«علوم و فناوری‌های پدافند نوین»

سال پانزدهم، شماره ۱، بهار ۱۴۰۳؛ ص ۲۶-۱۵

علمی- پژوهشی

ارائه و شبیه‌سازی یک طرح کارآمد برای توزیع کلید کوانتومی محیطی در فیبر نوری به طول بالاتر از ۱۵۰ کیلومتر

علی مهری تونابی

استادیار دانشگاه صنعتی مالک‌اشتر، شاهین شهر،ایران

(دریافت: ۱۴۰۲/۱۲/۲۰، بازنگری: ۱۴۰۳/۰۲/۱۶، پذیرش: ۱۴۰۳/۰۲/۲۲، انتشار: ۱۴۰۳/۰۳/۱۱)

چکیده

مسئله دستیابی به نرخ کلید امن بالاتر و مسافت توزیع کلید طولانی‌تر، همواره دغدغه اصلی محققین در زمینه توزیع کلید کوانتومی (QKD) بوده است. به دلیل اتلاف حالت‌های کوانتومی، انجام QKD در فیبر نوری با نرخ کلید امن از مرتبه $kbit/s$ و در مسافت‌های بالاتر از km ۵۰ با چالش‌های فراوانی روبرو است. در این مقاله، طراحی و شبیه‌سازی یک سامانه QKD کارآمد با استفاده از قطعات تمام فیبری ارائه‌شده است که قابلیت QKD با نرخ مطلوب تا مسافت km ۱۷۰ را دارد. این طرح، امکان QKD در فیبر نوری تک‌مد به طول km ۱۰۰، با نرخ خطای بیت کوانتومی (QBER) زیر ۳٪، نرخ کلید غربال‌شده $kbit/s$ ۶ و نرخ کلید امن $kbit/s$ ۴/۶ را فراهم می‌کند. کلیه طراحی‌ها و شبیه‌سازی‌ها باملاحظه محدودیت‌های تجربی و با استفاده از پارامترهای فیزیکی هماهنگ با ادوات در دسترس انجام‌شده است، به‌گونه‌ای که در صورت پیاده‌سازی احتمالی سامانه، نتایج حاصل از این شبیه‌سازی‌ها به نتایج تجربی کاملاً نزدیک باشد. توسعه این طرح می‌تواند یک گزینه مناسب برای دستیابی به سامانه‌های QKD تجاری و صنعتی بومی باشد.

کلیدواژه‌ها: توزیع کلید کوانتومی، QKD، پروتکل BB84، تک فوتون، فاز، قطبش، نرخ کلید

Present and Simulation of an Efficient Scheme for Environmental Quantum Key Distribution in Optical Fiber Longer than 150 km

A. Mehri Toonabi

Malek Ashtar University of Technology, Shahin-Shahr, Iran

(Received:2024/03/10, Revised: 2024/05/05, Accepted: 2024/05/11, Published: 2024/05/31)

DOR: https://dorl.net/dor/20.1001.1.26762935.1402.14.3.1.5

Abstract

The problem of achieving a higher secure key rate and a larger key distribution distance has always been the main concern of researchers in the field of quantum key distribution (QKD). Due to the loss of quantum states, there are many challenges in performing QKD in optical fiber with a secure key rate of the order of $kbit/s$ and lengths higher than 50 km. This paper presents the design and simulation of an efficient QKD system using all-fiber components, which has the capability of QKD at a reasonable rate up to a distance of 170 km. This design enables QKD in 100 km long single-mode optical fiber, with a quantum bit error rate (QBER) below 3%, a sifted key rate of 6 $kbit/s$, and a secure key rate of 4.6 $kbit/s$. All the designs and simulations have been done considering the experimental limitations and using physical parameters in harmony with the available tools, so that in case of possible implementation of the system, the results of these simulations are quite close to the experimental data. The development of this scheme can be a suitable candidate for achieving native commercial and industrial QKD systems.

Keywords: Quantum Key Distribution, QKD, BB84 Protocol, Single-Photon, Phase, Polarization, Key Rate

*Corresponding Author E-mail: amtoonabi@gmail.com

۱. مقدمه

توزیع کلید کوانتومی[1] (QKD) به‌عنوان عمومی‌ترین و توسعه‌یافته‌ترین فناوری کوانتومی، دارای کاربردهای متعدد در حوزه امنیت اطلاعات و ارتباطات است. برخلاف رمزهای کلاسیک، امنیت QKD بر مبنای قوانین پایه‌ای مکانیک کوانتوم و نه بر مبنای پیچیدگی‌های محاسباتی تضمین می‌شود [۱,۲]. سامانه‌های QKD، سامانه‌های پیچیده‌ای متشکل از سخت‌افزار (ادوات متنوع اپتیکی، لیزری، الکترواپتیکی و الکتریکی) و نرم‌افزار (پروتکل‌ها و روش‌های مرسوم پساپردازش کلاسیک به‌منظور استخراج کلید امن) هستند. طراحی و تحلیل این سامانه‌ها نیاز به مهارت در زمینه‌های متفاوتی همچون مکانیک کوانتومی، اپتیک کلاسیک و کوانتومی، نظریه اطلاعات، آمار و مخابرات دارد.

مهم‌ترین موضوع در هر سامانه QKD، امنیت آن است [۳]. مسئله دستیابی به نرخ کلید امن بالاتر و مسافت توزیع کلید طولانی‌تر، دغدغه اصلی محققین فعال در حوزه QKD است [۶-۴]. به دلیل نواقص و ناکاملی‌های ادوات و وجود محدودیت‌های تجربی متعدد، انجام QKD نقطه‌به‌نقطه در فیبر نوری با نرخ کلید امن از مرتبه چند $kbit/s$ در مسافت‌های بالاتر از km ۵۰ با چالش‌های فراوانی روبرو است و همواره گروه‌های مختلفی در تلاش برای یافتن راه‌حل‌های جدید برای مقابله با این چالش‌ها بوده‌اند [۷]. استفاده از پروتکل‌های "حالت فریب"[2] [۸,۹]، "مستقل از ادوات"[3] [۱۰]، میدان دوقلو[4] [۱۱]، "مبتنی بر تراشه"[5] [۱۲]، با "متغیرهای پیوسته"[6] [۱۳]، با "حالت‌های کوانتومی چندبعدی"[7] [۱۶-۱۴] و بهینه‌شده در بخش تولید [۱۷] و آشکارسازی [۱۸] حالت‌های کوانتومی، نمونه‌های مهمی از این تلاش‌ها هستند.

ازلحاظ ساختاری، هر سامانه QKD از سه بخش اصلی تشکیل می‌شود: ارسال‌کننده (آلیس[8])، کانال ارتباطی کوانتومی (فیبر نوری یا هوای آزاد) و دریافت‌کننده (باب[9]). در اغلب سامانه‌های QKD تجاری، صنعتی و شهری، از کانال کوانتومی فیبر نوری تک مد استاندارد استفاده می‌شود [۱۹]. به‌طورکلی سامانه‌های QKD مبتنی بر فیبر نوری متداول‌تر و پرکاربردتر از همتاهای فضای آزاد خود هستند؛ زیرا در آن‌ها از قطعات ارتباطی استاندارد استفاده می‌شود. فیبر نوری، کانال کوانتومی را در مقابل نورهای زمینه و تلاطم (آشوب)[10] [۲۰]، که در سامانه‌های QKD هوای آزاد از مهم‌ترین و آزاردهنده‌ترین منابع ایجاد نویز به شمار می‌روند [۲۱,۲۲]، حفظ می‌کند. در سامانه‌های فیبری برخلاف سامانه‌های هوای آزاد، سیگنال‌های کوانتومی محدود به طی یک مسیر مستقیم در خط دید پایگاه‌های آلیس و باب نیستند، بلکه در داخل فیبر نوری و مطابق با پیکربندی آن هدایت می‌شوند. سامانه‌های QKD فیبری را در هر ساعت از شبانه‌روز و تحت شرایط محیطی مختلف می‌توان استفاده کرد.

کانال فیبر نوری در کنار مزایای فراوانی که ایجاد می‌کند، دارای یک عیب برجسته است: فیبرها محیط‌های دوشکستی[11] هستند و بنابراین به هنگام استفاده از طرح‌واره‌های کدگذاری قطبشی، با ایجاد تغییرات غیرقابل‌اجتناب و کاتوره‌ای در قطبش، منجر به افزایش نرخ خطای بیت کوانتومی[12] (QBER) و بروز مشکلات تجربی و عملیاتی در سامانه خواهند شد. مشکل دوشکستی بودن فیبرها برای کارکردن در آزمایشگاه و در مقیاس‌های زمانی کوتاه، چندان جدی نیست. ولی وقتی قرار است یک چیدمان پایدار در دنیای واقعی و برای انجام QKD در فواصل طولانی برپا شود، به‌ناچار تغییرات القایی گرمایی یا مکانیکی در دوشکستی فیبر، می‌طلبد که به‌جای رمزنگاری بر اساس قطبش فوتون‌ها، از درجه آزادی دیگری از فوتون‌ها استفاده شود. راه‌حلی که عموماً برای این منظور به کار گرفته می‌شود، استفاده از فاز فوتون‌ها و انجام کدگذاری روی فاز اپتیکی به‌جای کدگذاری روی قطبش فوتون‌ها است. در چیدمان‌های مبتنی بر فاز، معمولاً از تداخل‌سنج ماخ - زندر[13] (MZI) برای کد کردن فوتون‌ها از طریق تغییردادن فاز اپتیکی در هر دو بخش آلیس و باب استفاده می‌شود [۲۳,۲۴]. در حالت کلی می‌توان گفت که کدگذاری روی قطبش برای انتقال اطلاعات در هوای آزاد مناسب‌تر از کدگذاری روی فاز فوتون‌ها است، ولی در فیبر نوری این قضیه کاملاً برعکس است.

در این مقاله، طراحی و شبیه‌سازی یک سامانه QKD جهت انجام QKD فیبری کارآمد در مسافت‌های km ۱۵۰ و بالاتر از آن، با استفاده از قطعات تمام فیبری و با کمک کدگذاری روی فاز فوتون‌ها توسط تداخل‌سنج‌های ماخ-زندر با نمایانی کوانتومی[14] بالا ارائه شده است.

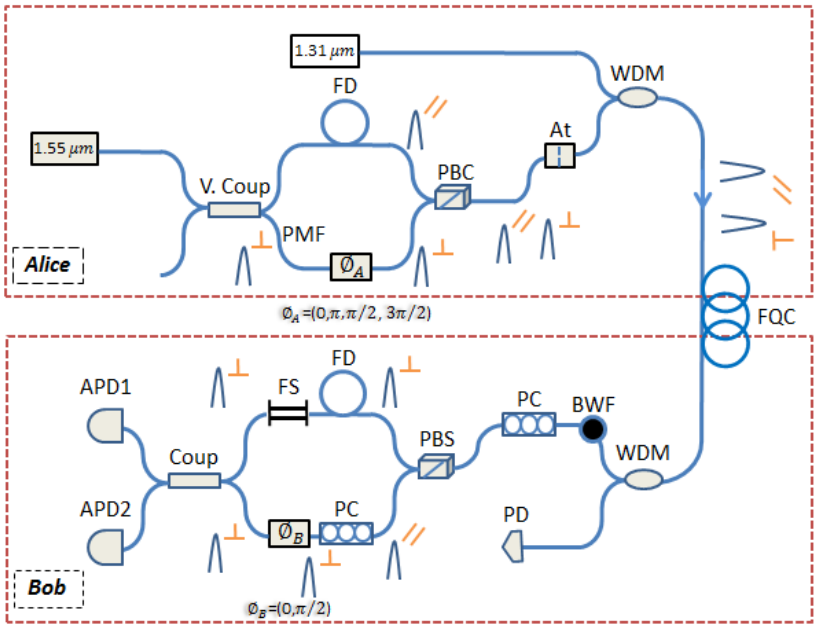
۲. روش تحقیق

در این بخش، طرح پیشنهادی جهت انجام QKD فیبری کارآمد در مسافت‌های km ۱۵۰ و بالاتر از آن معرفی و نحوه اجرای پروتکل QKD در طرح پیشنهادی بیان‌شده است.

[1] Quantum Key Distribution (QKD)
[2] Decoy states
[3] Device-independent
[4] Twin-field
[5] Chip-based
[6] Continuous-variables
[7] High-dimensional quantum states
[8] Alice
[9] Bob
[10] Turbulence
[11] Birefrigence
[12] Quantum Bit Error Rate (Qber)
[13] Mach-Zehnder Interferometer (Mzi)
[14] Quantum Visibility

۲-۱. معرفی طرح پیشنهادی

به دلیل تغییرات غیرقابل‌اجتناب و کاتوره‌ای قطبش در فیبر نوری، در سامانه‌های QKD فیبری عمدتاً از فاز فوتون‌ها و پدیده تداخل‌سنجی برای آماده‌سازی (کدگذاری) و اندازه‌گیری (کدگشایی) حالت‌های کوانتومی استفاده می‌شود [۲۳].



شکل ۱. طرح پیشنهادی جهت انجام QKD محیطی مبتنی بر تداخل‌سنجی بر اساس پروتکل BB84 استاندارد فازی، با استفاده از قطعات تمام فیبری و در کانال کوانتومی فیبر نوری.
(Coup: coupler; V. Coup: variable coupler; FD: fiber delay; PMF: Polarization Maintaining Fiber; $\emptyset_A$: Alice's phase modulator; At: attenuator; WDM: wavelength division multiplexer; FQC: fiber quantum channel; PD: photo detector; BWF: Bandpass Wavelength Filter ; PC: polarization controller; PBC/S: polarization beam Combiner/splitter; $\emptyset_B$: Bob's phase modulator; FS: fiber stretcher; APD: avalanche photodiode.)

طرح پیشنهادی جهت انجام QKD محیطی با استفاده از قطعات تمام فیبری و در کانال کوانتومی فیبر نوری، در شکل (۱) نشان‌داده‌شده است. همانند اغلب سامانه‌های QKD فیبری، در این طرح نیز از مدوله‌سازی فاز توسط تداخل‌سنج‌های ماخ - زندر نامتوازن، با اختلاف طول بازوهای کوتاه و بلند (Δl) به‌اندازه حدود m ۱-۲ متر، برای اجرای QKD در قالب پروتکل BB84 استاندارد فازی استفاده می‌شود.

به کیوبیت‌هایی که با استفاده از تداخل‌سنج‌ها تولید می‌شوند، کیوبیت‌های زمان - انبارک [1] گفته می‌شود. در حالت کلی، یک فوتون پس از عبور از یک تداخل‌سنج نامتوازن با بازوی کوتاه s و بلند l، در یک حالت برهم‌نهی از دو زمان متفاوت s یا l خواهد بود. بنابراین اگر یک مدولاتور الکترواپتیکی [2] (EOM) در بازوی کوتاه تداخل‌سنج آلیس، فاز $\emptyset_A$ را به فوتون اعمال کند، حالت کوانتومی در انتهای تداخل‌سنج را می‌توان به‌صورت $|l\rangle + e^{i\emptyset_A}|s\rangle$ نشان داد. سیگنال کوانتومی در بخش باب نیز از یک تداخل‌سنج نامتوازن مشابه با تداخل‌سنج آلیس عبور می‌کند و به باب این امکان را می‌دهد که با کمک یک EOM، پایه‌های اندازه‌گیری ویژه‌ای را انتخاب و فاز $\emptyset_B$ را در بازوی کوتاه خود به فوتون اعمال کند. توجه شود که برای استفاده از EOM به‌عنوان مدولاتور فاز، باید از نوری استفاده کرد که دارای قطبش خطی در راستای محور اپتیکی بلور باشد و ولتاژ مناسب برای تغییر فاز به‌اندازه دلخواه را به بلور اعمال کرد.

اگر اختلاف طول بازوهای کوتاه و بلند تداخل‌سنج‌های آلیس و باب به ترتیب Δl_A و Δl_B باشد، در حالت ایده‌آل باید $s_A = s_B$ و $l_A = l_B$. بنابراین $\delta l = \Delta l_A - \Delta l_B = 0$. بنابراین حالت برهم‌نهی در انتهای تداخل‌سنج باب به‌صورت زیر خواهد بود:

$$|\psi\rangle = e^{i\emptyset_A}|s_A l_B\rangle + e^{i\emptyset_B}|l_A s_B\rangle \propto |s_A l_B\rangle + e^{i(\emptyset_B-\emptyset_A)}|l_A s_B\rangle \quad (۱)$$

برای اجرای سامانه پیشنهادی، تَپ‌های با طول‌موج μm ۱/۵۵ در تضعیف‌گر (At) به‌گونه‌ای تضعیف می‌شوند که به‌طور میانگین

[1] Time-Bin Qubit
[2] Electro-Optical Modulator (Eom)

۰/۱ فوتون در هر دوره زمان‌بندی[1] از زیرسامانه آلیس خارج شود. با استفاده از یک جفت‌کننده متغیر (V.Coup) که در ابتدای تداخل‌سنج آلیس قرار دارد، نسبت شدت پالس مرجع (که از بازوی بلند آلیس عبور می‌کند) به پالس کد شده (که از بازوی کوتاه آلیس عبور می‌کند) روی ۱:۱/۶ تنظیم می‌شود. بنابراین هر سیگنال کد شده به‌طور میانگین دارای ۰/۰۴ فوتون خواهد بود. از پالس‌های با طول‌موج μm ۱/۳۱ که در شدت بالا هستند، برای زمان‌بندی سامانه استفاده می‌شود. این پالس‌ها، به‌عنوان مراجع زمانی، توسط یک ترکیب‌کننده تقسیم طول‌موج (WDM) با پالس‌های سیگنال ترکیب می‌شوند و در ادامه، در زیرسامانه باب، توسط یک WDM دیگر از هم جدا می‌شوند.

مطابق شکل (۱)، با به‌کارگیری یک پرتوترکیب قطبشی (PBC)، یک کنترل‌کننده قطبش (PC) و یک پرتوشکاف قطبشی (PBS)، فوتون‌هایی که از بازوی کوتاه آلیس عبور کرده‌اند لزوماً از بازوی بلند باب می‌گذرند و برعکس. بنابراین مسیرهای غیرتداخلی کوتاه-کوتاه و بلند-بلند توسط خود سامانه حذف می‌شوند و پارامتر غربال‌گری پروتکل ۲ برابر می‌شود (از ۲۵٪ به ۵۰٪ افزایش می‌یابد).

کانال کوانتومی برای تمام مسیرهای تداخلی یکسان است و فوتون‌ها راه نوری یکسانی را در بخشی از سامانه که نسبت به تغییرات محیطی حساس است می‌پیمایند؛ بنابراین اگر تغییرات در فیبرها کندتر از اختلاف زمانی دو مسیر کوتاه و بلند تداخل-سنج آلیس (حدود ns ۱۰-۵ معادل اختلاف طول m ۲-۱) باشد، فوتون‌های تمام مسیرهای تداخلی شرایط محیطی یکسانی را تجربه می‌کنند.

به‌منظور اطمینان از تمیزناپذیری فوتون‌ها در مسیرهای مختلف و ایجاد تداخل بین آن‌ها، قطبش حالت‌هایی که از مسیرهای تداخلی می‌گذرند باید مشابه باشد. به‌عبارت‌دیگر، هم-پوشانی قطبشی بین مسیرهای تداخلی در آخرین پرتو شکاف باید تاحدامکان بزرگ باشد؛ بنابراین بازوهای کوتاه و بلند هریک از تداخل‌سنج‌ها و نیز کانال کوانتومی بین آلیس و باب می‌بایست تغییر قطبش‌های یکسانی بر روی دو حالت زمانی ایجاد کنند. عملکرد بازوهای تداخل‌سنج از این نظر حساسیت بیش‌تری دارد. برای حصول اطمینان از برقراری این شرط، از ادوات دست‌کاری و کنترل قطبش در هر دو بخش آلیس و باب استفاده‌شده است. خوشبختانه تغییر قطبش در فیبرهای کوتاه مربوط به بازوهای تداخل‌سنج که دمای آن‌ها ثابت نگه داشته می‌شود و هیچ‌گونه فشار و تنشی را نیز تحمل نمی‌کنند، نسبتاً پایدار و ثابت است؛ بنابراین تنظیمات قطبش لازم نیست خیلی سریع انجام گیرد.

در فیبرهای نوری تک مد، پاشندگی مد قطبشی[2] (PMD) و پاشندگی رنگی[3] (CD) (گاهی پاشندگی زمانی نیز نامیده می-شود) حائز اهمیت است؛ بنابراین می‌توان کل پاشندگی در کانال فیبری را به‌صورت $\Delta t_{fiber} = (\Delta t_{PMD}{}^2 + \Delta t_{CD}{}^2)^{1/2}$ محاسبه کرد، که PMD ضریب پاشندگی مد قطبشی و CD ضریب پاشندگی رنگی در فیبر نوری است. با در نظر گرفتن کانال کوانتومی به‌صورت یک فیبر نوری تک‌مد با ضریب تلفات $\alpha \approx 0.15\ dB/km$، ضریب پاشندگی مد قطبشی PMD تقریباً $ps/\sqrt{km}$ ۰/۰۵ و ضریب پاشندگی رنگی CD تقریباً $ps/nm.\sqrt{km}$ ۲۰، آنگاه به‌عنوان نمونه، برای طول km ۱۰۰ از این فیبر، پاشندگی مد قطبشی Δt_{PMD} و پاشندگی رنگی Δt_{CD} فیبر به ترتیب ps ۰/۵ و ps ۲۰۰ خواهد بود. بنابراین کل پاشندگی کانال Δt_{fiber} تقریبا ps ۲۰۰ به دست می‌آید. اگر طول پالس لیزر FWHM تقریبا ps ۱۰ و زمان گیجی[4] (لغزش زمانی) آشکارساز و پردازشگر الکترونیکی آن هرکدام حدود ps ۱۰۰ باشد، پهنای پنجره زمانی آشکارساز t_w با رابطه زیر محدود خواهد شد:

$$t_w > Jitter\ time_{detector} + Jitter\ time_{processor} + \Delta t_{fiber} + FWHM_{source} \approx 410\ ps$$

یعنی به‌منظور تفکیک و آشکارسازی مطلوب پالس‌های ارسال‌شده در کانال فیبر نوری به طول km ۱۰۰، لازم است پهنای پنجره زمانی آشکارساز حداقل به‌اندازه ps ۴۱۰ باشد وگرنه پالس‌ها قابل‌تفکیک نخواهند بود. انتخاب یک آشکارساز تک‌فوتون با پهنای پنجره زمانی ns ۱ برای تحقق این شرط کفایت خواهد کرد. با این داده‌ها می‌توان به بیشینه نرخ تکرار $f_{rep} < 1/(2t_w)$ تقریباً GHz ۱/۲ برای پالس‌های لیزر دست یافت. ازآنجاکه در نرخ تکرارهای خیلی بالا نمی‌توان پس‌پالس آشکارسازها را نادیده گرفت، در اینجا برای این‌که بتوان از پس‌پالس صرف‌نظر کرد، نرخ تکرار پالس‌های لیزر MHz ۱۰۰ در نظر گرفته‌شده است. در این صورت، فاصله زمانی هر دو پالس پشت سر هم $\mathcal{T} = 1/f_{rep}$ که دوره پالس نامیده می‌شود، ns ۱۰ خواهد بود. بنابراین لازم است آشکارساز در هر دوره، ns ۱ باز و حدود ns ۹ بسته باشد.

در حالت استفاده از یک لیزر پالسی با طول‌موج مرکزی λ_0 برابر با nm ۱۵۵۰ (معادل فرکانس مرکزی $\nu_0 = c/\lambda_0$ برابر با THz ۱۹۳/۴ که c سرعت فوتون‌ها است) و پهنای طیفی (یا پهنای خط) $\Delta\lambda$ تقریبا nm ۰/۱ (معادل پهنای فرکانسی یا پهنای باند $\Delta\nu = c\Delta\lambda/\lambda^2$ تقریبا GHz ۱۲/۵)، زمان همدوسی

[1] Clock Cycle

[2] Polarization Mode Dispersion (Pmd)
[3] Chromatic Dispersion (Cd)
[4] Jitter Time

$l_c = c\tau_c$ تقریبا $\tau_c = 1/\Delta\nu$ ۸۰ ps (معادل طول همدوسی تقریبا ۲۴ mm) خواهد بود. بنابراین، ازآنجاکه اختلاف زمانی بین مسیرهای کوتاه-کوتاه، کوتاه-بلند و بلند-بلند خیلی بزرگ‌تر از زمان همدوسی است، هیچ تداخلی در هر یک از تداخل‌سنج‌ها رخ نمی‌دهد.

اختلاف طول بازوهای دو تداخل‌سنج δl باید در مقایسه با طول همدوسی l_c خیلی کوچک باشد. مشکل اصلی در سامانه-های فازی این است که باید δl در تمام مدت توزیع کلید، با دقت کم‌تر از کسری از طول‌موج سامانه ثابت بماند. بنابراین برای این-که رابطه فازی بین دو مسیر تداخلی پایدار بماند، باید طول مسیرها به‌طور مرتب بررسی و اختلاف آن‌ها -مثلاً به‌صورت غیرفعال و با قرار دادن تداخل‌سنج‌ها در جعبه‌های عایق و جلوگیری از تغییر دمای آن‌ها- ثابت نگه‌داشته شود. استفاده از روش‌های فعال برای اصلاح تغییرات احتمالی در طول مسیرهای تداخلی نیز امری ضروری است. در این طرح، با ایجاد یک خط تأخیر با طول متغیر در بازوی بلند آلیس و تنظیم دقیق یک کشنده فیبر در بازوی بلند تداخل‌سنج باب، طول مسیرهای تداخلی کوتاه-بلند و بلند-کوتاه با دقت موردنیاز بر هم منطبق می‌شود.

۲-۲. نحوه اجرای پروتکل QKD در طرح پیشنهادی

قراردادهای مربوط به انتخاب پایه و فاز توسط آلیس و باب و نحوه تعریف بیت‌های "0" و "1" باتوجه‌به آشکارسازی فوتون‌ها در APD1 یا APD2 برای اجرای چیدمان شکل (۱)، در جدول (۱) خلاصه شده است.

جدول ۱. قراردادهای بین آلیس و باب برای اجرای طرح پیشنهادی نشان داده‌شده در شکل (۱).

قراردادهای آلیس			قراردادهای باب		قراردادهای آشکارسازی		
1	0	بیت‌های کد شده / پایه‌های آلیس	فازهای باب (ϕ_B)	پایه‌های باب	اختلاف‌فاز ($\Delta\phi$)	بیت	آشکارساز
π	0	0	0	0	0	"0"	APD1
$3\pi/2$	$\pi/2$	1	$\pi/2$	1	π	"1"	APD2
	فازهای آلیس (ϕ_A)						

برای اجرای پروتکل BB84 با استفاده از طرح پیشنهادی، ابتدا آلیس باتوجه‌به بیت کد شده و پایه تصادفی خود، یکی از تغییر فازهای $(0, \pi, \pi/2, 3\pi/2)$ را به بخشی از پالس که از بازوی کوتاه تداخل‌سنج او عبور کرده اعمال می‌کند. طبیعتاً به بخش دیگر پالس که از بازوی بلند تداخل‌سنج عبور می‌کند تغییر فازی اعمال نخواهد شد و درواقع این فوتون‌ها حاوی هیچ اطلاعاتی نخواهند بود. دلیل انتخاب میانگین تعداد فوتون بالاتر برای بخش عبوری از بازوی بلند تداخل‌سنج آلیس، این است که ایو از حمله به این فوتون‌ها به اطلاعات معناداری دست نمی‌یابد. بخشی از پالس که به دلیل عبور از بازوی کوتاه تداخل‌سنج آلیس زودتر به باب می‌رسد، با کمک ادوات کنترل‌کننده قطبش موجود در سامانه، وارد بازوی بلند تداخل‌سنج باب شده، تغییر فازی به آن اعمال نمی‌شود. بخش دیگر پالس که با تأخیر به باب می‌رسد، پس از ورود به بازوی کوتاه تداخل‌سنج باب، به‌صورت تصادفی یکی از تغییر فازهای $(0, \pi/2)$ به آن اعمال می‌شود.

احتمال آن که فوتون عبور کرده از تداخل‌سنج، در آشکارساز APD1 یا APD2 اندازه‌گیری شود برابر است با:

$$\frac{1}{2}[1 \pm \cos(\phi_A - \phi_B)], \qquad (۲)$$

که در آن، ϕ_A و ϕ_B اختلاف فاز اعمال‌شده توسط مدولاتورهای فاز آلیس و باب است و علامت مثبت و منفی به ترتیب مربوط به‌احتمال آشکارسازی در APD1 و APD2 می‌باشد. اکنون با توجه به روابط

$$\cos\alpha + cos\beta = 2cos\frac{\alpha+\beta}{2}cos\frac{\alpha-\beta}{2}$$

و

$$cos\alpha - cos\beta = -2sin\frac{\alpha+\beta}{2}\,sin\frac{\alpha-\beta}{2}$$

می‌توان احتمال آشکارسازی فوتون در APD1 را به دست آورد:

$$P(\text{APD1}) = \frac{1}{2}(1 + \cos(\phi_A - \phi_B)) = cos^2\left(\frac{\phi_A - \phi_B}{2}\right) \qquad (۳)$$

به طریق مشابه، احتمال آشکارسازی فوتون در APD2 برابر است با:

$$P(\text{APD2}) = \frac{1}{2}(1 - \cos(\phi_A - \phi_B)) = sin^2\left(\frac{\phi_A - \phi_B}{2}\right) \qquad (۴)$$

با قراردادهای بیان‌شده در جدول (۱)، اگر پایه‌های آماده‌سازی آلیس و اندازه‌گیری باب مشابه انتخاب شوند، تغییر فاز نسبی اعمال‌شده توسط دو تداخل‌سنج $\phi_A - \phi_B = 0\ (\pi)$ خواهد بود. در این صورت، با توجه به روابط (۳) و (۴)، فوتون لزوماً وارد آشکارساز APD1 (APD2) باب خواهد شد و احتمال تیک خوردن آشکارساز دیگر صفر خواهد بود. درواقع این تغییر فازها با فرانژهای تداخلی روشن و تاریک در پدیده تداخل مطابقت دارند. در این صورت آلیس و باب نتایج مناسب را به دست آورده و آن‌ها را حفظ می‌کنند. به اندازه‌گیری در APD1 بیت "0" و به آشکارسازی در APD2 بیت "1" نسبت داده می‌شود. اما اگر پایه‌های آلیس و باب متفاوت باشند، تغییر فاز نسبی اعمال‌شده توسط دو تداخل‌سنج $\phi_A - \phi_B = \pi/2\ (3\pi/2)$ خواهد بود و

فوتون ممکن است با احتمال ۵۰٪ وارد هر یک از دو بازوی جفت کننده فیبری باب شود. بنابراین اندازه‌گیری باب می‌تواند مقادیر "0" یا "1" را با احتمال یکسان به دست آورد. این حالت معادل فوتونی است که با زاویه قطبش °45 وارد یک PBS می‌شود و می‌تواند وارد هرکدام از بازوهای خروجی آن شود. در این صورت نتایج به‌دست‌آمده کاملاً تصادفی است و بنابراین چنین فوتون‌هایی به‌طورکلی کنار گذاشته می‌شوند.

برای درک بهتر موضوع، یک نمونه تئوری از اجرای پروتکل BB84 مبتنی بر فاز با استفاده از طرح پیشنهادی، در جدول (۲) آورده شده است. داده‌های گام ۱ و ۲ به‌صورت جداگانه به‌وسیله یک مولد اعداد تصادفی کوانتومی (QRNG) تولید می‌شوند و در اختیار آلیس قرار می‌گیرند. تغییر فازهای انتخاب‌شده در گام ۳، باتوجه‌به داده‌های تصادفی گام‌های ۱ و ۲ و با مراجعه به جدول (۱) انتخاب می‌شوند. پایه‌های تصادفی گام ۴ نیز توسط یک QRNG تولید و در اختیار باب قرار می‌گیرند. تغییر فازهای اعمال‌شده در گام ۵، باتوجه‌به داده‌های تصادفی گام ۴ و با مراجعه به جدول (۱) انتخاب می‌شوند. داده‌های گام ۶ جدول نیز باتوجه‌به اختلاف تغییر فازهای اعمال‌شده توسط آلیس و باب به ترتیب در گام‌های ۳ و ۵ نوشته می‌شوند. درنهایت، داده‌های گام ۷ که بیت‌های کلید خام را تشکیل می‌دهند، باتوجه‌به قرارداد مربوط به آشکارسازی در APD1 یا APD2 تعیین می‌شوند.

جدول ۲. یک نمونه تئوری از اجرای پروتکل BB84 با استفاده از طرح پیشنهادی نشان داده‌شده در شکل ۱. اعداد پررنگ متمایز شده در گام‌های ۲ و ۴ به مفهوم انتخاب پایه‌های یکسان توسط آلیس و باب هستند. بیت‌های کدگذاری شده و کدگشایی‌شده‌ای که زیر آن‌ها خط کشیده شده، کلید غربال‌شده را تشکیل می‌دهند.

آلیس			باب		آشکارسازی	
بیت کدگذاری شده	پایه آماده‌سازی	ϕ_A	پایه اندازه‌گیری	ϕ_B	$\Delta\phi$	بیت کدگشایی‌شده
گام ۱	گام ۲	گام ۳	گام ۴	گام ۵	گام ۶	گام ۷
1	0	π	0	0	π	1
0	1	π/2	1	π/2	0	0
0	1	π/2	0	0	π/2	1 or 0
1	0	π	0	0	π	1
0	0	0	1	π/2	π/2	1 or 0
1	1	3π/2	1	π/2	π	1
1	1	3π/2	0	0	3π/2	1 or 0
0	0	0	1	π/2	π/2	1 or 0

می‌توان نشان داد که نرخ کلید امن[1] پروتکل BB84 استاندارد دوبعدی با نرخ خطای $QBER$ و در حالت عدم حضور ایو، برابر است با [۲۵]:

$$\begin{aligned} & R^{(BB84)} \\ & = R_{sift}{}^{(BB84)}\{1 \\ & - f(QBER)(-QBER\ \log_2(QBER) \\ & - (1-QBER)\log_2(1-QBER))\} \end{aligned} \quad (۵)$$

دراین‌رابطه، $R_{sift}{}^{(BB84)}$ نرخ کلید غربال‌شده[2] پروتکل BB84 است و به‌صورت زیر برحسب پارامترهای ثابت سامانه نوشته می‌شود:

$$R_{sift}{}^{(BB84)} = \frac{1}{2} f_{rep}\, \mu\, \eta\, 10^{-(\alpha l + L_B)/10} \quad (۶)$$

تابع $f(QBER) \geq 1$ نیز بیان‌گر کیفیت و بازدهی الگوریتم تصحیح خطای مورداستفاده در فرایند پساپردازش کلاسیک است. مقادیر $f(QBER)$ برای چند نرخ خطای مختلف در جدول (۳) داده‌شده است.

جدول ۳. مقادیر $f(QBER)$ برای چند نرخ خطای مختلف [۲۶].

$QBER$	$f(QBER)$
0.01	1.16
0.05	1.16
0.10	1.22
0.15	1.35

۳. نتایج و بحث

در مورد هر پروتکل QKD، آنچه درنهایت اهمیت بیش‌تری دارد، جنبه‌های امنیتی آن، ازجمله نرخ خطای قابل‌تحمل (توانمندی پروتکل برای مقابله با ناکاملی‌های موجود در سامانه)، نرخ کلید امن و بیشینه مسافت انتقال امن قابل حصول می‌باشد. در این بخش، ابتدا محاسبه، شبیه‌سازی و تحلیل QBER و نمایانی کوانتومی و در ادامه آن، شبیه‌سازی و تحلیل نرخ تولید کلید طرح پیشنهادی بیان‌شده است.

۳-۱. محاسبه، شبیه‌سازی و تحلیل QBER و V طرح پیشنهادی

قدم اول در راستای بررسی جنبه‌های امنیتی هر چیدمان، محاسبه QBER آن است. در حالت کلی، $QBER$ یک سامانه QKD مبتنی بر تداخل‌سنجی به‌صورت زیر محاسبه می‌شود [۲۷]:

[1] Secure Key Rate
[2] Sifted Key Rate

$$QBER = \frac{I_{min}}{I_{max} + I_{min}}, \quad (۷)$$

که I_{max} و I_{min} به ترتیب تعداد شمارش‌ها در واحد زمان به ازای تداخل‌های سازنده و مخرب در یکی از آشکارسازها هستند. در این صورت، نمایانی کوانتومی V مربوط به فرانژهای تداخلی کوانتومی، با کمک تعریف آن و به‌طور مستقیم به‌صورت زیر به دست می‌آید:

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}. \quad (۸)$$

همان‌طور که در روابط (۷) و (۸) دیده می‌شود، $QBER$ سامانه و نمایانی کوانتومی V به‌صورت زیر باهم مرتبط هستند:

$$QBER = \frac{1 - V}{2}. \quad (۹)$$

سه عامل عمده و اصلی در QBER سامانه پیشنهادی وجود دارد که هرکدام از آن‌ها به‌نوعی نمایانی کوانتومی V چیدمان را محدود می‌کند. اولین عامل، نویز ناشی از شمارش در حالت تاریک آشکارساز است. دومین عامل، نورهای پراکنده و پس‌زمینه ناشی از پالس‌های شدت بالای لیزر هم‌زمان‌ساز است که به طور کامل توسط فیلتر WDM حذف نشده‌اند. در صورت استفاده از آشکارسازهای تک فوتونی مناسب و باکیفیت، می‌توان گفت که سهم این نورهای سرگردان در شمارش خطا، بر سهم شمارش تاریک آشکارساز غلبه دارد؛ بنابراین با بهبود فرایند فیلتر پالس‌های لیزر هم‌زمان‌ساز، می‌توان QBER و V سامانه را ارتقاء داد. در اینجا به مجموعه این دو عامل، خطاهای ناشی از "شمارش‌های نادرست" اطلاق می‌شود. سومین عامل، خطاهای رخ‌داده در فرایند مدوله‌سازی فاز است که ممکن است به دلیل بروز عدم دقت جزیی در بایاس‌های اعمالی به مدولاتور فاز و همچنین انحراف فاز طی اجرای پروتکل به وجود آید. این عامل، که "خطای اپتیکی" نامیده می‌شود، منجر به بروز نقص در تداخل‌سنج‌ها و عدم تمایز کامل تداخل‌های سازنده و مخرب می‌شود. خطای اپتیکی سهم عمده در QBER سامانه در مسافت‌های انتقال کوتاه را خواهد داشت.

خوشبختانه در یک سامانه تداخل‌سنجی، امکان تفکیک خطای اپتیکی از خطای مربوط به شمارش‌های نادرست با بهره‌بردن از کمیتی به نام نمایانی کلاسیک V_c وجود دارد. درواقع V_c که به‌عنوان نمایانی فرانژهای تداخلی در حالت استفاده از پالس‌های با شدت بالا نیز شناخته می‌شود، معیاری برای سنجش کیفیت اپتیکی سامانه در اختیار می‌گذارد. اگر P_{opt} احتمال بروز خطای اپتیکی در سامانه تداخل‌سنجی به ازای هر پالس ارسالی آلیس باشد، مشابه رابطه (۹)، بین P_{opt} و V_c رابطه زیر برقرار است [۲۸]:

$$P_{opt} = \frac{1 - V_c}{2}. \quad (۱۰)$$

اگر P_{dark} احتمال ثبت یک شمارش تاریک در واحد زمان و در یک آشکارساز، n_t تعداد پنجره‌های زمانی (یا تعداد آشکارسازها در چیدمان‌های چند آشکارساز)، t_w مدت باز بودن دهانه آشکارسازهای باب برای دریافت کامل هر سیگنال آلیس، q احتمال ایجاد خطا توسط شمارش تاریک، μ میانگین تعداد فوتون‌های هر پالس، η بازده کوانتومی آشکارسازها، l طول کانال کوانتومی برحسب km، α ضریب تلفات کانال کوانتومی برحسب dB/km و L_B تلفات داخلی بخش باب برحسب dB باشند، می‌توان QBER یک سامانه فازی مبتنی بر تداخل‌سنجی را به‌صورت کلی زیر، برحسب پارامترهای فیزیکی ثابت سامانه نوشت [۲۸]:

$$QBER = \frac{1 - V_c}{2} + \frac{q\, P_{dark}\, t_w\, n_t}{\mu\, \eta\, 10^{-(\alpha l + L_B)/10}}. \quad (۱۱)$$

اکنون با کمک روابط (۹) و (۱۱) می‌توان نمایانی‌های کوانتومی و کلاسیک را به‌صورت زیر به هم مرتبط کرد:

$$V = V_c - \frac{2q\, P_{dark}\, t_w\, n_t}{\mu\, \eta\, 10^{-(\alpha l + L_B)/10}}. \quad (۱۲)$$

همان‌طور که از روابط (۱۱) و (۱۲) پیداست، QBER و نمایانی کوانتومی V به مسافت انتقال وابسته هستند و با افزایش مسافت انتقال به ترتیب افزایش و کاهش می‌یابند.

ازآنجاکه چیدمان پیشنهادی بر اساس پروتکل BB84 فازی استاندارد دوبعدی عمل می‌کند، بنابراین در اینجا برای نوشتن کمیت‌های مربوط به آن، از بالانویس BB84 استفاده‌شده است. در چیدمان شکل (۱)، از دو آشکارساز تک فوتون استفاده‌شده که هرکدام دارای یک پنجره زمانی هستند ($n_t^{(BB84)} = 2$). هر شمارش تاریک با احتمال ۵۰٪ ممکن است در پنجره زمانی مطلوب رخ دهد و منجر به ثبت یک نتیجه درست شود ($q^{(BB84)} = \frac{1}{2}$). بنابراین با جایگذاری مقادیر $n_t^{(BB84)}$ و $q^{(BB84)}$ در روابط (۱۱) و (۱۲)، $QBER$ و V چیدمان شکل (۱) به‌صورت زیر به دست می‌آید:

$$QBER^{(BB84)} = \frac{1 - V_c^{(BB84)}}{2} + \frac{P_{dark}\, t_w}{\mu\, \eta\, 10^{-\left(\alpha l + L_B^{(BB84)}\right)/10}} \quad (۱۳)$$

و

$$V^{(BB84)} = V_c^{(BB84)} - \frac{2\, P_{dark}\, t_w}{\mu\, \eta\, 10^{-(\alpha l + L_B)/10}}. \quad (۱۴)$$

اکنون با استفاده از روابط (۱۳) و (۱۴)، می‌توان نمودارهای QBER و V برحسب مسافت انتقال l را رسم کرد و با کمک آن‌ها، بیشینه مسافت انتقال قابل‌دستیابی توسط سامانه را تعیین کرد.

در صورت پیاده‌سازی چیدمان پیشنهادی، برای تعیین مقدار $QBER$ آن به‌صورت تجربی و با استفاده از رابطه (۷)، ابتدا

پالس‌ها را تا حد تک‌فوتون تضعیف کرده، سپس تعداد شمارش‌ها در واحد زمان به ازای تداخل‌های سازنده (I_{max}) و تداخل‌های مخرب (I_{min}) دریکی از آشکارسازها اندازه‌گیری می‌شود. یعنی با در نظر گرفتن تنها یک آشکارساز، ابتدا اختلاف‌فاز طوری تنظیم می‌شود که تداخل سازنده در آشکارساز ایجاد شود، سپس اختلاف‌فاز به‌گونه‌ای تنظیم می‌شود که برای آن آشکارساز تداخل مخرب شود. در این صورت، $QBER$ به‌سادگی با تقسیم تعداد شمارش‌های نادرست (یعنی تعداد شمارش‌ها در آشکارساز وقتی تداخل مخرب است) بر تعداد شمارش‌های به‌دست‌آمده در آشکارساز وقتی تداخل سازنده است به دست می‌آید. به‌این‌ترتیب، نرخ خطای تجربی سامانه قبل از تصحیح خطا به دست می‌آید.

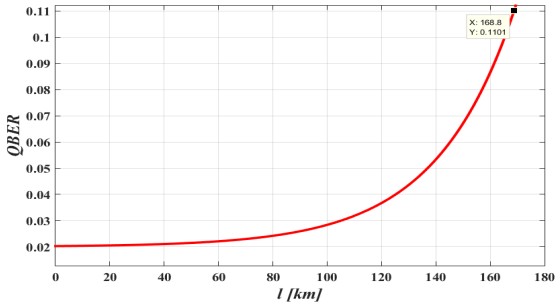
در سوی دیگر، برای تعیین تجربی P_{opt} و V_c چیدمان پیشنهادی، از پالس‌های کلاسیک (شدت بالا) استفاده می‌شود. برای این منظور، یک اختلاف‌فاز ثابت به‌گونه‌ای انتخاب و به پالس‌های کلاسیک ارسالی اعمال می‌شود که در یکی از آشکارسازها تداخل سازنده و در آشکارساز دیگر تداخل مخرب ایجاد شود (یا در یک آشکارساز، یک‌بار شرایط ایجاد تداخل سازنده و بار دیگر شرایط ایجاد تداخل مخرب فراهم می‌شود). با تقسیم تعداد شمارش‌ها در آشکارساز مخرب به تعداد شمارش‌ها در آشکارساز سازنده، مقدار P_{opt} تعیین می‌شود.

در ادامه، QBER و V چیدمان پیشنهادی برحسب پارامترهای فیزیکی ثابت سامانه (یعنی P_{opt}، P_{dark}، t_w، μ، η، α، l و L_B) شبیه‌سازی و تحلیل‌شده است. با ثابت نگه‌داشتن سایر پارامترهای ثابت سامانه، می‌توان تغییرات QBER و V نسبت به مسافت انتقال l را مطالعه و بررسی کرد. به‌طورکلی، هرچه QBER سامانه کم‌تر و V آن بالاتر باشد، مراقبت از آن در مقابل حملات ایو راحت‌تر است و دستیابی به مسافت انتقال امن بالاتر نیز با استفاده از آن محتمل‌تر خواهد بود.

با زمان‌بندی کاملاً دقیق سامانه QKD و تنظیم درست قطعات مختلف آن، می‌توان در مسافت‌های انتقال پایین (در گستره طول‌های حدود km ۵۰-۲۰ کیلومتر) شرایط دستیابی به P_{opt} حدود ۱٪ را فراهم کرد. در مسافت‌های طولانی‌تر، به دلیل دشوارتر شدن فرایندهای زمان‌بندی و تنظیم سامانه (و نه به خاطر تأثیر مستقیم خود افزایش مسافت!)، میزان P_{opt} افزایش و درنتیجه V_c کاهش می‌یابد. در سامانه‌های فیبر نوری، مشکلی که وجود دارد حفظ کردن این مقدار باوجود افت‌وخیزهای قطبش و واقطبیدگی[1] در فیبر است. در اینجا به‌منظور در نظر گرفتن یک حد بالا برای خطاهای احتمالی موجود در فرایند دقیق و حساس مدوله‌سازی فاز، مقدار P_{opt} برابر ۲٪ در نظر گرفته می‌شود. با انتخاب این عدد برای P_{opt}، انتظار می‌رود که نتایج حاصل از شبیه‌سازی و تحلیل نظری سامانه، تا حد زیادی به عملکرد تجربی آن نزدیک باشد.

برای تعیین QBER و V برحسب مسافت انتقال l، ابتدا باید تلفات داخلی بخش باب L_B را با توجه به تلفات هر یک از قطعات موجود در بخش باب چیدمان محاسبه کرد. با در نظر گرفتن مقادیر تقریبی و البته بسیار نزدیک به‌واقع ۰/۳، ۰/۱، ۰/۰۵، ۴، ۰/۱، ۰/۰۵، ۲، ۰/۴ و ۲ dB، به ترتیب برای تلفات داخلی مربوط به قطعات WDM، BWF، PC، PBS، FS، PC، $\emptyset_B$، Coup و مجموع اتصالات فیبری موجود در بخش باب، مقدار $L_B^{(BB84)}$ برابر با ۹ dB خواهد بود.

نمودار مربوط به QBER به‌دست‌آمده در رابطه (۱۳)، با استفاده از پارامترهای ثابت $P_{dark} = 10^3\ s^{-1}$، $t_w = 10^{-9}s$، $\mu = 0.1$، $\eta = 0.3$، $\alpha = 0.15\ dB\ km^{-1}$، $P_{opt} \approx 2\%$ و $L_B \approx 9\ dB$، به‌عنوان تابعی از مسافت انتقال l در شکل (۲) رسم شده است.



شکل ۲. نرخ خطای بیت کوانتومی (QBER) برحسب مسافت انتقال (l)، برای طرح پیشنهادی. پارامترها: $P_{dark} = 10^3\ s^{-1}$، $t_w = 10^{-9}s$، $\mu = 0.1$، $\eta = 0.3$، $\alpha = 0.15\ dB\ km^{-1}$، $P_{opt} \approx 2\%$ و $L_B \approx 9\ dB$.

مطابق این شکل، تا مسافت انتقال‌های حدود km ۵۰، نرخ خطای پروتکل اندکی بالاتر از $P_{opt} \approx 2\%$ است. تا این مسافت، سهم‌های ناشی از شمارش‌های نادرست (شمارش‌های تاریک آشکارساز و نورهای پس‌زمینه) کمتر از ۰/۲٪ است. در صورت تنظیم دقیق ادوات اپتیکی سامانه، ازجمله سامانه تداخل‌سنجی، عیوب و نواقص موجود در تداخل‌سنج و دیگر قطعات اپتیکی به‌کاررفته در چیدمان (خطای اپتیکی) نیز نقش کوچکی در این QBER ایفا خواهند کرد. بنابراین مطابق انتظار، عمده این خطا از مدوله‌سازی ناقص فاز ناشی می‌شود. با توجه به این شکل، در مسافت km ۱۰۰، مقدار QBER اندکی کم‌تر از ۳٪ خواهد بود. در مسافت‌های بالاتر، سهم شمارش‌های نادرست در QBER کل سامانه افزایش می‌یابد و در مسافت حدود km ۱۲۵، مقدار خطای ناشی از شمارش‌های نادرست و P_{opt} باهم برابر می‌شود. پس‌ازآن، هرچه مسافت افزایش می‌یابد، اثرات ناشی از

[1] Depolarization

شمارش‌های تاریک آشکارساز و نورهای پس‌زمینه برجسته‌تر می‌شود، درحالی‌که مقدار P_{opt} ثابت می‌ماند. بنابراین مشخصات آشکارساز است که بیشینه مسافت قابل حصول در سامانه را تعیین می‌کند.

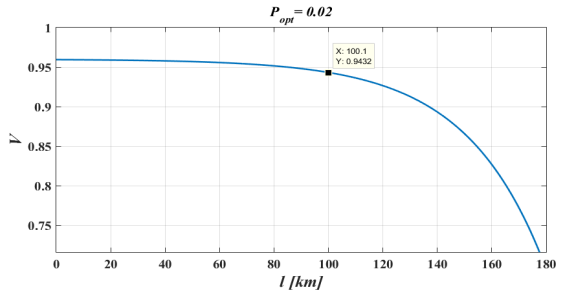
در هر چیدمان، بیشینه مسافت انتقال قابل‌دستیابی، عمدتاً باتوجه‌به نرخ شمارش تاریک آشکارساز و میزان تلفات فوتون‌ها در کانال کوانتومی تعیین می‌شود. با افزایش مسافت انتقال، QBER سامانه افزایش‌یافته و حالت‌های کوانتومی به‌قدری تضعیف می‌شوند که رفته‌رفته در رقابت با نویزهای موجود (که مقدارشان ثابت است) رو به افول می‌گذارند، تا جایی که با رسیدن به یک QBER آستانه، دیگر تشخیص یک حالت کوانتومی از نویز ممکن نخواهد بود. می‌توان نشان داد که باملاحظه حملات همدوس[1] احتمالی، در پروتکل BB84 دوبعدی وقتی QBER سامانه به ۱۱٪ نزدیک می‌شود، نرخ تولید کلید امن به صفر می‌رسد. محدوده QBER قابل‌تحمل در حالت حملات مجزا[2] نیز کم‌تر از ۱۵٪ است [۲۸]. همان‌طور که در شکل (۲) دیده می‌شود، در طول فیبر حدود $170\ km$، مقدار QBER چیدمان به ۱۱٪ می‌رسد و نرخ بیت خالص به صفر سقوط می‌کند. با کاهش تلفات داخلی بخش باب (کاهش L_B)، ارتقای فناوری آشکارسازی تک‌فوتون (کاهش P_{dark} و افزایش η آشکارسازها) و سرکوب بهتر نور لیزر هم‌زمان‌ساز (مثلاً زمان‌بندی الکترونیکی سامانه بجای هم‌زمان‌سازی نوری فعلی)، می‌توان مسافت توزیع امن کلید را افزایش داد.

برای حفظ پایداری عملکرد سامانه باید فاز و قطبش اعمالی به فوتون‌ها طی فرایند توزیع کلید پایدار بماند. ایجاد انحراف در فاز به دلیل ایجاد تغییر در طول نسبی دو بازوی تداخل‌سنج، می‌تواند مستقیماً منجر به افزایش QBER سامانه شود. قراردادن بخش‌های آلیس و باب در محفظه‌های بسته، به‌منظور جلوگیری از همرفت هوا، انجام توزیع کلید پایدار در مدت‌زمان چندین دقیقه را ممکن می‌سازد. انحراف قطبش نیز باعث کاهش نرخ بیت می‌شود، اما اگر نرخ سیگنال به میزان قابل‌توجهی بالاتر از نرخ خطای ذاتی سامانه باشد، باعث افزایش QBER نمی‌شود [۲۹].

نمودار مربوط به نمایانی کوانتومی V به‌دست‌آمده در رابطه (۱۴)، با در نظر گرفتن خطای مدولاسیون $P_{opt} = 2\%$، به‌صورت تابعی از مسافت انتقال l، در شکل (۳) رسم شده است. مطابق این شکل، نمایانی کوانتومی از ۹۶٪ آغاز و در مسافت $100\ km$ به حدود ۹۴٪ می‌رسد. با افزایش طول فیبر، رفته‌رفته تلفات فیبر باعث کاهش نرخ سیگنال به‌اندازه‌ای می‌شود که قابل‌مقایسه با نرخ خطای ذاتی آشکارساز باب باشد. در مسافت حدود $170\ km$، که با توجه به شکل (۲) مسافت قطع این سامانه است، میزان نمایانی کوانتومی حدود ۷۷٪ خواهد بود.

در حالت حدی $P_{opt} = 0$ (نمایانی کلاسیک کامل و وارد نشدن خطای مدولاسیون در محاسبه نمایانی، به دلیل ثابت نگه‌داشتن حالت‌های کوانتومی حین محاسبه)، نمایانی تداخل کوانتومی تا مسافت انتقال حدود $80\ km$، بزرگ‌تر از ۹۹٪ خواهد بود. با پارامترهای انتخاب‌شده برای قطعات سامانه که به مقادیر واقعی بسیار نزدیک هستند، امکان انجام QKD با نمایانی بالاتر از ۹۸٪ در مسافت $100\ km$ فراهم خواهد بود. در طول فیبر $150\ km$ نمایانی حدود ۹۰٪ برای این سامانه قابل حصول است. در مسافت قطع $170\ km$ نمایانی بالاتر از ۸۰٪ خواهد بود.

برای اندازه‌گیری تجربی نمایانی تداخل کوانتومی سامانه در حالت $P_{opt} = 0$، لیزر سیگنال $1/55\ \mu m$ تا حد ۰/۱ فوتون در هر چرخه، تضعیف و آشکارساز باب توسط لیزر هم‌زمان‌ساز $1/3\ \mu m$ با سامانه آلیس هم‌زمان می‌شود. با اعمال یک بایاس DC به کشنده فیبر موجود در بازوی بلند تداخل‌سنج باب، فاز اپتیکی تغییر کرده، میزان نمایانی اندازه‌گیری می‌شود. برای تعیین تجربی نمودار شکل (۳) نیز نمایانی در زمان اجرای پروتکل و در حالت مدولاسیون فاز اعمالی به پالس‌ها با خطای $P_{opt} = 2\%$ اندازه‌گیری می‌شود. نکته‌ای که باید به آن توجه کرد این است که برای دستیابی به نمایانی کلاسیک بالا، نقش کشنده فیبر بسیار مهم و حیاتی است و ولتاژ کاری آن عمیقاً بر روی نمایانی تداخل و درنتیجه نرخ کلید امن تأثیر می‌گذارد. با استفاده و تنظیم دقیق قطعات اپتیکی نگهدارنده قطبش، می‌توان به نمایانی تداخل کلاسیک کامل هم دست یافت.



شکل ۳. نمایانی کوانتومی (V) برحسب مسافت انتقال (l)، با در نظر گرفتن خطای اپتیکی $P_{opt} = 2\%$. سایر پارامترها مشابه پارامترهای شکل (۲) هستند.

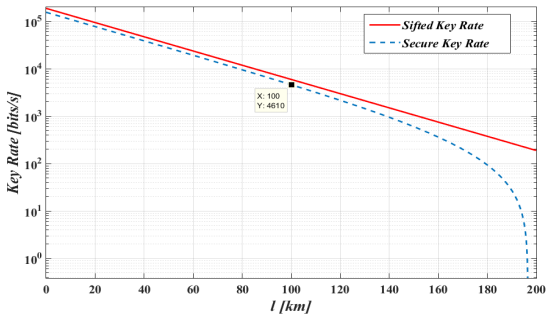
۳-۲. شبیه‌سازی و تحلیل نرخ تولید کلید در طرح پیشنهادی

نمودار نرخ کلیدهای مربوط به روابط (۵) و (۶)، به‌عنوان توابعی

[1] Coherent Attacks
[2] Individual Attacks

از طول کانال فیبر نوری، در شکل (۴) رسم شده است. ازآنجاکه با توجه به شکل ۲، میزان QBER طرح پیشنهادی تا مسافت حدود $140\ km$ کم‌تر از ۵٪ است، بنابراین برای مسافت‌های کم‌تر از $140\ km$، مطابق جدول (۳) می‌توان از مقدار $f(QBER) = 1.16$ برای بازدهی الگوریتم تصحیح خطا استفاده کرد. بااین‌حال، به‌منظور ملاحظه ناکاملی‌های احتمالی در الگوریتم تصحیح خطای مورداستفاده به هنگام پیاده‌سازی تجربی طرح پیشنهادی، برای تمام مسافت‌ها از مقدار $f(QBER) = 1.22$ استفاده‌شده است. این ملاحظه به نزدیک‌تر شدن نتایج حاصل از شبیه‌سازی به داده‌های تجربی کمک می‌کند.

مطابق شکل (۴)، در مسافت $20\ km$، نرخ کلید غربال‌شده حدود $95\ kbit/s$ قابل دستیابی است و پیش‌بینی می‌شود که این نرخ به حدود $35\ kbit/s$ در طول $50\ km$، $6\ kbit/s$ در طول $100\ km$ و $1\ kbit/s$ در طول $150\ km$ برسد. با استفاده از یک الگوریتم پساپردازش مناسب، می‌توان به کلید امن نهایی به نرخ تقریباً $77\ kbit/s$ در طول $20\ km$، $27\ kbit/s$ در طول $50\ km$، $4/6\ kbit/s$ در طول $100\ km$ و $600\ bit/s$ در طول $150\ km$ دست یافت. همان‌طور که در شکل (۴) دیده می‌شود، هرچه طول کانال و به طبع آن QBER سامانه بیش‌تر باشد، اختلاف نرخ کلیدهای غربال‌شده و امن سامانه از هم بیش‌تر می‌شود و درواقع احتمال مشارکت هر بیت از کلید غربال‌شده در ساخت کلید امن نهایی کاهش می‌یابد.



شکل ۴. نرخ کلیدهای غربال‌شده و امن طرح پیشنهادی به‌عنوان توابعی از طول کانال. با در نظر گرفتن خطای اپتیکی $P_{opt} = 2\%$، نرخ تکرار پالس‌های لیزر $f_{rep} = 100\ MHz$ و بازدهی الگوریتم تصحیح خطا $f(e) = 1.22$. سایر پارامترها مشابه پارامترهای شکل (۲) هستند.

همان‌طور که در این شکل دیده می‌شود، منحنی‌ها به دلیل افزایش سهم شمارش‌های تاریک با افزایش طول فیبر، دارای یک مسافت قطع هستند که بالاتر از آن دیگر امکان برقراری ارتباط امن وجود ندارد. با توجه به اینکه این نمودارها با فرض عدم حضور ایو رسم شده‌اند، بنابراین مطابق انتظار، مسافت قطع نرخ کلید امن در اینجا حدود ۳۰ کیلومتر بالاتر از مسافت قطع به‌دست‌آمده از شکل (۲) است.

مقایسه بین مشخصات عملکردی طرح پیشنهادشده در این مقاله با مجموعه‌ای از معتبرترین سامانه‌های QKD تک فوتون مبتنی بر متغیرهای گسسته و اجراشده در کانال فیبر نوری استاندارد، در جدول (۴) آورده شده است.

جدول ۴. مقایسه بین مشخصات عملکردی طرح پیشنهادشده در این مقاله با تعدادی از معتبرترین سامانه‌های QKD تک فوتون مبتنی بر متغیرهای گسسته و اجراشده در کانال فیبر نوری استاندارد.

ردیف	سال	روش کدگذاری	مسافت (کیلومتر)	نرخ ارسال (مگاهرتز)	نرخ کلید امن (بیت بر ثانیه)	مرجع
۱	۲۰۰۶	فاز	۶۰	۵	۴۲۲/۵	[۳۰]
۲	۲۰۰۷	قطبش	۱۰۲	۲/۵	۸/۱	[۳۱]
۳	۲۰۰۷	فاز	۱۰۷	۲/۵	۱۴/۵	[۳۲]
۴	۲۰۰۹	فاز	۱۰۰	۱۰۳۶	۱۰۱۰۰	[۳۳]
۵	۲۰۱۰	قطبش	۲۰۰	۳۲۰	۱۵	[۳۴]
۶	۲۰۱۳	فاز	۸۰	۱۰۰۰	۱۲۰۰۰۰	[۳۵]
۷	۲۰۱۷	فاز	۲۴۰	۱۰۰۰	۸/۴	[۳۶]
۸	۲۰۱۹	زمان	۲۰	۱۰۰	۸۵۷۰۰	[۳۷]
۹	۲۰۲۲	زمان	۱۵۰	۱۰۰۰	~۱۰۰۰	[۳۸]
۱۰	۲۰۲۴	زمان	۱۴۵	۵۰۰	~۱۰۰۰	[۳۹]
۱۱	۲۰۲۴	فاز	۱۰۰ (۱۵۰)	۱۰۰	۴۶۰۰ (۶۰۰)	مقاله حاضر

مطابق این جدول، سامانه شماره ۱ در مسافت امن زیر $100\ km$ اجراشده است. سامانه‌های شماره ۲ و ۳ باوجود دستیابی به مسافت امن بالای $100\ km$، دارای نرخ کلید امن بسیار پایین هستند. سامانه شماره ۴ با استفاده از نرخ ارسال $1036\ MHz$ توانسته است در مسافت $100\ km$ به نرخ کلید امن $10100\ bit/s$ دست پیدا کند. نکته‌ای که باید به آن توجه شود این است که تأمین چشمه‌ها و آشکارسازهای تک‌فوتون و همچنین مدولاتورهایی که بتوانند در نرخ ارسال‌های از مرتبه گیگاهرتز عملکرد مطلوبی داشته باشند، نیازمند صرف هزینه بسیار زیاد و تن‌دادن به پیچیدگی‌های فنی فراوان است. این مسئله در مورد سامانه‌های شماره ۶، ۷ و ۹ نیز برقرار است. سامانه شماره ۵ به‌عنوان یک سامانه موفق، با نرخ ارسال نسبتاً بزرگ $320\ MHz$، به نرخ کلید امن مثبت در مسافت امن $200\ km$ دست‌یافته است. سامانه شماره ۸ باوجود مطلوب بودن نرخ ارسال و نرخ کلید امن آن، تنها به مسافت امن $20\ km$ دست‌یافته است که در مقایسه با دیگر سامانه‌ها، یک عدد کوچک است. بنابراین طرح پیشنهادی که با نرخ ارسال $100\ MHz$، امکان دستیابی به مسافت امن $100\ km$ با نرخ تولید کلید امن $4600\ bit/s$ و مسافت امن $150\ km$ با نرخ تولید کلید امن $600\ bit/s$ را فراهم می‌آورد، در مقایسه با نمونه‌های موفق ذکرشده، باملاحظه هر سه مشخصه "مسافت توزیع کلید امن"، "نرخ ارسال حالت‌های کوانتومی" و "نرخ تولید کلید امن" از عملکرد کاملاً مطلوبی برخوردار است و می‌تواند یک

گزینه بسیار مناسب برای پیاده‌سازی تجربی باشد. توجه شود که مطابق جدول (۴)، عملکرد طرح پیشنهادی، درمجموع از عملکرد سامانه شماره ۱۰ (که یکی از جدیدترین کارهای گزارش‌شده است) نیز مطلوب‌تر است.

ردیف	سال	روش کدگذاری	مسافت (کیلومتر)	نرخ ارسال (مگاهرتز)	نرخ کلید امن (بیت بر ثانیه)	مرجع
۱	۲۰۰۶	فاز	۶۰	۵	۴۲۲/۵	[۳۰]
۲	۲۰۰۷	قطبش	۱۰۲	۲/۵	۸/۱	[۳۱]
۳	۲۰۰۷	فاز	۱۰۷	۲/۵	۱۴/۵	[۳۲]
۴	۲۰۰۹	فاز	۱۰۰	۱۰۳۶	۱۰۱۰۰	[۳۳]
۵	۲۰۱۰	قطبش	۲۰۰	۳۲۰	۱۵	[۳۴]
۶	۲۰۱۳	فاز	۸۰	۱۰۰۰	۱۲۰۰۰۰	[۳۵]
۷	۲۰۱۷	فاز	۲۴۰	۱۰۰۰	۸/۴	[۳۶]
۸	۲۰۱۹	زمان	۲۰	۱۰۰	۸۵۷۰۰	[۳۷]
۹	۲۰۲۲	زمان	۱۵۰	۱۰۰۰	تقریباً ۱۰۰۰	[۳۸]
۱۰	۲۰۲۴	زمان	۱۴۵	۵۰۰	تقریباً ۱۰۰۰	[۳۹]
۱۱	۲۰۲۴	فاز	۱۰۰ (۱۵۰)	۱۰۰	۴۶۰۰ (۶۰۰)	مقاله حاضر

۴. نتیجه‌گیری

در این مقاله، طرح‌واره یک سامانه QKD محیطی با استفاده از قطعات تمام فیبری ارائه و پارامترهای عملکردی آن شبیه‌سازی شد. طرح پیشنهادشده قابلیت QKD با نرخ مناسب تا مسافت $۱۷۰\ km$ را دارد. این طرح، انجام QKD در فیبر نوری تک‌مد استاندارد به طول $۱۰۰\ km$، با نرخ خطای بیت کوانتومی (QBER) زیر ۳٪، نمایانی کوانتومی بالای ۹۴٪، نرخ کلید غربال‌شده $۶\ kbit/s$ و نرخ کلید امن $۴/۶\ kbit/s$ را ممکن می‌سازد. با توسعه این طرح، از طریق اضافه کردن پروتکل حالت‌های طعمه و سپس ترکیب کردن آن با روش پیاده‌سازی plug&play، می‌توان به یک سامانه QKD تجاری و صنعتی بومی کارآمد دست یافت. با کاهش تلفات داخلی بخش باب (کاهش L_B)، ارتقای فناوری آشکارسازی تک‌فوتون (کاهش P_{dark} و افزایش η آشکارسازها) و سرکوب بهتر نور لیزر هم‌زمان‌ساز (مثلاً زمان‌بندی الکترونیکی سامانه بجای هم‌زمان‌سازی نوری فعلی)، می‌توان مسافت توزیع امن کلید را افزایش داد.

۵. مرجع‌ها

[1] Security of Practical Quantum Key Distribution"; Eur. Phys. J. D. 2007, 41, 599–627. doi: 10.1140/epjd/e2007-00010-4.

[2] Sun, S.; Huang, A. "A Review of Security Evaluation of Practical Quantum Key Distribution System"; Entropy , 2022, 24, 260. doi: 10.3390/e24020260.

[3] Portmann, C.; Renner, R. "Security in Quantum Cryptography"; Rev. Mod. Phys. 2022, 94, 025008. doi: 10.1103/revmodphys.94.025008.

[4] Li, Z.; Wei, K. "Improving Parameter Optimization in Decoy-State Quantum Key Distribution"; Quantum Eng. 2022, 1, 9717591. doi: 10.1155/2022/9717591.

[5] Li, W.; Zhang, L.; Tan, H.; Lu, Y.; Liao, S.-K.; Huang, J.; Li, H. "High-Rate Quantum Key Distribution Exceeding 110 Mb s–1"; Nat. Photonics, 2023, 17, 416–421. doi: 10.1038/s41566-023-01166-4.

[6] Zhang, C.-X.; Wu, D.; Cui, P.-W.; Ma, J.-C.; Wang, Y.; An, J.-M. "Research Progress in Quantum Key Distribution"; Chin. Phys. B. 2023, 32, 124207. doi: 10.1088/1674-1056/acfd16.

[7] Yang, Z.; Zolanvari, M.; Jain, R. "A Survey of Important Issues in Quantum Computing and Communications"; IEEE Communications Surveys & Tutorials, 2023, 25, 1059–1094. doi: 10.1109/comst.2023.3254481.

[8] Mehri Toonabi, A.; Davoudi Darareh, M. "Introducing a Decoy-State Version of the High-Dimensional Polarization-Phase (PoP) Quantum Key Distribution Protocol and Explaining its Implementation"; Journal of Electronical & Cyber Defence, 2024 (In Persian).https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.2.8.8

[9] Guarda, G.; Ribezzo, D.; Salvoni, D.; Bruscino, C.; Ercolano, P.; Ejrnaes, M.; Parlato, L. "Decoy-State Quantum Key Distribution Over Long-Distance Optical Fiber"; Quantum Computing, Communication, and Simulation IV, 2024, 12911, 120-125. doi: 10.1117/12.3003698.

[10] Zapatero, V.; Leent, T. v.; Arnon-Friedman, R.; Liu, W.-Z.; Zhang, Q.; Weinfurter, H.; Curty, M. "Advances in Device-Independent Quantum Key Distribution"; npj Quantum Inf. 2023, 9, 10. doi: 10.1038/s41534-023-00684-x.

[11] Liu, Y.; Zhang, W.-J.; Jiang, C.; Chen, J.-P.; Zhang, C.; Pan, W.-X.; Ma, D. "Experimental Twin-Field Quantum Key Distribution Over 1000 km Fiber Distance"; Phys. Rev. Lett. 2023, 130, 210801. doi: 10.1103/physrevlett.130.210801.

[12] Liu, Q.; Huang, Y.; Du, Y.; Zhao, Z.; Geng, M.; Zhang, Z.; Wei, K. "Advances in Chip-Based Quantum Key Distribution"; Entropy, 2022, 24, 1334. doi: 10.3390/e24101334.

[13] Jain, N.; Chin, H.-M.; Mani, H.; Lupo, C.; Nikolic, D. S.; Kordts, A.; Pirandola, S. "Practical Continuous-Variable Quantum Key Distribution with Composable Security"; Nat. Commun. 2022, 13, 4740. doi: 10.1038/s41467-022-32161-y.

[14] Zahidy, M.; Ribezzo, D.; De Lazzari, C.; Vagniluca, I.; Biagi, N.; Müller, R.; Occhipinti, T. "Practical High-Dimensional Quantum Key Distribution Protocol Over Deployed Multicore Fiber"; Nat. Commun. 2024, 15, 1651. doi: 10.1038/s41467-024-45876-x.

[15] Sun, Z.; Li, Y.; Ma, H. “Experimental High-Dimensional Quantum Key Distribution with Orbital Angular Momentum”; J. Opt. Soc. Am. B. 2024, 41, 351. doi: 10.1364/josab.507195.

[16] Mehri Toonabi, A.; Davoudi Darareh, M.; Janbaz, S. “High-Dimensional Quantum Key Distribution Using Polarization-Phase Encoding: Security Analysis”; Int. J. Quantum Inf. 2020, 18, 2050031. doi: 10.1142/s0219749920500318.

[17] Morrison, C. L.; Pousa, R. G.; Graffitti, F.; Koong, Z. X.; Barrow, P.; Stoltz, N. G.; Bouwmeester, D. “Single-Emitter Quantum Key Distribution Over 175 km of Fibre with Optimised Finite Key Rates”; Nat. Commun. 2023, 14, 3573. doi: 10.1038/s41467-023-39219-5.

[18] Jiang, S.; Safari, M. “High-Speed Quantum Key Distribution Using Dead-Time Compensated Detector Arrays”; J. Lightwave Technol. 2024, 1–13. doi: 10.1109/jlt.2024.3363145.

[19] Liu, R.; Rozenman, G. G.; Kundu, N. K.; Chandra, D.; De, D. “Towards the Industrialisation of Quantum Key Distribution in Communication Networks: A Short Survey”; IET Quantum Commun. 2022, 3, 151–163. doi: 10.1049/qtc2.12044.

[20] Safarbiranvand, M.; Qaani Gholamhosseini, Siahvoshi, S. N. “Investigation and Simulation of the Cn2 Parameter and its Effects on the Average Intensity Distribution, Spot Size, Radius of Curvature, and Rayleigh Length of the Laser Beam Propagation in the Atmosphere”; Advanced Defence Sci.& Technol. 2023, 2, 79-87 (In Persian). https://dor.isc.ac/dor/20.1001.1.26762935.1402.14.2.1.3

[21] Hassan, M. M.; Reaz, K.; Green, A.; Crum, N.; Siopsis, G. “Experimental Free-Space Quantum Key Distribution Over a Turbulent High-Loss Channel”; 2023 IEEE International Conference on Quantum Computing and Engineering (QCE). 2023, 1, 1182-1186. doi: 10.1109/qce57702.2023.00133.

[22] Li, Y.-H.; Li, S.-L.; Hu, X.-L.; Jiang, C.; Yu, Z.-W.; Li, W.; Liu, W.-Y. “Free-Space and Fiber-Integrated Measurement-Device-Independent Quantum Key Distribution under High Background Noise”; Phys. Rev. Lett. 2023, 131, 100802. doi: 10.1103/physrevlett.131.100802.

[23] Fox, M. “Quantum Optics”; 2006, 15, doi: 10.1093/oso/9780198566724.001.0001.

[24] Townsend, P. D.; Rarity, J. G.; Tapster, P. R. “Single Photon Interference in 10 km Long Optical Fibre Interferometer”; Electron. Lett. 1993, 29, 634. doi: 10.1049/el19930424.

[25] Mehri Toonabi, A.; Davoudi Darareh, M.; Janbaz, S. “A two-Dimensional Quantum Key Distribution Protocol Based on Polarization-Phase Encoding”; Int. J. Quantum Inf. 2019, 17, 1950058. doi: 10.1142/s0219749919500588.

[26] Waks, E.; Santori, C.; Yamamoto, Y. “Security Aspects of Quantum Key Distribution with Sub-Poisson Light”; Phys. Rev. A. 2002, 66, 042315. doi: 10.1103/physreva.66.042315.

[27] Zbinden, H.; Bechmann-Pasquinucci, H.; Gisin, N.; Ribordy, G. “Quantum Cryptography”; Appl. Phys. B: Lasers Opt. 1998, 67, 743–748. doi: 10.1007/s003400050574.

[28] Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. “Quantum Cryptography”; Rev. Mod. Phys. 2002, 74, 145–195. doi: 10.1103/revmodphys.74.145.

[29] Gobby, C.; Yuan, Z. L.; Shields, A. J. “Quantum Key Distribution Over 122 km of Standard Telecom Fiber”; Appl. Phys. Lett. 2004, 84, 3762–3764. doi: 10.1063/1.1738173.

[30] Zhao, Y.; Qi, B.; Ma, X.; Lo, H.-K.; Qian, L. “Experimental Quantum Key Distribution with Decoy States,”; Phys. Rev. Lett. 2006, 96, 070502. doi: 10.1103/physrevlett.96.070502.

[31] Peng, C. Z.; Zhang, J.; Yang, D.; Gao, W. B.; Ma, H. X.; Yin, H.; Zeng, H. P.; Yang, T.; Wang, X. B.; Pan, J. W. “Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding,”; Phys. Rev. Lett. 2007, 98, 010505. doi: 10.1103/physrevlett.98.010505.

[32] Rosenberg, D.; Harrington, J. W.; Rice, P. R.; Hiskett, P. A.; Peterson, C. G.; Hughes, R. J.; Lita, A. E.; Nam, S. W.; Nordholt, J. E. “Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber,”; Phys. Rev. Lett. 2007, 98, 010503. doi: 10.1103/physrevlett.98.010503.

[33] Dixon, A. R.; Yuan, Z. L.; Dynes, J. F.; Sharpe, A. W.; Shields, A. J. “Gigahertz Decoy Quantum Key Distribution With 1 Mbit/sS Secure Key Rate,”; Opt. Express, 2008, 16, 18790. doi: 10.1364/oe.16.018790.

[34] Liu, Y.; Chen, T. Y.; Wang, J.; Cai, W. Q.; Wan, X.; Chen, L. K.; Wang, J. H.; Liu, S. B.; Liang, H.; Yang, L.; Peng, C. Z. “Decoy-State Quantum Key Distribution wWith Polarized Photons Over 200 km,”; Opt. Express, 2010, 18, 8587-8594. doi: 10.1364/oe.18.008587.

[35] Lucamarini, M.; Patel, K. A.; Dynes, J. F.; Fröhlich, B.; Sharpe, A. W.; Dixon, A. R.; Yuan, Z. L.; Penty, R. V.; Shields, A. J. “Efficient Decoy-State Quantum Key Distribution wWith Quantified Security,” Opt. Express , 2013, 21, 24550-24565. doi: 10.1364/oe.21.024550.

[36] Fröhlich, B.; Lucamarini, M.; Dynes, J. F.; Comandar, L. C.; Tam, W. W. S.; Plews, A.; Sharpe, A. W.; Yuan, Z.; Shields, A. J. “Long-Distance Quantum Key Distribution Secure Against Coherent Aattacks,” Optica, 2017, 4, 163-167. doi: 10.1364/optica.4.000163.

[37] Geng, W.; Zhang, C.; Zheng, Y.; He, J.; Zhou, C.; Kong, Y. “Stable Quantum Key Distribution Using aA Silicon Photonic Transceiver,” Opt. Express, 2019, 27, 29045. doi: 10.1364/oe.27.029045.

[38] Shaw, G. K.; Sridharan, S.; Prabhakar, A. “Optimal temporal filtering for COW-QKD,” 2022 IEEE International Conference on Signal Processing and Communications (SPCOM), 2022, 1-4. doi: 10.1109/spcom55316.2022.9840768.

[39] Malpani, P.; Kumar, S.; Pathak, A. “Implementation of Coherent One Way Protocol fFor Quantum Key Distribution UUp tTo aAn Effective Distance of 145 km,” Opt. Quantum Electron. 2024, 56, 1369. doi: 10.1007/s11082-024-06934-2.