Scientific Journal of Electronic & Cyber Defense
Vol. 12, No. 2, Summer 2024, Serial No. 46
ISSN: 2322-4347 , E-ISSN: 2980-8979

Introducing a decoy-state version of the high-dimensional polarization-phase (PoP) quantum key distribution protocol and explaining its implementation

A. Mehri Toonabi[1], M. Davoudi[2]*
Assistant Professor, Malek Ashtar University of Technology, Shahin Shahr, Esfahan, Iran.
(Received: 2024/04/17, Revised: 2024/07/06, Accepted: 2024/08/03, Published: 2024/08/31)
DOR:

ABSTRACT

Single-photon generation is a constant problem in the experimental implementation of quantum key distribution (QKD) systems. Using the attenuated laser pulses is a standard process for generating single photons. In this case, the number of photons follows a Poisson distribution. Such pulses are highly vulnerable to the photon number splitting (PNS) attack. The decoy-state protocol is proposed as an important and effective weapon to deal with the PNS attack. High-dimensional quantum states are another solution to improve the performance of quantum communication systems in the presence of non-ideal components. Generally, the processes related to the production, control, transmission, and detection of high-dimensional quantum states are complex and expensive. The PoP protocol is a high-dimensional QKD protocol based on the polarization and phase of single photons, which, unlike most existing high-dimensional protocols, is simple and contains well-known general components such as conventional optical sources and quantum channels. Using decoy states in the PoP protocol can be a simple and effective solution to reduce the limitations caused by the use of imperfect and non-ideal components in quantum communication systems. This idea significantly improves the main parameters related to the performance of QKD systems (i.e., secure key generation rate and secure transmission distance). In this paper, a decoy-state version of the PoP protocol is introduced. Also, the details related to the schematic of the implementation, the execution method, and the classical post-processing operations required to extract its secure key are explained. .

Keywords: Quantum cryptography , Quantum key distribution, QKD , polarization , phase, BB84 protocol, decoy states, High-dimensional QKD.

*Corresponding Author Email: m.davoudi@mut-es.ac.ir

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۲، تابستان ۱۴۰۳، ص ۱۰۷-۹۹

علمی – پژوهشی

معرفی یک نسخه حالت فریب از پروتکل چندبعدی قطبش– فاز و تشریح نحوه پیاده‌سازی و اجرای آن

علی مهری تونابی[۱]، مهدی داودی دراره[۲*]

۱- مربی. ۲- استادیار، دانشگاه صنعتی مالک‌اشتر، شاهین‌شهر، اصفهان، ایران.

(دریافت: ۱۴۰۳/۰۱/۲۹، بازنگری: ۱۴۰۳/۰۴/۱۶، پذیرش: ۱۴۰۳/۰۵/۱۳، انتشار: ۱۴۰۳/۰۶/۱۰)

DOR:

چکیده

یک مشکل همیشگی در پیاده‌سازی تجربی سامانه‌های توزیع کلید کوانتومی (QKD)، تولید تک فوتون است. روند متداولی که برای تولید تک فوتون‌ها به کار می‌رود، استفاده از پالس‌های لیزری تضعیف شده است. در این صورت، شمار فوتون‌ها از یک توزیع پواسونی پیروی می‌کند. این‌گونه پالس‌ها در برابر حمله شناخته شده تقسیم تعداد فوتون (PNS) به‌شدت آسیب‌پذیر هستند. پروتکل حالت‌های فریب به‌عنوان یک سلاح مهم و مؤثر برای مقابله با حمله PNS پیشنهاد شده است. استفاده از حالت‌های کوانتومی چندبعدی یک راه‌حل دیگر برای بهبود عملکرد سامانه‌های ارتباط کوانتومی در حضور قطعات غیر ایده‌آل است. در حالت کلی فرایندهای مربوط به تولید، کنترل، انتقال و آشکارسازی حالت‌های کوانتومی چندبعدی پیچیده و پرهزینه است. پروتکل PoP یک پروتکل QKD چندبعدی بر مبنای قطبش و فاز تک فوتون‌ها است که برخلاف اغلب پروتکل‌های چندبعدی موجود، یک پروتکل ساده است و در آن از قطعات شناخته شده متداول (ازجمله چشمه‌های نوری و کانال‌های کوانتومی مرسوم) استفاده می‌شود. ترکیب پروتکل‌های حالت فریب و PoP می‌تواند یک راهکار ساده و کارآمد برای کاهش محدودیت‌های ناشی از قطعات ناکامل و غیر ایده‌آل در سامانه‌های ارتباط کوانتومی باشد و پارامترهای اصلی در سنجش عملکرد سامانه‌های توزیع کلید کوانتومی (نرخ تولید کلید امن و مسافت انتقال امن) را به میزان قابل‌توجهی بهبود ببخشد. در این مقاله، نسخه حالت فریب پروتکل PoP معرفی شده است. همچنین جزئیات مربوط به شماتیک پیاده‌سازی، نحوه اجرا و روش استخراج کلید امن این پروتکل تشریح شده است.

کلیدواژه‌ها: رمزنگاری کوانتومی، توزیع کلید کوانتومی، QKD، قطبش، فاز، پروتکل BB84، حالت‌های فریب، QKD چندبعدی

۱- مقدمه

استفاده از قوانین بنیادین مکانیک کوانتوم برای تولید و توزیع کلید تصادفی یک‌بار مصرف[۲] با طول دلخواه و در شرایط کاملاً امن، اصطلاحاً توزیع کلید کوانتومی[۳] (QKD) نامیده می‌شود. پروتکل BB84 نخستین و مهم‌ترین پروتکل QKD است [۱]. با وجود پروتکل‌های متنوعی که پس از آن ارائه شده است [۹-۲]، کماکان پروتکل BB84 نسبت به سایر پروتکل‌ها از استقبال بیش‌تری برخوردار است. یکی از مشکلات پیاده‌سازی سامانه‌های QKD، تولید تک‌فوتون است. یک روند متداول برای تولید تک‌فوتون‌ها، استفاده از پالس‌های لیزری تضعیف شده است. با ایجاد میانگین تعداد فوتون[۴] (MPN) خیلی کم‌تر از ۱، احتمال وجود دو یا بیش‌تر از دو فوتون در یک پالس به میزان بسیار زیادی کاهش می‌یابد. پالس‌های چندفوتونی در برابر حمله تقسیم تعداد فوتون[۵] (PNS) به شدت آسیب‌پذیر هستند [۱۰و۱۱]. برای مقابله با حمله PNS باید از چشمه‌هایی استفاده شود که در مقایسه با نور پواسونی بتوانند تقریب بهتری از حالت‌های تک‌فوتون را ایجاد کنند. یک راه برای کاهش این حملات، استفاده از دستگاه‌های تولید تک‌فوتون است که منابع نور زیرپواسونی[۶] نامیده می‌شوند [۱۶-۱۲]. میزان قابل قبول برای تلفات کانال کوانتومی در حضور منابع زیرپواسونی به‌طور قابل‌توجهی بزرگ‌تر از منابع پواسونی است [۱۷]. بنابراین استفاده از

*رایانامه نویسنده مسئول: m.davoudi@mut-es.ac.ir

[2] One-time-pad
[3] Quantum Key Distribution (QKD)
[3] Mean Photon Number (MPN)
[5] Photon Number Splitting (PNS)
[5] Sub-Poisson light sources

منابع نور زیرپواسونی عملکرد سامانه‌های QKD را عمیقاً بهبود می بخشد؛ اما از یک سو، هزینه تولید یک منبع زیرپواسونی خیلی بیش‌تر از یک لیزر است و از سوی دیگر، مشکلاتی در کاربرد تجربی منابع زیرپواسونی (مانند حساسیت بیش از حد نسبت به نویزهای زمینه و برخی پیچیدگی‌ها در روش آشکارسازی آن‌ها) وجود دارد که استفاده از آن‌ها را دشوار می‌کند.

با معرفی شکل جدیدی از برپایی پروتکل‌های QKD، تحت عنوان پروتکل حالت‌های فریب[1] [۲۳-۱۸]، میزان تمایل به استفاده از منابع زیرپواسونی به‌طور محسوسی کاهش یافت؛ زیرا به‌جای روبه‌رو شدن با دشواری‌های استفاده از منابع زیرپواسونی، می‌توان نرخ مشابهی را با کمک لیزر و با استفاده از حالت‌های فریب به دست آورد [۲۴].

با گذار از سامانه‌های کوانتومی با فضای هیلبرت[2] دو بعدی (کیوبیت‌ها) به سامانه‌های کوانتومی با فضای هیلبرت d بعدی (کیودیت‌ها[3]) [۲۵]، می‌توان به مزایای قابل توجهی از جمله افزایش ظرفیت اطلاعاتی حالت‌های کوانتومی [۲۶]، افزایش ظرفیت کانال کوانتومی [۲۷و۲۸]، افزایش نرخ کلید امن [۲۹] و افزایش مقاومت در برابر نویزهای محیطی و خطاهای ایجاد شده توسط اخلال‌گر [۳۲-۳۰] دست یافت [۳۳].

سامانه‌های QKD چندبعدی، علی‌رغم مزایای متعددی که نسبت به سامانه‌های دوبعدی دارند، معمولاً از یک مشکل بزرگ رنج می‌برند: پیچیدگی در برپایی و اجرا. در حالت کلی، فرایندهای مربوط به تولید، کنترل، انتقال و آشکارسازی کیودیت‌ها پیچیده‌تر و پرهزینه‌تر از کیوبیت‌ها است.

پروتکل ترکیبی قطبش-فاز[4] (PoP) [۳۴و ۳۵]، یک پروتکل QKD چند بعدی[5] (HD-QKD) است که در آن، مبادله کیودیت‌ها با استفاده از دو درجه آزادی فوتونی قطبش و فاز مربوط به یک ذره و از طریق ترکیب پروتکل‌های BB84 استاندارد قطبشی [۱] و فازی [۳۶] صورت می‌گیرد. برخلاف اغلب پروتکل‌های چند بعدی موجود، فرایند تولید کیودیت‌ها در این پروتکل ساده است و با استفاده از قطعات شناخته شده متداول (ازجمله چشمه‌های نوری و کانال‌های کوانتومی مرسوم) انجام می‌گیرد. این پروتکل، عملکرد سامانه‌های QKD در حالت استفاده از مولفه‌های غیرایده‌آل را به میزان قابل توجهی ارتقاء می‌دهد.

در این مقاله، با ترکیب پروتکل‌های چندبعدی و پروتکل‌های مبتنی بر حالت فریب، بدون به‌کارگیری هرگونه مؤلفه مختص سامانه‌های چندبعدی و تنها با استفاده از قطعات ناکامل متداول و در قالب یک طراحی ساده، به‌صورت هم‌زمان از مزایای ناشی از هر دو پروتکل بهره برده می‌شود. برای این منظور، پروتکل چندبعدی PoP مبتنی بر حالت‌های فریب معرفی می‌شود و جزئیات مربوط به پیاده‌سازی، اجرا، پساپردازش کلاسیک، نحوه ارزیابی امنیت و استخراج کلید امن در آن تشریح می‌گردد. این ایده می‌تواند یک راهکار ساده و کارآمد برای کاهش محدودیت‌های ناشی از قطعات تجربی در سامانه‌های ارتباط کوانتومی در اختیار بگذارد و نرخ تولید کلید امن و مسافت انتقال امن سامانه را بهبود ببخشد.

ساختار این مقاله بدین صورت شکل‌گرفته است: در بخش دوم، مبانی پروتکل‌های QKD دوبعدی حالت فریب بیان می‌شود. در بخش سوم، مبانی پروتکل‌های QKD چندبعدی ترکیب شده با حالت‌های فریب بیان می‌شود. در بخش چهارم، پروتکل چندبعدی PoP مبتنی بر حالت‌های فریب، معرفی و جزئیات مربوط به شماتیک پیاده‌سازی و نحوه اجرای آن تشریح می‌شود. در بخش پنجم، گام‌به‌گام عملیات پساپردازش کلاسیک و نحوه ارزیابی امنیت و استخراج کلید امن این پروتکل بیان می‌شود. نهایتاً در بخش ششم، نتایج و دستاوردهای این ایده بیان می‌شود.

۲- پروتکل‌های QKD حالت فریب

در پالس‌های لیزری تضعیف شده، آمار فوتون‌ها از یک توزیع پواسونی[6] پیروی می‌کند [۳۷]. هرچه میانگین تعداد فوتون‌های موجود در یک پالس لیزری (μ) کوچک‌تر باشد، احتمال وجود پالس‌های چند فوتونی در آن کم‌تر است. باوجود تمایل اولیه به کاهش هرچه بیش‌تر مقدار μ جهت غلبه بر حمله PNS، متأسفانه نمی‌توان آن را به هر میزان دلخواهی کوچک کرد؛ زیرا μ خیلی کوچک، منجر به ضعیف شدن توان کوانتومی سامانه می‌شود و نرخ تولید کلید امن را به شدت کاهش می‌دهد. بنابراین لازم است روشی را بکار بگیریم که با وجود کار کردن در مقدار μ نزدیک به ۱، امنیت فرایند توزیع کلید در مقابل حملات PNS را تضمین کند. پروتکل حالت‌های فریب دقیقاً برای پاسخ به همین نیاز پیشنهاد شده است.

ایده اصلی در پروتکل حالت‌های فریب این است که فرستنده پیام (آلیس[7]) افزون بر دنباله پالس‌های تک فوتونی که آن‌ها را برای کد کردن اطلاعات کوانتومی به کار می‌گیرد (حالت‌های سیگنال)، دنباله‌ای پالسی از حالت‌های فریب که در واقع حاوی هیچ‌گونه اطلاعات مفید و معنی‌داری نیستند را نیز ارسال می‌کند. حالت‌های سیگنال در تولید کلید محرمانه و حالت‌های فریب برای تحلیل امنیت به کار می‌روند. حالت‌های سیگنال و فریب از نظر همه خصوصیات فیزیکی (همانند طول‌موج، نرخ تکرار، اطلاعات زمانی و دیگر پارامترها) کاملاً یکسان هستند و

[1] Decoy states protocol
[2] Hilbert space
[3] Qudits
[4] Polarization-Phase (PoP) protocol
[5] High-Dimensional QKD (HD-QKD)
[6] Poisson distribution
[7] Alice

تنها تفاوت بین آن‌ها، شدت یا همان پارامتر μ است. ازآنجاکه آلیس به‌صورت کاملاً تصادفی انتخاب می‌کند که یک حالت فریب را ارسال کند یا یک پالس سیگنال را، بنابراین اخلال‌گر احتمالی (ایو[1]) هیچ راهی برای تفکیک دو حالت از یکدیگر در اختیار ندارد. در واقع این پروتکل اجازه می‌دهد که از طریق انتقال و سپس بررسی خصوصیات انتقالی چند حالت فریب، شرایط مناسب‌تری جهت کشف حضور ایو فراهم شود. می‌توان نشان داد که در پروتکل‌های QKD باحالت فریب، مقدار بهینه میانگین تعداد فوتون‌های سیگنال، μ_{opt}، خیلی بزرگ‌تر از پروتکل‌های استاندارد با منبع نور پواسونی است [۲۴] و این امر دستیابی به نرخ کلید امن بالاتر و رسیدن به مسافت‌های انتقال بزرگ‌تر را ممکن می‌سازد.

در اجرای سامانه‌های QKD با حالت فریب، می‌بایست یک مدوله کننده‌ی شدت[2] به چیدمان آلیس اضافه شود تا بتواند حالت‌های همدوس با MPN متغیر را برای گیرنده پیام (باب[3]) ارسال کند. در عمل، به‌جای استفاده از تعداد نامحدودی از حالت‌های فریب، آلیس می‌تواند از یک حالت سیگنال با MPN از مرتبه‌ی ۱ و تنها از دو حالت فریب، یکی با تعداد فوتون کم‌تر از واحد (حالت ضعیف[4]) و دیگری بدون فوتون (حالت خلأ) استفاده کند. این ایده را پروتکل با دو حالت فریب خلأ + ضعیف[5] می‌نامند که اولین بار در [۱۹] مطرح شد و سپس امنیت آن در مقابل حملات متداول در [۲۰] اثبات گردید و نتایج آن نشان داد که عملکرد پروتکل حالت فریب خلأ + ضعیف به حد عملکرد استفاده از تعداد نامحدودی از حالت‌های فریب میل می‌کند. در پروتکل خلأ + ضعیف، از حالت خلأ برای تخمین نرخ آشکارسازی زمینه و تعیین نرخ شمارش تاریک آشکارساز استفاده می‌شود، درحالی‌که حالت ضعیف برای محاسبه محدوده‌های مورد نیاز و افزایش احتمال شناسایی مداخله PNS (از طریق اختلاف آماری آن با حالت سیگنال) به کار می‌رود. بهینه‌سازی‌های مورد نیاز برای انتخاب شدت حالت‌های سیگنال و فریب در [۲۰] انجام شده است. پروتکل خلأ + ضعیف بدلیل ارائه عملکردی کاملاً نزدیک به حالت استفاده از منابع تک‌فوتون ایده‌آل، یک گزینه جذاب برای برپایی سامانه‌های تجربی رمزنگاری کوانتومی است.

۳- پروتکل‌های QKD چند بعدی حالت فریب

می‌توان با کمک سامانه‌های فیزیکی چهار ترازی، حالت‌های کوانتومی چهار بعدی، که اصطلاحاً کوانتوم کوارت (کیوکوارت)[6] نامیده می‌شوند، را تولید کرد و پروتکل BB84 استاندارد را به پروتکل BB84 چهار بعدی گسترش داد. درصورت اجرای سامانه‌های QKD چند بعدی به روش حالت فریب خلأ + ضعیف، که از یک منبع پواسونی برای تولید حالت‌های سیگنال و فریب به ترتیب با میانگین تعداد فوتون‌های μ و ν در وضعیت $\nu \ll \mu < 1$ بهره می‌گیرد، می‌توان نرخ کلید امن یک سامانه d بعدی که از M پایه متقابلاً بایاس نشده[7] (MU) [۳۸] استفاده می‌کند را در کلی‌ترین حالت، به صورت زیر نوشت [۳۲]:

$$R^{Decoy\ HD} \geq \frac{1}{M} f_{rep}(Q_0\, log_2(d) + Q_1[log_2(d) - h^{(d)}(e_1)] - Q_\mu\, f(E_\mu)\, h^{(d)}(E_\mu)), \quad (۱)$$

که f_{rep} نرخ تکرار پالس‌های لیزر، $Q_0\, log_2(d)$ بهره مربوط به شمارش‌های تاریک آشکارساز (که ایو هیچ گونه اطلاعاتی در مورد آن‌ها ندارد)، Q_1 و e_1 به ترتیب بهره و QBER حالت‌های سیگنال تک‌فوتونی، Q_μ و E_μ به ترتیب بهره و QBER حالت‌های سیگنال، Q_ν و E_ν به ترتیب بهره و QBER حالت فریب ضعیف، $h^{(d)}(x) := -x \log_2(x/(d-1)) - (1-x)\log_2(1-x)$ تابع آنتروپی شانون d بعدی و f تابع بازدهی الگوریتم تصحیح خطا هستند. با تعیین یک مقدار کمینه برای Q_1 و یک مقدار بیشینه برای e_1، می‌توان کمینه نرخ کلید امن را به دست آورد [۲۰].

در سامانه‌های تجربی، مقادیر Q_0، Q_μ، E_μ، Q_ν و E_ν را می‌توان به ترتیب با ارسال جداگانه حالت‌های خلأ، سیگنال و فریب ضعیف توسط آلیس، به طور مستقیم اندازه گرفت و پس از مقایسه با روابط نظری موجود، سامانه را اعتبارسنجی کرد.

۴- معرفی پروتکل چند بعدی PoP در حضور حالت‌های فریب

پروتکل قطبش - فاز (PoP) یک پروتکل چندبعدی است که با ترکیب پروتکل‌های متداول BB84 قطبشی و فازی به دست می‌آید. در این پروتکل، از دو درجه آزادی فاز (با نماد ph) و قطبش (با نماد po) مربوط به یک فوتون، به‌صورت آمیخته (هیبریدی)، برای کدگذاری اطلاعات در چارچوب حالت‌های کوانتومی چندبعدی (کیودیت‌ها) استفاده می‌شود. حالت کلی پروتکل d بعدی PoP به‌صورت $\mathrm{PoP}^{(d,M)}$ بیان می‌شود که در آن، $d > 2$ بعد کیودیت‌های آمیخته و M تعداد پایه‌های MU است. در صورت افزایش ابعاد فضای هیلبرت به چهار بعد و کدگذاری حالت‌های کوانتومی چهار بعدی (کیوکوارت‌ها) به وسیله دو پایه MU، نخستین حالت چند بعدی از پروتکل $\mathrm{PoP}^{(d,M)}$ به دست می‌آید، که به اختصار آن‌را پروتکل $\mathrm{PoP}^{(4,2)}$ می‌نامیم. در پروتکل $\mathrm{PoP}^{(4,2)}$ از کیودیت‌های چهار بعدی استفاده می‌شود. بنابراین این پروتکل قادر است چهار نماد α، β، γ و δ را منتقل کند، که این نمادها به صورت زیر به ترتیب متناظر با حالت‌های کوانتومی $|0\rangle$، $|1\rangle$، $|2\rangle$

[1] Eve
[2] Intensity modulator
[3] Bob
[4] Weak state
[5] vacuum+weak
[6] Quantum quart (qu-quart)
[7] Mutually Unbiased (MU)

و $|3\rangle$ خواهند بود [۳۴]:

$$\begin{aligned}\alpha &\equiv |0\rangle_{PoP^{(4,2)}} = |00\rangle_{ph\otimes po} = |0\rangle_{ph}\otimes|0\rangle_{po},\\ \beta &\equiv |1\rangle_{PoP^{(4,2)}} = |01\rangle_{ph\otimes po} = |0\rangle_{ph}\otimes|1\rangle_{po},\\ \gamma &\equiv |2\rangle_{PoP^{(4,2)}} = |10\rangle_{ph\otimes po} = |1\rangle_{ph}\otimes|0\rangle_{po},\\ \delta &\equiv |3\rangle_{PoP^{(4,2)}} = |11\rangle_{ph\otimes po} = |1\rangle_{ph}\otimes|1\rangle_{po}.\end{aligned} \quad (۲)$$

برای اجرای پروتکل $\mathrm{PoP}^{(4,2)}$ حالت فریب خلأ + ضعیف، می‌توان از چیدمانی مشابه شکل (۱) استفاده کرد. اولین گام از اجرای این پروتکل، انتقال کوانتومی[1] است. برای اجرای این گام، ابتدا تعداد N بیت تصادفی توسط یک دستگاه مولد اعداد تصادفی کوانتومی[2] (QRNG) در اختیار آلیس قرار می‌گیرد. سپس این N بیت به $N/2$ دسته دو بیتی تقسیم می‌شوند، که هر دسته تشکیل یک کیوکارت می‌دهد و هر یک از کیوکوارت‌ها متناظر با یک نماد چهار بعدی هستند. پالس‌های لیزری آلیس با عبور از یک قطبنده خطی (Pol) عمودی، قطبش مناسب برای عملکرد بهینه مدولاتور فاز آلیس (PM_A) را به خود می‌گیرند. پس از آن، یک تابع تولید اعداد شبه‌تصادفی با توجه به احتمال وقوع از قبل مشخص شده (مثلاً با نسبت ۷:۲:۱ از سمت راست به ترتیب برای حالت‌های خلأ، فریب و سیگنال)، تعیین می‌کند که هر یک از پالس‌ها می‌بایست توسط مدولاتور شدت (IM)، به یک حالت سیگنال با میانگین تعداد فوتون μ، یا یک حالت فریب با میانگین تعداد فوتون ν و یا یک حالت خلأ با میانگین تعداد فوتون تقریباً صفر تبدیل شود. توجه شود که دیگر مشخصات تمام پالس‌ها، از جمله طول موج و دوره زمانی می‌بایست کاملاً یکسان و مشابه باشد، بطوری‌که ایو تا قبل از اجرای غربال‌گری[3] جداگانه روی پالس‌های سیگنال و فریب نتواند یک حالت سیگنال را از حالت فریب و خلأ تشخیص دهد.

پس از IM، پالس‌ها توسط یک پرتو شکاف ۵۰/۵۰ با احتمال برابر وارد یکی از دو بازوی تداخل‌سنج نامتوازن آلیس می‌شوند. اگر فوتون وارد بازوی کوتاه تداخل‌سنج آلیس (s_A) شود، در مدولاتور فاز آلیس (PM_A)، ابتدا یکی از پایه‌های Ψ یا Φ به تصادف انتخاب می‌شود و سپس با توجه به نماد تصادفی که از QRNG دریافت می‌شود، مطابق جدول (۱-الف)، یکی از چهار فاز "0، π، $\pi/2$ و $3\pi/2$" به فوتون اعمال می‌شود ($\emptyset_A$). اما اگر فوتون از بازوی بلند تداخل‌سنج آلیس (l_A) بگذرد فازی روی آن اعمال نمی‌شود. در ادامه، در واحد آماده‌سازی قطبش مربوط به آلیس ($Pol.Mod_A$)، یکی از چهار قطبش "0، 90، 45 و 135 درجه (نسبت به محور افق)"، با توجه به جدول (۱-الف) و متناظر با همان پایه و نمادی که پیش از این در واحد آماده‌سازی فاز انتخاب شده بود، به فوتون اعمال می‌شود (P_A). آلیس پایه‌ها-ی تصادفی انتخاب شده را ثبت می‌کند و فوتون‌ها را در فواصل زمانی منظم و از طریق کانال کوانتومی برای باب ارسال می‌نماید.

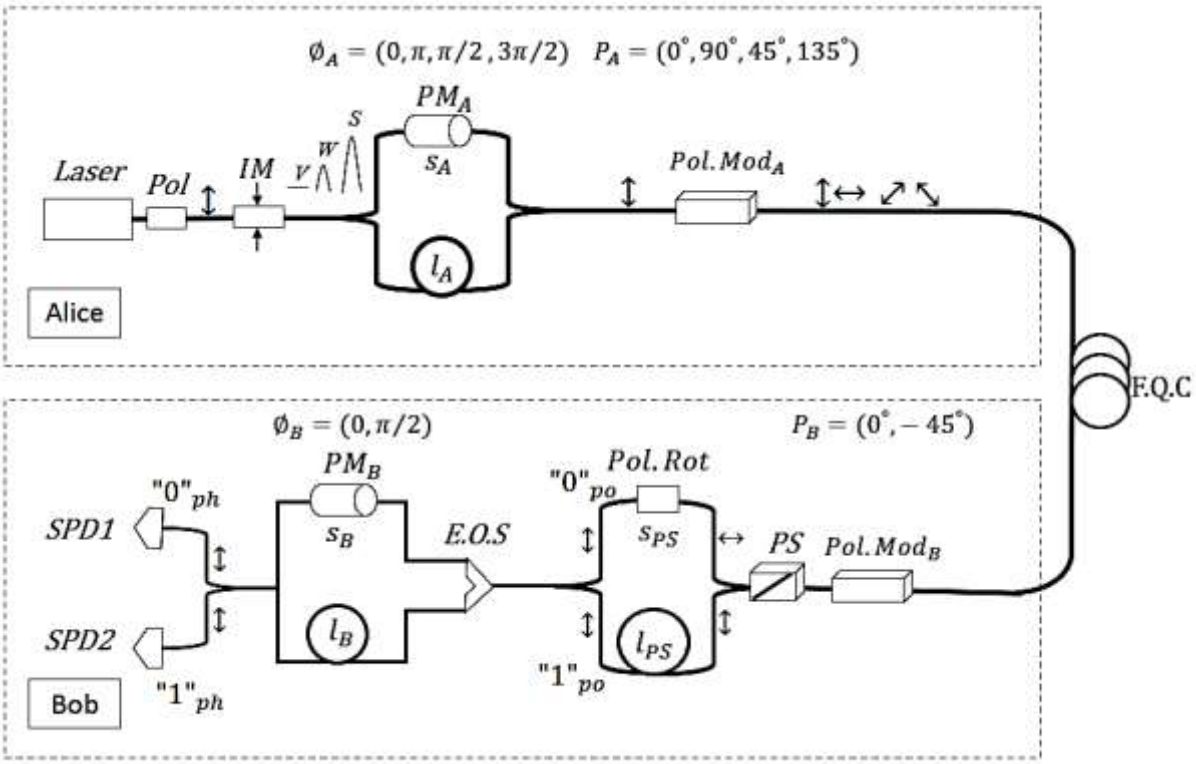
در زیرسامانه باب، برای هر پالس ارسالی آلیس، ابتدا یکی از پایه‌های تصادفی Ψ یا Φ توسط QRNG باب انتخاب و در اختیار مدولاتور قطبش باب ($Pol.Mod_B$) قرار می‌گیرد. سپس $Pol.Mod_B$ با توجه به جدول (۱-ب)، چرخش قطبش متناظر با آن پایه را به فوتون اعمال و قطبش آن‌را اندازه‌گیری می‌کند (P_B). اگر پایه‌های مشابه برای آماده‌سازی و اندازه‌گیری قطبش انتخاب شده باشند، فوتون از یک بازوی مشخص پرتوشکاف قطبشی (PS) عبور خواهد کرد. در غیر این صورت، با احتمال ۵۰٪ وارد هر یک از بازوهای کوتاه و بلند PS (به ترتیب s_{PS} و l_{PS}) می‌شود. بعداً با استفاده از زمان رسیدن فوتون به یکی از آشکارسازها، می‌توان تعیین کرد که آن فوتون از کدام بازوی PS عبور کرده است. اگر فوتون از بازوی s_{PS} عبور کرده باشد به آن بیت قطبش 0 و اگر از بازوی l_{PS} عبور کرده باشد بیت قطبش 1 نسبت داده می‌شود. توجه شود که فوتون‌هایی که از بازوی s_{PS} عبور می‌کنند دارای قطبش افقی هستند. به عنوان یک نکته کاربردی مهم، برای ایجاد یک تداخل با کیفیت، لازم است قطبش این فوتون‌ها نیز همانند قطبش فوتون‌های بازوی l_{PS} به صورت عمودی و منطبق بر قطبش مناسب برای عملکرد بهینه مدولاتور فاز باب (PM_B) باشد. این کار توسط یک چرخاننده قطبش ($Pol.Rot$) انجام می‌شود. در اقدام بعد، فوتون‌هایی که از بازوی s_A عبور کرده‌اند، با استفاده از یک سوییچ الکترواپتیکی ($E.O.S$) وارد بازوی بلند تداخل‌سنج نامتوازن باب (l_B) می‌شوند و برعکس. این ترفند باعث حذف مسیرهای غیرتداخلی s_As_B و l_Al_B می‌شود و پارامتر غربال‌گری سامانه را دو برابر می‌کند. اگر فوتون وارد بازوی s_B شود، مطابق جدول (۱-ب) و متناظر با همان پایه‌ایی که پیش از این در واحد $Pol.Mod_B$ انتخاب شده بود، فاز آن توسط PM_B اندازه‌گیری و ثبت می‌شود ($\emptyset_B$). اگر $\Delta\emptyset = |\emptyset_B - \emptyset_A| = 0\ (\pi)$، فوتون قطعاً به آشکارساز تک‌فوتون $SPD1$ ($SPD2$) می‌رسد و بیت فاز 0 (1) به آن نسبت داده می‌شود. در غیر این صورت، $\Delta\emptyset = \pi/2\ (3\pi/2)$ و مسیر فوتون به سمت آشکارسازها قطعی نیست و فوتون با احتمال یکسان ممکن است وارد هر یک از دو آشکارساز شود. واضح است که هر یک از دو آشکارساز ممکن است در یکی از دو زمان زیر برخورد یک فوتون را ثبت کند:

$$\begin{aligned}t_1 &\equiv s_A(l_A)\ s_{PS}\ l_B(s_B),\\ t_2 &\equiv s_A(l_A)\ l_{PS}\ l_B(s_B).\end{aligned}$$

تیک خوردن آشکارساز $SPD1$ در زمان t_1 به معنای دریافت نماد α و در زمان t_2 به معنای دریافت نماد β خواهد بود. همچنین تیک خوردن آشکارساز $SPD2$ در زمان t_1 به معنای دریافت نماد γ و در زمان t_2 به معنای دریافت نماد δ است.

باتوجه‌به آنچه گفته شد، می‌توان شبه کد یا الگوریتم اجرای پروتکل $\mathrm{PoP}^{(4,2)}$ به روش حالت فریب خلأ + ضعیف را در جدول (۲) خلاصه کرد.

[1] Quantum transmission
[2] Quantum Random Number Generator (QRNG)
[3] Sifting



شکل (۱): شماتیک چیدمان پروتکل $PoP^{(4,2)}$ به روش حالت فریب خلأ + ضعیف.

Pol: قطبنده خطی؛ IM: مدولاتور شدت؛ V، W و S به ترتیب برای نمایش پالس‌های خلأ، ضعیف و سیگنال؛ PM_A و PM_B به ترتیب مدولاتورهای فاز آلیس و باب؛ $Pol.Mod_A$ و $Pol.Mod_B$: به ترتیب مدولاتورهای قطبش آلیس و باب؛ $F.Q.C$: کانال کوانتومی فیبری؛ PS: پرتوشکاف قطبشی؛ $Pol.Rot$: چرخاننده قطبش؛ $E.O.S$: سوییچ الکترواپتیکی؛ SPD: آشکارساز تک‌فوتون.

جدول (۱): قراردادهای پروتکل $PoP^{(4,2)}$.

الف) قراردادهای مربوط به آلیس؛ ب) قراردادهای مربوط به باب. توجه شود که زوایای قطبش نسبت به محور افقی در نظر گرفته شده‌اند.

(الف)

Alice's preparation			
Basis	Symbol	Phase $\emptyset_A$	Polarization P_A
	α	0	0°
Ψ	β	0	90°
	γ	π	0°
	δ	π	90°
	α	$\pi/2$	45°
Φ	β	$\pi/2$	135°
	γ	$3\pi/2$	45°
	δ	$3\pi/2$	135°

(ب)

Bob's measurement		
Basis	Polarization rotation P_B	Phase $\emptyset_B$
Ψ	0°(off)	0
Φ	-45° (on)	$\pi/2$

جدول (۲): الگوریتم اجرای پروتکل $PoP^{(4,2)}$ به روش حالت فریب خلأ + ضعیف.

زیرسامانه‌ها	گام‌های فرعی	نحوه اجرای گام‌ها
۱- زیرسامانه آلیس	۱-۱: دریافت بیت‌های تصادفی	تعداد N بیت تصادفی از یک QRNG در اختیار آلیس قرار می‌گیرد. سپس این N بیت به $N/2$ دسته دو بیتی (کیوکارت) تقسیم می‌شوند. هر یک از کیوکوارت‌ها متناظر با یکی از چهار نماد α، β، γ و δ هستند.
	۱-۲: تنظیم قطبش پالس‌ها	پالس‌های لیزری آلیس با عبور از یک قطبنده خطی ثابت، به‌صورت عمودی قطبیده می‌شوند (قطبش مناسب برای عملکرد بهینه مدولاتور فاز آلیس).
	۱-۳: تنظیم شدت پالس‌ها	مدولاتور شدت آلیس، شدت هر یک از پالس‌ها را باتوجه‌به یک احتمال وقوع مشخص، بر روی یک حالت سیگنال با میانگین تعداد فوتون μ، یا یک حالت فریب با میانگین تعداد فوتون ν و یا یک حالت خلأ تنظیم می‌کند.
	۱-۴: انتخاب پایه آماده‌سازی	برای هر یک از پالس‌های آلیس، یکی از پایه‌های Ψ یا Φ توسط QRNG به‌تصادف انتخاب می‌شود.
	۱-۵: اعمال فاز	مدولاتور فاز آلیس باتوجه‌به نماد و پایه تصادفی که به ترتیب در گام‌های ۱-۱ و ۱-۴ دریافت شده، یکی از چهار فاز "0، π، $\pi/2$ و $3\pi/2$" را مطابق جدول (۱-الف) به فوتون‌هایی که از بازوی کوتاه تداخل‌سنج آلیس عبور می‌کنند اعمال می‌کند ($\emptyset_A$).
	۱-۶: اعمال قطبش	مدولاتور قطبش آلیس باتوجه‌به نماد و پایه تصادفی که به ترتیب در گام‌های ۱-۱ و ۱-۴ از QRNG دریافت شده است، یکی از چهار قطبش "0، 90، 45 و 135 درجه (نسبت به محور افق)" را مطابق جدول (۱-الف) به فوتون اعمال می‌کند (P_A).
	۱-۷: ارسال حالت‌های کوانتومی	آلیس برای هر یک از پالس‌ها، موارد انتخاب شده در گام‌های ۱-۱، ۱-۳، ۱-۴، ۱-۵ و ۱-۶ را ثبت و فوتون‌ها را در فواصل زمانی منظم و از طریق کانال کوانتومی برای باب ارسال می‌کند.
۲- زیرسامانه باب	۲-۱: انتخاب پایه اندازه‌گیری	برای هر پالس دریافتی از آلیس، یکی از پایه‌های تصادفی Ψ یا Φ توسط QRNG باب انتخاب می‌شود.
	۲-۲: اندازه‌گیری قطبش	مدولاتور قطبش باب باتوجه‌به پایه تصادفی انتخاب شده در گام ۲-۱ و مطابق جدول (۱-ب)، چرخش قطبش متناظر را به فوتون اعمال و قطبش آن‌را اندازه‌گیری می‌کند (P_B).
	۲-۳: تفکیک قطبش‌های متعامد	اگر پایه‌های تصادفی انتخاب شده در گام‌های ۱-۴ و ۲-۱ مشابه باشند، فوتون از یک بازوی مشخص پرتوشکاف قطبشی باب عبور می‌کند. در غیر این صورت، با احتمال ۵۰٪ وارد هر یک از بازوهای کوتاه و بلند آن می‌شود. فوتونی که از بازوی کوتاه عبور می‌کند قطبش افقی آن توسط یک چرخاننده قطبش به قطبش عمودی تبدیل می‌شود.
	۲-۴: حذف مسیرهای غیرتداخلی	فوتونی که از بازوی کوتاه تداخل‌سنج آلیس عبور می‌کند، با استفاده از یک سوئیچ الکترواپتیکی وارد بازوی بلند تداخل‌سنج باب می‌شود و برعکس. این ترفند باعث حذف مسیرهای غیرتداخلی کوتاه - کوتاه و بلند - بلند می‌شود.
	۲-۵: اندازه‌گیری فاز	اگر فوتون وارد بازوی کوتاه تداخل‌سنج باب شود، باتوجه‌به پایه تصادفی انتخاب شده در گام ۲-۱ و مطابق جدول (۱-ب)، یکی از فازهای "0 و $\pi/2$" توسط مدولاتور فاز باب به آن اعمال می‌شود ($\emptyset_B$).
	۲-۶: تعیین نتایج اندازه‌گیری قطبش و فاز	اگر $\Delta\emptyset = \lvert\emptyset_B - \emptyset_A\rvert = 0\ (\pi)$، فوتون قطعاً به آشکارساز تک‌فوتون ۱ (۲) می‌رسد و بیت فاز 0 (1) به آن نسبت داده می‌شود. در غیر این صورت، $\Delta\emptyset = \pi/2\ (3\pi/2)$ و فوتون با احتمال یکسان ممکن است وارد هر یک از دو آشکارساز شود. با استفاده از زمان رسیدن فوتون به آشکارساز، تعیین می‌شود که فوتون از کدام بازوی پرتو شکاف قطبشی باب عبور کرده است. اگر فوتون از بازوی کوتاه (بلند) عبور کرده باشد به آن بیت قطبش 0 (1) نسبت داده می‌شود.
۳- پساپردازش کلاسیک	گام‌به‌گام عملیات پساپردازش کلاسیک و نحوه ارزیابی امنیت و استخراج کلید امن، در بخش ۵ آمده است.	

۵- گام به گام عملیات پساپردازش کلاسیک و نحوه ارزیابی امنیت و استخراج کلید امن

پس از اتمام انتقال کوانتومی، عملیات پساپردازش کلاسیک انجام می‌شود. برای این منظور در گام اول، آلیس و باب فرایند غربال-گری را به‌صورت زیر انجام می‌دهند:

باب پایه‌هایی را که برای اندازه‌گیری هر کیوبیت استفاده کرده است به آلیس اعلام می‌کند. آلیس پاسخ می‌دهد که کدام-یک از پایه‌های باب درست بوده است و علاوه بر این، حالت هر کیوبیت، اعم از سیگنال، فریب و خلأ را نیز به باب می‌گوید. آلیس و باب روی کیوبیت‌های مربوط به حالت‌های سیگنال و فریب که برای آن‌ها پایه‌های یکسان استفاده شده باشد فرآیند غربال‌گری را انجام می‌دهند. فرآیند غربال‌گری به این صورت است که برای حالت‌های سیگنال و فریب، پایه‌های نا مشابه از کلید خام حذف می‌شوند، آن‌گاه از بین حالت‌هایی که برای آن‌ها پایه‌های تصادفی مشابه انتخاب شده است، حالت‌های سیگنال در کلید غربال شده و حالت‌های فریب برای تحلیل امنیت به کار می‌روند. غربال‌گری حالت‌های خلأ ضرورتی ندارد، زیرا صرف‌نظر از پایه‌های اندازه‌گیری، آشکارسازی هر حالت خلأ یک شمارش تاریک قلمداد می‌شود.

در گام دوم، شمارش خطای موجود در حالت‌های فریب انجام می‌شود. برای این کار، آلیس برای کیوبیت‌های حالت فریب غربال شده، عدد بیت کد شده را از طریق یک کانال کلاسیک به باب اعلام می‌کند. باب اعداد اعلام شده توسط آلیس را با اعدادی که خودش به دست آورده است مقایسه و تعداد خطاها را به‌منظور استفاده در گام چهارم پروتکل یادداشت می‌کند.

در گام سوم، اصلاح خطا[1]ی حالت‌های سیگنال انجام می‌گیرد. برای این منظور، آلیس و باب خطاهای مربوط به کیوبیت‌های حالت سیگنال غربال شده را به‌وسیله الگوریتم‌های تصحیح خطا و از طریق کانال کلاسیک محاسبه و تصحیح می-کنند. تعداد خطاهای تصحیح شده در این گام، به‌منظور استفاده در گام چهارم یادداشت می‌شود.

در گام چهارم، محاسبهٔ بهره‌ها، QBERها و شمارش‌های تاریک صورت می‌گیرد. این محاسبات تخصصی تنها مختص پروتکل‌های مبتنی بر حالت‌های فریب هستند و باتوجه‌به اندازه-گیری‌های قبلی انجام می‌شوند. بهره سیگنال (نسبت آشکارسازی‌های سیگنالی باب به تعداد پالس‌های سیگنال ارسال شده توسط آلیس)، Q_μ، و بهره حالت فریب (نسبت آشکارسازی‌های مختص حالت فریب توسط باب به تعداد پالس-های فریب ارسال شده توسط آلیس)، Q_ν، به ترتیب از تعداد اندازه‌گیری شده کیوبیت‌ها و تعداد کل پالس‌های ارسال شده محاسبه می‌شوند. QBER مربوط به سیگنال (نسبت خطاهای حالت سیگنال به تعداد پالس‌های سیگنال غربال شده)، E_μ، از تعداد اندازه‌گیری شده خطاها در کلید تصحیح شده و تعداد حالت‌های سیگنال غربال شده به دست می‌آید، درحالی‌که QBER مختص حالت فریب (نسبت خطاهای حالت فریب به تعداد پالس‌های فریب غربال شده)، E_ν، از تعداد خطاهای اندازه‌گیری شده در کیوبیت‌های حالت فریب غربال شده به دست می‌آید. تعداد آشکارسازی‌های صورت گرفته توسط باب، در حالتی که آلیس برای آن‌ها یک حالت خلأ ارسال کرده است، برای تعیین نرخ شمارش تاریک سامانه (نسبت آشکارسازی‌های نادرست باب به کل تعداد پالس‌های خلأ ارسال شده توسط آلیس)، Y_0، به‌کار می‌روند.

در گام پنجم، ارزیابی امنیت صورت می‌گیرد و در صورت تأیید آن، اطمینان حاصل می‌شود که هیچ‌گونه مداخله غیرمجاز در کانال کوانتومی صورت نگرفته است. در این گام، یک مقایسه بین بازدهی‌ها و/یا QBERهای تخمین زده شده مربوط به تعداد فوتون‌ها به‌ازای حالت‌های سیگنال و فریب انجام می‌گیرد. اگر این مقادیر با هم برابر نباشند (با یک رواداری از قبل تعیین شده)، نتیجه گرفته می‌شود که یک اخلال‌گر در کانال کوانتومی حضور داشته و کلید ناامن تلقی می‌شود. برای کسب جزئیات بیش‌تر در مورد پارامترهای متنوع دخیل در محاسبه نرخ کلید امن این پروتکل، می‌توان به [۳۹] مراجعه کرد.

در گام ششم و نهایی، تقویت محرمانگی[2] انجام می‌شود. در پایان این گام، ایو هیچ اطلاعاتی از کلید توزیع شده نخواهد داشت. فرایند تقویت محرمانگی به آلیس و باب این امکان را می‌دهد که با فشرده کردن طول کلید و کاهش‌دادن بیشینه احتمال شناسایی درست هر بیت توسط ایو، اطلاعات ایو از کلید نهایی را به حدی که کاملاً قابل‌چشم‌پوشی است برسانند. پس از اتمام تقویت محرمانگی، نمادهای موجود به‌صورت بیت ترجمه شده و کلید محرمانه نهایی استخراج می‌شود.

۶- نتیجه‌گیری

در این مقاله، پروتکل چندبعدی PoP مبتنی بر حالت‌های فریب معرفی شد و جزئیات مربوط به پیاده‌سازی، اجرا، پساپردازش کلاسیک، نحوه ارزیابی امنیت و استخراج کلید امن در آن تشریح گردید. پروتکل $\text{PoP}^{(4,2)}$ با بهره‌گیری هم‌زمان از مزیت استفاده از حالت‌های فریب و نیز مزیت استفاده از حالت‌های کوانتومی چندبعدی، امکان دستیابی به نرخ کلیدهای امن بالا در حضور قطعات ناکامل (همانند چشمه‌های لیزری تضعیف شده) را فراهم می‌کند. این پروتکل می‌تواند یک گزینه عملیاتی ساده و کارآمد برای برپایی سامانه‌های QKD با استفاده از قطعات غیر ایده‌آل متداول و در مسافت‌های انتقال بالا باشد.

[1] Error correction

[2] Privacy amplification

۶- مراجع

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci., vol. 560, pp. 7–11, Dec. 2014, doi: 10.1016/j.tcs.2014.05.025.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/physrevlett.67.661.

[3] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., vol. 68, no. 21, pp. 3121–3124, May 1992, doi: 10.1103/physrevlett.68.3121.

[4] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," Appl. Phys. Lett., vol. 87, no. 19, Nov. 2005, doi: 10.1063/1.2126792.

[5] A. Aghanians1, S. N. Doustimotlagh, "Generalized Version of the BB84 QKD Protocol with n Polarization Bases and Unequal Probabilities, " Journal of Electronical & Cyber Defence, vol. 9, no. 1, Serial No. 33, Aug. 2020 (In Persian). https://dor.isc.ac/dor/DOR:20.1001.1.23224347.1400.9.1.10.7

[6] S. M. Hosseini, S. Janbaz, M. Davoudi Darareh, A. Zaghian, "A New Approach for Estimating the Rate of Emission in Quantum Bit Exchange Systems Using Binomial Distribution," Journal of Electronical & Cyber Defence, Vol. 7, No. 1, Serial No. 25, 2019, (In Persian).

[7] Z. Karimifard, S. Mashhadi, D. Ebrahimi Bagha, "Semiquantum Secret Sharing Using Three Particles Without Entanglement" Journal of Electronical & Cyber Defence, Vol. 4, No. 3, Serial No. 15, 2016, (In Persian). https://dor.isc.ac/dor/20.1001.1.23224347.1395.4.3.8.4

[8] S. A. Oskoueian and N. Bagheri, "Differential cryptanalysis of round-reduced SIMON32 and SIMON48 and SIMON64," Journal of Electronical & Cyber Defence, vol. 5, pp. 1-8, 2017 (In Persian). https://dor.isc.ac/dor/20.1001.1.23224347.1396.5.1.1.0

[9] A. Gaeeni, "An introduction to the probability theory," Imam Hossein Univ. Press, Tehran, 2006 (In Persian).

[10] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on Practical Quantum Cryptography," Phys. Rev. Lett., vol. 85, no. 6, pp. 1330–1333, Aug. 2000, doi: 10.1103/physrevlett.85.1330.

[11] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A, vol. 61, no. 5, Apr. 2000, doi: 10.1103/physreva.61.052304.

[12] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, "Triggered Single Photons from a Quantum Dot," Phys. Rev. Lett., vol. 86, no. 8, pp. 1502–1505, Feb. 2001, doi: 10.1103/physrevlett.86.1502.

[13] B. Lounis and W. E. Moerner, "Single photons on demand from a single molecule at room temperature," Nature, vol. 407, no. 6803, pp. 491–493, Sep. 2000, doi: 10.1038/35035032.

[14] P. Michler et al., "A Quantum Dot Single-Photon Turnstile Device," Science, vol. 290, no. 5500, pp. 2282–2285, Dec. 2000, doi: 10.1126/science.290.5500.2282.

[15] T. Gao , M. von Helversen, C. Antón-Solanas, C. Schneider, and T. Heindel, "Atomically-thin single-photon sources for quantum communication," npj 2D Mater. Appl., vol. 7, no. 4 ,Jan. 2023, doi: 10.1038/s41699-023-00366-4.

[16] C. Couteau et al., "Applications of single photons to quantum communication and computing," Nature Rev. Phys., vol. 5, no. 6, pp. 326–338, May 2023, doi: 10.1038/s42254-023-00583-2.

[17] E. Waks, C. Santori, and Y. Yamamoto, "Security aspects of quantum key distribution with sub-Poisson light," Phys. Rev. A, vol. 66, no. 4, Oct. 2002, doi: 10.1103/physreva.66.042315.

[18] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett., vol. 91, no. 5, Aug. 2003, doi: 10.1103/physrevlett.91.057901.

[19] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett., vol. 94, no. 23, Jun. 2005, doi: 10.1103/physrevlett.94.230504.

[20] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A, vol. 72, no. 1, Jul. 2005, doi: 10.1103/physreva.72.012326.

[21] V. Zapatero, W. Wang, and M. Curty, "A fully passive transmitter for decoy-state quantum key distribution," Quantum Sci. Technol., vol. 8, no. 2, p. 025014, Feb. 2023, doi: 10.1088/2058-9565/acbc46.

[22] S. Dong et al., "Decoy state semi-quantum key distribution," EPJ Quant. Technol., vol. 10, no. 1, May 2023, doi: 10.1140/epjqt/s40507-023-00175-0.

[23] Y. Zhou et al., "Effect of weak randomness flaws on security evaluation of practical quantum key distribution with distinguishable decoy states," Chin. Phys. B, vol. 32, no. 5, p. 050305, May 2023, doi: 10.1088/1674-1056/ac8730.

[24] E. Diamanti, "Security and implementation of differential phase shift quantum key distribution systems," Doctoral Dissertation, Stanford University, 2006.

[25] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," Phys. Rev. A, vol. 61, no. 6, May 2000, doi: 10.1103/physreva.61.062308.

[26] M. Krenn, A. Hochrainer, M. Lahiri, and A. Zeilinger, "Entanglement by Path Identity," Phys. Rev. Lett., vol. 118, no. 8, Feb. 2017, doi: 10.1103/physrevlett.118.080401.

[27] I. Vagniluca et al., "Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution," Phys. Rev. Appl., vol. 14, no. 1, Jul. 2020, doi: 10.1103/physrevapplied.14.014051.

[28] D. Cozzolino et al., "Air-core fiber distribution of hybrid vector vortex-polarization entangled states," Adv. Photonics, vol. 1, no. 04, p. 1, Aug. 2019, doi: 10.1117/1.ap.1.4.046005.

[29] M. A. Ciampini et al., "Stimulated emission tomography: beyond polarization," Opt. Lett., vol. 44, no. 1, p. 41, Dec. 2018, doi: 10.1364/ol.44.000041.

[30] F. Steinlechner et al., "Distribution of high-dimensional entanglement via an intra-city free-space

polarization-phase encoding: security analysis," Int. J. Quantum Inf., vol. 18, no. 06, p. 2050031, Sep. 2020, doi: 10.1142/s0219749920500318.
[36] C. Marand and P. D. Townsend, "Quantum key distribution over distances as long as 30 km," Opt. Lett., vol. 20, no. 16, p. 1695, Aug. 1995, doi: 10.1364/ol.20.001695.
[37] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/revmodphys.74.145.
[38] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, "A New Proof for the Existence of Mutually Unbiased Bases," Algorithmica, vol. 34, no. 4, pp. 512–528, Nov. 2002, doi: 10.1007/s00453-002-0980-7.
[39] L. O. Mailloux, R. D. Engle, M. R. Grimaila, D. D. Hodson, J. M. Colombi, and C. V. McLaughlin, "Modeling decoy state Quantum Key Distribution systems," J. Def. Model. Simul., vol. 12, no. 4, pp. 489–506, Jun. 2015, doi: 10.1177/1548512915588572.
link," Nat. Commun., vol. 8, no. 1, Jul. 2017, doi: 10.1038/ncomms15971.
[31] B. Galmès, K. Phan-Huy, L. Furfaro, Y. K. Chembo, and J.-M. Merolla, "Nine-frequency-path quantum interferometry over 60 km of optical fiber," Phys. Rev. A, vol. 99, no. 3, Mar. 2019, doi: 10.1103/physreva.99.033805.
[32] Y. Ding et al., "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," npj Quantum Inf., vol. 3, no. 1, Jun. 2017, doi: 10.1038/s41534-017-0026-2.
[33] J. Wang et al., "Multidimensional quantum entanglement with large-scale integrated optics," Science, vol. 360, no. 6386, pp. 285–291, Apr. 2018, doi: 10.1126/science.aar7053.
[34] A. M. Toonabi, M. D. Darareh, and S. Janbaz, "A two-dimensional quantum key distribution protocol based on polarization-phase encoding," Int. J. Quantum Inf., vol. 17, no. 07, p. 1950058, Oct. 2019, doi: 10.1142/s0219749919500588.
[35] A. M. Toonabi, M. D. Darareh, and S. Janbaz, "High-dimensional quantum key distribution using