. Shields. "Long-distance quantum key distribution secure against coherent attacks", Optica, vol. 4, no.1, pp. 163-167, Jan. 2017 (doi:10.1364/OPTICA.4.000163).
[68] A.M. Lewis, M.Travagnin, "A Secure Quantum Communications Infrastructure for Europe: Technical background for a policy vision", Publications Office of the European Union, 2022 (doi: 10.2760/180945)

[69] I. Garcia-Cobo, H.D. Menéndez. "Designing large quantum key distribution networks via medoid-based algorithms", Future Generation Computer Systems, no. 115, pp. 814-824, Feb. 2021 (doi: 10.1016/j.future.2020.09.037).
[70] Y. Yu, J. Zhang, Y. Zhao, X. Cao, X. Lin, W. Gu, "The first single-link exact model for performance analysis of flexible grid WDM networks", Proceeding of the NFOEC, Anaheim, California, United States, Mar. 2013 (doi: 10.1364/NFOEC.2013.JW2A.68).
[71] Y. Zhao, B. Chen, J. Zhang, X. Wang, "Energy efficiency with sliceable multi-flow transponders and elastic regenerators in survivable virtual optical networks", IEEE Trans. on Communications,vol. 64, no.6, pp. 2539-2550, April 2016 (doi: 10.1109/TCOMM.2016.2554110).
[72] N. Skorin-Kapov, M. Furdek, S. Zsigmond, L. Wosinska, "Physical-layer security in evolving optical networks", IEEE Communications Magazine, vol. 54, no. 8, pp. 110-117, Aug. 2016 (doi: 10.1109/MCOM.2016.7537185).
[73] H.M. Salim, "Cyber safety: A systems thinking and systems theory approach to managing cyber security risks", PhD Thesis, Massachusetts Institute of Technology, 2014.
[74] P. Eraerds, N. Walenta, M. Legré, N. Gisin, H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre", New Journal of Physics, vol. 12, no. 6, Article Number: 063027, June 2010 (doi: 10.1088/1367-2630/12/6/063027).
[75] L.J. Wang, L.K. Chen, L. Ju, M.L. Xu, Y. Zhao, K. Chen, Z.B. Chen, T.Y. Chen, J.W. Pan, "Experimental multiplexing of quantum key distribution with classical optical communication", Applied Physics Letters, vol. 106, no. 8, Article Number: 081108, Feb. 2015 (doi:10.1063/1.4913483).
[76] S. Bahrani, M. Razavi, J.A. Salehi, "Wavelength assignment in hybrid quantum-classical networks", Scientific reports, vol. 8, no. 1, pp. 1-13, Feb. 2018 (doi:10.48550/arXiv.1701.08270).
[77] G.B. Xavier, G. Lima. "Quantum information processing with space-division multiplexing optical fibres", Communications Physics, vol. 3, no. 1, pp. 1-11, Jan. 2020 (doi: 10.1038/s42005-019-0269-7).
[78] P. Wright, C. White, R.C. Parker, J.S. Pegon, M. Menchetti, J. Pearse, A. Bahrami, A. Moroz, A. Wonfor, R.V. Penty, T.P. Spiller. "5G network slicing with QKD and quantum-safe security", Journal of Optical Communications and Networking, vol. 13, no. 3, pp. 33-40, Mar. 2021 (doi:10.48550/arXiv.2007.03377).
[79] S. Guo, S. Shao, Y. Wang, H. Yang, "Cross stratum resources protection in fog-computing-based radio over fiber networks for 5G services", Optical Fiber Technology, vol. 37, pp. 61-68, Sept. 2017 (doi: 10.1016/j.yofte.2017.07.001).
[80] F. Sadeghi, A. Avokh, "Load-balanced data gathering in Internet of Things using an energy-aware cuckoo-search algorithm", International Journal of Communication Systems, vol. 33, no. 9, Article Number: e4385, June 2020 (doi: 10.1002/dac.4385).
[81] P. Afsharlar, A. Deylamsalehi, J.M. Plante, J. Zhao, V.M. Vokkarane, "Routing and spectrum assignment with delayed allocation in elastic optical networks", Journal of Optical Communications and Networking, vol. 9, no. 3, pp. B101-B111, Mar. 2017 (doi: 10.1364/JOCN.9.00B101).
[82] B.C. Chatterjee, S. Ba, E. Oki, "Fragmentation problems and management approaches in elastic optical networks: A survey", IEEE Communications Surveys & Tutorials, vol. 20, no.1, pp. 183-210, Nov. 2017 (doi: 10.1109/COMST.2017.2769102).
[83] E.E. Moghaddam, H. Beyranvand, J.A. Salehi "Resource allocation in space division multiplexed elastic optical networks secured with quantum key distribution", IEEE Journal on Selected Areas in Communications, vol. 39, no. 9, pp. 2688-2700, Mar. 2021 (doi: 10.1109/JSAC.2021.3064641).
[84] R. Goścień, M. Kucharzak, "On the efficient optimization of unicast, anycast and multicast flows in survivable elastic optical networks", Optical Switching and Networking, vol. 31, pp. 114-126, Jan. 2019 (doi: 10.1016/j.osn.2018.10.010).
[85] M.S. Aboomasoudi, A. Avokh, "Improving acceptance rate of QoS-guaranteed point-to-multipoint traffic flows in elastic optical networks", Optical Fiber Technology, vol. 59, Article Number: 102327, Oct. 2020 (doi: 10.1016/j.yofte.2020.102327).
[86] E.E. Moghaddam, H. Beyranvand, J.A. Salehi "Resource allocation in space division multiplexed elastic optical networks secured with quantum key distribution", IEEE Journal on Selected Areas in Communications, vol. 39, no. 9, pp. 2688-2700, Mar. 2021 (doi: 10.1109/JSAC.2021.3064641).
[87] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh. "Current status of the DARPA quantum network", Quantum Information and computation III, SPIE, vol. 5815, pp. 138-149, May 2005 (doi: 10.48550/arXiv.quant-ph/0503058).
[88] P. Toliver, R.J. Runser, T.E. Chapuran, M.S. Goodman, J. Jackel, S. McNown, R.J. Hughes, C.G. Peterson, K. McCabe, J.E. Nordholt, K. Tyagi, "Demonstration of 1550 nm QKD with ROADM-based DWDM Networking and the Impact of Fiber FWM", Proceeding of the Conference on Lasers and Electro-Optics, Baltimore, Maryland, United States, May 2007 (doi: 10.1109/CLEO.2007.4452689).

[89] S. Tibuleac, M. Filer. "Transmission impairments in DWDM networks with reconfigurable optical add-drop multiplexers", Journal of Lightwave Technology, vol. 28, no. 4, pp. 557-568, Feb. 2010 (doi: 10.1109/JLT.2009.2037832).
[90] T.E. Chapuran, P. Toliver, N.A. Peters, J. Jackel, M.S. Goodman, R.J. Runser, S.R. McNown, N. Dallmann, R.J. Hughes, K.P. McCabe, J.E. Nordholt, "Optical networking for quantum key distribution and quantum communications", New Journal of Physics, vol. 11, no. 10, Article Number: 105001, Oct. 2009 (doi: 10.1088/1367-2630/11/10/105001).
[91] R. Wang, R.S. Tessinari, E. Hugues-Salas, A. Bravalheri, N. Uniyal, A.S. Muqaddas, R.S. Guimaraes, T. Diallo, S. Moazzeni, Q. Wang, G.T. Kanellos, "End-to-end quantum secured inter-domain 5G service orchestration over dynamically switched flex-grid optical networks enabled by a q-ROADM", Journal of Lightwave Technology, vol. 38, no. 1, pp. 139-149, Oct. 2019 (doi: 10.1109/JLT.2019.2949864).
[92] T.A. Eriksson, T. Hirano, B.J. Puttnam, G. Rademacher, R.S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, M. Sasaki, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels", Communications Physics, vol. 2, no. 1, pp. 1-8, Jan. 2019 (doi: 10.1038/s42005-018-0105-5).
[93] K.A. Patel, J.F. Dynes, M. Lucamarini, I. Choi, A.W. Sharpe, Z.L. Yuan, R.V. Penty, A.J. Shields, "Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks", Applied Physics Letters, vol. 104, no. 5, Article Number: 051123, Feb. 2014. (doi: 10.1063/1.4864398).
[94] R. Lin, A. Udalcovs, O. Ozolins, X. Pang, L. Gan, L. Shen, M. Tang, S. Fu, S. Popov, C. Yang, W. Tong, "Telecom Compatibility Validation of Quantum Key Distribution Co-Existing with 112 Gbps /λ/core Data Transmission in Non-Trench and Trench-Assistant Multicore Fibers", Proceeding of the IEEE/ECOC, pp. 1-3, Roma, Italy, Sept. 2018 (doi: 10.1109/ECOC.2018.8535406).
[95] E. Hugues-Salas, O. Alia, R. Wang, K. Rajkumar, G.T. Kanellos, R. Nejabati, D.Simeonidou, "11.2 tb/s classical channel coexistence with dv-qkd over a 7-core multicore fiber", Journal of Lightwave Technology, vol. 38, no. 18, pp. 5064-5070, Sept. 2020 (doi: 10.1109/JLT.2020.2998053).
[96] A. Aguado, V. Martin, D. Lopez, M. Peev, J. Martinez-Mateo, J.L. Rosales, F. de la Iglesia, M. Gomez, E. Hugues-Salas, A. Lord, R. Nejabati "Quantum-aware software defined networks", 7th International Conference on Quantum Cryptography (QCrypt), United Kingdom, Sept. 2016.
[97] Y. Peng, C. Wu, B. Zhao, W. Yu, B. Liu, S. Qiao "QKDFlow: QKD based secure communication towards the openflow interface in SDN", International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystem, pp. 410-415, Hong Kong, China, Nov. 2016 (doi: 10.1007/978-981-10-3969-0_45).
[98] J.M. Merolla, Y. Mazurenko, J.P. Goedgebuer, W.T. Rhodes."Single-photon interference in sidebands of phase-modulated light for quantum cryptography", Physical Review Letters, vol. 82, no. 8, Article Number: 1656, Feb. 1999 (doi:10.1103/PhysRevLett.82.1656).
[99] A.V. Glejm, A.A. Anisimov, L.N. Asnis, Y.B. Vakhtomin, A.V. Divochiy, V.I. Egorov, V.V. Kovalyuk, A.A. Korneev, S.M. Kynev, Y.V. Nazarov, R.V. Ozhegov. "Quantum key distribution in an optical fiber at distances of up to 200 km and a bit rate of 180 bit/s", Bulletin of the Russian Academy of Sciences: Physics, vol. 78, no. 3, pp. 171-175, Mar. 2014 (doi: 10.3103/S1062873814030095).
[100] A.V. Gleim, V.I. Egorov, Y.V. Nazarov, S.V. Smirnov, V.V. Chistyakov, O.I. Bannik, A.A. Anisimov, S.M. Kynev, A.E. Ivanova, R.J. Collins, S.A. Kozlov. "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference", Optics Express, vol. 24, no. 3, pp. 2619-2633, Feb. 2016 (doi: 10.1364/OE.24.002619).
[101] J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V.G. Muñoz, J. Capmany, "Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON", Optics Express, vol. 20, no. 15, pp. 16358-16365, July 2012 (doi: 10.1364/OE.20.016358).
[102] V.V. Chistyakov, O.L. Sadov, A.B. Vasiliev, V.I. Egorov, M.V. Kompaniets, P.V. Fedchenkov, O.I. Lazo, A.E. Shevel, N.V. Buldakov, A.V. Gleim, S.E. Khoruzhnikov, "Software-defined subcarrier wave quantum networking operated by OpenFlow protocol", arXiv preprint arXiv:1709.09081, Sept. 2017 (doi:10.48550/arXiv.1709.09081).
[103] A. Aguado, E. Hugues-Salas, P.A. Haigh, J. Marhuenda, A.B. Price, P. Sibson, J.E. Kennard, C. Erven, J.G. Rarity, M.G. Thompson, A. Lord, "First Experimental demonstration of secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution", Proceeding of the 42nd European Conference on Optical Communication (ECOC), pp. 1-3, Düsseldorf, Germany, Sept. 2016 (doi:10.48550/arXiv.1604.05861).
[104] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, J. Zhang, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)", Optics Express, vol. 25, no. 22, pp. 26453-26467, Oct. 2017 (doi: 10.1364/OE.25.026453).

[105] H. Wang, Y. Zhao, Y. Li, X. Yu, J. Zhang, C. Liu, Q. Shao, "A flexible key-updating method for software-defined optical networks secured by quantum key distribution", Optical Fiber Technology,vol. 45, pp. 195-200, Nov. 2018 (doi:10.1016/j.yofte.2018.07.005).

[106] Cao Y, Zhao Y, Yu X, Wu Y,"Resource assignment strategy in optical networks integrated with quantum key distribution", Journal of Optical Communications and Networking, vol. 9, no. 11, pp. 995-1004, Nov. 2017 (doi: 10.1364/JOCN.9.000995).

[107] A. Aguado, E. Hugues-Salas, P.A. Haigh, J. Marhuenda, A.B. Price, P. Sibson, J.E. Kennard, C. Erven, J.G. Rarity, M.G. Thompson, A. Lord, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources", Journal of Lightwave Technology, vol. 35, no. 8, pp. 1357-1362, April 2017 (doi: 10.1109/JLT.2016.2646921).

[108] Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, B. Mukherjee. "Resource allocation in optical networks secured by quantum key distribution", IEEE Communications Magazine, vol. 56, no. 8, pp. 130-137, Aug. 2018 (doi: 10.1109/MCOM.2018.1700656).

[109] E. Hugues-Salas, F. Ntavou, D. Gkounis, G.T. Kanellos, R. Nejabati, D. Simeonidou, "Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks", Journal of Optical Communications and Networking, vol. 11, no. 2, pp. A209-A218, Feb. 2019 (doi: 10.1364/JOCN.11.00A209).

[110] A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez, V. Martin, "Virtual network function deployment and service automation to provide end-to-end quantum encryption", Journal of Optical Communications and Networking, vol. 10, no. 4, pp. 421-430, April 2018 (doi: 10.1364/JOCN.10.000421).

[111] Y. Cao, Y. Zhao, X. Yu, J. Zhang, "Secure virtual optical network embedding over optical networks integrated with quantum key distribution", Proceeding of the IEEE/ACP, pp. S4C-4. Guangzhou, Guangdong, China, Nov. 2017 (doi: 10.1364/ACPC.2017.S4C.4).

[112] K. Dong, Y. Zhao, X. Yu, A. Nag, J. Zhang, "Auxiliary graph based routing, wavelength, and time-slot assignment in metro quantum optical networks with a novel node structure", Optics Express, vol. 28, no. 5, pp. 5936-5952, Mar. 2020 (doi:10.1364/OE.380329).

[113] X. Yu, Y. Wang, L. Lu, Y. Zhao, H. Zhang, J. Zhang "VON embedding in elastic optical networks (EON) integrated with quantum key distribution (QKD)", Optical Fiber Technology, vol. 63, Article Number: 102486, May 2021 (doi: 10.1016/j.yofte.2021.102486).

[114] C. Elliott, "The DARPA quantum network", Quantum Communications and Cryptography, CRC Press, pp. 91-110, Oct. 2018 (doi: 10.1201/9781420026603.ch4).

[115] A. Poppe, M. Peev, O.Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna", International Journal of Quantum Information, vol. 6, no. 02, pp. 209-218, April 2008 (doi: 10.48550/arXiv.0804.0122).

[116] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, "Using quantum key distribution for cryptographic purposes: a survey", Theoretical Computer Science, vol. 560, pp. 62-81, Dec. 2014 (doi: 10.48550/arXiv.quant-ph/0701168).

[117] M. Dianati, R. Alléaume, "Transport layer protocols for the secoqc quantum key distribution (QKD) network", Proceeding of the IEEE/LCN, pp. 1025-1034, Dublin, Ireland Oct. 2007 (doi: 10.1109/LCN.2007.107).

[118] W. Chen, Z.F. Han, T. Zhang, H. Wen, Z.Q. Yin, F.X. Xu, Q.L. Wu, Y. Liu, Y. Zhang, X.F. Mo, Y.Z. Gui, "Field experiment on a “star type” metropolitan quantum key distribution network", IEEE Photonics Technology Letters, vol. 21, no. 9, pp. 575-577, Feb. 2009 (doi: 10.1109/LPT.2009.2015058).

[119] A. Mirza, F. Petruccione, "Realizing long-term quantum cryptography", JOSA B, vol. 27, no. 6, pp. A185-A188, June 2010 (doi:10.1364/JOSAB.27.00A185).

[120] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat. "Long-term performance of the SwissQuantum quantum key distribution network in a field environment", New Journal of Physics, vol. 13, no. 12, Article Number: 123001, Dec. 2011 (doi:10.48550/arXiv.1203.4940).

[121] D. Lancho, J. Martinez, D. Elkouss, M. Soto, V. Martin, "QKD in standard optical telecommunications networks", Proceeding of the Springer/Quantum Comunication and Quantum Networking, pp. 142-149 Berlin, Heidelberg, Oct. 2009 (doi: 10.48550/arXiv.1006.1858).

[122] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han. "Field experiment on a robust hierarchical metropolitan quantum cryptography network", Chinese Science Bulletin, vol. 54, no. 17, pp. 2991-2997, Sept. 2009 (doi: 10.1007/s11434-009-0526-3).

[123] S. Wang, W. Chen, Z.Q. Yin, Y. Zhang, T. Zhang, H.W. Li, F.X. Xu, Z. Zhou, Y. Yang, D.J. Huang, L.J. Zhang, "Field test of wavelength-saving quantum key distribution network", Optics Letters, vol. 35, no. 14 pp. 2454-2456, July 2010 (doi:10.1364/OL.35.002454).

[124] M. Travagnin, A. Lewis, "Quantum Key Distribution in-field implementations", Publications Office of the European Union, 2019 (doi: 10.2760/38407).
[125] S. Wang, W. Chen, Z.Q. Yin, H.W. Li, D.Y. He, Y.H. Li, Z. Zhou, X.T. Song, F.Y. Li, D. Wang, H. Chen."Field and long-term demonstration of a wide area quantum key distribution network", Optics Express, vol. 22, no. 18, pp. 21739-21756, Sept. 2014 (doi:10.1364/OE.22.021739).
[126] R.Courtland "China's 2,000-km quantum link is almost complete [News]", IEEE Spectrum, vol. 53, no. 11, pp. 11-12, Oct. 2016 (doi: 10.1109/MSPEC.2016.7607012).
[127] V. Martin, A. Aguado, P. Salas, A.L. Sanz, J.P. Brito, D.R. Lopez, V. López, A. Pastor, J. Folgueira, H.H. Brunner, S. Bettelli, "The Madrid quantum network: a quantum-classical integrated infrastructure", Proceeding of the Photonic Networks and Devices, pp. QtW3E-5, Burlingame, California, United States, Jul/Aug. 2019 (doi: 10.1364/NETWORKS.2019.QtW3E.5).
[128] Y.L. Tang, H.L. Yin, Q. Zhao, H. Liu, X.X. Sun, M.Q. Huang, W.J. Zhang, S.J. Chen, L. Zhang, L.X. You, Z. Wang, "Measurement-device-independent quantum key distribution over untrustful metropolitan network", Physical Review X, vol. 6, no. 1, Article Number: 011024, Mar. 2016 (doi: 10.1103/PhysRevX.6.011024).
[129] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, T. Tsurumaru, "Implementation of continuous-variable quantum key distribution with discrete modulation", Quantum Science and Technology, vol. 2, no. 2, Article Number: 024010, June 2017 (doi: 10.1088/2058-9565/aa7230).
[130] V. Martín, A. Aguado, J.P. Brito, A.L. Sanz, P. Salas, D.R. López, V. López, A. Pastor-Perales, A. Poppe, M. Peev. "Quantum aware SDN nodes in the Madrid quantum network", Proceeding of the IEEE/ICTON, pp. 1-4, Angers, France, July 2019 (doi: 10.1109/ICTON.2019.8840338).
[131] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li "Continuous-variable QKD over 50 km commercial fiber", Quantum Science and Technology, vol. 4, no. 3, Article Number: 035006, May 2019 (doi:10.48550/arXiv.1709.04618).
[132] T.Y. Chen, X. Jiang, S.B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.K. Chen, W.Y. Liu, H.F. Zhang, K. Cui, H. Liang, X.G. Li, Y. Mao, L.J. Wang, S.B. Feng, Q. Chen, Q. Zhang, L. Li, N.L. Liu, C.Z. Peng, X. Ma, Y. Zhao, J.W. Pan, “Implementation of a 46-node quantum metropolitan area network,” npj Quantum Inf, vol. 7, no. 134, Sept. 2021 (doi: 10.1038/s41534-021-00474-3).
[133] J. F. Dynes, A. Wonfor, W. W.S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.P. Elbers, H. Greißer, I. H. White, R. V. Penty, A. J. Shields, “Cambridge quantum network”, npj Quantum Inf, vol. 5, no. 101, Nov. 2019 (doi: 10.1038/s41534-019-0221-4).
[134] A. Wonfor, C. White, A. Bahrami, J. Pearse, G. Duan, A. Straw, T. Edwards, T. Spiller, R. Penty, A. Lord, “Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5x100G DWDM transmission system”, Proceeding of the IEEE/ ECOC 2019, Dublin, Ireland, Sept. 2019 (doi: 10.1049/cp.2019.0962)
[135] N. Gisin, R.Thew, "Quantum communication", Nature photonics, vol. 1, no. 3, pp. 165-171, Mar. 2007 (doi: 10.48550/arXiv.quant-ph/0703255)
[136] M. Lucamarini, K.A. Patel, J.F. Dynes, B. Fröhlich, A.W. Sharpe, A.R. Dixon, Z.L. Yuan, R.V. Penty, A.J. Shields. "Efficient decoy-state quantum key distribution with quantified security", Optics Express, vol. 21, no. 21, pp. 24550-24565, Oct. 2013 (doi:10.1364/OE.21.024550).
[137] C.Z. Peng, J. Zhang, D. Yang, W.B. Gao, H.X. Ma, H. Yin, H.P. Zeng, T. Yang, X.B. Wang, J.W. Pan "Experimental long-distance decoy-state quantum key distribution based on polarization encoding", Physical Review Letters, vol. 98, no. 1, Article Number: 010505, Jan. 2007 (doi: 10.48550/arXiv.quant-ph/0607129).
[138] X. Ma, C.H. Fung, H.K. Lo, "Quantum key distribution with entangled photon sources", Physical Review A, vol. 76, no. 1, July 2007 (doi: 10.48550/arXiv.quant-ph/0703122).
[139] I. Marcikic, A. Lamas-Linares, C. Kurtsiefer, "Free-space quantum key distribution with entangled photons", Applied Physics Letters, vol. 89, no. 10, Article Number: 101122, Sept. 2006 (doi: 10.48550/arXiv.quant-ph/0606072).
[140] X. Liu, X. Yao, H. Wang, H. Li, Z. Wang, L. You, Y. Huang, W. Zhang, "Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km", Applied Physics Letters, vol. 114, no. 14, Article Number: 141104, April 2019 (doi:10.48550/arXiv.1901.06662).
[141] X. Liu, X. Yao, R. Xue, H. Wang, H. Li, Z. Wang, L. You, X. Feng, F. Liu, K. Cui, Y. Huang, "An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution", APL Photonics, vol. 5, no. 7, Article Number: 076104, July 2020 (doi:10.1063/5.0002595).
[142] S. Wehner, D. Elkouss, R. Hanson, "Quantum internet: A vision for the road ahead", Science, vol. 362, no. 6412, Article Number: eaam9288, Oct. 2018 (doi: 10.1126/science. aam9288).

[143] S. Wengerowsky, S.K. Joshi, F. Steinlechner, H. Hübel, R. Ursin. "An entanglement-based wavelength-multiplexed quantum communication network", Nature, vol. 564, no. 7735, pp. 225-228, Dec. 2018 (doi:10.48550/arXiv.1801.06194).
[144] I. Ali-Khan, C.J. Broadbent, J.C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states", Physical Review Letters, vol. 98, no. 6, Article Number: 060503, Feb. 2007 (doi:10.1103/PhysRevLett.98.060503).
[145] D. Bunandar, Z. Zhang, J.H. Shapiro, D.R. Englund, "Practical high-dimensional quantum key distribution with decoy states", Physical Review A, vol. 91, No. 2, Article Number: 022336, Feb. 2015 (doi:10.48550/arXiv.1411.1070).
[146] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J.H. Shapiro, "High-dimensional quantum key distribution using dispersive optics", Physical Review A, vol. 87, no. 6, Article Number: 062322, June 2013 (doi:10.48550/arXiv.1210.4501).
[147] C. Lee, Z. Zhang, G.R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R.D. Horansky, V.B. Verma, A.E. Lita, "Entanglement-based quantum communication secured by nonlocal dispersion cancellation", Physical Review A, vol. 90, no. 6, Article Number: 062331, Dec. 2014 (doi:10.1103/PhysRevA.90.062331).
[148] X. Liu, R. Xue, Y. Huang, W. Zhang, "Fully connected entanglement-based quantum communication network without trusted node", Proceeding of the OFC, pp. F4E-4, Washington, DC, United States, June. 2021 (doi: 10.1364/OFC.2021.F4E.4).
[149] J.Y. Liu, X. Liu, W. Zhang, Y.D. Huang, "Impact of fiber dispersion on the performance of entanglement-based dispersive optics quantum key distribution", Journal of Electronic Science and Technology, vol. 19, no. 4, Article Number: 100119, Dec. 2021 (doi: 10.1016/j.jnlest.2021.100119).
[150] R. Sabbaghi-Nadooshan, "Evolutionary QCA Universal and Testable Gate", International Journal of Smart Electrical Engineering, vol. 9, no. 02, pp. 83-88, June 2020 (doi: 20.1001.1.22519246.2020.09.02.6.0).
[151] M. Shirichian, R. Akbari-Hasanjani, R. Sabbaghi-Nadooshan, "Energy Analysis of Metal QCA Circuits Behavior Based on Particle-Wave Duality", IETE Journal of Research, pp. 1-11, Mar. 2022 (doi: 10.1080/03772063.2022.2048701).
[152] A. Navidi, R. Sabbaghi-Nadooshan, M. Dousti, "Introducing an Innovative D Flip-Flop for Designing Quaternary QCA Register", Journal of Intelligent Procedures in Electrical Technology, vol. 13, no. 49, pp. 91-101, May 2021 (doi: 20.1001.1.23223871.1401.13.49.6.5).
[153] SS. Hashemipour, K. Navi, "A Smart Four-Input Minority Gate Based on QCA Technology", International Journal of Smart Electrical Engineering, vol. 10, No. 01, pp. 33-37, Mar. 2021 (doi: 10.30495/IJSEE.2-021.682521).
[154] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S.X. Ng, L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet", IEEE Communications Surveys and Tutorials, vol. 24, no. 2, pp. 839-894, Jan. 2022 (doi: 10.1109/COMST.2022.3144219)
[155] Quantum networking: deployment, components and opportunities, Inside Quantum Technology, 2017.

زیرنویس‌ها

1. Metrology
2. Quantum sensors
3. Quantum cryptography
4. Superposition
5. Entanglement
6. Quantum key distribution network (QKDN)
7. Device-dependent QKD
8. Alice
9. Bob
10. Charles bennett
11. Gilles brassard
12. Decoy state
13. Measurement-device-independent QKD (MDI-QKD)
14. Weak coherent pulse (WCP)
15. Twin-field QKD (TF-QKD)
16. One-time pad (OTP)
17. XOR
18. Advanced Encryption Standard (AES)
19. Data encryption standard

20. Trusted-node and untrusted-node QKD network
21. Optical nodes network
22. Optical process control (OPC)
23. Laser source suite
24. Private Ethernet
25. VPN
26. Internet protocol suit (IPsec)
27. Raw key
28. Secret key
29. Internet key exchange protocol (IKE)
30. Triple data encryption standard
31. Trusted node
32. Key relays
33. Quantum back bone (QBB)
34. Bennet-Brassard-1984(BB84)
35. Medoid
36. IP
37. Active optical network (AON)
38. Elastic optical networks (EON)
39. Passive optical network (PON)
40. All optical network (AON)
41. Dense wavelength-division multiplexing (DWDM)
42. Space-division multiplexing (SDM)
43. UKQNtel
44. BT
45. Slice
46. Gigabit passive optical network (GPON)
47. Ethernet passive optical network (EPON)
48. Optical line terminal (OLT)
49. Optical splitter
50. Optical network unite (ONU)
51. Upstream
52. LAN
53. WAN
54. Reconfigurable optical add-drop multiplexer (ROADM)
55. Circulator
56. q-ROADM
57. Quantum Bit Error Rate (QBER)
58. Secret key rate (SKR)
59. Software defined network (SDN)
60. Quantum communication (QC)
61. Openflow
62. Stand subcarrier wave (SCW)
63. FPGA
64. Secure socket layer (SSL)
65. Network function virtualization (NFV)
66. Virtual network function
67. Virtual optical network (VON)
68. MQON
69. Optical network function virtualization (ONFV)
70. Virtual optical network embedding (VONE)
71. Discrete-variable quantum key distribution (DV-QKD)
72. Continuous-variable quantum key distribution (CV-QKD)
73. MagiQ technologies
74. ID Quantique
75. QuintessenceLabs
76. SeQureNet
77. Toshiba
78. HP

79. IBM
80. Mitsubishi
81. NEC
82. NTT
83. Defense advanced research project agency (DARPA)
84. BBN Technologies
85. Secure Communication based on Quantum Cryptography (SECOQC)
86. Quantum city
87. ID Quantique
88. Quantum city
89. Batelle
90. Quantum xchange
91. Telefónica de España
92. Zayo
93. Gazprombank
94. Sberbank
95. Dispersive optics quantum key distribution (DO-QKD)
96. Post-processing
97. U.K. national quantum technologies program (UKNQTP)
98. Airbus
99. BT
100. Google
101. Lockheed martin
102. Raytheon
103. Inside quantum technology (IQT)