



بیست و پنجمین کنفرانس اپتیک و
فوتونیک ایران و یازدهمین کنفرانس
مهندسی و فناوری فوتونیک ایران،
دانشگاه شیراز،
شیراز، ایران.
۹-۱۱ بهمن ۱۳۹۷



مخابرات کوانتومی با استفاده از حالت‌های ترکیبی قطبش-تکانه زاویه‌ای مداری فوتون

¹ محدثه مداحی، ² فرناز فرمان و ³ علیرضا بهرامپور

دانشکده فیزیک، دانشگاه صنعتی شریف، تهران

رایانامه: 1 madahi.tm@gmail.com

2 farnaz_farman@yahoo.com 3 bahrampour@sharif.edu

چکیده - تکانه زاویه‌ای مداری نور یکی از درجات آزادی نور در فضای هیلبرت نامتناهی‌البعد است که در ارتباطات کوانتومی و توزیع کلید کوانتومی استفاده می‌شود. در این مقاله با کدکردن اطلاعات بر روی حالت‌های ترکیبی قطبش و تکانه زاویه‌ای مداری فوتون روشی جهت پیاده سازی پروتکل BB84 در ابعاد بالاتر ارائه می‌دهیم. نشان می‌دهیم در این روش نیازی به همترازی دستگاه‌های مرجع فرستنده و گیرنده نیست.

کلید واژه- تکانه زاویه‌ای مداری نور، توزیع کلید کوانتومی، درهم‌تنیدگی

Quantum communication using polarization-orbital angular momentum of photon hybrid states

Mohaddeseh Maddahi¹, Farnaz Farman², Alireza Bahrampour³

Departemant of Physics, Sharif University of Technology, Tehran

Emails: 1 madahi.tm@gmail.com

2 farnaz_farman@yahoo.com 3 bahrampour@sharif.edu

Abstract- Orbital angular momentum (OAM) is one of the photon's degrees of freedom in infinite-dimensional Hilbert space, which is used in quantum communication and quantum key distribution. In this paper we propose a method for implementing BB84 protocol in higher dimensions by encoding information on hybrid states of OAM and spin of photons. It has been shown that this method does not need for alignment of the transmitting and receiving frames.

Keywords: Orbital angular momentum, Quantum key distribution, entanglement

مقدمه

تکانه زاویه‌ای مداری^۱ (OAM) نور یکی از درجات آزادی نور است که می‌تواند به عنوان بستر مناسبی جهت انتقال اطلاعات به صورت کلاسیکی و کوانتومی مورد استفاده قرار گیرد. تکانه زاویه‌ای نور به دو بخش قطبش نور S و تکانه زاویه‌ای مداری نور L تقسیم می‌شود ($J=L+S$). در مخابرات نوری کوانتومی از قطبش فوتون به وفور استفاده می‌شود. هر تک فوتون دارای قطبش دایروی راست‌گرد یا چپ‌گرد، به ترتیب دارای تکانه زاویه‌ای اسپینی $\hbar$ یا $-\hbar$ است. در این حالت به فوتون‌های حامل اطلاعات کیوبیت می‌گویند که هر یک حامل یک بیت اطلاعات هستند. چنانچه بخواهیم ظرفیت انتقال اطلاعات توسط فوتون را بالا ببریم، باید از تکانه زاویه‌ای مداری نور استفاده کنیم [1]. عملگر تکانه زاویه‌ای مداری نور دارای تعداد نامتناهی ویژه‌حالت با ویژه‌مقدار $l\hbar$ است که l عدد صحیح می‌باشد. اندازه l نشان‌دهنده میزان و علامت آن نشان‌دهنده جهت پیش جبهه فاز است. بسته به اینکه از چه تعداد از این حالت‌های عمود بر هم برای انتقال اطلاعات استفاده کنیم، ظرفیت کانال بالا می‌رود و به $(\log_2 d)$ می‌رسد که d بعد فضای OAM مورد استفاده است. در این حالت به فوتون‌های حامل اطلاعات کیودیت گفته می‌شود. از مزایای دیگر استفاده از تکانه زاویه‌ای مداری نور، بالابردن امنیت در پروتکل‌های رمزنگاری کوانتومی است. پروتکل BB84 اولین و معروف‌ترین پروتکل QKD^۲ است که هم اکنون نیز بسیار کاربرد دارد [2]. یکی از روش‌های پیاده‌سازی این پروتکل در فضای آزاد مخصوصاً ارتباطات ماهواره‌ای استفاده از قطبش فوتون است. در این روش فرستنده و گیرنده که به آلیس و باب مشهور هستند باید مرجع مختصات یکسانی داشته باشند در غیر این صورت گیرنده نمی‌تواند اطلاعات را به درستی دریافت و مقدار خطا

افزایش می‌یابد. بنابر این فرستنده علاوه بر اطلاعات فوتون، مشخصات مرجع مختصات را نیز باید برای گیرنده بفرستد که منجر به گرفتن پهنای باند کانال شده نرخ ارسال اطلاعات را کاهش می‌دهد. در سال ۲۰۱۲ گروهی از محققین روشی جهت انتقال اطلاعات بر روی قطبش فوتون پیشنهاد دادند که مستقل از زاویه مراجع آلیس و باب نسبت به هم بود [3]. آنها با استفاده از OAM نور مشکل همراستا نبودن مراجع آلیس و باب را حل کرده موفق به ارسال یک بیت اطلاعات در هر بار ارسال فوتون شدند. در سال ۲۰۱۵ محققین پروتکل BB84 را با استفاده از OAM نور در فضای ۷ بعدی پیاده‌سازی کردند [4]. با استفاده از دو دسته پایه نامتوازن^۳ موفق به ارسال $\log_2 7$ بیت اطلاعات در هر بار ارسال فوتون شدند. چنانچه دو عملگر در فضای d بعدی داشته باشیم که با هم جابجا نشوند و تمام ویژه‌حالت‌های آنها نسبت به هم جابجا نشوند، به آنها پایه‌های نامتوازن گفته می‌شود. در این مقاله قصد داریم با استفاده از حالت‌های ترکیبی قطبش-تکانه زاویه‌ای مداری فوتون روشی جهت پیاده‌سازی پروتکل BB84 در ابعاد بالاتر ارائه دهیم. در این روش تنها از یک دسته پایه OAM و دو دسته پایه نامتوازن نسبت به قطبش نور استفاده می‌کنیم. نشان می‌دهیم که آلیس و باب احتیاج به همراستاکردن مراجع خود نداشته و ظرفیت کانال نیز افزایش می‌یابد.

مبانی نظری

یکی از مشکلات ارسال اطلاعات توسط قطبش فوتون همراستاکردن دستگاه‌های مرجع آلیس و باب است. با استفاده از حالت‌های ترکیبی مستقل از چرخش می‌توان بر این مشکل غلبه کرد. برای تولید حالت‌های ترکیبی قطبش-تکانه زاویه‌ای مداری از کیوپلیت‌ها استفاده می‌کنیم [5]. این صفحات که از کریستال مایع دوشکستی ساخته شده‌اند، قطبش و تکانه زاویه‌ای مداری نور را به هم

^۳ Unbiased

^۱ Orbital Angular Momentum
^۲ Quantum Key Distribution

$$Z=\{|H,0\rangle, |H,1\rangle, |H,-1\rangle, |V,0\rangle, |V,1\rangle, |V,-1\rangle\}$$

$$X=\{|R,0\rangle, |R,1\rangle, |R,-1\rangle, |L,0\rangle, |L,1\rangle, |L,-1\rangle\}$$

که در آن $|H\rangle$ و $|V\rangle$ نمایانگر قطبش افقی و عمودی،
 $|L,R\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i|V\rangle)$ نمایانگر قطبش دایروی
 چپ‌گرد و راست‌گرد و $|1\rangle, |0\rangle, |-1\rangle$ به ترتیب نمایانگر
 تکانه زاویه‌ای مداری 1، 0 و -1 هستند. آلیس از قبل طبق
 قرارداد با باب به هر حالت یک بیت کلاسیک نسبت داده
 است: $|V,0\rangle, |L,0\rangle \rightarrow 3$ ، $|H,0\rangle, |R,0\rangle \rightarrow 0$
 $|V,1\rangle, |L,1\rangle \rightarrow 4$ ، $|H,1\rangle, |R,1\rangle \rightarrow 1$
 $|V,-1\rangle, |L,-1\rangle \rightarrow 5$ ، $|H,-1\rangle, |R,-1\rangle \rightarrow 2$

آلیس به طور تصادفی اطلاعات خود را در یکی از دو پایه
 اولیه به وسیله چهار لیزر با قطبش‌های مختلف و آینه‌های
 میکرونی دیجیتالی^۴ (DMD) کد کرده با استفاده از
 کیوپلیت خودش به حالت ترکیبی مستقل از چرخش
 تبدیل می‌کند. سپس آن را برای باب می‌فرستد. باب با
 استفاده از کیوپلیتی در دستگاه مرجع خودش حالت
 ترکیبی را مشابه روابط (۲) و (۳) علی‌رغم وجود اختلاف
 زاویه دو مرجع به حالت اولیه‌ای که در دست آلیس بوده
 تبدیل کرده و توسط ادوات نوری آن را اندازه‌گیری
 می‌کند (شکل ۱). به همین ترتیب محاسبات برای تمام
 حالت‌های ممکن ورودی نشان می‌دهد که وجود اختلاف
 زاویه بین دو مرجع اثری در نتایج باب ندارد و باب بطور
 دقیق می‌تواند اطلاعات آلیس را استخراج کند. پس در
 نتیجه آلیس و باب نیازی به همترازی مراجع خود با
 یکدیگر ندارند. پس از اینکه مقدار قابل‌توجهی معمولاً در
 حدود ۱۰۰۰۰ فوتون (بسته به ظرفیت حافظه موقت
 آلیس و باب) منتقل شد این روند متوقف شده آلیس و

تبدیل می‌کنند. کیوپلیت مورد استفاده در اینجا دارای بار
 توپولوژیکی $q = 1/2$ و $\delta = \pi$ است. δ تاخیر فاز دوطرفه
 کیوپلیت است. (ماتریس جونز آن به صورت زیر
 است: (1) $M(r,\varphi) = i \begin{pmatrix} \cos \varphi & \sin \varphi \\ \sin \varphi & -\cos \varphi \end{pmatrix}$
 اثر کیوپلیت بر روی حالت $E_{in}(r,\varphi) = E_0(r) \begin{pmatrix} 1 \\ \pm i \end{pmatrix} e^{im\varphi}$
 بصورت $E_{out}(r,\varphi) = iE_0(r) \begin{pmatrix} 1 \\ \mp i \end{pmatrix} e^{i(m\mp 1)\varphi}$ است. در اینجا
 $e^{im\varphi} \begin{pmatrix} 1 \\ \pm i \end{pmatrix}$ بردار جونز مربوط به حالتی با قطبش چپ‌گرد و
 تکانه زاویه‌ای مداری m است. اگر فرض کنیم بین مراجع
 آلیس و باب به اندازه θ اختلاف فاز وجود داشته باشد، اثر
 آن بر روی قطبش فوتون در دو دستگاه بصورت $|R\rangle \rightarrow$
 $e^{-i\theta}|R\rangle$ است. اثر اختلاف زاویه دو مرجع بر روی
 ویژه‌حالت‌های OAM نیز به صورت $|m\rangle \rightarrow e^{im\theta}|m\rangle$
 خواهد بود. با استفاده از این اثرها می‌توان کیودیت‌های
 مستقل از چرخش طراحی کرد. به عنوان مثال اگر آلیس
 بخواهد حالت ورودی $|H,0\rangle$ را برای باب بفرستد آن را از
 یک کیوپلیت عبور داده و وارد خط انتقال می‌کند:

$$|H,0\rangle \xrightarrow{Q_{plate}} \frac{1}{\sqrt{2}}(|L,-1\rangle + |R,1\rangle) \quad (2)$$

باب نیز پس از دریافت این حالت کیوپلیت خودش را روی
 آن اثر می‌دهد که اثرش به صورت زیر است:

$$\frac{1}{\sqrt{2}}(|L,-1\rangle + |R,1\rangle) \xrightarrow{Q_{plate}} |H,0\rangle \quad (3)$$

این روابط با در نظر گرفتن زاویه بین دو مرجع آلیس و باب
 به‌دست آمده‌اند. به این ترتیب باب علی‌رغم همراست نبودن
 با آلیس می‌تواند اطلاعات قطبش_تکانه زاویه‌ای مداری
 فوتون را به صورت دقیق استخراج کند.

نحوه پیاده‌سازی پروتکل BB84

برای پیاده‌سازی پروتکل BB84 به دو دسته پایه نامتوازن
 نیاز داریم. در اینجا فرض می‌کنیم آلیس قصد دارد یکی از
 ۶ عدد مختلف را در هر بار ارسال فوتون برای باب
 بفرستد. او برای ارسال بیت‌های کلاسیکی از شماره ۰ تا
 ۵ دو دسته پایه نامتوازن را در اختیار دارد.

^۴ Digital Micro Mirror

زاویه‌ای مداری نور آن را افزایش داد. برای مثال می‌توان از حالت‌های $|+2\rangle, |-2\rangle, |+3\rangle, |-3\rangle$ و ... نیز برای کد کردن اطلاعات استفاده کرد.

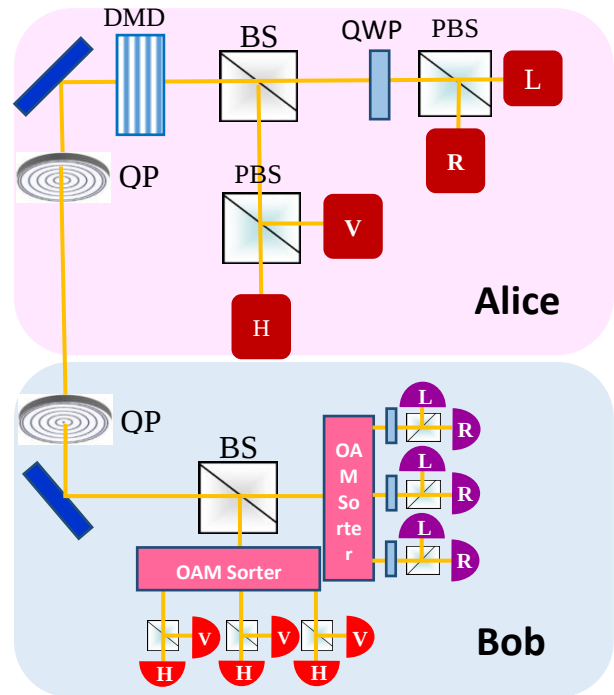
نتیجه‌گیری

در این مقاله نشان دادیم با استفاده از حالت‌های ترکیبی قطبش-تکانه زاویه‌ای مداری فوتون می‌توان روشی جهت پیاده‌سازی پروتکل BB84 پیشنهاد داد. در این روش تنها از یک دسته پایه OAM و دو دسته پایه نامتوازن قطبش نور استفاده کردیم. نشان دادیم که آلیس و باب با استفاده از کیوبلیت حالت‌های ورودی را به حالت‌های مستقل از چرخش قطبش-تکانه زاویه‌ای تبدیل کرده و به این ترتیب احتیاج به همراستاکردن مراجع خود ندارند. به علاوه با استفاده از OAM نور، می‌توان ظرفیت کانال را جهت ارسال اطلاعات نیز افزایش داد.

مرجع‌ها

- [1] Farman, Farnaz, Bahrapour, Alireza. Journal of the Optical Society of America B, Vol. 35, No. 10, (2018).
- [2] Bennett, C.H, Brassard, G, in Workshop on the Theory and Application of Cryptographic Techniques (Springer, 1984), pp. 475–480.
- [3] D'ambrosio, Vincenzo, et al. Nature communications 3 (2012): 961.
- [4] Mirhosseini, Mohammad, et al. New Journal of Physics 17.3 (2015): 033033.
- [5] Vallone, Giuseppe, et al. Physical review letters 113.6 (2014): 060503.

باب از طریق شبکه کلاسیکی با هم ارتباط برقرار می‌کنند. به این ترتیب که آلیس اطلاع می‌دهد هر فوتونی را از کدام دسته پایه انتخاب کرده‌بوده است.



شکل ۱. نمایی شماتیک از پیاده‌سازی پروتکل. آینه‌های DMD جهت تولید فوتون با OAM های ۱ و -۱ به کار می‌روند.

همین‌طور باب اعلام می‌کند در کدام پایه اندازه‌گیری انجام داده‌است. آن‌ها تنها اطلاعاتی که مربوط به فوتون‌هایی است که در پایه مشترک تولید و اندازه‌گیری شده‌اند را نگاه داشته بقیه را دور می‌ریزند که به این عمل غربالگری^۵ گفته می‌شود. پس از انجام این کار آلیس و باب یک رشته هماهنگ دارند که البته ممکن است ایو نیز به مقداری از اطلاعات دسترسی داشته‌باشد. چنانچه ایو به کانال حمله‌کند رد پای خود را به‌جامی‌گذارد که قابل تشخیص توسط آلیس و باب است. ظرفیت کانال در اینجا $\log_2 6$ است که می‌توان با زیاد کردن حالت‌های تکانه

^۵ sifting