تاریخ دریافت:۱۴۰۰/۰۱/۲۳ پژوهشنامه علوم دفاعی، شماره ۲، تابستان ۱۴۰۰

تاریخ پذیرش:۱۴۰۰/۰۳/۱۳ ص ص ۱۹ تا ۴۷

طراحی کلید کوانتومی ابعاد بالا در جهت افزایش ایمنی بین فرستنده و گیرنده و انتقال بیشتر اطلاعات توسط امواج الکترومغناطیس

محمد هادی محمدی[۱]، عباس مبشری[۲*]

چکیده

در این تحقیق ارتباط حفاظت شده‌ای میان دو شخص برقرار می‌شود که شخص سومی نتواند شنود یا به اطلاعات مبادله شده بین طرفین دسترسی پیدا کند. این روزها دشمن به راحتی ارتباطات را کنترل می‌کند (از طریق اینرنت و شنود) ما در این تحقیق یک ارتباط کوانتومی ارائه می‌دهیم تا زمانی که دشمن بخواهد ارتباط را شنود کند یا همان اندازه‌گیری کند طبق اصل عدم قطعیت هایزنبرگ اندازه گیری‌اش مختل شود. در این تحقیق شخص فرستنده و گیرنده آلیس و باب نامیده می‌شوند شخص شنود کننده Ene نامیده می‌شود. و ما در این تحقیق به این دست پیدا می‌کنیم که در صورت درز اطلاعات مقدار این اطلاعات را می‌توانیم اندازه‌گیری کنیم.

واژگان کلیدی: کلید کوانتومی، پروتکل HDQKD، امواج الکترومغناطیس، فیزیک کوانتومی

۱. پژوهشگر فیزیک، دانشگاه افسری امام علی(ع)، تهران، ایران.

۲. (*نویسنده مسئول): مدرس گروه فیزیک، دانشکده علوم پایه، دانشگاه امام علی (ع)، تهران، ایران.

ایمیل: mobasheri_112@yahoo.com

مقدمه

در ابتدا به تعریف رمز نگاری کوانتومی می‌پردازیم. به عمل پنهان کردن اطلاعات، رمزنگاری گفته می‌شود که هدف از آن انتقال اطلاعات به صورت امن است. یکی از راه‌های ایجاد امنیت در انتقال پیام استفاده از کلیدهای مشترک است. اگر از رمزنگاری سنتی بگذریم، رمزنگاری کنونی را می‌توان به دو دسته‌ی کلاسیک و نوین تقسیم‌بندی کرد. منظور از رمزنگاری کلاسیک، رمزنگاری منسوخ شده نیست. از روش‌های رمزنگاری کلاسیک می‌توان به روش‌هایی که در آن از الگوریتم‌هایی مانند DES استفاده می‌شود، نام برد. استفاده از این الگوریتم‌ها به علت وابستگی ریاضی کلیدها به یکدیگر قابل رمزگشایی است. محققان IT با موفقیت نشان داده‌اند که اصول فیزیک کوانتومی و رمزنگاری کوانتومی در شبکه‌های نوری قادر به محافظت بهتر از ارتباطات استرمزنگاری کوانتمی اولین بار توسط Wiesner Stephenدر دهه ۱۹۷۰ مطرح شد. در سال ۱۹۹۱ Ekert Artur دانشجوی دوره دکتری در دانشگاه Oxford، روش دیگری برای رمزنگاری کوانتومی ارائه کرد. این نکته قابل ذکر است که رمزنگاری کوانتومی فقط برای تولید و توزیع کلید استفاده می‌شود و این روش برای رمزنگاری اطلاعات و انتقال آن‌ها کاربردی ندارد.

برای بررسی دقیق رمزنگاری کوانتومی و اینکه با اصطلاحات و مفاهیم اولیه آشنا شوید ابتدا مختصری به بررسی امواج الکترومغناطیسی و کوانتوم می‌پردازیم؛ سپس در رمزنگاری کوانتومی و ایجاد و توزیع کلید در این رمزنگاری بررسی عمیق‌تری خواهیم داشت[2-1].

امواج الکترومغناطیسی، دارای ماهیت و سرعت یکسانی هستند در طیف امواج الکترومغناطیس شکافی وجود ندارد، یعنی هر فرکانس دلخواه را می‌توان تولید کرد. این امواج برای انتشار خود نیاز به محیط مادی ندارند. امواج الکترومغناطیسی جزو امواج عرضی هستند. از جمله منابع زمینی امواج الکترومغناطیسی می‌توان به امواج دستگاه رله تلفن، چراغ‌های روشنایی و غیره اشاره کرد. فوتون به عنوان ذره بنیادینی است که واحد کوانتومی نور یا هر نوع تابش الکترومغناطیسی محسوب می‌شود. هر فوتون مقدار معینی انرژی، اندازه حرکت و اندازه حرکت زاویه‌های یا اسپین دارد. قطبش نیز یکی دیگر از خاصیت‌های هر امواج الکترومغناطیسی مثل نور است. قطبش نور نخستین بار توسط Huygens در سال ۱۹۶۰ میلادی کشف شد. از قطبش می‌توان در زمینه رمزنگاری کوانتومی استفاده نمود.

اصول رمزنگاری کوانتومی

همان‌طور که گفته شد امواج الکترومغناطیسی می‌توانند قطبیده شوند. قطبیدگی بنابر قرارداد با جهت میدان الکتریکی تعریف می‌شود که در آن یا جهت نوسانات میدان الکتریکی ثابت است یا به شکل معینی تغییر می‌کند. اگر در فرآیند قطبیدگی دقت کافی شود می‌توان فرآیند ایجاد فوتون‌ها را به گونه‌ای قرار داد که همیشه فوتون‌هایی با قطبش‌های عمودی و افقی ایجاد شوند. یک قطبشگر یا پولارایزر وسیله‌ای است که تنها اجازه عبور نور با جهت قطبیدگی خاص را می‌دهد. بنابراین اگر نور کاملا قطبیده نشده باشد تنها نیمی از آن از قطبشگر عبور می‌کند. همانطور که گفته شد هر فوتون اندازه حرکت زاویه‌ای یا اسپین دارد. در این نظریه فوتون مستقل از اینکه چه قطبش اولیه‌ای داشته یا از قطبشگر رد می‌شود یا خیر، اما اگر رد شد با محور قطبشگر هم خط می‌شود. اصل عدم قطعیت Heeisberg نظریه کوانتومی بیشتر بر این موضوع استوار است که بعضی از کمیت‌هایی که در فیزیک کلاسیک پیوسته در نظر گرفته می‌شوند، در حقیقت کوانتیده یا گسسته هستند. به طور خلاصه تنها دو نوع توصیف در مورد یک ذره مادی یا یک فوتون وجود دارد: یکی توصیف موجی و دیگری توصیف ذره‌ای. بدین صورت که به یک ذره می‌توان هم خصوصیات مادی (مانند اندازه حرکت و مکان) هم خصوصیات موجی (مانند طول موج و بسامد) نسبت دهیم. تابش الکترومغناطیسی هم جنبه‌های موجی و هم جنبه‌های ذرهای را نشان می‌دهد. نظریه عدم قطعیت Heiseberg را می‌توان در دو حالت زیر بیان کرد: اگر تابش الکترومغناطیسی را به زبان ذرات بیان کرده و مکان فوتون را در هر لحظه با دقت کامل تعیین کنیم در آن صورت عدم قطعیت در مکان و زمان صفر می‌شود اما از طرف دیگر عدم قطعیت در آنچه به موج فوتون نسبت داده می‌شود (مانند طول موج) بینهایت بزرگ است؛ از طرفی دیگر اگر بتوانیم آنچه به موج فوتون منسوب است را دقیق مشخص کنیم در این صورت عدم قطعیت در موج فوتون صفر شده و مکان فوتون نامشخص خواهد بود. رمزنگاری کوانتومی تنها برای تولید و توزیع کلید استفاده می‌شود. این کلید در مرحله‌های بعدی می‌تواند همراه با هر الگوریتم رمزنگاری برای تبدیل پیام به رمز یا بالعکس استفاده شود. رمزنگاری کوانتومی به هر دو طرف ارتباط این امکان را می‌دهد که کلید رمز خود را از طریق کانال خصوصی کاملاً امنی انتقال دهند. برای تولید و توزیع کلیدهای کوانتومی می‌توان از پروتکل‌های بسیاری استفاده کرد.

- BB84

- T12 protocol
- Decoy state protocol: A practical QKD scheme using imperfect single photon sources, such as weak coherent state sources
- SARG04
- Six-State protocol
- E91 protocol: entanglement protocol
- B92 protocol: protocol using only two nonorthogonal states by Charles Bennett
- BBM92 protocol: entanglement protocol
- MSZ96 protocol
- COW protocol: coherent one way protocol by Gisin
- DPS protocol: differential phase shift by Yamamoto
- KMB09 protocol: High Error-rate QKD protocol by Khan et al.
- HDQKD: High-dimensional Quantum Key Distribution

پروتکل HDQKD

در این تحقیق به منظور افزایش امنیت و تحمل نویز بیشتر و افزایش اطلاعات مبادله شده از پروتکل HDQKD استفاده کرده‌ایم. برای استفاده از این پروتکل از دستگاه SPDC شده است. این دستگاه یک فوتون با انرژی بالا را تبدیل به ۲ فوتون با انرژی کم می‌کند، که در این صورت اطلاعات بیشتری مبادله می‌شود چرا که هر فوتون یک کیوبیت را حمل می‌کند. که هر کیوبیت ابعاد آن بیشتر از ۲ می‌باشد. در این پروتکل از decoy state protocol استفاده می‌شود. به منظور یافتن اینکه آیا Ene توانسته به اطلاعات طرفین دسترسی پیدا کند یا خیر. PNS ATTACK حمله‌ای است که شخص سوم برای دستیابی به اطلاعات انجام می‌دهد که اطلاعات را ازآلیس دریافت می‌کند و کپی را به باب می‌فرستد، با decoy state protocol این مشکل تا حدی حل می‌شود. اما فرق اساسی در decoy state این پروتکل (HDQKD) با BB84 در این است که در BB84 برای اینکه بفهمیم Ene چه مقدار اطلاعاتی بدست آورده است از Quantum bit error استفاده می‌کنیم اما در HDQKD اندازه‌گیری را کم کرده تا اطلاعات کمتر مختل بشوند تا بفهمیم چه مقدار اطلاعات درز کرده است.

اما هدف اصلی در این تحقیق اندازه‌گیری پارامترهایی مانند نویز و حالت‌های دیکوی (متوجه شدن مقدار اطلاعات درز کرده یا حمله‌ی PNS) است که آلیس و باب می‌توانند در یک ارتباط امن در

غالب پروتکل HDQKD که منجرب به افزایش امنیت و تحمل نویز بیشتر و افزایش اطلاعات مبادله شده و سرعت انتقال بالای اطلاعات می‌باشد.[3-4-5-6]

پروتکل BB84:

این پروتکل توسط Bennet و Brassard در سال ۱۹۸٤ ارائه شد که مبتنی بر اصل عدم قطعیت Heisenberg است. بنابر این اصل که در بخش‌های قبلی هم به آن اشاره شد، وقتی در اندازه‌گیری قطبش فوتون جهت اندازه‌گیری خاصی را انتخاب می‌کنیم این انتخاب تمام اندازه‌گیری‌های بعدی را تحت تاثیر قرار می‌دهد. به عنوان مثال بدون اینکه بدانیم فوتون دارای چه حالت اولیه‌ای است، اگر جهت عمودی را برای اندازه‌گیری قطبش یک فوتون انتخاب کنیم فوتون با قطبش عمودی از قطبشگر رد می‌شود و قطبش افقی اصلاً رد نمی‌شود. حال اگر اندازه‌گیری دیگری در زاویه ٤٥ درجه از اندازه‌گیری اول انجام دهیم احتمال عبور فوتون از قطبشگر دوم دقیقاً ۱/۲ است و اینگونه بیان می‌کنیم که قطبشگر اول اندازه‌گیری قطبشگر دوم را کاملاً تصادفی می‌کند. بنابراین در صورتی می‌توان جهت این قطبش را تشخیص داد که یک قطبشگر با صفر تا ۹۰ درجه انتخاب گردد. زیرا یک قطبشگر ٤٥ یا ۱۳٥ درجه نیز یک خروجی با همین قطبش‌ها می‌دهد.

به طور کلی با توجه به توضیحات داده شده، ارسال کننده با استفاده از منبع، یکی از چهار حالت قطبش بالا (صفر، ٤٥، ۹۰، ۱۳٥)را برای گیرنده ارسال می‌کند. در طرف دیگر از گیرنده برای اندازه‌گیری قطبش استفاده می‌شود.

گیرنده نتیجه اندازه‌گیری را ذخیره می‌کند. در ادامه گیرنده با استفاده از کانال عمومی، نوع فیلترهای اندازه‌گیری خود Rectilinear و Diagonal را بیان می‌کند. در تمام این مراحل نتیجه اندازه‌گیری توسط گیرنده پنهان نگه داشته می‌شود. سپس فرستنده نیز به گیرنده درباره اینکه کدام فیلتر گیرنده درست بوده اطلاع می‌دهد. تنها در حالتی که فرستنده و گیرنده از نوع یکسانی برای اندازه‌گیری استفاده کرده باشند، می‌توان مطمئن بود که اندازه‌گیری درستی انجام گرفته است. با استفاده از اندازه‌گیری‌های مشترک بین فرستنده و گیرنده و در نهایت به بیت تبدیل شدن آنها، کلید ساخته می‌شود[7].

پروتکل E91

مبتنی بر همبستگی کوانتومی در سال ۱۹۹۱، Ekert Artur پروتکل جدیدی برای توزیع کلید ارائه کرد. این پروتکل از یک کانال کوانتومی و منبع تولید تک فوتون استفاده می‌کند. عملکرد این پروتکل به این صورت است که دو زوج همبستگی از یکدیگر تفکیک شده و هر یک از فرستنده و گیرنده یکی از آن دو زوج را دریافت می‌کنند. با توجه به این پروتکل، هر یک فیلتری برای اندازه‌گیری جزئی دریافتی خود استفاده می‌کنند. این پروتکل نیز مانند پروتکل BB84 در قسمت دوم عملکردی خود تبادلاتی در کانال کلاسیک انجام می‌دهد تا فیلترهای اندازه‌گیری هر دو طرف مشخص گردد. در نهایت به ازای هر اندازه‌گیری که فرستنده و گیرنده از فیلتر یکسانی استفاده می‌کنند باید انتظار نتیجه‌ای متضاد بر اساس قوانین همبستگی کوانتومی داشته باشند. این موضوع به این معناست که هر دو طرف تبادل، اندازه‌گیری‌های خود را مثل قبل تفسیر می‌کنند با این تفاوت که رشته بیتی هر یک از آن دو، مکمل باینری دیگری است. در این صورت اگر یکی از طرفین کلید خود را معکوس کند، یک کلید مخفی بین آن دو به اشتراک گذاشته شده است[8].

روش انجام تحقیق

رمزنگاری در برگیرنده‌ی ارتباطی می‌باشد که اطلاعات انتقال داده شده اطلاعاتی کد گذاری شده می‌باشد. مستقیم‌ترین کد گذاری پد یک‌بار مصرف می‌باشد که پیام کد گذاری می‌شود توسط رندوم بیت رشته‌ها که به عنوان کلید عمل می‌کنند. رندوم بیت رشته‌ها توسط عملگر منطقی XOR (عملگری که مقایسه می‌کند دو بیت ورودی را سپس تولید می‌کند یک بیت خروجی) پالاییده می‌شوند تا پیام کدگذاری یا رمزگشایی شود. این روش اثبات شده است که روش ایمنی می‌باشد [9]. در پروژه این رندوم بیت رشته‌ها کلیدی هستند که تولید می‌شوند از اطلاعات مبادله شده‌ی بین آلیس و باب. حال برای این کار باید برای اطلاعات کمیت تعریف کنیم یک راه برای این کار تعریف آنتروپی اطلاعات می‌باشد. آنتروپی اطلاعات می‌تواند استفاده شود برای اندازه‌گیری میانگین اطلاعاتی که در الفبای X وجود دارد که x متغییر گسسته و $P(x)$ احتمال آن می‌باشد که به صورت زیر تعریف می‌شود[10] :

$$H(X) = \sum_{x} P(x) \log_2 \frac{1}{P(x)'}$$

همچنین به این آنتروپی عدم قطعیت X هم گفته می‌شود به طور کلی از لگاریتم پایه‌ی ۲ استفاده می‌شود؛ بنابرین آنتروپی اطلاعات می‌تواند تفسیر شود توسط سوالات بله و خیر که یکی از آنها جواب است که منجر به مشخص شدن اطلاعات می‌شود.

Mutual Information

در این جا ما به اطلاعاتی می‌پردازیم که انتقال آنها بین دو کنش‌گر می‌باشد به همین علت آنتروپی را به صورت زیر تعریف می‌کنیم:

$$H(X,Y)=\sum_{x,y}P(x,y)\log_2\frac{1}{P(x,y)'}$$

$$I(X;\gamma)=H(X)+H(\gamma)-H(X,\gamma)=H(\gamma)-H(\gamma|X)=H(X)-H(X|\gamma)\,(\mathrm{q})$$

آنتروپی x به شرط γ به صورت زیر است :

$$H(X|\gamma)=\sum_{y}P(y)\left[\sum_{x}P(x|y)\log_2\frac{1}{P(x|y)}\right]=\sum_{x,y}P(x,y)\log_2\frac{1}{P(x,y)'}\,(\mathrm{qq})$$

با توجه به قضیه‌ی بیز داریم

$$P(x,y)=P(x)P(y|x)=P(y)P(x|y)$$

بنابراین با توجه به معادله‌ی qq و قضیه‌ی بیز، آنتروپی مساوی می‌شود با:

$$H(X|\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(y)}{P(y|x)P(x)}=$$
$$=\sum_{x,y}P(x,y)\log_2\frac{1}{P(x)}+\sum_{x,y}P(x,y)\log_2\frac{P(y)}{P(y|x)}$$

بنابراین با توجه به معادله‌ی q، Mutual Information برابر می‌شود با:

$$I(X;\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(x,y)}{P(x)P(y)}$$

عملگر اندازه‌گیری

تا به حال درمورد نظریه‌ی اطلاعات کلاسیک صحبت کردیم برای درک مکانیک کوانتومی در نظریه‌ی اطلاعات باید استراتژی را انتخاب کنیم که بتواند حالت‌های کوانتومی را اندازه‌گیری کند

[11]. اندازه‌گیری کوانتومی توصیف می‌شود توسط عملگرهای کوانتومی $[M_m]$ که در معادله‌ی زیر صدق می‌کند:

$$\sum_m M_m^+ M_m = 1$$

برای هر ویژه حالت $|\psi\rangle$ m بار اندازه‌گیری با احتمال زیر رخ داده می‌شود:

$$p(m) = \langle\psi| M_m^+ M_m |\psi\rangle \qquad (1)$$

عملگر $E_m = M_m^+ M_m$ هرمیتی و یژه مقداری انتظاری مثبت دارد $\langle\psi|E_m|\psi\rangle \geq 0$. اگر عملگر اندازه‌گیری هرمیتی و این شرط را دارا باشد $M_m M_{m'} = \delta_{m,m'} M_{m'}$ به آن اندازه‌گیری افکنشی می‌گوییم که در اپتیک آن را قبلا با آن برخورد داشته‌ایم. و یژه مقداری انتظاری مثبت را PVOMمی‌گویند.

State discrimination

ساده‌ترین مثال از State discrimination تمایز بین دو کیوبیت است.یک کیوبیت یک حالت کوانتومی دوبعدی است $a|0\rangle + b|1\rangle$ $(a,b \in \mathbb{C}, |a|^2 + |b|^2 = 1)$ که ویژه بردارها $|0\rangle, |1\rangle$برهمدیگر عمود هستند. از آنجا که باب می‌تواند بین ویژه حالت‌ها تمایز قائل شود پس در نتیجه ویژه حالت‌ها orthogonal یا بهم عمود هستند. برای مثال وقتی آلیس دو ویژه حالت را $|\psi_1\rangle = |1\rangle, |\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ آماده می‌کند تا برای باب بفرستند که باید تصمیم بگیرد که کدام ویژه حالت را باب دریافت نماید. اندازه‌گیری افکنشی تعریف می‌کند دو ویژه حالت $|\varphi_1\rangle, |\varphi_2\rangle$ متقارن را که نمیساز زاویه‌ایی $|\psi_1\rangle$ و $|\psi_2\rangle$ می‌باشند.که $|\varphi_1\rangle$ زاویه‌ی بیشتری را از $|\psi_1\rangle$ پوشش می‌دهد.افکنش انجام می‌شودتوسط عملگرهای $|\varphi_1\rangle\langle\varphi_1|$ و $|\varphi_2\rangle\langle\varphi_2|$.اگر سیستم افکنده شود بر روی $|\varphi_1\rangle$ ما حدس می‌زنیم $|\psi_1\rangle$ را نتیجه دهد و احتمال موفقیت آن در زیر محاسبه شده است:

$$P_{GUESS} = \frac{1}{2} + \frac{1}{2}(1 - |\langle\psi_1|\psi_2\rangle|^2)^{\frac{1}{2}}) = \frac{1+\sqrt{2}}{2\sqrt{2}} \approx 0.85$$

مشخصا با محاسبه‌ی این احتمال خطا در تشخیص حالت‌ها پدید می‌آید. با این حال روشی وجود دارد که بتوان ۲ حالت را از هم تمیز داد گاهی اوقات بدون هیچ گونه خطایی. به این روش unambiguous state discrimination گفته می‌شود[12]. اولین سناریو این است که باب اندازه‌گیری افکنشی انجام دهد روی ویژه حالت‌های اورتوگنال.

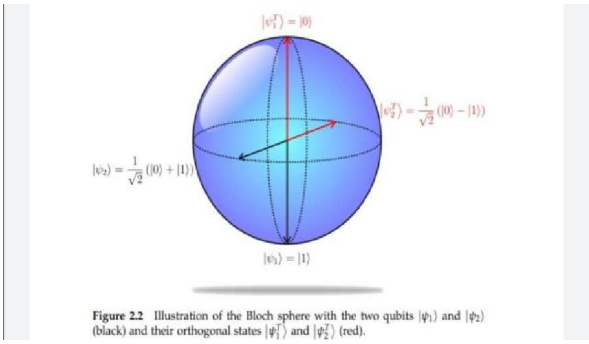


Figure 2.2 Illustration of the Bloch sphere with the two qubits $|\psi_1\rangle$ and $|\psi_2\rangle$ (black) and their orthogonal states $|\psi_1^T\rangle$ and $|\psi_2^T\rangle$ (red).

شکل ۱: نمایش کره مشکی با ۲ کیوبیت $|\psi_1\rangle$ و $|\psi_2\rangle$ مشکی رنگ و ۲ موج قرمز رنگ عمود برهم $|\psi_1^T\rangle\langle\psi_1^T|$

نصفی از زمان اندازه‌گیری باب عمل می‌کند روی عملگر $|\psi_1\rangle\langle\psi_1|$ و $|\psi_1^T\rangle\langle\psi_1^T|$ (در پایه‌ی ۱)و نصفی دیگر از زمان این اندازه‌گیری روی $|\psi_2\rangle\langle\psi_2|$ و $|\psi_2^T\rangle\langle\psi_2^T|$ (در پایه‌ی ۲)عمل می‌کند. فرض کنید باب اندازه‌گیری افکنشی را در پایه‌ی ۱ انجام می‌دهد.اگر سیستم بعد از اندازه‌گیری افکنده شود بر $|\psi_1^T\rangle$ باب با قطعیت می‌داند که ویژه حالت ما $|\psi_2\rangle$ زیرا که اجزای $|\psi_2\rangle$ در مسیر $|\psi_1^T\rangle$ می‌باشد. اگر سیستم بعد از اندازه‌گیری افکنده شود بر $|\psi_1\rangle$ نتیجه‌ایی در پی نخواهد داشت زیرا که $|\psi_2\rangle$ در جهت $|\psi_1\rangle$ اجزا دارد.

$$P_{proj} = \frac{1-|\langle\psi_1|\psi_2\rangle|^2}{2} = \frac{1}{4}$$

اطلاعات کوانتومی و محدوده‌ی Holevo

بخش Mutual Information شامل اندازه‌گیری اطلاعات به اشتراک گذاشته شده بین آلیس وباب برخلاف دو حالت کلاسیکی، اندازه‌گیری کوانتومی همیشه قادر به تمایز بین حالت‌های کوانتومی نیست. این مقدار اطلاعاتی را که می‌توان در مورد یک سیستم کوانتومی دانست، اطلاعات قابل دسترسی نامیده می‌شود [11]. در صورت ارتباط با حالات کوانتومی، این اطلاعات در دسترس معیاری است برای اطلاعات مشترک بین آلیس و باب. شاید هیچ فرمول شناخته شده‌ای برای محاسبه وجود ندارد با این حال محدوده‌های بالایی از قبیل Holevo این نابرابری را به ما نتیجه می‌دهد.

فرض کنید آلیس یک حالت احتمالی مخلوط با عملگر چگالی ρx را آماده می‌کند جایی که X= 1,..,d با احتمالات p1 ,p2,...pd که باب این اندازه‌گیری را انجام می‌دهد توسط PVOM={E1، ...، Em}که در قسمت عملگر اندازه‌گیری اشاره شد. که در آن حالت، با نتیجه اندازه‌گیری γ. برای هر اندازه‌گیری، محدوده‌ی Holevo بیان می‌کند که:

$$I(X;Y) \le S(\rho) - \sum_x \rho_x S(\rho_x)$$

که در معادله‌ی بالا $\rho = \sum_x p_x \rho_x$, و $S(\rho) = -Tr(\rho \log_2 \rho)$ که آنتروپی نیومن می‌باشد. حداکثر اطلاعات قابل دسترسی برای حالت‌های کوانتومی مخلوط به دست می‌آید. $\rho = \sum_n \frac{1}{d} |n\rangle\langle n|$ با پایه‌های اورتوگنال $\{|n\rangle\}$ که شامل احتمال‌های یکسان برای هر ویژه حالت می‌باشد ($p_1,...p_d = \frac{1}{d}$). از آنجا که آلیس می‌تواند مقدار نامحدودی اطلاعات را برهم نهی دهد اما باب فقط دسترسی به $\log_2 d$ دارد؛ بنابراین در سیستم اورتوگنال اطلاعات کوانتومی و اطلاعات کلاسیک باهم برابری می‌کنند اما دلیل اینکه ما به اطلاعات کوانتومی علاقمند هستیم این است که اطلاعات محدود شده کمتر از اطلاعات آماده شده توسط آلیس می‌تواند باشد.

رمز نگاری کوانتومی

راهی که بتوان ازذات کوانتومی نور برای تولید کلید بین آلیس و باب استفاده کرد استفاده از توزیع کلید کوانتومی یا QKD می‌باشد [13]. اولین پرتوکل QKD در سال ۱۹۸٤ توسط بنت و همکارش ساخته شد [14]. آلیس داری منبع نور تک فوتون می‌باشد او کدگذاری می‌کند یک بیت از اطلاعات را با ۰ یا ۱ در یک قطبش دوبعدی با توجه به پایه‌های فوتون‌ها.او کدگذاری می‌کند پایه‌های افقی و عمودی با توجه به ماتریس‌های پائولی $\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

یا پایه‌های قطری یا غیر قطری با $\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ به این صورت آلیس و باب می‌توانند تغییر بدهند پایه‌های خود را.با چرخش دستگاه PBS در زاویه‌ی ٤٥ درجه آلیس و باب این دستگاه را نسبت بهم تنظیم می‌کنند و کیوبیت‌ها را کدگذاری می‌کنند.

Intercept resend attack

مستقیم‌ترین استراتژی حمله از طرف حوا intercept resend گفته می‌شود. حوا فوتون‌ها را رهگیری می‌کند از طریق کانال کوانتومی و اندازه‌گیری افکنشی انجام می‌دهد همان‌طور که باب این کار را انجام می‌دهد. چون آلیس و باب به تنهایی کلیدی را تولید می‌کنند که باب آن را دریافت کند، حوا نیاز دارد که همان فوتون را دوباره ارسال کند. دوسناریو در اینجا وجود دارد اولی اینکه آلیس و حوا به صورت تصادفی پایه‌های یکسانی را انتخاب کنند (ماتریس پائولی یکسان) بنابراین توسط اندازه‌گیری، حالت

فوتون تغییر نمی‌کند پس حوا دارای اطلاعات ارسال شده‌ی توسط آلیس است و هیچ خطایی در آن نیست. سناریوی دوم این است که آلیس و حوا پایه‌های غیر یکسان انتخاب کنند که این به این معنی است که اطلاعات ارسال شده توسط آلیس آشکار نخواهند شد.

حملات دسته جمعی

حملات دسته جمعی باعث می‌شودکه حوا حافظه کوانتومی نداشته باشد. اومی‌تواند لوازم حمله خود را تا زمانی که مایل است نگه دارد و می‌تواند با توجه به دانش خود، که اندازه‌گیری جمعی است، بهترین اندازه‌گیری را انجام دهد. اندازه‌گیریی مخفی این حمله توسط Devetak-Winter انجام داده شده است [15].

$$\lim_{N\to\infty} r = S(X|E) - H(X|\gamma)$$

که $\begin{matrix} S(X|E) = S(X,E) - S(E) \\ H(X|\gamma) = H(X,\gamma) - H(\gamma) \end{matrix}$ می‌باشد.

کد گذاری

در این تحقیق موقعیت فوتون‌ها به صورت عرضی کدگذاری می‌شوند که برای اولین بار والبورن آن را انجام داده است [16]. اگر $f(r)$ دامنه‌ی آشکارسازی در صفحه‌ی x,y باشد پس:

$$|\psi\rangle = \int |r\rangle\langle r|d^2r|\psi\rangle = \int f(r)|r\rangle d^2r \quad (3)$$

این یک ویژه حالت تک فوتون در این صفحه‌ی x,y می‌باشد. حال اندازه‌گیری مکان این ویژه حالت $|\psi\rangle$ تک فوتون انجام می‌شود. از طرفی قائده‌ی تکمیل برای عملگر اندازه‌گیری داریم:

$$\int |r'\rangle\langle r'|d^2r' = 1$$
$$\langle r'|r\rangle = \delta^2(r'-r)$$

با توجه به معادله‌ی (1) احتمال آشکارسازی فوتون در مکان r' برابر است با:

$$p(r') = \langle\psi|r'\rangle\langle r'|\psi\rangle = |f(r')|^2$$

تابع موج تک فوتون می‌تواند در فضای k با استفاده از معادله‌ی تکامل تعریف شود:

$$|\psi\rangle = \int f(r)|r\rangle d^2r = \int\int f(r)\langle k|r\rangle|k\rangle d^2r d^2k = \int \frac{1}{2\pi}\int f(r)e^{-ik.r}d^2r|k\rangle d^2k$$

که در معادله‌ی بالا تابع موج و دامنه‌ی تبدیل فوریه به صورت زیر هستند:

$$\langle k|r\rangle = \frac{1}{2\pi} e^{-ik.r}$$

$$\mathcal{F}(f(r))[k] = \frac{1}{2\pi}\int f(r) e^{-ik.r} d^2 r$$

برای تابع گاوسی دوبعدی در نقطه‌ی $r_0 = (x_0, y_0)$ با واریانس Δx، دامنه به صورت زیر است:

$$f(r) = f(x,y) = \frac{1}{\sqrt{2\pi\Delta r^2}} \exp(-\frac{(x-x_0)^2 + (y-y_0)^2}{4\Delta r^2})$$

بنابراین با توجه به دو معادله‌ی بالا دامنه‌ی در فضای k به صورت زیر می‌شود:

$$\mathcal{F}(f(x,y))[k_x, k_y] = \frac{2\Delta r}{\sqrt{2\pi}} \exp(-\Delta r^2 (k_x^2 + k_y^2)) \exp(-i(x_0 k_x + y_0 k_y))$$

از آنجا که واریانس در فضای k به صورت $\Delta k = \frac{1}{2\Delta r}$ در نهایت دامنه در فضای k به صورت زیر می‌شود:

$$\mathcal{F}(f(x,y))[k_x, k_y] = \frac{1}{\sqrt{2\pi\Delta k^2}} \exp(-\frac{(k_x^2 + k_y^2)}{4\Delta k^2}) \exp(-i(x_0 k_x + y_0 k_y))$$

واریانس این دو شرط عدم قطعیت را برآورد می‌کند [17]

$$\Delta k \Delta r = \frac{1}{2}$$

حال احتمال را می‌توان با توجه به معادله‌ی ۱ حساب کرد:

$$p(k') = \left|\mathcal{F}(f(x,y))[k_x, k_y]\right|^2 = \frac{1}{2\pi\Delta k^2} \exp(-\frac{(k_x^2 + k_y^2)}{2\Delta k^2})$$

قابل ذکر است که احتمال بستگی به مرکز نقطه‌ی گاوسی ندارد. اندازه‌گیری در فضای k هیچ اطلاعاتی در مورد مرکز نقطه در فضای x به ما نمی‌دهد و بلعکس. فضای x وفضای k فوریه یک دیگر هستند. بنابر محدودیت‌هایی بردارهای پایه $|k\rangle$ و $|r\rangle$ نمی‌توانند برای کدگذاری استفاده شوند. بنابر کران داشتن معادله‌ی (3)، $f(r)$ بسط غیر صفر دارد که این باعث می‌شود $\langle a_i|b_j\rangle = \frac{1}{d}$ دچار تفاوت میان مقداری نظری و مشاهداتی شود. موقعیت مکانی فوتون‌ها توسط آشکارساز گسسته اندازه‌گیری می‌شود.

تا اینجا، فرض بر این بود که محتوای اطلاعاتی فوتون‌های منفرد تنها با انتخاب حالت‌های کوانتومی رمزگذاری شده، همانطور که دیده شد، اگر کسی ارتباط خط دید فضای آزاد با نور را در نظر بگیرد، باید با چندین منبع نویز مقابله کند [۱۸، ۱۹]. منبع دیگر آشفتگی جوی ناشی از گرادیان‌های باد و دما می‌باشد [۲۰]. تحت شرایط واقعی، کارایی تشخیص آشکارسازها و تعداد تاریک آن‌ها نیز باید در نظر گرفته شود. ظرفیت اطلاعات فوتون‌های کدگذاری شده به صورت طیفی [۲۱] و زمانی [۲۲] و حد بالایی از اطلاعات که می‌تواند توسط فوتون‌های رمزگذاری شده فضایی حمل شود، مورد بررسی قرار گرفت. بررسی ماکزیمم اطلاعات رمزگذاری شده در یک پالس منفرد با معرفی اثر چند فوتونی بر سهم نویز آشکارساز تمرکز می‌کند. در نهایت، پهن‌شدگی پرتو عرضی به وسیله کانال‌های انتقال نویزی انجام شده است.

حد بالای رمزگذاری اطلاعات

حد بالایی برای محتوای اطلاعات انتقالی تحت شرایط بدون صدا قابل ترجمه است. تعداد فوتون‌ها در هر پالس سیگنال Np می‌تواند بزرگ‌تر از یک باشد. تعدادی از آشکارسازهای Nd (متعامد) برای خواندن سیگنال مورد استفاده قرار می‌گیرند. آشکارسازها قابلیت شمارش تعداد فوتون‌ها را ندارند. ورود همزمان چندین فوتون منجربه تنها یک آشکارساز می‌شود، درست مانند یک فوتون. به همین دلیل، ما فرض می‌کنیم که هر آشکارساز تنها یک واقعه تک فوتونی دارد و تعداد نمادهای قابل‌تشخیص N_sها توسط ضریب دو جمله‌ای داده شده‌است.

$$N_s = \binom{N_d}{N_p} = \frac{N_d!}{N_p!(N_d - N_p)!} \quad (3.1)$$

این عدد زمانی به حداکثر خود می‌رسد که تعداد نمادها برابر با نصف تعداد آشکارسازها باشد.

حد بالایی شامل نویز آشکارساز

با الهام از یک توصیف واقعی‌تر، تاثیر نویز ردیاب باید آنالیز شود. همانند بخش قبل، پالس‌های سیگنال با حداکثر یک فوتون در هر ناحیه آشکارسازی در نظر گرفته شده‌اند. تشخیص این سیگنال‌ها به کلاس خاصی از دوربین‌های حساس تک فوتونی نیاز دارد. حساسیت بالای آن‌ها به قیمت داشتن است احتمالات محدود است. نمادها در رابطه (۳,۱) Np تعداد فوتون‌ها در یک پالس سیگنال و Nd تعداد آشکارسازها. اگر تعداد کلیک‌های آشکارساز با تعداد فوتون‌ها در پالس سیگنال مطابقت نداشته

باشد، این نتیجه اندازه‌گیری نادیده گرفته خواهد شد، زیرا این یک نشانه غیرقابل انکار از وقوع رویداد نویز است. آشکارسازهای قبلی برای آنها چهار رویداد مجزا ممکن است. دو حالت ایده‌آل منفی صحیح و مثبت صحیح هستند: هیچ فوتونی ارسال نشد و هیچ فوتونی ارسال نشد. اندازه‌گیری شده با احتمال K_{00} یا یک فوتون ارسال می‌شود و باعث کلیک بر روی آشکارساز می‌شود. با احتمال K_{11}. دو رویداد ناخواسته مثبت و نادرست هستند. منفی: هیچ فوتونی ارسال نشد، اما آشکارساز با احتمال K_{01} یا یک فوتون ارسال می‌شود اما با احتمال K_{10} تشخیص داده نمی‌شود.

با دو مورد از این احتمالات می‌توان احتمال اندازه‌گیری صحیح نماد را به صورت زیر محاسبه کرد:

$$R = K_{00}^{N_d - N_p} K_{11}^{N_p} \quad (3.2)$$

در این مورد، تمام آشکارسازهای Np با فوتون‌های تابشی کلیک می‌کنند، در حالی که در $N_d - N_p$ تعداد تاریکی رخ نمی‌دهد. احتمال تشخیص یک نماد اشتباه $1-R$ نیست، زیرا اندازه‌گیری‌هایی که تعداد رخدادهای تشخیص برابر نیست. با تعداد فوتون‌های تابشی Np که کنار گذاشته می‌شوند، و یک شمارش صحیح معادل با اندازه‌گیری‌های صحیح در هر آشکارساز نیست. برای یک تعداد ثابت و صحیح از رخدادهای آشکارسازی، هر فوتون که باعث کلیک آشکارساز نمی‌شود باید با یک شمارش تاریک از یک آشکارساز شمارش اشتباه جبران شود. بنابراین احتمال کلیک‌های غلط k با رابطه زیر داده می‌شود:

$$W = K_{00}^{N_d - N_p - k} K_{11}^{N_p - k} K_{01}^{k} K_{10}^{k} (3.3)$$

در اینجا، آشکارسازهای $N_p - k$ با فوتون‌های تابشی کلیک می‌کنند، در حالی که در زمان‌های $N_d - N_p$، حالت تاریک به وقوع نمی‌پیوندد. برای تحقق شرایط چارچوب کلیک‌های کلی Np، آشکارسازهای k که با احتمال K_{01} کلیک نکرده‌اند، در حالی که آشکارسازهای k که با احتمال K_{10} کلیک نکرده‌اند. بدون شمارش تاریک بالای عدد مورد نیاز برای Np، $k = 0, W_0 = R$ برای محاسبه‌ی خطای W. احتمال W_k باید در تعداد جایگشت‌ها ضرب شود. این منجربه این می‌شود:

$$W = \sum_{k=1}^{\min(N_p, N_d - N_p)} W_k \binom{N_d - N_p}{k} \binom{N_p}{k} \quad (3.4)$$

احتمال متوسط برای اندازه‌گیری نماد اشتباه $\frac{W}{N_s - 1}$ می‌باشد. احتمال مشترک به صورت زیر تعریف می‌شود:

$$P(x,y)=\frac{R}{N_s(R+W)} \qquad \forall x=y \qquad (3.5)$$

$$P(x,y)=\frac{W}{N_s(N_s-1)(R+W)} \qquad \forall x\neq y \qquad (3.6)$$

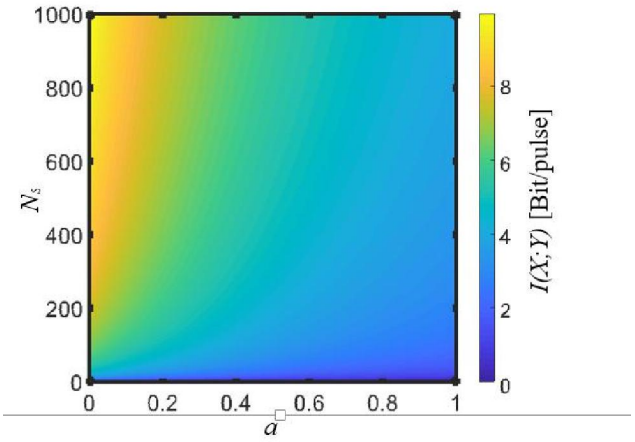
احتمالات می‌توانند برای محاسبه اطلاعات متقابل با استفاده از معادله $I(X;\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(x,y)}{P(x)P(y)}$ مورد استفاده قرار گیرند. در نتیجه معادله‌ی نهایی برابر می‌شود با:

$$I(X;Y)=\frac{R}{R+W}\log_2(\frac{N_sR}{R+W})+\frac{W}{R+W}\log_2(\frac{\frac{N_s}{N_s-1}W}{R+W}) \qquad (3.7)$$

حال اگر $a=\frac{W}{R}$ داریم:

$$I(X;Y)=\frac{1}{1+a}\log_2(\frac{N_s}{1+a})+\frac{a}{1+a}\log_2(\frac{\frac{N_s}{N_s-1}a}{1+a})=\log_2(N_s)+\log_2(\frac{1}{1+a})+\frac{a}{1+a}\log_2(\frac{a}{N_s-1}) \qquad (3.8)$$

اطلاعات متقابل در شکل زیر نشان‌داده شده‌است.



شکل ۲: اطلاعات فرمول فوق در شکل بالا نشان‌داده شده‌است.

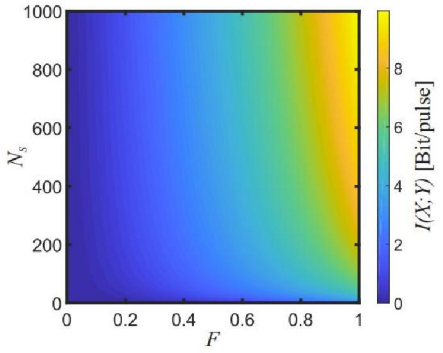
همان‌طور که انتظار می‌رفت اطلاعات متقابل برای نسبت‌های کوچک‌تر $a=\frac{W}{R}$ افزایش می‌یابد. هر چه احتمال تشخیص نماد درست R بیشتر باشد و احتمال اندازه‌گیری نماد غلط W کم‌تر باشد، اطلاعات متقابل بیشتر خواهد بود. علاوه بر این، همان‌طور که در بخش قبل دیده شد، اطلاعات متقابل با تعداد نمادها افزایش می‌یابد.

در این بخش، تعداد رویداده‌ای آشکارسازی برابر با تعداد فوتون‌های سیگنال در نظر گرفته شد. به عنوان نتیجه‌ای از این محدودیت، از دست دادن سیگنال مربوط به رویدادهایی است که در آن این اعداد نابرابر هستند. این امر منجر به از دست رفتن کلی $L=1-W-R$ می‌شود، که تمام رویدادها را در نظر می‌گیرد که به عنوان یک نماد اشتباه یا درست تشخیص داده نشده‌اند. این اتلاف چند جمله‌ای را در تعداد آشکارسازها و فوتون‌های سیگنال اندازه‌گیری می‌کند. در این مدل، یک حالت موج فوتونی Np توسط آشکارسازهای Nd با بازده η هر کدام تشخیص داده می‌شود. اگر تعداد تاریکی‌ها N_{dark} احتمال هر مشاهده‌گر برای تاریک $\frac{N_{dark}}{N_d}$ بنابراین فیدلیتی پیدا کردن نماد درست برابر است با:

$$F=\frac{N_p(\eta+\frac{N_{dark}}{N_d})}{N_p(\eta+\frac{N_{dark}}{N_d})+(N_d-N_p)\frac{N_{dark}}{N_d}}=\frac{N_p(\eta+\frac{N_{dark}}{N_d})}{N_p\eta+N_{dark}} \quad (3.9)$$

فیدلیتی را می‌توان در فرمول اطلاعات متقابل قرار داد:

$$I(X;Y)=\log_2(N_s)+F\log_2(F)+(1-F)\log_2(\frac{1-F}{N_s-1}) \quad (3.10)$$



شکل ۳: اطلاعات فیدلیتی در شکل بالا نشان‌داده شده‌است.

نمودار سطح کران بالا بر روی اطلاعات متقابل $I(X;Y)$ به عنوان تابعی از تعداد نمادهای NS و فیدلیتی F.

تاثیر صحت بر روی اطلاعات متقابل در شکل بالا نشان‌داده شده‌است. اطلاعات هر پالس با صحت افزایش می‌یابد و با صحت به حداکثر خود می‌رسد که مربوط به حالت بدون نویز متقابله $\log_2(N_s)$ است.

حد بالا شامل نویز کانال

همان‌طور که در بخش قبل بحث شد، اگر کسی بخواهد تشکیل متقابل را به شیوه‌ای موثر از فوتون افزایش دهد، باید یک فوتون منفرد را بر روی تعداد زیادی از آشکارسازها در نظر بگیرد. به همین دلیل است که در این بخش تعداد فوتون‌ها به یک فوتون در هر پالس سیگنال محدود می‌شود. آشکارسازها در یک آرایه تشخیص دو بعدی مرتب شده‌اند و فوتون به یک آشکارساز خاص هدایت می‌شود. نویز کانال به صورت گستردگی تابع $F(x-x_0,y-y_0,\sigma)$ از فوکوس با عرض σدر اطراف مرکز (x_0,y_0) . فرض بر این است که احتمال کلی شمارش تاریک در مقایسه با کارایی آشکارساز کوچک است، که این امکان را فراهم می‌کند که تحلیل را تنها با در نظر گرفتن آشکارسازی تک فوتونی ساده نماییم. به دلیل گستردگی کانون فوتون و آرایش دو بعدی آشکارسازها، گفت و گوی متقابل بین آشکارسازها قابل‌توجه می‌شود. اندازه آشکارسازها را می‌توان افزایش داد تا تبادل نظر را به حداقل برساند، اما در سناریوهای واقع گرایانه با دیافراگم‌های با اندازه محدود، این امر امکان پذیر نیست. منتهی‌الیه دیگر یک گستره تمرکز بر روی بسیاری از آشکارسازها خواهد بود، که اطلاعات متقابل را به حداقل می‌رساند. برای محاسبه اطلاعات متقابل از رابطه $I(X;\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(x,y)}{P(x)P(y)}$، توزیع احتمال مشترک $P(X;Y)$ باید دانسته شود. از $P(X;Y)$ در دو جا مشارکت می‌کند. اولی در سیگنال شبیه‌سازی شده‌ی تابع $F(x-x_0,y-y_0,\sigma)$ با بازده ی η .حالت دوم اینکه شمارش حالت‌های تاریک. برای توصیف این دو حالت باید یک فرمول-بندی درست کنیم و با یک نماد آن را تعریف کنیم که شکل آن $M(X,Y)$ می‌باشد. برای هر نماد x، این تابع آماری را می‌توان با انتگرال‌گیری منعکس‌کننده شدت تمرکز بر روی آشکارسازهایی که مشخص می‌شوند، محاسبه کرد.

$$M(X,Y)=\eta\int_{floor(\frac{y}{\sqrt{N_d}})}^{floor(\frac{y}{\sqrt{N_d}})+1}\int_{(y \bmod\sqrt{N_d})-1}^{y \bmod\sqrt{N_d}}F(k-floor(\frac{x}{\sqrt{N_d}})-0.5l-x \bmod\sqrt{N_d}+0.5\sigma)dkdl+\frac{N_{dark}}{N_d}\quad(3.11)$$

از طرفی در تابع گاوسی داریم:

$$F(x-x_0,y-y_0,\sigma)=\frac{1}{2\pi\sigma^2}\exp(-\frac{(x-x_0)^2+(y-y_0)^2}{2\sigma^2})\quad(3.12)$$

نهایتا برای نرمالیزه کردن احتمال از شرط زیر استفاده می‌کنیم:

$$\sum_{x\in X, y\in Y} P(x,y)=1 \qquad (3.13)$$

بنابراین داریم:

$$P(x,y)=\frac{M(x,y)}{\sum_{x\in X, y\in Y} M(x,y)}\approx\frac{M(x,y)}{N_d(\eta+N_{dark})} (3.14)$$

حالت ماکزیمم اطلاعات متقابل که فرستاده و دریافت می‌شود برابر است با $P(X)=P(Y)=\frac{1}{N_s}$ با این داده‌ها می‌توانیم اطلاعات متقابل را از رابطه‌ی $I(X;\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(x,y)}{P(x)P(y)}$ بدست آوریم.

انتقال اطلاعات بیش از ۱۰ بیتی با یک تک فوتون

کدگذاری اطلاعات در موقعیت فوتون‌های تکی هیچ محدودیت مشخصی با توجه به منابع نامحدود ندارد. با استفاده از یک منبع تک فوتونی خرد شده و یک ماژول نور فضایی (SLM)، ما فوتون‌های منفرد را به موقعیت‌های خاص در یک شبکه مجازی در یک منطقه بزرگ که آشکارساز شمارش فوتون (ICCD) را حل می‌کند، هدایت می‌کنیم. ما آدرس دهی انتخابی هر مکان (نماد)را در یک شبکه اندازه ۹۰۷۲ (الفبا) برای رسیدن به ۱۰,۵ بیت اطلاعات متقابل در هر فوتون شناسایی‌شده بین فرستنده و گیرنده به صورت تجربی نشان می‌دهیم. نتایج ما می‌تواند برای پردازش اطلاعات کوانتومی با ابعاد بسیار بالا مفید باشد. تعامل ضعیف آن با محیط، نور را برای به اشتراک‌گذاری اطلاعات بین طرفین دور ایده‌آل می‌سازد. به همین دلیل، نور برای انتقال اطلاعات در سراسر جهان استفاده می‌شود. با ظهور منابع تک فوتونی، طبقه جدیدی از کاربردها پدیدار شده‌است. به دلیل خواص کوانتومی آن‌ها، فوتون‌های منفرد برای سیستم‌های کوانتومی زاویه حمله یا برای انجام رمزنگاری کوانتومی مورد استفاده قرار می‌گیرند [23]. یک مثال معروف، توزیع کلید کوانتوم (QKD) با استفاده از پروتکل BB84 [24] برای ایجاد یک کلید محرمانه مشترک بین آلیس و باب است. امنیت این روش براساس قضیه عدم شبیه‌سازی است [25]، که کپی کردن حالت‌های کوانتومی را منع می‌کند. پیاده‌سازی استاندارد پروتکل BB84 از مبنای پلاریزاسیون دو بعدی برای رمزگذاری اطلاعات در فوتون‌ها استفاده می‌کند. بنابراین الفبا تنها شامل دو نماد "۰" و "۱" است که محتوای اطلاعات در هر فوتون را به یک بیت محدود می‌کند. افزایش بعد پایه با استفاده از یک الفبای بزرگ، محتوای اطلاعات هر فوتون را به همراه بهبود در امنیت افزایش می‌دهد [26، 27، 28]. این انگیزه استفاده از الفباهای بزرگ‌تر با استفاده از نیروی

حرکت زاویه‌ای اوربیتال [30,29]، بافینگ زمانی [31، 32] یا ترجمه فضایی [33, 34] است. در میان طرح‌های رمزگذاری فضایی، حالت‌های چرخش زاویه‌ای مداری (OAM) برای رمزگذاری اطلاعات با ابعاد بالا پیشنهاد شده‌اند [35]. با این حال در یک سناریوی عملی، با فرض پیکربندی فرستنده – گیرنده با دیافراگم‌های با اندازه محدود، یک نقطه محدود به پراش که در فضا ترجمه می‌شود یا مده‌ای لاگر رگاوس دارای حد ظرفیت بالاتری نسبت به زیرمجموعه‌ای از حالت‌های خالص OAM می‌باشد [36، 37]. این امر موقعیت یابی فضایی نور یا به طور معادل، کج کردن امواج صفحه‌ای، یک روش ایده‌آل برای افزایش محتوای اطلاعات به ازای هر فوتون را ایجاد می‌کند. جالب توجه است که با توجه به منابع نامحدود، هیچ حد بالایی برای محتوای اطلاعات منتقل‌شده توسط فوتون‌های واحد وجود ندارد. به عنوان مثال، استفاده از یک مول از آشکارسازهای تک فوتونی حساس به موقعیت ایده‌آل منجر به محتوای اطلاعاتی ۷۹ بیت در هر فوتون کشف‌شده می‌شود. واضح است که این امر در یک موقعیت عملی دور از دسترس است. بنابراین یک سوال بسیار مرتبط این است که چه چیزی را می توان به صورت تجربی محقق کرد. در این فصل ما آزمایش خود را گزارش می‌کنیم که در آن به صورت قطعی بیش از ۱۰ بیت اطلاعات را به یک فوتون رمزگذاری کرده‌ایم. ما ۲ تا ۳ برابر بیشتر از کاره‌ای قبلی در رمزگذاری فضایی به کار بردیم، که ۷ بیت در هر فوتون را به عنوان بالاترین مقدار برای کلیدهای تصادفی گزارش کرد [38]، و قابل مقایسه با چیزی است که در رمزگذاری زمانی و قطبیدگی به دست آمده‌است [39].

شیوه‌ی عملکرد راه اندازی

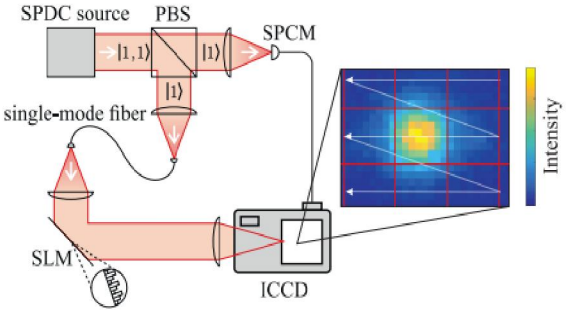
راه‌اندازی در شکل (٤,١) نشان‌داده شده‌است. ما از روش پارامتریک خود به خودی برای تولید منبع تبدیل برای تولید زوج فوتون استفاده می‌کنیم[40]. یک لیزر پیسکوند قفل‌شده با مد ۷۹۰ نانومتر با نرخ تکرار پالس ٧٦ مگاهرتز در یک کریستال LBO فرکانس را دو برابر کرده و به ۳۹۵ نانومتر می‌رساند. نور دو برابر شده بسامد در یک کریستال فوتون‌های قطبیده دوره‌ای پتاسیم تیتسیل فسفات (PPKTP) متمرکز است، که به طور خود به خود جفت فوتون‌های قطبیده عمودی را در طول‌موج ۷۹۰ نانومتر تولید می‌کند. زوج فوتون گیرافتاده در یک تقسیم کننده پرتو باریک پولاریزه کننده به دو حالت فوتون‌های تکی از هم جدا می‌شوند. یکی از این فوتون‌ها به یک ماژول شمارش تک فوتونی فرستاده می‌شود که به عنوان هرالد عمل می‌کند، در حالی که فوتون دوم از طریق یک فیبر ۲۸,۵ متری

تک مد با توان عملیاتی ٤٧ ٪ به تنظیمات رمزگذاری هدایت می‌شود. برای ارتباط آزادانه، یکی به یک دستگاه کدکننده در موقعیت فرستنده و یک دستگاه کدگشایی در موقعیت گیرنده نیاز دارد. به عنوان دستگاه رمزگذاری، ما از یک ماژول کننده نور فضایی برای تنظیم جبهه موج فوتون‌های تکی استفاده می‌کنیم. با نوشتن یک توری درخشان بر روی SLM، ما زاویه بازتاب را در محدوده زاویه‌ای ۰٫۸ در جهت عمودی و افقی با بازده شکست ٧٦ ٪ در مرتبه اول تغییر می‌دهیم. تبدیل فوریه SLM با یک لنز فاصله کانونی ۱ متری در پیکربندی ۲ f بر روی یک آشکار ساز شمارش فوتون با فضای فضایی بزرگ تصویربرداری شده‌است. یک فیلتر عبور باند در ٤۰nm ±۸۰۰ در مقابل ردیاب قرار داده می‌شود تا نور سرگردان را مسدود کند.

ردیاب

دستگاه رمزگشایی باید قادر به اندازه‌گیری ورود یک فوتون در یک عکس واحد در یک ناحیه بزرگ باشد. یکی از تکنولوژی‌هایی که می‌تواند به این هدف دست یابد، دستگاه مجهز به شارج – کوپله است [18, 19]. ICCDها یک گزینه روشن کردن نانوثانیه را فراهم می‌کنند، که مقدار تعداد تاریکی را به طور قابل‌توجهی کاهش می‌دهد و چنین ICCDای را قادر به اندازه‌گیری آشکار می‌سازد، و تعداد تاریکی را به یک در هزار خواندن کاهش می‌دهد. تعداد تاریک ICCDها منشا خود را در الکترون‌های گرمایی آزاد شده توسط فوتوکاتد ICCD دارند. علاوه بر این، اتم‌های باقی مانده گاز را می‌توان با بهمنی الکترونی درون صفحه میکروکانال (MCP) تقویت‌کننده یونیزه کرد. این یون‌ها با ولتاژ بایاس MCP به سمت فوتوکاتد شتاب می‌گیرند و بهمن‌های الکترونی ثانویه را آزاد می‌کنند. تاثیر یون باعث ایجاد الکترون‌های بسیار بیشتری نسبت به فوتون ورودی می‌شود. این امر منجربه افزایش سیگنال محلی در دوربین ICCD می‌شود که روشن‌تر از سیگنال تولید شده توسط یک فوتون است. بنابراین این سیگنال‌های یونی جعلی را می‌توان در پس پردازش فیلتر کرد. مدل ما (Andor iStar A -DH ٣٣٤ - ١٨T - A u٣) دارای بازده کوانتومی فوتوکاتد ٥٪ است. هر فوتون گلچین شده از منبع SPDC، دروازه ICCD را برای ۲ نانومتر باز می‌کند. در تصویر ٤٫۲ با زمان نوردهی ۰٫۱ ثانیه گرفته شده‌است. رویدادی تک فوتونی با استفاده از شمارش فوتون آستانه [41]، با سطح آستانه‌ای که بالای نویز بازخوانی دوربین CCD تنظیم شده‌بود، تحلیل شدند. با توجه به SPDC به نرخ هرالد ٤۰۰ کیلو هرتز، ما به طور متوسط ۷٫۳ تشخیص فوتون در هر نماد را اندازه‌گیری کردیم. FWHM از

فوکوس، با یک الگوی فاز ثابت در SLM و ادغام بیش از میانگین ۱۰۰۰ رویداد تشخیص فوتون، به صورت افقی ۷٫۹ ± ۰٫۳ پیکسل و به صورت عمودی ۷٫٤ ± ۰٫۲ پیکسل یافت شد.



شکل ۴: نمایش شماتیک چیدمان دستگاه رمز گشایی مجهز به شارج - کوپله است

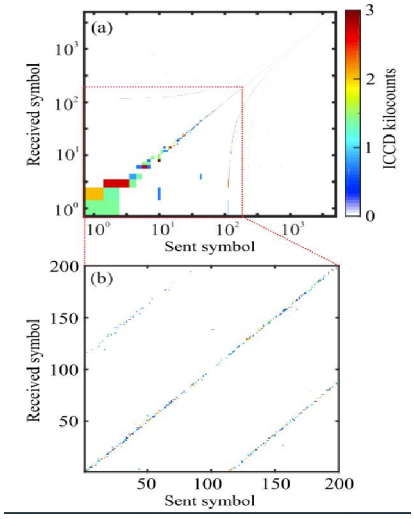
نمایش شماتیک چیدمان را مشاهده می‌کنید. منبع کاهشی پارامتریک خودبه‌خودی نوع II (SPDC) جفت فوتون تولید می‌کند، که توسط یک شکاف‌دهنده پرتو پرتو قطبی (PBS) تقسیم می‌شود. یکی از فوتون‌ها توسط یک ماژول شمارش تک فوتونی (SPCM) تشخیص داده می‌شود که به عنوان خبر دهنده برای یک CCD حساس شده (ICCD) عمل می‌کند. فوتون دیگر فیبر جفت شده و بر روی یک ماژول نور فضایی (SLM) اتفاق می‌افتد. تصویر فوریه آن بر روی ICCD نمایش داده می‌شود. موقعیت تمرکز با توجه به میله‌های آهنی که با تیر و کمان نشان داده می‌شود، با دقت اسکن می‌شود. موقعیت تمرکز با توجه به میله‌های آهنی که با تیر و کمان نشان داده می‌شود، با دقت اسکن می‌شود. خطوط قرمز، ماکل بندی ۸ * ۸ پیکسل نمادها را نشان می‌دهند.

رمز گذاری

موقعیت هدف فوتون بر روی ICCD با زاویه پراش افقی و عمودی شبکه در SLM تعیین می‌شود. اگرچه می توان از آینه اسکن برای رمزگذاری فضایی استفاده کرد، SLM یک ابزار انعطاف‌پذیرتر است. از طریق هولوگرافی، فاز و دامنه جبهه موج را می‌توان دستکاری کرد که امکان استفاده از جبهه موج پیچیده را فراهم می‌آورد. علاوه بر این، مسیر نور را می‌توان برای اختلالات اصلاح کرد با استفاده از روش‌های شکل‌دهی جبهه موج [42]. SLM (گام پیکسل: ۲۰ µm، رزولوشن: ۸۰۰ x ٦۰۰ پیکسل) با لبه‌های افقی و عمودی برای اسکن در سطح تشخیص ICCD برنامه‌ریزی می‌شود. محدوده زاویه‌ای الفباهای کدگذاری شده کوچک (۰٫۳۳ – ۰) و گام توری بیش از ۵ پیکسل است، که کارایی پراش یکنواخت و بالا را برای همه نمادها تضمین می‌کند. به منظور تعریف نماد ارسالی، موقعیت روی

ICCD باید به نمادهای جداگانه نگاشت شود. به همین دلیل، یک شبکه روی ICCD تعریف می‌شود. پیکسل‌های ICCD در نواحی شناسایی ۸ * ۸ یا ۱۲ * ۱۲ پیکسل با هم ترکیب می‌شوند و به ترتیب یک الفبای ۹۰۷۲ یا ٤۰۵۰ نماد را تشکیل می‌دهند. این نقشه مستطیلی در سطح شناسایی ICCD هر منطقه شناسایی را به یک برچسب منحصر به فرد متصل می‌کند، که از چپ به راست و از بالا به پایین شماره‌گذاری شده‌است.

رمزگذاری فضایی اطلاعات بر روی یک شبکه مجازی مستطیلی شکل که از پیکسل‌های یک دوربین تشکیل شده‌است، تحقق می‌یابد. در صورتی که کل تراشه دوربین مورد استفاده قرار گیرد، حداکثر اطلاعات $\log_2(1024*1024) = 20bit$ بیت است. اگر پارامترهای تجربی خود یعنی نسبت سیگنال به شمارش تاریک ۱۰,۰۸ و اندازه تمرکز ۸ پیکسل در هر جهت بر روی ICCD را پر کنیم، این عدد به ١٤,٤٥ بیت کاهش می‌یابد. ما در آزمایش خود از شبکه‌ای به ابعاد ۱۱۲ * ۸۱ پیکسل استفاده کردیم که ۹۰۷۲ نماد از الفبای ما هستند. این مقدار متناظر با حداکثر محتوای اطلاعاتی $\log_2(9072) = 13.15$ بیت است. نور با اسکن کردن فوکوس با استفاده از SLM به عنوان یک پنجره مشتعل به نمادهای متمایز بر روی شبکه هدایت می‌شود. ما فرض می‌کنیم که فرستنده از الفبای X و گیرنده از الفبای Y استفاده می‌کند. در این سیستم، ما توزیع احتمال مشترک $P(Y ،X)$ را بررسی می‌کنیم، که احتمالات $p(y ،x)$ برای تشخیص یک نماد خاص y خارج از الفبای Y را نشان می‌دهد اگر یک نماد x خارج از الفبای X ارسال شده‌باشد. نتیجه در شکل ٤,۲ نشان‌داده شده‌است. با اعمال یک آستانه بر روی سیگنال اندازه‌گیری شده، نویز ICCD کاهش یافت تا تنها سیگنال تشدید شده را نشان دهد. یک خط مورب در نمودار نماد ارسالی در مقابل دریافت، حداکثر همبستگی را نشان می‌دهد. در واقع یک همبستگی قوی بین مجموعه نمادهای ارسال‌شده و دریافت‌شده در گراف (a) وجود دارد که کل الفبا را در یک نمودار لوگ – لوگ نشان می‌دهد. گراف (b)یک بزرگنمایی را به ۲۰۰ مورد اول از ۹۰۷۲ نماد نشان می‌دهد. به دلیل تداخل بین نمادها، خطوط خارج از قطر قابل‌مشاهده هستند که متناظر با فوتون‌هایی هستند که به نماد در بالا یا پایین هدف برخورد می‌کنند. فاصله ۱۱۲ نماد بین این خطوط و قطر متناظر با طول ستون شبکه نوشته شده بر روی دوربین است. سیگنال سمت چپ و راست قطر از تداخل با نماد سمت چپ و راست در شبکه ناشی می‌شود. همچنین نویز می‌تواند ناشی از شمارش تاریک ICCD باشد.



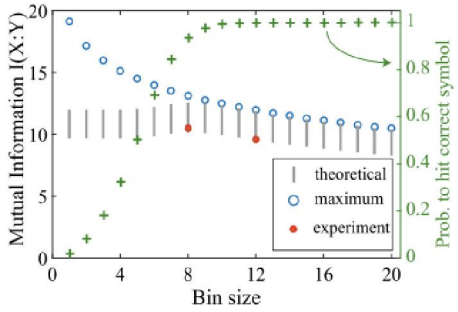
شکل۵: موقعیت هدف فوتون بر روی ICCD با زاویه پراش افقی و عمودی شبکه در SLM از هولوگرافی فاز و جبهه موج

آی سی‌دی اندازه‌گیری شده در هر یک از نمادهای اندازه‌گیری شده به عنوان تابعی از نماد ارسالی با اندازه ماکل ۸ * ۸ پیکسل حساب می‌شود. زمان نوردهی برای هر نماد ۰,۶ ثانیه بود. گراف (a) همبستگی بین تمام ۹۰۷۲ نماد را در یک نمودار لوگ – لوگ نشان می‌دهد. نمودار (b) همبستگی اندازه‌گیری شده بین ۲۰۰ نماد اول را در یک نمودار خطی نشان می‌دهد. نمودار (b) همبستگی اندازه‌گیری شده بین ۲۰۰ نماد اول را در یک نمودار خطی نشان می‌دهد. برای کمی کردن محتوای اطلاعات در هر فوتون، ما اطلاعات متقابل بین فرستنده و گیرنده را محاسبه می‌کنیم. اطلاعات متقابل I (X: Y) معیاری برای کاهش میانگین عدم قطعیت در مورد یک مجموعه نماد ارسالی X است که از یادگیری مقدار مجموعه نماد دریافتی Y حاصل می‌شود؛ یا برعکس، مقدار میانگین اطلاعاتی که X در مورد Y انتقال می‌دهد [43]. اطلاعات متقابل در هر رویداد آشکارسازی سیستم فرستنده – گیرنده از نظر ریاضی به صورت زیر نمایش داده می‌شود:

$$I(X:Y)=\sum_{x\in X,y\in Y}P(x,y)\log_2\frac{P(x,y)}{P(x)P(y)} \qquad (4.1)$$

که در آن P(y ،x) احتمال دریافت نماد y در زمانی است که نماد x ارسال می‌شود. P(y) احتمالی برای اندازه‌گیری نماد y و P(x) احتمالی است که فرستنده نماد x را رمزگذاری می‌کند. از لحاظ نظری اطلاعات متقابل به تعداد نمادهای N بستگی دارد که دارای ماکزیمم $I_{\max}=\log_2(N)$ با فرض $P(x)=\frac{1}{N}$ برای هر نماد $x\in X$ است. در این مقاله، احتمال یکنواخت x را برای تحقق بیشینه تئوری در غیاب نویز تضمین می‌کنیم. حداکثر تعداد نمادها با اندازه محدود CCD محدود می‌شود. با استفاده از اندازه

پوست ناحیه شناسایی ۸ * ۸، حد نظری ما ۱۳,۱۵ بیت است. در واقع، اطلاعات متقابل نه تنها توسط تعداد نمادها و آنتروپی الفبای ارسالی محدود می‌شود، بلکه توسط تداخل بین نمادهای ناشی از نقاط کانونی محدود به پراش و همچنین نویز از محیط و آشکارساز کاهش می‌یابد. به منظور کاهش تداخل بین نمادها، اندازه ماکل نواحی شناسایی را می‌توان افزایش داد. با این حال، این امر تعداد نمادهای داده‌شده به تعداد محدودی از پیکسل‌های آشکار ساز را کاهش می‌دهد. دایره‌های آبی در شکل ٤,٣ وابستگی ماکزیمم اطلاعات متقابل را برای نمادهای ساخته‌شده با اندازه پیکسل‌های مختلف نشان می‌دهد. اطلاعات متقابل اندازه‌گیری شده برای اندازه‌های ۸ * ۸ و ۱۲ * ۱۲ پیکسل به صورت دایره‌های قرمز نشان‌داده شده‌اند. داده‌های اندازه‌گیری شده کم‌تر از حد تئوری هستند. این امر را می‌توان از میانگین احتمال برخورد، که توسط نشانگرهای + سبز نشان‌داده شده‌است، درک کرد. علاوه بر این، با در نظر گرفتن نسبت سیگنال به تاریکی محدود بین ۱۰ و ۱۰۰، منجر به اطلاعات متقابل مورد انتظار می‌شود، که به صورت میله‌های خاکستری در شکل نشان‌داده شده‌است. همانطور که از شکل مشهود است، حداکثر اطلاعات متقابل با توجه به محدودیت‌های فیزیکی تداخل و نویز وجود دارد. برای اندازه‌های بزرگ سطل با تداخل نزدیک به صفر بین نمادها، می‌توان به اطلاعات متقابل بسیار بالایی از بیش از ۹ بیت در هر فوتون دست یافت. با توجه به اندازه نقطه FWHM تقریبا برابر با ۸ پیکسل، ما یک بونینگ ۸ * ۸ را انتخاب می‌کنیم که به مقدار ۱۰,۵ بیت اطلاعات متقابل در هر فوتون شناسایی‌شده دست می‌یابد. برای محاسبه اطلاعات متقابل در هر فوتون ارسالی، باید تلفات در راه‌اندازی ما در نظر گرفته شود. این شامل تلفات کوپلینگ در فیبرهای تک مد ۵۵ ٪، تلفات شکست در SLM ۲٤ ٪، تلفات در فیلتر طیفی ۳۰ ٪ و تلفات در آشکارساز به دلیل بهره‌وری کوانتومی محدود ۵ ٪ می‌باشد. این امر منجر به ظرفیت کانال ۰,۱ بیت بر فوتون می‌شود.



شکل ٦: نمودار وابستگی اطلاعات متقابل و میانگین احتمال برخورد در یک قطر کانونی محدود با FWHM ار ۸ پیکسل

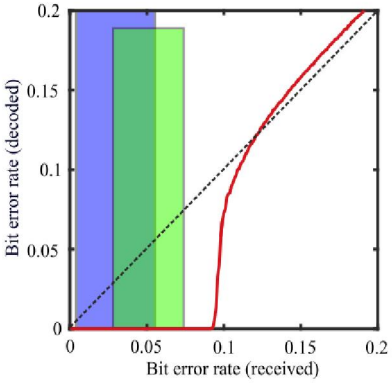
دایره‌های آبی نشان‌دهنده حد نظری Imax بدون هیچ سر و صدا یا تداخل هستند. نقاط قرمز متناظر با اطلاعات متقابل اندازه‌گیری شده برای اندازه ۸ * ۸ و ۱۲ * ۱۲ پیکسل می‌باشند. اطلاعات متقابل نظری به صورت میله‌های خاکستری در شکل نشان‌داده شده‌است، که برای نسبت فوتون با تعداد سیگنال به تاریکی بین ۱۰ و ۱۰۰ اصلاح شده‌است. نشانگرهای + سبز میانگین احتمال برخورد در ناحیه صحیح برای یک قطر کانونی محدود با FWHM از ۸ پیکسل را همانطور که در شکل نشان‌داده شده‌است، نشان می‌دهند.

نتیجه گیری

در این تحقیق حد بالای اطلاعات متقابل بین یک فرستنده و یک گیرنده برای یک مدل خاص را مورد بررسی قرار دادیم. نشان‌داده شد که به منظور به حداکثر رساندن اطلاعات در هر فوتون، یک تک فوتون باید در هر پالس سیگنال رمزگذاری شود. بخش بعدی نویز آشکارساز را در محدوده طرح معرفی می‌کند. نویز آشکارساز اطلاعات متقابل را در هر فوتون کاهش می‌دهد.

ارتباطات مفید، خطاهای پیام دریافتی باید اصلاح شوند. یک روش کارآمد برای تصحیح خطا، بررسی مقدار (LDPC) است [44]. برای اعمال این تصحیح خطا، تمام نمادهای مجموعه باید به یک رشته بیتی ترجمه شوند. بنابراین ما موقعیت x و y نمادهای خود را به طور مستقل کدگذاری می‌کنیم که هر کدام نیمی از بیت‌ها را اختصاص می‌دهند. از آنجا که عبارت نویز غالب، تداخل بین نمادهای همسایه است، ما از یک کد گری [45] برای هر جهت استفاده می‌کنیم. این امر باعث می‌شود که یک بیت برای تشخیص اشتباه توسط یک نماد همسایه چه در جهت x و چه در جهت y تغییر کند. شکل ٤,٤ نرخ خطای بیت (BER) را پس از تصحیح خطا با LDPC در مقابل BER رشته بیتی دریافتی نشان می‌دهد. کد LDPC بر روی LDPC نصف شده مورد استفاده در پخش تلویزیونی دیجیتال استاندارد .DVD B - S ۲. تنظیم شد. میله‌های عمودی شسته شده نشان‌دهنده خطای تخمین زده‌شده در حالت ۸ * ۸ و ۱۲ * ۱۲ می‌باشد. تخمین، تداخل اندازه‌گیری شده بین نمادها را در نظر می‌گیرد. لبه‌های چپ و راست آن‌ها به ترتیب نسبت فوتون با تعداد سیگنال به تاریکی ۱۰۰ و ۱۰ را نشان می‌دهند. برای ICCD به کار رفته دراین اندازه‌گیری برابر با ۱۰/۷۰ است. سایر ICCDهای تجاری موجود دارای نسبت‌های نزدیک به ۱۰۰ هستند که انتخاب حد دیگر را توضیح می‌دهد. واضح است

که در حال حاضر یک کد استاندارد تصحیح خطا امکان برقراری ارتباط عملی بدون خطا با سیستم کنونی را فراهم می‌کند.



شکل ۷: نمودارنرخ خطای بیت (BER)رشته بیتی دریافت‌شده در مقابل BER رشته بیتی پس از انجام تصحیح خطا نشان می دهد.

خط مورب خط‌چین شده نتیجه را بدون تصحیح خطا نشان می‌دهد. میله‌های عمودی نشان‌دهنده خطای برآورد شده آزمایش ما در حالت ۸ * ۸ (سبز) و ۱۲ * ۱۲ (آبی) می‌باشد. لبه‌های چپ و راست آن‌ها به ترتیب نسبت فوتون با تعداد سیگنال به تاریکی ۱۰۰ و ۱۰ را نشان می‌دهند. در نتیجه، ما رمزگذاری با ابعاد بالا از فوتون‌های تکی که به ۱۰,۵ بیت در هر فوتون می‌رسند را نشان می‌دهیم ظرفیت این رمزگذاری فضایی تنها توسط اپتیک و تعداد پیکسل‌های موجود در ردیاب محدود می‌شود. ظرفیت کانال ۰,۱ بیت را می توان با کاهش تلفات در سیستم افزایش داد. سهم اصلی تلفات در راه‌اندازی ما از بازده کوانتومی پایین (٪۵) ICCD ناشی می‌شود، که می‌تواند تا ٪۳۰ با مواد فتوکاتد مختلف بهبود یابد. این امر رسیدن به نسبت سیگنال به تعداد تاریکی ۱۰۰ را امکان پذیر می‌سازد و مقادیر اندازه‌گیری شده را به حداکثر نظری خود نزدیک‌تر می‌کند. نتایج ما به طور مستقیم برای ارتباطات خط دید فضای آزاد قابل اعمال است. اگر بتوان درهم‌ریختگی جبهه موج در فیبرهای چند حالته را کنترل کرد [46، 47]، یک حامل دوم و به طور بالقوه قوی‌تر برای این رمزگذاری با ابعاد بالا می‌تواند محقق شود. سپس یک مسیر بسیار امیدوار کننده برای این کار، پیاده‌سازی یک الفبای فضایی بزرگ رمزگذاری شده برای توزیع کلید کوانتومی یا قفل داده‌های کوانتومی با ابعاد بالا خواهد بود [48، 49].

فهرست منابع

1. Bennett C.H., Brassard G., Breidbart S., Wiesner S. (1983) Quantum Cryptography, or Unforgeable Subway Tokens. In: Chaum D., Rivest R.L., Sherman A.T. (eds) Advances in Cryptology. Springer, Boston, MA. https://doi.org/10.1007/978-1-4757-0602-4_26
2. Artur K. Ekert," Quantum cryptography based on Bell's theorem", Phys. Rev. Lett. 67, 661 – Published 5 August 1991, DOI:https://doi.org/10.1103/PhysRevLett.67.661
3. Darius Bunandar, Zheshen Zhang, Jeffrey H. Shapiro, and Dirk R. Englund," Practical high-dimensional quantum key distribution with decoy states", Phys. Rev. A 91, 022336 – Published 27 February 2015 DOI:https://doi.org/10.1103/PhysRevA.91.022336
4. Ding, Y., Bacco, D., Dalgaard, K. et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. npj Quantum Inf 3, 25 (2017). https://doi.org/10.1038/s41534-017-0026-2
5. C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York, 1984) pp. 175–179
6.] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
7. Quantum Cryptography : On the Security of theBB84 Key-Exchange Protocol, Thomas Baign`eres
8. Quantum Key Distribution Protocols and Applications, Sheila Cobourne, 8th March 2011
9. C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Tech. J. 28, 656–715 (1949).
10. C. E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J. 27, 379–423 (1984).
11. M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (Cambridge University, 2010)
12. I. D. Ivanovic, "How to differentiate between non-orthogonal states," Phys. Lett. A 123, 257–259 (1987)
13. N. Gisin, G. Ribody, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. 74, 145–195 (2002).
14. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984, (1984), pp. 175–179.
15. I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A 461, 2053, 207–235 (2005)
16. S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, "Quantum key distribution with higher-order alphabets using spatially encoded qudits," Phys. Rev. Lett. 96, 090501 (2006).
17. W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," Z. Phys. 43, 172–198 (1927).
18. M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (Cambridge University, 2010
19. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984, (1984), pp. 175–179
20. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature 299, 802–803 (1982).

21. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. 81, 1301–1350 (2009)
22. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," Phys. Rev. Lett. 88, 127902 (2002).
23. H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," Phys. Rev. A 61, 062308 (2000)
24. M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "Highdimensional quantum cryptography with twisted light," New J. Phys. 17, 033033 (2015).
25. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," New J. Phys. 8, 75 (2
26.] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," Phys. Rev. Lett. 98, 060503 (2007)
27. T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," New J. Phys. 17, 022002 (2015).
28. S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, "Quantum key distribution with higher-order alphabets using spatially encoded qudits," Phys. Rev. Lett. 96, 090501 (2006).
29. P. B. Dixon, G. A. Howland, J. Schneeloch, and J. C. Howell, "Quantum mutual information capacity for high-dimensional entangled states," Phys. Rev. Lett. 108, 143603 (2012).
30. 30. J. Wang, J-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. E. Willner, "Terabit free-space data transmission employing orbital angular momentum multiplexing," Nat. Photon. 6, 488- 496 (2012).
31. N. Zhao, X. Li, G. Li, and J. M. Kahn, "Capacity limits of spatially multiplexed free-space communication
32. J. M. Kahn, G. Li, X. Li, and N. Zhao, "To Twist or Not to Twist: Capacity Limits of Free-Space Channels," in "Advanced Photonics 2016 (IPR, NOMA, Sensors, Networks, SPPCom, SOF)" (2016), SpM4E.1
33. D. J. Gauthier, C. F. Wildfeuer, H. Stipcevi´c, B. Christensen, D. Kumor, ˇ P. Kwiat, K. McCusker, T. Brougham, and S. M. Barnett, "Quantum Key Distribution Using Hyperentangled Time-Bin States," in "Proceedings of The Tenth Rochester Conference on Coherence on Quantum Optics (CQO10)," (2014), pp. 234–239.
34. T. A. W. Wolterink, R. Uppu, G. Ctistis, W. L. Vos, K.-J. Boller, and P. W. H. Pinkse, "Programmable two-photon quantum interference in 10^3 channels in opaque scattering media," Phys. Rev. A 93, 053817 (2016).
35. B. Jost, A. Sergienko, A. Abouraddy, B. Saleh, and M. Teich, "Spatial correlations of spontaneously down-converted photon pairs detected with a single-photon-sensitive ccd camera," Opt. Express 3, 81–88 (1998).
36. R. Chrapkiewicz, W. Wasilewski, and K. Banaszek, "High-fidelity resolved multiphoton counting for quantum imaging applications," Opt. Lett. 39, 5090-5093 (2014).
37. I. M. Vellekoop and A. P. Mosk, "Focusing coherent light through opaque strongly scattering media," Opt. Lett. 32, 2309–2311 (2007)

38. D. J. C. MacKay, Information theory, inference and learning algorithms (Cambridge University, 2003).
39. R. Gallager, “Low-density parity-check codes,” IRE Transactions on information theory 8, 21–28 (1962).
40. F. Gray, “Pulse code communication,” (1953). US Patent 2,632,058.
41. T. Cižmár and K. Dholakia, “Shaping the light transmission through a ˇ multimode optical fibre: complex transformation analysis and applications in biophotonics,” Opt. Express 19, 18871–18884 (2011
42. L. V. Amitonova, A. P. Mosk, and P. W. H. Pinkse, “Rotational memory effect of a multimode fiber,” Opt. Express 23, 20569–20575 (2015).
43. D. J. Lum, J. C. Howell, M. S. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, and S. Lloyd, “Quantum enigma machine: Experimentally demonstrating quantum data locking,” Phys. Rev. A 94, 022315 (2016).
44. D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, “Locking classical correlations in quantum states,” Phys. Rev. Lett. 92, 067902 (2004).
45. D. Korff, “Analysis of a method for obtaining near-diffraction-limited information in the presence of atmospheric turbulence,” 2010 Int. Conf. Wirel. Commun. Sens. Comput. 63, 971–980 (1973)
46. A. A. B. Raj, J. A. V. Selvi, and S. Raghavan, “Terrestrial free space line of sight optical communication (tfslsoc) using adaptive control steering system with laser beam tracking, aligning and positioning (atp),” 2010 Int. Conf. Wirel. Commun. Sens. Comput. 1–5 (2010).
47. A. M. Oboukhov, “Some specific features of atmospheric tubulence,” J. Fluid Mech. 13, 77–81 (1962)
48. P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist,“Information capacity of a single photon,” Phys. Rev. A 88, 022310 (2013).
49. T. Brougham, C. F. Wildfeuer, S. M. Barnett, and D. J. Gauthier, “The information of high-dimensional time-bin encoded photons,” Eur. Phys. J. D 70, 214 (2016).