دوره هجدهم، شماره تابستان ۱۴۰۴

مجله فناوری اطلاعات در طراحی مهندسی

Information Technology in Engineering Design

http://sanad.iau.ir/journal/ited

ارائه راهکاری جهت افزایش سرعت توزیع کلید در رمزنگاری کوانتومیِ مستقل از دستگاه‌های اندازه‌گیری

محمدرضا سلطان آقایی[۱] فرزانه کاویانی*[۲]

(۱) گروه مهندسی کامپیوتر، واحد اصفهان، دانشگاه آزاد اسلامی، اصفهان، ایران

(۲) گروه مهندسی کامپیوتر، واحد اصفهان، دانشگاه آزاد اسلامی، اصفهان، ایران*

(تاریخ دریافت: ۱۴۰۳/۰۴/۱۸ تاریخ پذیرش: ۱۴۰۴/۰۲/۲۸)

چکیده

الگوریتم توزیع کلید کوانتومی مستقل از دستگاه‌های اندازه‌گیری (MDI-QKD) به علت سازگاری با تکنولوژی رایج، سرعت و برد بالاتر نسبت به سایر روش‌های رمزنگاری کوانتومی و پوشش دادن نواقص دستگاه‌ها، استفاده شده است. علی‌رغم مزیت‌های ذکر شده، سرعت تبادل کلید در روش‌های رمزنگاری کوانتومی از جمله MDI-QKD، نیازمند بهینه‌سازی است. هدف مقاله حاضر، ارائه راهکاری است که ضمن تضمین کامل امنیت و برد مناسب انتقال اطلاعات در الگوریتم MDI-QKD، سرعت توزیع کلید رمز را نسبت به روش‌های فعلی، بهبود ببخشد. مقاله حاضر مدلی جدید برای الگوریتم MDI-QKD ارائه نموده است که از طریق حذف فرد میانی، استفاده از پالس منسجم تضعیف شده به جای تک فوتون، استفاده از حالات سیگنال-تله و استفاده از یک مسیر منسجم به جای دو مسیر مستقل برای کانال کوانتومی، موفق شده است با اعمال داده‌های تصادفی با توزیع یکنواخت و با فرکانس ۲۰MHz، سرعت توزیع کلید ۲,۱ Mbps و برد مؤثر ۲۲۰ کیلومتر را بدست آورد. در حالی که بهینه‌سازی‌های ارائه شده پیشین در زمینه الگوریتم MDI-QKD سرعت ۱ Mbps را حاصل نموده است که برتری مدل ارائه شده نسبت به آنان مشهود است.

کلمات کلیدی: رمزنگاری کوانتومی، سرعت توزیع کلید رمز، MDI-QKD

*عهده‌دار مکاتبات:

محمدرضا سلطانی آقایی

نشانی: گروه مهندسی کامپیوتر، واحد اصفهان، دانشگاه آزاد اسلامی، اصفهان، ایران

پست الکترونیکی: soltan@khuisf.ac.ir

۱- مقدمه

قبل از ظهور رمزنگاری کوانتومی، امنیت روش‌های کلاسیک بر پایه فرضیات محاسباتی اثبات نشده از جمله پیچیدگی تجزیه اعداد بزرگ به عامل‌های اول [1] قرار داشته است اما رمزنگاری کوانتومی برای اولین بار روشی با امنیت صد در صد و خدشه ناپذیر ارائه نموده است [7,2]. امنیت رمزنگاری کوانتومی نه بر پایه فرضیات محاسباتی اثبات نشده بلکه بر مبنای قوانین اثبات شده فیزیک کوانتوم قرار گرفته است. تحقق تمامی شرایط پیش‌بینی شده در روش توزیع کلید کوانتومی، در پیاده‌سازی‌های انجام شده، امری خطیر است که باعث شده گروهی از حملات، به عنوان تنها حملات ممکن، بر اساس نقص در دستگاه‌های اندازه‌گیری و نه نقص پروتکل‌های رمزنگاری کوانتومی، سازمان‌دهی شوند [6,5,4,3]. لذا شیوه نوینی در رمزنگاری کوانتومی با عنوان توزیع کلید کوانتومیِ مستقل از دستگاه‌های اندازه‌گیری مطرح گردیده که خلاء مذکور را کاملاً برطرف نموده است. همچنین این شیوه جدید مسافت قابل دستیابی برای تبادل داده را نیز تا دو برابر نسبت به روش‌های معمول، ارتقاء داده است [8,7]. علی‌رغم بهینه‌سازی امنیتی ذکر شده سرعت تبادل کلید در این شیوه نوین، هنوز تا روش‌های کلاسیک فاصله دارد [9] و بهینه‌سازی سرعت، ضروری و لازم است. سوال اصلی اینجاست که چگونه می‌توان به راهکاری دست یافت که ضمن تضمین کامل امنیت و برد مناسب انتقال اطلاعات، سرعت توزیع کلید رمز را نسبت به روش‌های فعلی، بهبود بخشد.

بعد از ظهور رمزنگاری کوانتومی همواره ساخت تجهیزات فیزیکی که تمامی الزامات پروتکل‌ها را تحقق بخشند، چالش برانگیز بوده است. در پی این نواقص، روش‌هایی با نام روش‌های هک کوانتومی مطرح گردیده است [10,6,5,4,3] که البته هیچ یک از روش‌های ارائه شده نقص الگوریتم نبوده و تماماً به خاطر نقص دستگاه‌های به کار برده شده، به‌وجود آمده است. به‌عنوان یکی از راهکارهای رفع این مشکل پژوهشگران و دانشمندان حوزه رمزنگاری کوانتومی، الگوریتم‌های تکمیلی ارائه نمودند که با اتخاذ تدابیری وابستگی خود را به دستگاه‌های به کار رفته کم نمایند. یکی از موفق‌ترین این روش‌ها، الگوریتم توزیع کلید کوانتومی مستقل از دستگاه‌های اندازه‌گیری (MDI-QKD) می‌باشد [9]. الگوریتم یاد شده، یکی از بهترین الگوریتم‌هایی است که ضمن ارائه استقلال مناسب الگوریتم از دستگاه-های اندازه‌گیری، توانسته است پهنای باند قابل توجه و برد حدود دو برابر نسبت به الگوریتم‌های توزیع کلید کوانتومی قبلی ارائه نماید [11]. الگوریتم MDI-QKD در حال حاضر مناسب‌ترین گزینه برای راه‌اندازی شبکه‌های کوانتومی و ترویج رمزنگاری کوانتومی در شبکه‌های فیبر نوری موجود، می‌باشد [12]. هدف از این مقاله، اصلاح و به روزرسانی ساختار الگوریتم MDI-QKD است به نحوی که ضمن حفظ نقاط قوت الگوریتم فوق، سرعت توزیع کلید ارتقاء داده شود. ارتقاء سرعت مذکور می‌تواند به عنوان نوآوری مورد انتظار مطرح شود. در عین حال، حفظ کامل امنیت

روش MDI-QKD در بهینه‌سازی انجام شده و همچنین حفظ برد ارسال کلید کوانتومی، از الزامات بهینه‌سازی ارائه شده می‌باشد.

۲- مرور کارهای پیشین

به لحاظ تاریخی، پروتکل BB84 را می‌توان اولین پروتکل کاربردی برای رمزنگاری کوانتومی دانست که در سال ۱۹۸۹ در محیط آزمایشگاهی اجرا شد [13]. اساس کار این الگوریتم برپایه استفاده از روش One-Time-Pad و نیز استفاده از اسپین حالت کوانتومی است، روش‌های پیاده‌سازی انجام شده عموماً از پلاریزه‌ی فوتون‌ها به عنوان یک نمونه خوب از اسپین حالت کوانتومی استفاده نموده‌اند. روش One-Time-Pad به بیان ساده استفاده از یک کلید برای هر بلوک داده و عدم تکرار استفاده از آن کلید برای رمزنگاری است. در این پروتکل آلیس و باب هر دو از یک کانال عمومی و غیر ایمن برای ارسال داده به صورت کلاسیک و نیز ارسال وضعیت‌های کوانتومی استفاده می‌کنند و این باعث محتمل بودن دسترسی فرد سوم به داده‌های ارسالی می‌شود اما بر مبنای تئوری no-cloning در فیزیک کوانتوم کپی کردن هر حالت کوانتومی (Quantum State) از جمله پلاریزه‌ی فوتون که یک حالت کوانتومی از فوتون می‌باشد غیر ممکن است [14]. پس حمله‌ی مرد میانی برای این پروتکل غیر قابل انجام است. این پروتکل برای پیاده‌سازی به منبع ارسال تک فوتون احتیاج دارد که با تکنولوژی‌های امروزی ساخت منبع تک فوتون با کارایی مناسب و عدم نقص کاری مشکل و چالش برانگیز است. همچنین برمبنای احتمالات در ۵۰ درصد فوتون‌های ارسالی محورهای انتخاب شده در سمت فرستنده و گیرنده هماهنگی لازم را ندارند و داده‌های اندازه‌گیری شده بی‌اعتبار خواهند بود که این موجب کندی کار ارسال داده و پایین آمدن سرعت انتقال خواهد شد. مشکل دیگر پروتکل BB84 را می‌توان استفاده از تک فوتون به جای پرتوی قوی لیزر دانست که باعث کاهش برد ارسال اطلاعات در فیبر نوری و همچنین در فضای آزاد می‌شود. باید توجه داشت که به علت عدم امکان کپی کردن حالت کوانتومی فوتون، استفاده از تکرار کننده کلاسیکی برای افزایش برد ارسال اطلاعات غیرممکن است.

در سال ۱۹۹۱ آرتور اکرت پروتکل رمزنگاری کوانتومی را تحت عنوان E91 معرفی نمود [15]. در این روش به جای ارسال تک فوتون که در پروتکل BB84 وجود دارد از ارسال دو فوتون عجین شده[۱] استفاده می‌شود. طبق قوانین فیزیک کوانتوم، دو ذره کوانتومی که تحت شرایط خاصی با هم عجین شده‌اند صرف نظر از بعد زمان و مکان، اندازه‌گیری حالت کوانتومی یکی، باعث مشخص شدن حالت کوانتومی در ذره دوم خواهد شد. در E91 به یک منبع برای تولید و

[۱] entangled photon

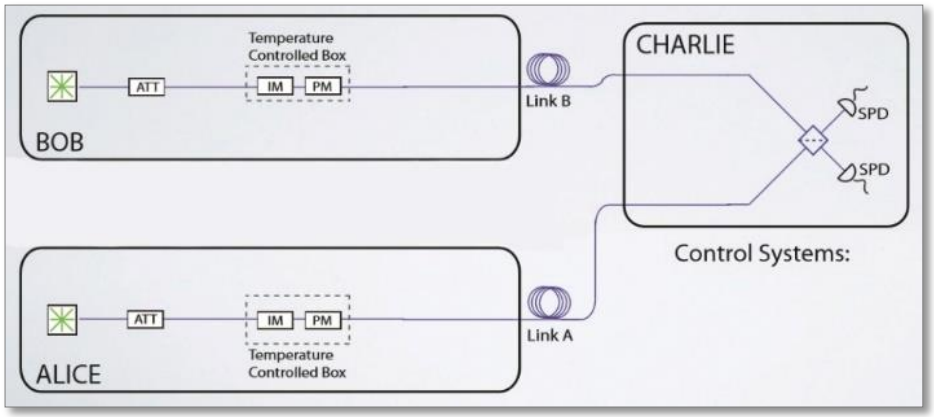
ارسال فوتون‌های عجین شده نیاز است. این منبع می تواند در سمت فرستنده (آلیس)، گیرنده (باب) و یا حتی پیش فرد سومی باشد. در این پروتکل، آلیس و باب می تواند از طریق "آزمون نامساوی بل" صحت کلید را بررسی کنند. اگر منبع ارسال فوتون‌های عجین شده در میان مسیر، بین فرستنده و گیرنده قرار داشته باشد می توان انتظار بُرد دو برابر در ارسال اطلاعات را داشت. همچنین ساخت منبع فوتون‌های عجین شده از منبع فوتون‌های تکی ساده‌تر خواهد بود. اما طبق احتمالات ریاضی، به طور میانگین از ۵۰ درصد مقادیر اندازه‌گیری شده، می‌توان در کلید استفاده کرد و سایر مقادیر، به علت متفاوت بودن محورهای انتخاب شده نامعتبر هستند و این باعث کند شدن روند ارسال داده در این پروتکل رمزنگاری می‌شود.

گروهی از محققان دانشگاه تورنتو پروتکل Decoy-state را معرفی نمودند تا نواقص ناشی از عدم بلوغ تکنولوژی حاضر را جبران نمایند [16]. ایده‌ی هوشمندانه‌ی به کار رفته، استفاده از آنالیزی غیرقطعی (هیوریستیک) در اطلاعات ارسالی است. همچنین در این پروتکل، برخلاف پروتکل‌های قبلی که تمامی اطلاعات ارسالی برای تولید کلید رمز استفاده می‌شد، اطلاعاتی به عنوان طعمه در خط ارتباطی ارسال می‌شود که هدف آنها تنها حفظ امنیت و برملا کردن وجود شنود در خط است. اگر چه این روش مقداری بار اضافی برای ارسال حالات کوانتومی طعمه برسیستم وارد می‌کند اما تا زمانی که تکنولوژی مناسب برای ساخت منبع تک فوتون در اختیار قرار گیرد، راه حلی هوشمندانه است. در پروتکل‌های قبلی برای اجتناب از ارسال ناخواسته‌ی چندین فوتون تکراری، سعی می‌شود فوتون‌ها با انرژی پایین‌تری ارسال گردند ولی در پروتکل Decoy-state بدون نگرانی می‌توان فوتون‌ها را با انرژی بالاتری ارسال نمود که این باعث افزایش برد ارسال اطلاعات می‌شود [16]. از معایب این پروتکل می‌توان به بار اضافی برای ارسال حالات تله و احتمال آسیب‌پذیری در صورت نقص در دستگاه‌های اندازه‌گیری اشاره نمود.

در پروتکل DI-QKD ایده‌ی اصلی، تخمین اطلاعات شنود شده بر اساس رخداد تناقضات در نامساوی بل است [17]. این ایده از کارهای قبلی در معرفی پروتکل E91 [15] نشأت گرفته است. در این پروتکل داشتن منبع قابل اطمینانی برای تولید اعداد تصادفی نیز مورد نیاز است. بعد از انجام عمل اندازه‌گیری پلاریزه‌ی فوتون‌های عجین شده صحت کار منبع فوتون‌های عجین شده از طریق تست نامساوی بل مورد ارزیابی قرار می‌گیرد و تنها در صورتی مقادیر پذیرفته می‌شوند که شنودی انجام نگرفته باشد و صحت کار منبع اثبات شود. اگر چه این پروتکل با بکاربردن ایده‌ای هوشمندانه گامی مؤثر در اجرای سیستم‌های رمزنگاری برداشته است، اما واقعیت این است که سیستم‌های رمزنگاری کوانتومی که در پیاده‌سازی خود از این پروتکل استفاده کردند، به پهنای باند و بُرد بسیار کمی دست یافتند، همچنین این پروتکل برای پیاده‌سازی نیازمند ردیاب فوتون با بهره‌وری نزدیک به یک می‌باشد که ساخت آن با تکنولوژی حاضر

بسیار مشکل است، این پروتکل نیازمند پیاده‌سازی منبع کوانتومی قابل اطمینان برای تولید اعداد تصادفی (QRNG) نیز می‌باشد [18] که به اندازه‌ی رمزنگاری کوانتومی چالش برانگیز خواهد بود.

روش دیگری با عنوان "توزیع کلید کوانتومی مستقل از دستگاه‌های اندازه‌گیری" (MDI-QKD) توسط لو و همکاران ارائه گردید [19]. ایده این روش ظاهر شدن آلیس و باب در نقش فرستنده است، آنان سیگنال مورد نظر را به فرد سومی که غیر قابل اطمینان در نظر گرفته می‌شود، ارسال می‌کنند. فرد سوم، عمل "اندازه‌گیری حالت بل" را انجام می‌دهد. صحت این عمل توسط آلیس و باب قابل ارزیابی است و آنان می‌توانند توانند تشخیص دهند که فرد سوم در کار خود صادق بوده و یا نه. در پروتکل فرض می‌شود آلیس و باب بر منابع خود اطمینان دارند، اگر این فرض محقق گردد، پروتکل MDI-QKD می‌تواند تمامی تهدیدات امنیتی کانال ارتباطی را حذف کند [19]. مهم‌تر از همه، این پروتکل می‌تواند با تکنولوژی فعلی پیاده‌سازی گردد و از این نظر کاملاً کاربردی است. به عنوان یک مدل پیاده‌سازی شده از پروتکل MDI-QKD می‌توان به یکی از پیاده‌سازی‌های انجام شده توسط شنگ و همکاران اشاره نمود [20] که در شکل (۱) نمایش داده شده است.



شکل ۱: نمونه‌ای پیاده‌سازی شده از الگوریتم MDI-QKD [20]

در این پروتکل، بعد از انتشار نتایج اندازه‌گیری توسط فرد سوم، فرستنده و گیرنده، محورهای انتخابی خود را به صورت عمومی، برای یکدیگر انتشار می‌دهند و زوج‌هایی از فوتون‌ها به عنوان کلید برگزیده می‌شوند که اولاً نتیجه آزمایش اندازه‌گیری حالت بل برای آنان موفقیت آمیز بوده باشد و ثانیاً محورهای انتخاب شده برای تولید آن‌ها در سمت آلیس و باب یکسان بوده باشد. پیاده‌سازی‌های انجام گرفته از MDI-QKD به برد قابل توجه ۲۰۰ کیلومتر و پهنای باند سه برابر نسبت به پیاده‌سازی‌های پروتکل‌های مشابه، دست یافته‌اند [20]. از مشکلات این پروتکل، می‌توان تأثیر خطای پیمانه برسرعت ارسال اطلاعات و پیچیدگی ساختار و مدیریت مشکل‌تر را ذکر نمود. با توجه به مزیت‌های MDI-QKD برسایر پروتکل‌های ذکر شده، چندین پیاده‌سازی موفق از آن انجام شده است.

ادغام توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI QKD) با شبکه‌های کلاسیک امنیت و صرفه‌جویی را تضمین می‌کند. زیرا الگوریتم MDI-QKD با طراحی خاص خود این امکان را فراهم می‌سازد که حتی در صورتی که دستگاه‌های اندازه‌گیری آسیب‌پذیر یا در اختیار یک دشمن باشند، امنیت تبادل کلید همچنان حفظ شود؛ به‌عبارت دیگر، این الگوریتم نیاز به اعتماد به تجهیزات اندازه‌گیری را از میان برداشته و به همین دلیل در محیط‌های غیرقابل اطمینان عملکرد بهتری نسبت به روش‌های سنتی دارد. با این حال، یکی از نقاط ضعف اساسی این الگوریتم، ناتوانی در ایجاد اتصال امن مستقیم میان دو گره کاملاً غیرقابل اعتماد است [23]؛ چرا که همچنان نیاز به یک گره‌میانی (مانند ایستگاه تداخل‌سنجی) وجود دارد که اگرچه به آن اعتماد کامل لازم نیست، اما بدون آن برقراری کلید ممکن نیست. این ویژگی، محدودیت‌هایی را در پیاده‌سازی در شبکه‌های توزیع‌شده واقعی ایجاد می‌کند، به‌ویژه در سناریوهایی که زیرساخت میانی قابل تضمین در دسترس نیست .

مقاله [29] نشان داد که MDI QKD نامتقارن عملکرد بهتری در سیستم‌های یکپارچه دارد. با مدل‌سازی مکانیسم اثر نامتقارن در سیستم‌های MDI یکپارچه و تجزیه و تحلیل اثر سرکوب نویز سازه‌های نامتقارن، افزایش پیش‌بینی‌نشده نرخ کلید تا ۲۶۰ درصد مشاهده شد که نتیجه‌گیری کاملاً مخالف سیستم اصلی است. پدیده یافت شده و مدل تحلیلی پیشنهادی روشی را برای سرکوب نویز و بهبود عملکرد ارائه می‌کنند، که امکان سازگاری بالا را برای شبکه‌های نامتقارن واقعی فراهم می‌کند. همچنین در مقاله [30] پروتکل MDI-MQKA پیشنهاد شده است که مشارکت محدود به افراد تایید شده است، و از امکان جعل هویت شرکت کنندگان جلوگیری می‌شود. پس از اجرای MDI-MQKA، هر شرکت کننده احراز هویت شده می‌تواند کلیدهای خصوصی مربوطه خود را به شیوه‌ای منصفانه و با کمک شخص ثالث بدست آورد. پروتکل MDI-MQKA یک تحقیق امیدوارکننده در مورد پروتکل‌های MQKA و فناوری‌های مستقل دستگاه اندازه‌گیری است که می‌تواند به پیشرفت کاربرد عملی فناوری اطلاعات کوانتومی کمک کند.

پیاده‌سازی الگوریتم MDI-QKD به شیوه‌ها و مدل‌های متنوعی انجام شده است که هر یک با هدف ارتقای عملکرد، برد یا امنیت طراحی شده‌اند. اولین مدل، مبتنی بر استفاده از پدیده عجین‌شدگی کوانتومی است. در این روش، از عجین‌شدگی برای اطمینان از عملکرد صحیح منبع فوتون و تجهیزات اندازه‌گیری استفاده می‌شود. صحت عملکرد این تجهیزات از طریق جمع‌آوری داده‌های آماری مربوط به ویژگی‌های عجین‌شدگی و توسط یک کاربر شاهد (trusted witness) بررسی می‌گردد. سایر مراحل این مدل با ساختار استاندارد MDI-QKD مطابقت دارد. این رویکرد با ارائه مکانیزمی نوین برای راستی‌آزمایی عملکرد دستگاه‌ها، موفق به دستیابی به سرعت تبادل کلید تا ۱ Mbps شده است. مدل دوم، الگوریتم MDI-QKD را با بهره‌گیری از حالت‌های منسجم زوج‌های اعلان‌شده پیاده‌سازی می‌کند. در این مدل، به جای استفاده از تک‌فوتون‌ها در تبادل کیوبیت‌ها، از حالت‌های منسجم استفاده شده

تا اثرات منفی تأخیر در آشکارسازها (dark time) بر نرخ خطای کوانتومی، به‌ویژه در فواصل طولانی، کاهش یابد. این روش توانسته است برد ارسال کلید را تا حدود ۳۰۰ کیلومتر افزایش دهد. در مدل سوم، پیاده‌سازی الگوریتم MDI-QKD با بهره‌گیری از جفت پرتوهای بردار حلقوی (vector vortex beams) انجام شده است. در این ساختار، پدیده عجین‌شدگی کوانتومی به‌طور مؤثر شبیه‌سازی شده و مشکلات ناشی از ناهماهنگی در پلاریزاسیون فوتون‌ها که موجب چرخش تصادفی آن‌ها می‌شود، مرتفع گردیده است. همچنین، استفاده از منبع فوتون پیشرفته SPDCS در این مدل، به افزایش سرعت توزیع کلید کمک کرده است. این مدل در زمینه افزایش برد نیز موفق عمل کرده و به بیش از ۳۰۰ کیلومتر دست یافته است .

در مدل چهارم، محققان با بهینه‌سازی پروتکل و بهره‌گیری از منابع منسجم زوج‌های اعلان‌شده، به بهبود سرعت و برد تبادل اطلاعات پرداخته‌اند. در این پژوهش، از آنالیز آماری دقیق نوسانات داده‌های ارسالی برای تأیید اعتبار نتایج بهره‌گیری شده است و بهبودهایی نسبت به پیاده‌سازی‌های قبلی حاصل گردیده است. مدل پایانی، پیاده‌سازی الگوریتم MDI-QKD بربستر ارتباطات ماهواره‌ای است که بین دو ایستگاه زمینی صورت گرفته است. فضای آزاد به دلیل تضعیف کمتر نسبت به فیبر نوری، امکان ارسال کیوبیت‌ها را در فواصل بسیار طولانی‌تر فراهم می‌سازد. در این مدل، تجهیزات اندازه‌گیری حالت بل (Bell state) در ایستگاه فضایی مستقر شده‌اند و ایستگاه‌های زمینی به عنوان آلیس و باب عمل می‌کنند. تحلیل امنیتی این روش در دو حالت، با فرض اعتماد و عدم اعتماد به ایستگاه فضایی انجام شده است. با وجود دستیابی به برد چشمگیر ۱۰۰۰ کیلومتر، پیچیدگی‌های هماهنگی بین اجزای سیستم و تغییرات نرخ تضعیف در لایه‌های مختلف اتمسفر از چالش‌های این روش هستند. همچنین، به‌رغم برد بالا، سرعت تبادل کلید در این مدل نسبت به سایر پیاده‌سازی‌ها پایین‌تر گزارش شده است.

جدول ۱: مقایسه روش‌های مختلف پیاده‌سازیMDI-QKD

ردیف	مدل پیاده‌سازی	نوع منبع/حالت فوتون	نوآوری کلیدی	مزایا	معایب / چالش‌ها
۱	مبتنی بر عجین‌شدگی کوانتومی	منبع فوتون + داده‌های آماری عجین‌شدگی	احراز صحت منبع و تجهیزات از طریق شاهد	تضمین صحت تجهیزات	پیچیدگی در استخراج داده‌های آماری عجین‌شدگی
۲	با حالت منسجم زوج‌های اعلان‌شده	حالت منسجم	کاهش تأثیر زمان تاریک ردیاب	مناسب برای فواصل دور	نیاز به تنظیم دقیق منبع منسجم
۳	با جفت پرتوهای بردار حلقوی SPDCS +	جفت پرتوهای برداری + SPDCS	شبیه‌سازی عجین‌شدگی + رفع ناهماهنگی پلاریزاسیون	برد بالا، پایداری بیشتر	پیچیدگی نوری و اپتیکی سیستم
۴	بهینه‌سازی با تحلیل آماری دقیق	منابع منسجم زوج‌های اعلان‌شونده	بهبود همزمان سرعت و برد با تحلیل نوسانات	کارایی بهینه در شرایط واقعی	نیازمند تحلیل پیچیده و دقیق آماری

۵	ماهواره‌ای بین دو ایستگاه زمینی	پالس نوری در فضا	استفاده از ایستگاه فضایی به عنوان دستگاه اندازه‌گیری	کمترین تضعیف، بیشترین برد	سرعت پایین، چالش هماهنگی و مدیریت سیستم فضایی

در جدول (۱) روشهای مختلف پیاده‌سازی الگوریتم MDI-QKD آمده است. در بررسی پنج مدل مختلف پیاده‌سازی این الگوریتم، می‌توان دریافت که هر روش تلاش کرده تا با تمرکز بر یک چالش کلیدی، محدودیت‌های موجود در ارتباطات کوانتومی را کاهش دهد. مدل مبتنی بر عجین‌شدگی کوانتومی با تمرکز بر احراز صحت تجهیزات، قابلیت اطمینان بالایی را فراهم می‌کند، اما پیچیدگی تحلیل داده‌های آماری عجین‌شدگی آن را محدود می‌سازد. مدل استفاده‌کننده از حالت منسجم در زوج‌های اعلان‌شده توانسته با کاهش تأثیر زمان تاریک ردیاب، برای فواصل دور مفید واقع شود، گرچه تنظیم دقیق منبع منسجم چالشی جدی در عمل خواهد بود. مدل مبتنی بر جفت پرتوهای بردار حلقوی و SPDCS با شبیه‌سازی عجین‌شدگی و حذف ناهماهنگی پلاریزاسیون، به برد بالا و پایداری بیشتر دست یافته، اما پیچیدگی‌های نوری و طراحی اپتیکی آن مانعی برای پیاده‌سازی گسترده محسوب می‌شود. در روش مبتنی بر تحلیل آماری دقیق، با بهره‌گیری از تحلیل نوسانات آماری منابع زوج‌های اعلان‌شده، افزایش سرعت و برد حاصل شده و کارایی در شرایط واقعی بهبود یافته است، هرچند نیاز به تحلیل‌های پیچیده آماری همچنان باقی‌ست. نهایتاً، مدل ماهواره‌ای بین ایستگاه‌های زمینی با استفاده از فضای آزاد و تضعیف کم سیگنال، بیشترین برد را فراهم می‌کند، اما با چالش‌های عمده‌ای همچون هماهنگی فضایی و سرعت پایین روبروست. در مجموع، هر مدل بسته به اولویت‌های عملیاتی و زیرساخت‌های موجود، می‌تواند برای کاربرد خاصی انتخاب شود.

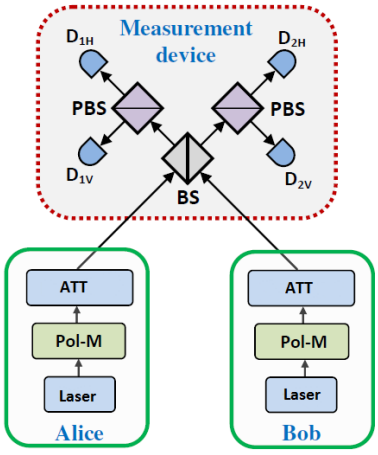
با توجه به مطالب مطرح‌شده و بررسی‌های صورت‌گرفته بر روی پروتکل‌های مختلف رمزنگاری کوانتومی، مشخص می‌شود که هر پروتکل بسته به هدف طراحی و توانمندی‌های تکنولوژیکی زمان خود، مزایا و محدودیت‌های خاصی دارد. پروتکل BB84 با ساختاری ساده و شفاف، مناسب‌ترین گزینه برای مفاهیم آموزشی و پیاده‌سازی‌های اولیه است، اما محدودیت‌های فناوری فعلی باعث شده سرعت پایین و برد محدود آن به‌ویژه در کاربردهای واقعی مشهود باشد. پروتکل E91 با بهره‌گیری از درهم‌تنیدگی کوانتومی، بنیانی علمی برای توسعه بسیاری از روش‌های مدرن فراهم ساخته است، اما محدودیت در برد و نرخ کلید، همچنان چالش‌برانگیز است. از سوی دیگر، پروتکل Decoy-State با استفاده از پالس‌های تضعیف‌شده و ایجاد تمایز میان فوتون‌های واقعی و تقلبی، گام مهمی در افزایش امنیت عملیاتی برداشته و موجب بهبود چشمگیر سرعت شده است. در نقطه مقابل، DI-QKD با وجود دستیابی به بالاترین سطح امنیت نظری، به دلیل سخت‌گیری‌های اجرایی و نیاز به تجهیزات بسیار پیشرفته، در عمل پیاده‌سازی‌پذیر نبوده و عملکرد ضعیفی دارد. در نهایت، پروتکل MDI-QKD با حذف وابستگی به دستگاه‌های اندازه‌گیری و مقاومت بالا در برابر حملات

مبتنی برنقص تجهیزات، توانسته عملکرد متعادل‌تری از نظر برد، سرعت و امنیت ارائه دهد و به‌عنوان گزینه‌ای مناسب برای بهینه‌سازی و پیاده‌سازی‌های پیشرفته انتخاب شود.

۳- اصلاح ساختار پروتکل MDI-QKD و ارائه مدل بهینه شده

در این بخش، به بررسی محدودیت‌های موجود در ساختار پایه‌ای پروتکل MDI-QKD پرداخته و اصلاحاتی جهت بهبود کارایی و پایداری آن پیشنهاد می‌شود. مطابق شکل ۲ که نمایی شماتیک از این پروتکل را نشان می‌دهد، تبادل فوتون‌ها از دو مسیر مجزا صورت می‌گیرد: مسیر نخست از فرستنده آلیس به چارلز (که وظیفه اندازه‌گیری را برعهده دارد) و مسیر دوم از باب به چارلز. عملکرد صحیح سیستم به هماهنگی زمانی بسیار دقیق میان این دو مسیر وابسته است؛ به‌گونه‌ای که فوتون‌های آلیس و باب باید همزمان در آشکارساز بل متعلق به چارلز حضور داشته باشند. کوچک‌ترین ناهماهنگی در زمان‌بندی یا بروز خطا در یکی از این مسیرها، منجر به از بین رفتن کل تبادل اطلاعات خواهد شد.

از دیگر چالش‌های مهم، کاهش بهره‌وری در یکی از منابع ارسال فوتون یا افت عملکرد در تجهیزات جانبی آلیس یا باب است که می‌تواند عملکرد کلی سیستم را تحت تأثیر قرار دهد. در واقع، این مشکلات بخشی از هزینه‌هایی هستند که در ازای دستیابی به برد بالاتر در پروتکل MDI-QKD پرداخت می‌شود.



شکل ۲: شمائی از پروتکل MDI-QKD

به عنوان مورد دیگری که مستعد بهینه‌سازی است می‌توان از لزوم وجود فرد سوم (چارلز) در سیستم نام برد. بدیهی است هماهنگی دستگاه‌ها، بین سه ایستگاه، مسلماً از انجام هماهنگی بین دو ایستگاه دشوارتر می‌باشد و در MDI-

QKD سیستم به مراتب پیچیده‌تری نسبت به پروتکل‌های توزیع کلید کوانتومی قبلی خواهیم داشت. پیچیدگی بیشتر باعث هزینه بالاتر برای اجرای سیستم و دشواری در رفع ایرادات خواهد شد. همچنین پیچیدگی، باعث وجود مراحل بیشتر در الگوریتم و کندی سرعت توزیع کلید خواهد شد. با ارائه یک مسیر منسجم تبادل کیوبیت، وابستگی سیستم به دو بستر ارسال داده و نیز پیچیدگی بیان شده در MDI-QKD تعدیل خواهد شد. اما باید توجه داشت که برد سیستم به عنوان یکی از مؤلفه‌های کلیدی تحت الشعاع قرار خواهد گرفت .

از دیگر مواردی که مستعد بهینه‌سازی در ساختار پروتکل MDI-QKD است، لزوم حضور واسط سوم (چارلز) در سیستم است. هماهنگی عملکرد تجهیزات در سه ایستگاه (آلیس، باب، چارلز) به‌مراتب دشوارتر از هماهنگی بین دو ایستگاه معمول در سایر پروتکل‌های توزیع کلید کوانتومی است. این افزایش پیچیدگی نه‌تنها هزینه‌های پیاده‌سازی و نگهداری سیستم را بالا می‌برد، بلکه عیب‌یابی و رفع خطاها را نیز پیچیده‌تر می‌کند. همچنین، افزایش اجزای سیستمی و گام‌های الگوریتمی منجر به کاهش سرعت توزیع کلید خواهد شد. در ادامه، روشی برای کاهش این چالش‌ها و افزایش پایداری و سرعت تبادل کلید ارائه می‌گردد.

برای حفظ بُرد در این مقاله، تلفیق روش ارسال فوتون‌ها در الگوریتم Decoy-State با الگوریتم MDI-QKD پیشنهاد می‌گردد. در الگوریتم Decoy-State به جای ارسال تک فوتون از ارسال پالس‌های لیزر با تعداد چندین فوتون همسان استفاده می‌شود، پالس‌های ارسالی در فرکانس‌های مختلف ارسال می‌شوند و تنها یکی از این فرکانس‌ها (فرکانس سیگنال) برای ارسال داده‌ها و مابقی برای ارسال حالات طعمه به کار می‌روند. بعد از ارسال چندین کیوبیت، فرستنده، فرکانس سیگنال را به گیرنده اعلام می‌کند و گیرنده برای تمامی فرکانس‌ها (فرکانس سیگنال و فرکانس‌های طعمه) مقدار خطا را محاسبه می‌کند در صورت وقوع تفاوت مشهود، به وجود شنود کننده در خط پی می‌برد و اطلاعات شنود شده را از کلید حذف می‌کند. در نتیجه این روش ضمن داشتن مزایای بیان شده در مقابل روش هک کوانتومی جداسازی فوتون‌ها ایمن خواهد بود و ارسال پالس حاوی چندین فوتون با پلاریزه یکسان مشکلی برای امنیت روش ایجاد نخواهد نمود. همچنین باید توجه داشت که در این حالت می‌توان بازدهی ردیاب‌ها را نیز ارتقاء داد زیرا در این روش ردیاب‌های فوتون معمولی مورد استفاده قرار می‌گیرند که با پالس‌های دارای حداقل هفت فوتون فعال می‌شوند و دارای بازده به مراتب بالاتری نسبت به ردیاب‌های تک فوتون هستند. این ردیاب‌ها در مقابل حملات کور کردن ردیاب مقاومت بالاتری دارند چون می‌توانند پرتو با انرژی بالاتری را در ورودی بپذیرند و عملکرد عادی خود را حفظ می‌کنند. برای غلبه برمشکل پیچیدگی در الگوریتم MDI-QKD در این پژوهش، مدلی اصلاحی ارائه می‌گردد که در آن به جای نیاز به فرد سومی برای انجام عمل اندازه‌گیری حالت بل (BSM) این کار توسط یکی از طرفین ارتباط انجام گیرد. این کار علاوه برکاهش پیچیدگی پیاده‌سازی، کاهش هزینه قطعات را نیز به همراه خواهد داشت. همچنین به علت حذف شدن

چارلز تعداد مراحل الگوریتم کاهش خواهد یافت و عملکرد توزیع کلید سریع تر خواهد گردید. به علت کاهش تعداد ایستگاه‌هایی که نیاز به هماهنگی دارند، مدیریت و هماهنگی دستگاه‌ها نیز ساده‌تر و سریع‌تر انجام خواهد شد و به طبع آن اشکال زدایی سیستم نیز ساده‌تر خواهد بود. همچنین با توجه به بررسی‌های انجام شده مشخص گردید که فرکانس-های مختلف در فیبر نوری برد متفاوتی در ارسال اطلاعات دارند [21]. این موضوع به خاطر این است که ضریب شکست یک ماده شفاف (از جمله فیبر نوری) برای فرکانس‌های مختلف، متفاوت است و این باعث می‌شود فوتون ارسالی در فرکانس‌های مختلف با ضریب شکست متفاوتی در فیبر نوری حرکت کند، این تفاوت در زاویه شکست نور در کانال، باعث می‌شود مسیر طی شده متفاوت بوده و در پایان برد متفاوتی را ارسال پرتو نوری در هر فرکانس شاهد باشیم. فرکانس‌های متفاوت، برد متفاوتی در فیبر نوری دارند و ساختار فیبر نوری به گونه‌ای است که پالس‌های لیزر در محدوده فروسرخ در آن با میرایی کمتری رو به رو می‌شوند و می‌توانند تا مسافت بیشتری در فیبر نوری به پیش بروند.

بهینه‌سازی دوم استفاده از پالس لیزر منسجم تضعیف شده[1] به جای استفاده از تک فوتون می‌باشد. همانطور که قبلاً بررسی شد منبع تک فوتون به علت عدم بلوغ تکنولوژی فعلی باعث برخی تهدیدات می‌شود و همچنین به علت پایین بودن انرژی تک فوتون، ارسال آن، برد مناسب برای شبکه‌های فیبر نوری را ندارد. پس به عنوان بهینه‌سازی دوم، به جای ارسال تک فوتون، از پالس لیزر منسجم تضعیف شده (WCP) پیشنهاد می‌شود که می‌تواند مسافت بالاتری را در فیبر نوری بپیماید. استفاده از پالس لیزر منسجم تضعیف شده، باعث می‌شود استفاده از ردیاب تک فوتون مناسب سیستم نباشد و باید ردیاب تک فوتون را با ردیاب‌های پالس نوری معمولی جایگزین کنیم. این تغییر نیز از چند جهت به افزایش کارائی سیستم کمک می‌کند. این ردیاب‌ها بازده بسیار بالاتری دارند و همچنین زمان نیستی آن نیز بسیار پایین‌تر است و ردیاب می‌تواند در زمان کوتاه‌تری آماده ردیابی پالس بعدی باشد. همچنین تهیه آنها نیز به آسانی صورت می‌گیرد. مشکلی که با تعویض تک فوتون‌ها با پالس لیزر منسجم تضعیف شده پیش می‌آید این است که سیستم حاصل مستعد حملات جداسازی فوتون‌ها می شود. برای رفع این مشکل از تکنیک حالت تله استفاده می‌شود. در این تکنیک ابتدا بازه فرکانسی بهینه‌ای را با توجه به بهینه‌سازی اول در نظر می‌گیریم سپس از این فرکانس‌ها در سمت فرستنده، چند فرکانس را به عنوان فرکانس انتقال اطلاعات کلید رمز (فرکانس سیگنال) و سایر فرکانس‌ها را به عنوان فرکانس‌های ارسال حالت تله در نظر گرفته و شروع به ارسال داده‌ها می‌کنیم. در پایان نرخ خطای بیت کوانتومی را به ازای هر فرکانس محاسبه می‌کنیم. اختلاف نرخ خطای بیت کوانتومی برای فرکانس‌های مختلف با در نظر گرفتن تضعیف کانال

[1] Weak Coherent Pulse

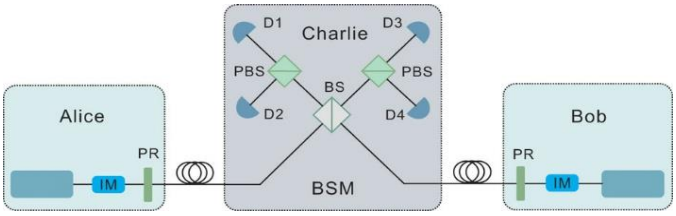
نباید از مقدار آستانه، بیشتر باشد. از این طریق می‌توان از وجود و یا عدم وجود استراق سمع‌کننده در کانال مطمئن شد. در پایان داده‌های مطمئن در تشکیل کلید استفاده می‌شوند. این روش برای اولین بار در الگوریتم Decoy-State معرفی گردید و باعث شد سرعت توزیع کلید در این الگوریتم به بالاترین میزان در بین سایر الگوریتم های توزیع کلید کوانتومی برسد [23,22]. در این پژوهش این سبک استفاده از حالت تله به عنوان بهینه‌سازی پیشنهادی بر روی الگوریتم MDI-QKD ارائه می‌گردد و انتظار می‌رود بتواند تأثیر قابل ملاحظه‌ای در سرعت توزیع کلید، داشته باشد.

مهم‌ترین بهینه‌سازی این تحقیق مربوط به محل انجام عمل BSM می‌باشد. برای بیان این بهینه‌سازی باز به سراغ الگوریتم MDI-QKD می‌رویم. می‌دانیم که امنیت در این الگوریتم مسئله اثبات شده‌ای است [24,9,8]. همچنین این الگوریتم می‌تواند عدم صداقت فرد میانی را استنباط نماید، اما براساس روشی که توسط برت و همکاران ارائه گردیده است است [25] می‌تواند در الگوریتم MDI-QKD قسمتی از کلید رمز را بدون تأثیر قابل توجه کشف کند. این روش به علت اینکه تنها می‌تواند بخش کوچکی از کلید را بدست آورد، روش هک موفقی محسوب نمی‌شود اما در این پژوهش، از آن به‌عنوان جرقه‌ای برای اجرای یک بهینه‌سازی قابل توجه استفاده شده است. روش هک ارائه شده به این صورت است که در الگوریتم MDI-QKD فرد میانی که آن را چارلز نامیدیم به جای ردیاب‌های معمول از ردیاب‌هایی با حداکثر راندمان استفاده می‌کند و این طور وانمود می‌نماید که ردیاب‌هایی که در اختیار دارد دارای راندمان یا بهره‌وری پایینی هستند. برای این منظور وی باید نتایج عمل BSM را به تعداد محدودتری منتشر کند و طوری عمل نماید که مقدار QBER (نرخ خطای بیت کوانتومی) در حد قابل قبولی باقی بماند. با توجه به اینکه در پیاده‌سازی‌ها معمولاً مقداری آستانه برای QBER در نظر گرفته می‌شود و برای مقادیر زیر آستانه مورد نظر اغماض صورت می‌گیرد چارلز می‌تواند قسمت جزئی از کلید را استخراج نماید.

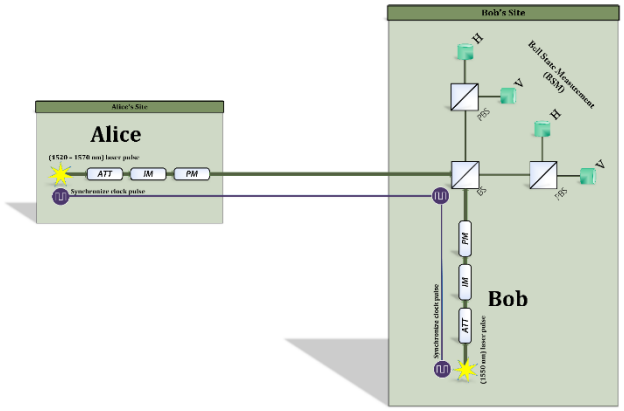
با توجه به این روش ارائه شده، به عنوان یک بهینه‌سازی در الگوریتم MDI-QKD پیشنهاد می‌شود دستگاه‌هایی که برای انجام عمل BSM مورد استفاده قرار می‌گیرند به جای قرار گرفتن در مکان فرد سوم، در محل گیرنده (باب) قرار داده شوند مطابق شکل(۴). این تغییر چندین مزیت دارد:

- اولین مزیت این است که همچنان صرفه جویی انجام شده در دستگاه‌هایی چون ردیاب را خواهیم داشت. الگوریتم MDI-QKD به خاطر اینکه به جای قرار دادن ردیاب‌ها در دو سوی فرستنده و گیرنده، ردیاب‌ها را در مکان فرد سومی قرار داده بود و تعداد تجهیزات مورد نیاز فرستنده و گیرنده را نیز کاهش داده بود، از جهت بهره‌روی اقتصادی توجه بسیاری از محققین را به سوی خود جلب نموده است. این روش همچنین پتانسیل خوبی در بحث شبکه‌های کوانتومی دارد و می‌تواند به عنوان روش پایه برای راه‌اندازی شبکه‌های کوانتومی مورد استفاده قرار گیرد. در بهینه‌سازی پیشنهادی در این پژوهش این مزیت برجسته حفظ خواهد گردید.

- دومین مزیت این است که در حالتی که دستگاه‌های مورد نیاز برای انجام عمل BSM در سمت گیرنده قرار داشته باشند امکان نشت حتی قسمتی از اطلاعات (همانند آنچه در روش هک ارائه شده بود) از بین خواهد رفت و کنترل کامل این سیستم در اختیار گیرنده خواهد بود که می‌تواند از تکنیک‌هایی چون استفاده از فیلترها، استفاده از محدود کننده‌های اُپتیکی، نظارت بر شدت پرتو ورودی و غیره بدین منظور استفاده نمود.
- سومین و مهم‌ترین مزیت افزایش قابل توجه در سرعت الگوریتم است زیرا در مدل ارائه شده در MDI-QKD (شکل ۳) به علت وجود دو کانال ارسال فوتون مجزا در صورت وقوع خطا در یک کانال اثر ارسال صحیح کانال دیگر خنثی شده و این باعث کاهش سرعت می‌شود همچنین در صورت عدم تجانس لازم در فیبر نوری دو کانال و تفاوت در سرعت کیوبیت‌ها در یک کانال، کل سیستم باید با سرعت پایین‌تر خود را وفق دهد که باعث کندی عملکرد کلی سیستم خواهد شد. همچنین پیچیدگی بیشتر در هماهنگی بین سه طرف تبادلات کیوبیت نیز باعث کندی عملکرد الگوریتم می‌شود. در حالی که در مدل پیشنهادی تنها یک مسیر ارسال کیوبیت می‌باشد که از آلیس تا باب امتداد دارد و عملکرد الگوریتم در این مدل منسجم‌تر و به دور از پیچیدگی خواهد بود. ارسال فوتون‌ها در بخش باب درونی بوده و با خطای بسیار کمی انجام خواهد شد. ایجاد کلاک مشترک نیز بین دو طرف انجام می‌شود و هماهنگ کردن دستگاه‌ها نیز ساده‌تر و سریع‌تر انجام می‌پذیرد. با توجه به بهینه‌سازی‌های پیشنهادی بیان شده، مدل ارائه شده در پژوهش حاضر مطابق شکل (۴) ساختار یافته است.



شکل ۳: روش MDI-QKD



شکل ۴: مدل پیشنهادی پژوهش

۴- مدل ریاضی مورد استفاده و تحلیل مدل پیشنهادی

در این مرحله جهت تحلیل مدل پیشنهادی از طریق مدل‌های ریاضی، با بررسی دقیق، مدلی که توسط محققین فیزیک کوانتوم و رمزنگاری کوانتومی در دانشگاه کلگری کانادا برای الگوریتم توزیع کلید کوانتومی مستقل از دستگاه-های اندازه‌گیری (MDI-QKD) ارائه گردیده است [26] به عنوان مدل ریاضی دقیق و مناسب تشخیص داده شد. این مدل براساس نتایج بدست آمده از پیاده‌سازی‌های تجاری موفق و نیز مباحث تئوری مطرح شده برای الگوریتم MDI-QKD تعریف شده است. در این مدل نواقص دستگاه‌هایی که برای مهیا کردن فوتون‌ها به کار می‌روند، اتلاف در کانال کوانتومی، بهره‌وری محدود ردیاب‌ها و همچنین نویز با دقت در مدل لحاظ شده‌اند.

مدل ریاضی ارائه شده برای الگوریتم MDI-QKD برپایه‌ی نسخه‌ای از پروتکل‌های توزیع کلید کوانتومی مبتنی بر *عجین‌شدگی معکوس در زمان* طراحی شده است. در این مدل، آلیس و باب به‌طور تصادفی یکی از چهار حالت کیوبیت شامل $|0\rangle$، $|1\rangle$، $|-\rangle$و $|+\rangle$ را انتخاب کرده و آن را به سمت ایستگاه واسط (که در نسخه سنتی چارلز است) ارسال می‌کنند. اما در مدل پیشنهادی مقاله حاضر، ساختار به گونه‌ای بازطراحی شده است که چارلز از معماری حذف شده و تبادل کیوبیت‌ها مستقیماً بین آلیس و باب انجام می‌گیرد. در این حالت، عمل *اندازه‌گیری حالت بل* (BSM) که در پروتکل اصلی توسط چارلز انجام می‌شد، اکنون در سمت باب صورت می‌گیرد. با این تغییر در معماری، اگرچه موقعیت انجام عملیات تغییر یافته است، اما فرمول‌بندی ریاضی برای عملیات BSM یکسان باقی می‌ماند، و تنها نحوه‌ی مدل‌سازی کانال کوانتومی متفاوت خواهد بود.

باید توجه داشت که منظور از $|-\rangle$و $|+\rangle$ کیوبیت‌های در نظر گرفته شده در راستای محورهای قطری می‌باشد که $|-\rangle$ را معادل صفر و $|+\rangle$ را معادل یک، نگاشت می‌کند و به ازای آن‌ها در دستگاه مختصات، رابطه (۱) برقرار خواهد بود.

$$|1\rangle)+|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \qquad (1)$$
$$|1\rangle)-|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle$$

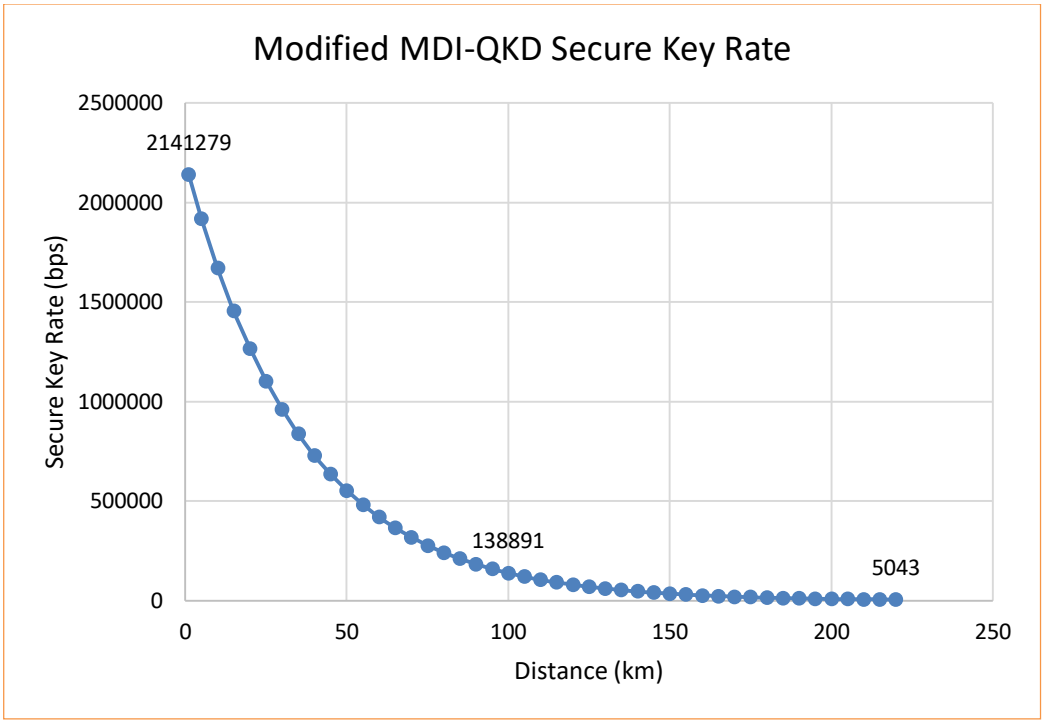
در ادامه، برای انجام عمل BSM از دو روش مرسوم استفاده می‌شود: در روش نخست، دو ردیاب و یک جداساز پرتو ۵۰:۵۰ استفاده شده و موفقیت BSM تنها زمانی حاصل می‌شود که یکی از ردیاب‌ها که معرف حالت $|\Psi^-\rangle$ است کلیک کند. این روش دقت هم‌زمانی بالایی را میان منابع نوری آلیس و باب طلب می‌کند و بازدهی نسبتاً کمی دارد. اما روش دوم با افزودن دو جداساز پرتو پلاریزه (PBS) عملکرد بهتری ارائه داده و امکان شناسایی دقیق‌تر چهار حالت

بل را فراهم می‌سازد. در این ساختار، فوتون‌ها پس از عبور از جداسازها به چهار ردیاب هدایت می‌شوند و یکی از چهار حالت بل شامل $|\Psi^-\rangle$، $|\Psi^+|$، $\langle\Phi^-|$ و $|\Phi^+\rangle$ به عنوان خروجی اندازه‌گیری تعیین می‌گردد. در این مدل نیز حالت $|\Psi^-\rangle$ به عنوان موفقیت در BSM تلقی شده و سایر حالات ناموفق در نظر گرفته می‌شوند. روابط ریاضی مربوط به این چهار حالت بل در معادله (۲) نمایش داده شده‌اند و مبنای تحلیل احتمال موفقیت در این اندازه‌گیری خواهند بود.

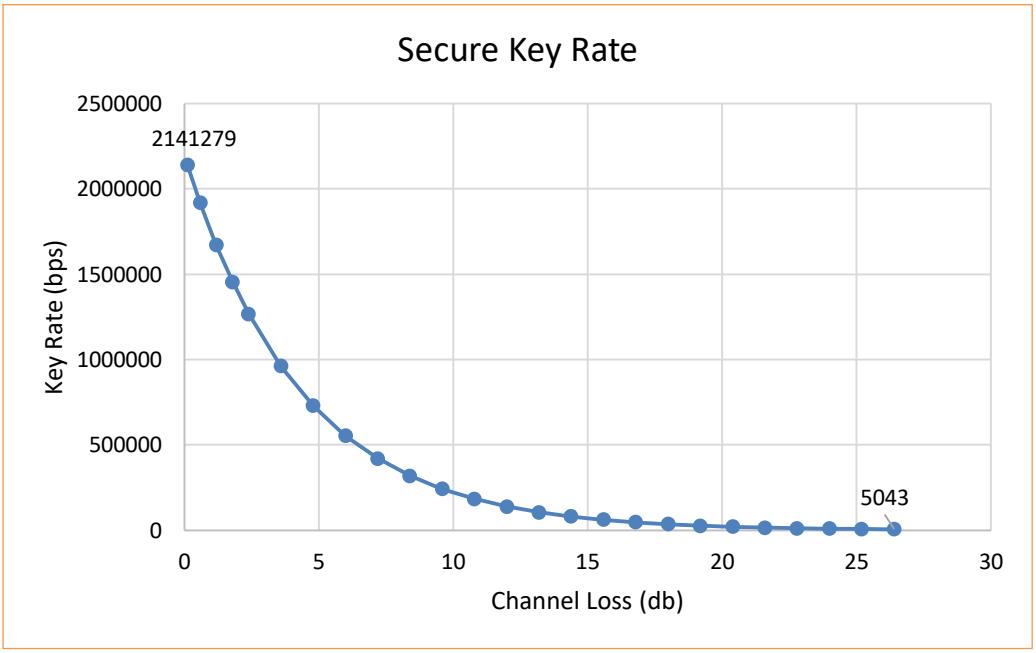
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \quad (2)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|1\rangle_A|1\rangle_B - |0\rangle_A|0\rangle_B)$$
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|1\rangle_A|1\rangle_B + |0\rangle_A|0\rangle_B)$$

در ابتدا برای تعریف مدل از کیوبیت‌های شامل زمان (time-bin) و نمونه آزمایشگاهی اجرا شده از MDI-QKD استفاده شده است. سپس داده‌های تجربی اندازه‌گیری شده توسط مدلی دقیق و بدون پارامتر آزاد و با درنظر گرفتن تحلیل آماری متغیرهای الگوریتم MDI-QKD، باز تولید شده‌اند. صحت عملکرد مدل برای بازتولید داده‌ها تا سه برابر نمونه اولیه ادامه یافته و صحت آن به اثبات رسیده است. مدل مذکور سپس جهت بهینه‌سازی دقت و سرعت مورد ارزیابی قرار گرفته و انواع بستر فیبر نوری، به عنوان کانال کوانتومی در آن لحاظ شده‌اند. این مدل به گونه‌ای طراحی شده است که اجرای الگوریتم MDI-QKD را در شرایط حداقل بی‌نظمی ناشی از عوامل محیطی، مدل‌سازی نماید.

فاکتورهای پیش‌بینی شده در این مدل، بارها با داده‌های سیستم‌های توزیع کلید کوانتومی که اصول کارکردشان اثبات شده است، مقایسه گردیده و به دقت قابل قبول دست یافته است. محاسبات انجام شده برای ۵۱۲ کیوبیت با توجه به نرخ ۲ مگا هرتز در تولید کیوبیت‌ها تعمیم داده شد و سرعت توزیع کلید همراه با نمودار آن شکل (۵) در مسافت بین ۱ تا ۲۲۰ کیلومتر رسم گردید. همچنین مقدار کارائی روش در مقابل میزان تضعیف کانال در نمودار شکل (۶) نشان داده شده است.



شکل ۵: نمودار سرعت توزیع کلید مدل ارائه شده برای الگوریتم MDI-QKD



شکل ۶: نمودار سرعت توزیع کلید در مقابل مقادیر تضعیف کانال

در مقایسه مدل پیشنهادی با توزیع کلید کوانتومی مبتنی برعجین شدگی و مستقل از دستگاه‌های اندازه‌گیری [28]، مشاهده شد که چه از لحاظ سرعت توزیع کلید و چه از لحاظ برد ارسال کلید دارای برتری مشهور می‌باشد. سرعت

توزیع کلید در مدل پیشنهادی ۲/۱ برابر پژوهش یانگ و همکاران می‌باشد و برد مدل پیشنهادی نیز به میزان ۷۶ کیلومتر (۵۲ درصد) ارتقاء یافته است.

در مقایسه مدل پیشنهادی با رمزنگاری کوانتومی MDI-QKD از طریق حالت منسجم زوج‌های اعلان شده، مقایسه بعدی با پژوهشی که توسط شِن و همکاران [27] ارائه گردیده است، انجام خواهد شد. در پژوهش مذکور پروتکل MDI-QKD به گونه‌ای اصلاح گردیده که به جای استفاده از تک فوتون در تبادل کیوبیت‌ها، حالت منسجم زوج‌های اعلان شده (۲) استفاده می‌شود. این بهینه‌سازی به منظور فائق آمدن بر تأثیر زمان تاریک ردیاب‌ها در فواصل دور، بر نرخ خطای کوانتومی، انجام گردیده است. شِن و همکاران در این پژوهش مدعی شده‌اند که تغییر ایجاد شده در پروتکل MDI-QKD باعث افزایش سرعت توزیع کلید کوانتومی گردیده است. صحت این موضوع از طریق تحلیل ریاضی مدل، اثبات گردیده است. مدل ارائه شده در پژوهش مذکور، بردی بالاتر از مدل ارائه شده در پژوهش حاضر دارد (۴۵ درصد برد بالاتر) ولی از لحاظ نرخ توزیع کلید، مدل ارائه شده در پژوهش حاضر دارای برتری مشهود می‌باشد.

در مقایسه مدل پیشنهادی با الگوریتم MDI-QKD به کمک جفت پرتوهای بردار حلقوی، برد الگوریتم اصلاح شده در پژوهش دان شِن و همکاران از برد مدل ارائه شده در پژوهش حاضر، تنها ۲۰ کیلومتر (۹ درصد) بیشتر است. در مورد سرعت توزیع کلید کوانتومی پژوهش دان شِن و همکاران موفق گردیده است در بهترین حالت به سرعت ۰٫۰۱ Mbps برسد که با اختلاف مشهودی کمتر از مدل ارائه شده در پژوهش حاضر است (۲٫۱ Mbps). همچنین مدل پیشنهادی با الگوریتم بهبود یافته MDI-QKD از طریق بکارگیری منابع منسجم زوج‌های اعلان شده، مشاهده گردید که برد دست یافته در پژوهش مذکور در نهایت حدود ۳۰۰ کیلومتر است که نسبت به مدل ارائه شده در پژوهش حاضر (۲۲۰ کیلومتر) به میزان ۳۶ درصد بالاتر است اما همان‌گونه که در نمودار مشخص است نرخ توزیع کلید در ابتدای مسیر حدود ۱۰۵ bps یا به عبارت دیگر ۱۰۰ kbps می‌باشد که اختلاف قابل توجهی با مدل ارائه شده در پژوهش حاضر (۲٫۱ Mbps) دارد.

۵- نتیجه‌گیری

این پژوهش با هدف اصلی افزایش سرعت توزیع کلید در رمزنگاری کوانتومی مستقل از دستگاه‌های اندازه‌گیری (MDI-QKD) موفق به ارائه مدلی نوین گردید که توانست به نرخ توزیع کلید کوانتومی ۲٫۱ Mbps دست یابد و به‌صورت ملموسی کارایی این نوع رمزنگاری را ارتقاء بخشد. با انجام سه بهینه‌سازی در ابعاد مختلف شامل تغییر مکان تجهیزات BSM، به‌کارگیری پالس منسجم تضعیف‌شده (WCP) و یکپارچه‌سازی مسیر تبادل کیوبیت‌ها، بدون ایجاد

اخلال در مبانی امنیتی الگوریتم، اهداف فرعی پژوهش نیز محقق شد. این بهینه‌سازی‌ها نه تنها باعث حفظ کامل امنیت روش MDI-QKD شدند، بلکه حتی در برخی ابعاد امنیت سیستم را ارتقاء بخشیدند. همچنین افزایش سرعت کلی تبادل داده نیز با توجه به ارتباط مستقیم آن با سرعت توزیع کلید، حاصل شد. مدل پیشنهادی از نظر برد ارسال نیز عملکردی قابل قبول داشته و با دستیابی به برد ۲۲۰ کیلومتر، توانسته است عملکردی رقابتی با جدیدترین پژوهش‌های مشابه داشته باشد. هرچند نسبت به برخی مدل‌ها دارای برد کمتر بوده، اما در مقابل، نسبت به برخی دیگر، بهبود قابل توجهی را ارائه داده است. بدین ترتیب، پژوهش حاضر در تحقق سه هدف اصلی خود شامل افزایش سرعت، حفظ امنیت و بهبود برد توزیع کلید کوانتومی در بستر الگوریتم MDI-QKD موفق عمل کرده و زمینه‌ساز پژوهش‌های آتی در حوزه بهینه‌سازی‌های عمیق‌تر، استفاده از حافظه‌های کوانتومی و توسعه شبکه‌های کوانتومی خواهد بود.

منابع

[1] D. K. Sharma, N. C. Singh, D. A. Noola, A. N. Doss, and J. Sivakumar, "A review on various cryptographic techniques & algorithms," Materials Today: Proceedings, vol. 51, pp. 104-109, 2022.

[2] C. Portmann and R. Renner, "Security in quantum cryptography," Reviews of Modern Physics, vol. 94, no. 2, p. 025008, 2022.

[3] X.-L. Pang et al., "Hacking quantum key distribution via injection locking," Physical Review Applied, vol. 13, no. 3, p. 034008, 2020.

[4] F.-X. Wang, J. Wu, W. Chen, S. Wang, and D.-Y. He, "Perceiving Quantum Hacking for Quantum Key Distribution Using Temporal Ghost Imaging," Physical Review Applied, vol. 15, no. 3, p. 034051, 2021.

[5] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, "Protecting fiber-optic quantum key distribution sources against light-injection attacks," PRX Quantum, vol. 3, no. 4, p. 040307, 2022.

[6] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-seeding attack in quantum key distribution," Physical Review Applied, vol. 12, no. 6, p. 064043, 2019.

[7] A. Sharma and A. Kumar, "A survey on quantum key distribution," in 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2019, vol. 1: IEEE, pp. 1-4.

[8] Y. Liu et al., "Experimental measurement-device-independent quantum key distribution," Physical review letters, vol. 111, no. 13, p. 130502, 2013.

[9] Y.-L. Tang et al., "Measurement-device-independent quantum key distribution over untrustful metropolitan network," Physical Review X, vol. 6, no. 1, p. 011024, 2016.

[10] Y.-J. Qian et al., "Hacking the quantum key distribution system by exploiting the avalanche-transition region of single-photon detectors," Physical Review Applied, vol. 10, no. 6, p. 064062, 2018.

[11] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Physical review letters, vol. 108, no. 13, p. 130503, 2012.

[12] M. Mehic et al., "Quantum key distribution: a networking perspective," ACM Computing Surveys (CSUR), vol. 53, no. 5, pp. 1-41, 2020.

[13] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Physical review letters, vol. 85, no. 2, p. 441, 2000.

[14] W. K. Wootters and W. H. Zurek, "The no-cloning theorem," Physics Today, vol. 62, no. 2, pp. 76-77, 2009.

[15] A. Ling, M. Peloso, I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Experimental E91 quantum key distribution," Advanced Optical Concepts in Quantum Computing, Memory, and Communication, vol. 6903, p. 69030U, 2008.

[16] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," Physical Review A, vol. 89, no. 2, p. 022307, 2014.

[17] U. Vazirani and T. Vidick, "Fully device independent quantum key distribution," Communications of the ACM, vol. 62, no. 4, pp. 133-133, 2019.

[18] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Reviews of Modern Physics, vol. 89, no. 1, p. 015004, 2017.

[19] V. Padamvathi, B. V. Vardhan, and A. Krishna, "Quantum cryptography and quantum key distribution protocols: a survey," in 2016 IEEE 6th International Conference on Advanced Computing (IACC), 2016: IEEE, pp. 556-562.

[20] X.-Y. Zhou, H.-J. Ding, C.-H. Zhang, J. Li, C.-M. Zhang, and Q. Wang, "Experimental three-state measurement-device-independent quantum key distribution with uncharacterized sources," Optics Letters, vol. 45, no. 15, pp. 4176-4179, 2020.

[21] F. e. Poletti et al., "Towards high-capacity fibre-optic communications at the speed of light in vacuum," Nature Photonics, vol. 7, no. 4, pp. 279-284, 2013.

[22] H.-W. Li, C.-M. Zhang, M.-S. Jiang, and Q.-Y. Cai, "Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology," Communications Physics, vol. 5, no. 1, p. 53, 2022.

[23] F. Grasselli and M. Curty, "Practical decoy-state method for twin-field quantum key distribution," New Journal of Physics, vol. 21, no. 7, p. 073001, 2019.

[24] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, "Versatile security analysis of measurement-device-independent quantum key distribution," Physical Review A, vol. 99, no. 6, p. 062332, 2019.

[25] J. Barrett, R. Colbeck, and A. Kent, "Memory attacks on device-independent quantum cryptography," Physical review letters, vol. 110, no. 1, p. 010503, 2013.

[26] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, "Modeling a measurement-device-independent quantum key distribution system," Optics express, vol. 22, no. 11, pp. 12716-12736, 2014.

[27] D. Chen, Z. Shang-Hong, and S. Lei, "Measurement device-independent quantum key distribution with heralded pair coherent state," Quantum Information Processing, vol. 15, no. 10, pp. 4253-4263, 2016.

[28] X. Yang et al., "Measurement-device-independent entanglement-based quantum key distribution," Physical Review A, vol. 93, no. 5, p. 052303, 2016.

[29] W.-X. Xie *et al.*, "Higher key rate in asymmetric quantum-classical integrated measurement-device-independent quantum-key-distribution systems," vol. 20, no. 5, p. 054042, 2023.

[30] G.-D. Li, W.-C. Cheng, Q.-L. Wang, and J.-C. J. Q. I. P. Liu, "A measurement device independent multi-party quantum key agreement protocol with identity authentication," vol. 22, no. 12, p. 443, 2023.