مقاله پژوهشی

پروتکل بهبودیافته مخابره مستقیم نیمه‌کوانتومی

زینب رشیدی و منیره هوشمند

چکیده: برخلاف رمزنگاری کلاسیک که امنیت آن مبتنی بر پیچیدگی محاسباتی است، رمزنگاری کوانتومی دارای امنیت بی‌قید و شرط بوده که بر مبنای محدودیت‌های فیزیکی تأمین می‌شود. تا کنون نسخه نیمه‌کوانتومی بسیاری از مسایل پروتکل‌های مخابره امن کوانتومی پیشنهاد شده است. در این پژوهش به بررسی پروتکل‌های نیمه‌کوانتومی پرداخته‌ایم که کاربران بدون توزیع کلید، به صورت مستقیم به پیام محرمانه دست خواهند یافت. فاکتور مهمی که برای تحلیل عملکرد پروتکل‌های ارتباط مستقیم امن کوانتومی به کار گرفته می‌شود، بازدهی می‌باشد. پروتکل پیشنهادی مخابره امن نیمه‌کوانتومی، در برابر انواع حملات کوانتومی بررسی شده است. در طرح پیشنهادی برای کدگشایی پیام محرمانه توسط گیرنده، نیاز به دنباله‌ای از تک فوتون‌ها است که در مرحله اول توسط کنترل‌کننده تولید می‌شود. پروتکل پیشنهادی دارای بازدهی ۵۰٪ است که نسبت به پروتکل قبلی که دارای بازدهی ٦٦/٦٪ است، بازدهی بالاتری دارد.

کلیدواژه: **رمزنگاری کوانتومی، رمزنگاری نیمه‌کوانتومی، مخابره امن نیمه‌کوانتومی، کنترل‌کننده.**

۱- مقدمه

امروزه مخابرات و انتقال اطلاعات، جزئی جدایی‌ناپذیر از زندگی بشر است. این مفهوم به معنی انتقال داده‌ها و اطلاعات از یک مکان به مکان دیگر است. اگرچه می‌توان به روش‌های متفاوتی مخابرات را تعریف کرد، اما مخابرات در محیط‌های عملی با تعریف نظریه اطلاعاتی آن شناخته می‌شود. ارتباط و مخابرات نقش بسیار مهمی را در نظریه اطلاعات ایفا می‌کنند. رمزنگاری[1] به دو روش کلاسیک و کوانتومی انجام می‌شود. در رمزنگاری به روش کلاسیک مبنای کار حل مسایل ریاضی می‌باشد که در آن برای بازگشایی اطلاعات از یک کلید استفاده می‌شود. چنانچه هنگام انتقال اطلاعات، استراق سمع کننده‌ای به کلید دسترسی پیدا کند، می‌تواند با آن تمام اطلاعات رمزشده و مخفی را بازگشایی نماید. بنابراین امنیت اطلاعات به خطر افتاده و مسیر انتقال اطلاعات امن نخواهد بود. این در حالی است که در رمزنگاری کوانتومی[2]، اگر استراق سمع کننده‌ای در کانال بخواهد به اطلاعات دسترسی پیدا کند، به دلیل خواص رفتاری ذرات که می‌توانند در لحظه تغییر کنند، استراق سمع کننده نمی‌تواند به اطلاعات دسترسی پیدا کند و بنابراین کانال کوانتومی کاملاً ایمن است. در حال حاضر، یک ابررایانه اگر بخواهد عددی ۶۰۰ رقمی را به ضرایب خود تجزیه کند، نیاز به اندازه عمر یک کیهان دارد، در حالی که برای یک رایانه کوانتومی، این زمان فوق‌العاده کوتاه می‌باشد. با اطلاع‌داشتن از محاسبات کوانتومی، می‌توان از حالت‌های کوانتومی برای انتقال امن اطلاعات کلاسیک (رمزنگاری کوانتومی) استفاده کرد.

۲- پیشینه مطالعات

اولین بار در سال ۲۰۰۷، Boyer و همکارانش در [۱] نشان دادند که برای یک پروتکل رمزنگاری با امنیت بی‌قید و شرط لازم نیست هر دو کاربر در پروتکل دارای امکانات کوانتومی باشند و تنها یک کاربر با قابلیت‌های کامل کوانتومی کفایت می‌کند و چنین پروتکل‌هایی را نیمه‌کوانتومی[3] نامیدند. امکان انتقال حالت کوانتومی از یک مکان به مکان دیگر وجود دارد که به آن مخابره از راه دور کوانتومی[4] گفته می‌شود [۲]. G. E. Moore، یکی از بنیان‌گذاران شرکت اینتل در ۱۹۶۵ به صورت تجربی بیان کرد که قدرت رایانه‌ها هر ۱۸ ماه به طور تقریبی دو برابر می‌شود [۳]. در ۲۰۲۰ اندازه ترانزیستورها روی یک تراشه سیلیکونی به اندازه یک اتم خواهد رسید [۴]. رفتار مسلط بر اتم‌ها، قوانین مکانیک کوانتومی است. از این پس محاسبات کلاسیکی پاسخگوی رفتار کوانتومی ذرات نخواهد بود، زیرا اتم‌ها در حدود ابعاد نانومتری اثرات کوانتومی دارد [۵]. برای اولین بار Benioff در ۱۹۸۰ ارتباط بین محاسبه و مکانیک کوانتومی را مطرح کرد. در محاسبات کوانتومی نحوه انتقال و ماهیت پیام تحت تأثیر آثار کوانتومی است [۶] و [۷]. ایده اصلی ساخت رایانه‌هایی بر مبنای قوانین مکانیک کوانتومی را R. Feynman در ۱۹۸۲ مطرح کرد [۸]. L. Grover در ۱۹۹۵ طرحی برای الگوریتم جستجو در میان مجموعه‌ای از اطلاعات نامرتب بیان کرد [۹]. الگوریتم Grover به دلیل کاربرد گسترده الگوریتم‌های جستجو دارای اهمیت زیادی نسبت به الگوریتم‌های معادل کلاسیکی‌اش است [۱۰]. رمزنگاری کوانتومی اولین بار توسط Wiesner در اوایل دهه ۱۹۷۰ ارائه شد که مقاله وی در این زمینه در ۱۹۸۳ به چاپ رسید [۱۱] و در ۱۹۹۰، Artur Ekert روش دیگری برای رمزنگاری کوانتومی ارائه داد. در ۱۹۸۲ مقاله‌ای توسط Bennet و همکارانش ارائه گردید [۱۲] که در آن برای اولین بار اصطلاح رمزنگاری کوانتومی مورد استفاده قرار گرفت. اولین شاخه رمزنگاری کوانتومی توزیع کلید کوانتومی است که توسط Bennet و Brassard در ۱۹۸۴ مطرح شد [۱۳]. در پروتکل مخابره نیمه‌کوانتومی یکی از کاربران قانونی مخابره کاملاً کلاسیکی است و بنابراین هزینه‌های دستگاه‌های سخت‌افزاری کوانتومی در پیاده‌سازی عملی کاهش می‌یابد. ارتباط امن نیمه‌کوانتومی را می‌توان در حالت کلی به صورت ترکیبی از رمزنگاری کوانتومی و کلاسیک در نظر گرفت که در بستر سیستم‌های فیزیکی با مبانی مکانیک کوانتومی پیاده‌سازی می‌شود [۱۴].

این مقاله در تاریخ ۱۱ دی ماه ۱۳۹۸ دریافت و در تاریخ ۱۱ شهریور ماه ۱۳۹۹ بازنگری شد.

زینب رشیدی، کارشناس ارشد، گروه برق، دانشگاه بین‌المللی امام رضا (ع)، مشهد، ایران، (email: Zeinab.rashidi@imamreza.ac.ir).

منیره هوشمند، دانشیار، گروه برق، دانشگاه بین‌المللی امام رضا (ع)، مشهد، ایران، (email: m.hooshmand@imamreza.ac.ir).

1. Cryptography
2. Quantum Cryptography
3. Semi-Quantum
4. Quantum Teleportation

در این مقاله یک پروتکل مخابره امن نیمه‌کوانتومی کنترل‌شده با استفاده از حالت اولیه سه‌ذره‌ای ارائه می‌گردد و امنیت آن مورد بررسی قرار می‌گیرد. در این پروتکل، کنترل‌کننده حالت اولیه سه‌ذره‌ای را تولید می‌کند. ذره اول از کیوبیت‌ها را برای خود نگه می‌دارد و یک ذره را به فرستنده و ذره دیگر را به گیرنده ارسال می‌کند تا آنها بتوانند پیام محرمانه خود را به یکدیگر، ارسال و نیز امنیت کانال را بررسی کنند. در این طرح اطلاعات به سادگی و بدون انجام عملیات پیچیده‌ای مخابره می‌شوند.

این مقاله بدین صورت سازماندهی شده است: در ابتدا مفاهیم اولیه محاسبات کوانتومی بیان می‌گردد. سپس در بخش پژوهش‌های پیشین، پروتکل‌های مخابره مستقیم امن نیمه‌کوانتومی بدون حضور و در حضور کنترل‌کننده معرفی می‌شوند. پس از آن مراحل پروتکل پیشنهادی را شرح می‌دهیم. در بخش امنیت، پروتکل پیشنهادی تحلیل شده و سپس با محاسبه بازدهی، طرح پیشنهادی با پروتکل مشابه پیشین مقایسه می‌گردد و در انتها نتیجه‌گیری ارائه می‌شود.

۳- مفاهیم اولیه محاسبات کوانتومی

برای این که وارد دنیای محاسبات کوانتومی شویم، نیازمند یک سری اصول اساسی و مفاهیم اولیه هستیم. حالات کوانتومی بر حسب بردارهایی توصیف می‌شوند که با نماد ket نمایش داده می‌شود. حالت ket با نماد $|\ \rangle$ نمایش داده می‌شود و ترانهاده مزدوج[1] آن Bra با نماد $\langle\ |$ نمایش داده می‌شود. واحد اطلاعات در محاسبات کوانتومی، به نام بیت کوانتومی یا کیوبیت[2] نام‌گذاری شده است. هر کیوبیت با یک بردار یکه در فضای هیلبرت دوبعدی توصیف می‌شود. بردارهای پایه این فضا به صورت (۱) تعریف می‌شود

$$|۱\rangle=\begin{pmatrix}۰\\۱\end{pmatrix}\quad,\quad |۰\rangle=\begin{pmatrix}۱\\۰\end{pmatrix} \tag{۱}$$

از پایه‌های معروف دیگر محاسبات کوانتومی پایه X است که به صورت (۲) تعریف می‌شود

$$|+\rangle=\frac{۱}{\sqrt{۲}}(|۰\rangle+|۱\rangle)$$
$$|-\rangle=\frac{۱}{\sqrt{۲}}(|۰\rangle-|۱\rangle) \tag{۲}$$

کیوبیت‌ها می‌توانند در برهم‌نهی[3] $|۰\rangle$ از $|۱\rangle$ و همانند $\alpha|۰\rangle+\beta|۱\rangle$ قرار بگیرند. همچنین α و β اعداد مختلط هستند به گونه‌ای که $|\alpha|^۲+|\beta|^۲=۱$ برقرار باشد.

خاصیت بسیار شگفت‌انگیز در مکانیک کوانتومی خاصیت درهم‌تنیدگی[4] است که تفاوت اساسی بین فیزیک کلاسیک و کوانتومی را تعیین و مشخص می‌کند. کیوبیت‌های تشکیل‌دهنده یک حالت درهم‌تنیده به گونه‌ای با هم ترکیب شده‌اند که حالت کوانتومی یک جزء تشکیل‌دهنده آن را نمی‌توان مستقل از حالت سایر اجزای تشکیل‌دهنده آن توصیف کرد، حتی اگر ذرات به صورت فیزیکی از هم دور باشند. برای مثال می‌توان به جفت‌های EPR یا حالات Bell با بیشینه درهم‌تنیدگی در فضای دوکیوبیتی اشاره کرد که به صورت (۳) تعریف می‌شوند

$$\beta_{۰۰}=\frac{۱}{\sqrt{۲}}(|۰۰\rangle+|۱۱\rangle)$$
$$\beta_{۱۱}=\frac{۱}{\sqrt{۲}}(|۰۱\rangle-|۱۰\rangle) \tag{۳}$$

۴- مخابره مستقیم امن نیمه‌کوانتومی

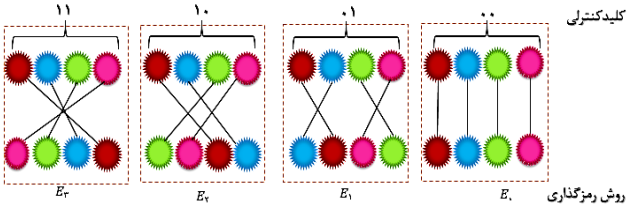
فرایند مخابره مستقیم امن نیمه‌کوانتومی یا به اختصار SQSDC[5]، شاخه‌ای مهم از مخابرات امن نیمه‌کوانتومی بوده که توسط آن، پیام‌های محرمانه به طور مستقیم انتقال می‌یابند. در مخابره مستقیم امن نیازی به اشتراک‌گذاری کلید میان دو کاربر مجاز و قانونی (آلیس و باب) نیست. در ارتباط مستقیم امن نیمه‌کوانتومی لازم است که امنیت کانال پس از ارسال بررسی شود تا در صورت تشخیص شنودگر مخابره قطع گردد.

۵- پژوهش‌های پیشین پروتکل‌های مستقیم امن نیمه‌کوانتومی

در [۱۵]، نویسندگان یک پروتکل مخابره مستقیم امن نیمه‌کوانتومی سه‌مرحله‌ای SQSDC را بر اساس منابع تک‌فوتون ارائه داده‌اند که در آن فرستنده، آلیس کلاسیکی است. پروتکل SQSDC پیشنهادشده دارای دو مزیت است. فرستنده تنها نیازمند توانایی‌های کلاسیکی است و همچنین در بررسی اختلال ایو پس از انتقال کوانتومی، هیچ اطلاعات کلاسیک اضافی مورد نیاز نیست. دانشمندان در [۱۶] با استفاده از m-qubit، پروتکلی پیشنهاد کرده‌اند که ارتباطات کوانتومی را کنترل می‌کند و تنها با استفاده از حالت Bell و جایگزینی ذرات امکان‌پذیر است. در [۱۷] پروتکل‌های ارتباط مستقیم نیمه‌کوانتومی ASQD[6]، بدون استفاده از کانال کلاسیک ارائه شده است. در طرح‌های پیشنهادی با اشتراک‌گذاری یک کلید محرمانه قبل از شروع مخابره بین دو کاربر، فرستنده با دستگاه‌های کوانتومی پیشرفته قادر به انتقال پیام محرمانه بدون هیچ گونه نشت اطلاعات به گیرنده‌ای است که تنها قادر به انجام عملیات کلاسیک است. در [۱۸] یک پروتکل توافق کلید بین دو طرف کلاسیکی و کوانتومی با نام CDSSQC ارائه گردیده که در آن هر دو طرف به یک اندازه در تعیین کلید نهایی نقش دارند که دو طرح برای آن پیشنهاد شده است. در طرح‌های پیشنهادی فقط آلیس کلاسیک در نظر گرفته می‌شود، در حالی که باب و چارلی کوانتومی هستند و کاربران تنها با اجازه کنترل‌کننده قادر به بازخوانی پیام محرمانه خواهند بود. این دو طرح مخابره مستقیم امن کنترل‌شده، امنیت بی‌قید و شرط را برای یک خریدار کلاسیک تأمین می‌کنند و در طراحی طرح‌های تجارت الکترونیک نیمه‌کوانتومی مفید می‌باشند. امنیت طرح‌های پیشنهادی برای حمله‌های احتمالی بررسی شده است. میزان بازدهی طرح‌های پیشنهادی ۴/۳۵ و ۵/۵۶ درصد محاسبه شده است. نویسندگان در [۱۹] به بررسی ارتباط مستقیم امن بین فرستنده آلیس کلاسیک و گیرنده باب با قابلیت کوانتومی محدود پرداخته‌اند. قبلاً چندین پروتکل برای SQDC ارتباط مستقیم کوانتومی ارائه شده است.

اخیراً Zou و همکارانش در [۲۰] پیشنهاد یک پروتکل ارتباط مستقیم سه‌مرحله‌ای نیمه‌کوانتومی را دادند که در آن یک شرکت‌کننده، کلاسیک بوده و قدرت کوانتومی ندارد یک پیام مخفی را به یک شرکت‌کننده کوانتومی ارسال می‌کند. در [۲۱] به تازگی ایده طراحی نیمه‌کوانتومی

1. Transpose Conjugate
2. Qubit
3. Superposition
4. Entanglement
5. Semi Quantum Secure Direct Communication
6. Authenticated Semi-Quantum Direct Communication Protocols



شکل ۱: یک مثال خاص از CORE با جفت EPR [۲۴].

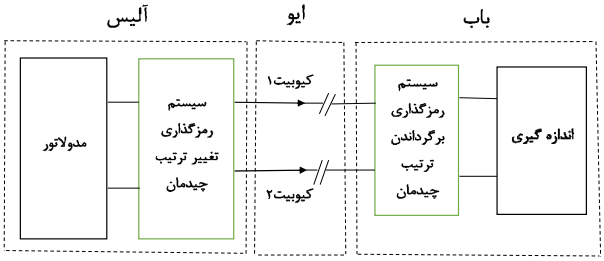
استفاده قرار گرفته است. در [۲۲] پروتکل توزیع کلید نیمه‌کوانتومی با یک کلید مخفی بین دو کاربر، امنیت را برقرار می‌کند که در مقایسه با پروتکل‌های تماماً کوانتومی به منابع کمتری نیاز دارد. در [۲۳] تعدادی از کیوبیت‌های اولیه تولیدشده برای بررسی امنیت کانال ارسالی استفاده می‌شوند. میزان بازدهی طرح پیشنهادی ۵۰/۰ درصد محاسبه شده است.

۶- روش به هم ریختن امنیت در توزیع کلید کوانتومی

امنیت توزیع کلید[1] مهم‌ترین بخش در ارتباطات امن است. توزیع کلید کوانتومی یک رویکرد بهره‌برداری از اصول مکانیک کوانتومی می‌باشد که ارتباطات امن را برای انتقال کلید فراهم می‌کند. از زمان پروتکل BB۸۴، توزیع کلید کوانتومی توجه زیادی از دانشمندان را به خود متمرکز نموده و مطالعات تجربی درباره توزیع کلید کوانتومی در دو دهه گذشته بسیار سریع رشد کرده است. امنیت توزیع کلید کوانتومی مبتنی بر تفاوت اساسی، بین اطلاعات کلاسیک و کوانتومی است. اطلاعات کلاسیک قابلیت کپی‌شدن را دارد اما اطلاعات کوانتومی خاصیت کپی‌شدن را ندارد. در حالات کوانتومی ایو تنها یک فرصت برای انتخاب دستگاه به صورت تصادفی دارد و با اندازه‌گیری مناسب می‌توان از دستبرد در امنیت پروتکل‌های توزیع کلید کوانتومی جلوگیری نمود. به عنوان مثال در BB۸۴ و پروتکل‌های مشابه آن خاصیت غیر قابل کلاسیک سیستم‌های کوانتومی مانند پیوندها، غیر مستقیم و فقط مربوط به سیستم کوانتومی است. اینجا یک حالت کوانتومی به دو بخش تقسیم می‌شود، به عنوان نمونه دو بخش شکل ۱ بسته موج فوتون یا دو ذره همبسته می‌باشند که ما آنها را QIC یا کانال‌های اطلاعات کوانتومی می‌نامیم. در پروتکل توزیع کلید کوانتومی مبتنی بر غیر قابل انطباق بودن حالت کوانتومی متعامد استفاده می‌شود. امنیت در هر دو مرحله تأمین می‌شود. این پروتکل‌ها در شکل ۲ نشان داده شده است. آلیس و باب در موقعیت‌های امن قرار دارند و خطوط انتقال، ناامن هستند. آلیس زوج EPR را به صورت تصادفی در یکی از حالت‌ها، تولید و سپس کیوبیت‌ها را در دو مسیر مختلف به باب ارسال می‌کند. در کانال پایین، اطلاعات کوانتومی با تأخیر و در کانال پایین بدون تأخیر ارسال می‌شود.

در بخش باب (بخش بالایی ۱ که تأخیر بخش پایین را ندارد)، دو بخش از کانال‌های اطلاعات کوانتومی، به طور هم‌زمان به دست باب می‌رسد و اندازه‌گیری می‌شوند. این پروتکل‌ها کامل بوده و از حالت‌های متعامد استفاده می‌کنند. پروتکل Koashi-Imoto از یک اینترفرم[2] نامتقارن استفاده می‌کند و زمان تصادفی و تأخیر زمانی می‌تواند کاهش یابد.

ایو پس از تأخیر زمان t'، شروع به دریافت متناظر قسمت‌های بالا می‌کند که ترکیب بخش‌هایی از کانال‌های اطلاعات کوانتومی را نگه می‌دارد. سپس او اندازه‌گیری جمعی را می‌تواند انجام دهد و کلید درست را



شکل ۲: نمایش تصویری از تغییر ترتیب چیدمان در یک نوع سیستم توزیع کلید کوانتومی [۲۴].

به طور کامل بازخوانی کند. پس از آن ایو در کلیدهای مخفی خطاها را ایجاد نموده و فقط در زمان تأخیر می‌تواند پیام‌های صحیح را به باب ارسال کند. پس از آن آلیس و باب تنها تغییر در رشته کلید باب نسبت به آلیس را می‌توانند متوجه شوند و مجدداً ایو از مزیت اختلال در کانال پر سر و صدا می‌تواند استفاده کند و به تدریج این تغییر مکان را شکل بدهد. ایو می‌تواند اگر زمان تأخیر طولانی نباشد، به سرعت نسبت به آن دست یابد. در این مرحله، آلیس ترتیب ذرات هم‌بسته را مرتب و آنها را به باب ارسال می‌کند و باب سپس ذرات را بازیابی و هم‌بستگی صحیح را بهبود می‌بخشد و اندازه‌گیری درست را انجام می‌دهد. این کار به صورت کنترل‌شده تکرار می‌شود. در جایی که آلیس و باب همگام‌سازی می‌کنند، استفاده از یک کلید کنترل کوتاه به عنوان اصلاح طرح BB۸۴ استفاده شده است. برای ارائه ایده ما از جفت EPR به عنوان کانال‌های اطلاعات کوانتومی استفاده می‌کنیم. یک جفت EPR می‌تواند در یکی از چهار حالت Bell در (۴) باشد

$$
\begin{aligned}
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)\\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)\\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)\\
|\phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)
\end{aligned}
\qquad (۴)
$$

شاخص A و B نشان‌دهنده دو فوتون هم‌بسته است. هر جفت آنها به ترتیب می‌توانند ۰۰، ۰۱، ۱۰ و ۱۱ را مدل کنند. همان طور که در شکل ۲ نشان داده است، روش CORE از دو کانال استفاده می‌کند. آلیس از یک مدولاتور برای هدایت جفت EPR خود به طور تصادفی استفاده می‌کند که چهار حالت Bell پایه است و سپس آنها را با فواصل زمانی برابر به باب ارسال می‌کند. قبل از این مرحله جفت EPR وارد خطوط انتقال ناامن می‌شود. کیوبیت‌های دریافتی در دست باب می‌مانند تا زمانی که اثر برگشت‌پذیر توسط آلیس اندازه‌گیری شوند. شکل ۱ ایده اصلی CORE را نشان می‌دهد. این قسمت‌های کانال اطلاعات کوانتومی بخش بالا با توجه به زمان‌بندی مرتب شده‌اند. مرتب‌سازی کلید کنترل برای تنظیم مجدد استفاده می‌شود، به طور مثال خاص در اینجا چهار گزینه عملیات CORE وجود دارد و CORE برای هر چهار جفت EPR انجام می‌شود. اگر مقدار کلید کنترل ۰۰ باشد، عملیات E۰ اعمال می‌شود و در غیر این صورت جفت‌های EPR تغییر نمی‌کند و همان طور که در شکل ۱ نشان داده شده است اجرا می‌شود.

1. Key Distribution
2. Interform

جدول ۱: رمزگذاری کیوبیت‌های دست آلیس.

حاصل اندازه‌گیری ذرات دنباله H	کیوبیت دریافتی از آلیس	بیت پیام محرمانه آلیس
۰	$\|۰\rangle$	۰
۰	$\|۱\rangle$	۱
۱	$\|۰\rangle$	۱
۱	$\|۱\rangle$	۰

۷- پروتکل پیشنهادی

آلیس n حالت را به صورت (۵) تولید می‌کند و برای امنیت کانال ارتباطی قبل از ارسال، دنباله‌ها را به صورت تصادفی به هم می‌ریزد و دو دنباله از ذرات اول، دوم و سوم تشکیل می‌دهد. به این صورت که دنباله H شامل ذره اول است و این دنباله را برای خودش نگه می‌دارد و دنباله T شامل ذرات دوم و سوم است که این دنباله را برای باب ارسال می‌کند

$$|\phi_۱\rangle = |۰\rangle(\frac{|۰۰\rangle+|۱۱\rangle}{\sqrt{۲}}).|۰\rangle = \frac{|۰۰\rangle-|۱۱\rangle}{\sqrt{۲}}$$
$$|\phi_۲\rangle = |۱\rangle(\frac{|۰۱\rangle+|۱۰\rangle}{\sqrt{۲}}).|۱\rangle = \frac{|۰۱\rangle-|۱۰\rangle}{\sqrt{۲}} \quad (۵)$$

۷-۱ مخابره مستقیم امن کوانتومی

پس از دریافت دنباله به وسیله آلیس، ترتیب درست کیوبیت‌ها را چارلی به آلیس اعلام می‌کند. آن گاه آلیس دنباله اصلی را بازیابی می‌کند و پیام محرمانه خود را روی دنباله دریافتی رمز می‌کند. در ابتدا آلیس دو ذره کنار یکدیگر را یک گروه در نظر می‌گیرد و آنها را دسته‌بندی می‌کند. کیوبیت‌های هر دسته را در پایه‌های محاسباتی اندازه‌گیری و حالت آنها را ثبت می‌کند. سپس آلیس بر اساس جدول ۱ کیوبیت‌ها را رمز می‌کند. در جدول ۲ به عنوان مثال وقتی حالت پس از اندازه‌گیری کیوبیت‌های دست آلیس هر دو یکسان باشد، به طوری که هر دو ۰۰ یا ۱۱ باشند و آلیس نیز قصد فرستادن بیت ۱ را به باب داشته باشد، باید ۱ را برای باب ارسال نماید. برای برقراری امنیت دنباله رمزشده، آلیس تعدادی فوتون منفرد در پایه z تولید می‌کند، آنها را به صورت تصادفی به عنوان فوتون دام قرار می‌دهد و پس از آن به باب ارسال می‌کند.

۷-۲ مرحله امنیت کانال کوانتومی

در این مرحله دنباله به دست باب می‌رسد و به محض دریافت دنباله، جایگاه و حالت فوتون‌های دام را آلیس به باب اعلام می‌کند تا امنیت کانال را با اندازه‌گیری فوتون‌های دام در پایه محاسباتی بررسی کند. سپس بعد از تأیید امنیت باب، فوتون‌های دام را دور می‌ریزد، سایر کیوبیت‌ها را اندازه‌گیری می‌کند و دنباله رمزشده را مجدداً بازیابی می‌کند. پس از آن باب اگر از ذرات دنباله H اطلاع نداشته باشد، نمی‌تواند پیام باب را متوجه شود. سپس چارلی باید ذرات دنباله H را به باب ارسال کند.

۷-۳ مرحله بهره‌برداری از پیام محرمانه

پس از بررسی امنیت کانال، دنباله H از چارلی به باب ارسال می‌شود. باب ذرات دنباله H را در پایه محاسباتی اندازه‌گیری می‌کند و طبق جدول ۳ با توجه به نتیجه اندازه‌گیری، کیوبیت دریافتی از آلیس را XOR می‌کند تا پیام ارسالی آلیس استخراج شود. در این جدول، به عنوان مثال اگر کیوبیت دریافتی از آلیس $|۰\rangle$ باشد و کیوبیت ارسالی چارلی از حاصل اندازه‌گیری $|۱\rangle$ باشد، چارلی به این نتیجه می‌رسد که آلیس قصد فرستادن بیت ۱ را برای او داشته است.

۷-۴ تحلیل امنیت کلی در کانال کوانتومی

تحلیل امنیت و محاسبه بازدهی، پارامترهای مهم در ارزیابی پروتکل‌های ارتباط مستقیم امن هستند که در ادامه به بررسی آنها خواهیم پرداخت.

۷-۴-۱ تحلیل امنیت در کانال کوانتومی بدون اجازه کنترل‌کننده

یکی از نگرانی‌های مهم در طراحی و تحلیل پروتکل‌های ارتباط مستقیم امن کوانتومی کنترل‌شده این است که گیرنده به هیچ بخشی از پیام محرمانه بدون اجازه کنترل‌کننده دسترسی نداشته باشد. در مرحله رمزگشایی پروتکل پیشنهادی چارلی کنترل‌کننده است برای بازیابی و خواندن پیام آلیس حتماً باید دنباله H را برای باب ارسال کند. به علت قابل محاسبه‌نبودن حاصل XOR، گیرنده فقط با اجازه کنترل‌کننده اطلاعات محرمانه را دریافت می‌کند. برای واضح‌ترشدن مثالی را مطرح کرده‌ایم. اگر اطلاعات ارسالی آلیس ۰ یا ۱ باشد. باب طبق (۶) بدون اطلاعات چارلی نمی‌تواند پیام را بازخوانی کند. در اینجا x بیانگر بیت محرمانه ارسالی آلیس و y اطلاعات کلاسیک چارلی است

$$\text{prob}(x=\frac{۰}{y}) = \text{prob}(x=\frac{۱}{y}) = \frac{۱}{۲} \quad (۶)$$

۷-۴-۲ تحلیل امنیت با فرض آشکارشدن تمام اطلاعات کلاسیک

تحلیل امنیت دیگری که باید به آن توجه کرد این است که پروتکل ارائه‌شده با فرض آشکارشدن تمام اطلاعات کلاسیک امن باشد. به عبارتی دیگر اگر استراق سمع کننده، کنترل کانال کوانتومی را در دست داشته باشد و تمامی اطلاعات کلاسیک آشکار شود پروتکل همچنان امن باشد و استراق سمع کننده به هیچ بخشی از پیام محرمانه دست نیابد.

۷-۴-۳ تحلیل امنیت حمله‌های کوانتومی در برابر استراق سمع کننده

برای بررسی امنیت پروتکل پیشنهادی، سه نوع حمله‌ای که استراق سمع کننده ممکن است در مرحله تشکیل کانال کوانتومی آنها را به کار گیرد با جزئیات بررسی می‌کنیم. در حملات اسب تروجان برای جلوگیری از انواع حملات، اگر تمامی کاربران دستگاه شکاف فوتون و دستگاه فیلتر طول موج را اتخاذ کنند کافی است.

- حمله مرد میانی

در این مرحله به بررسی امنیت کانال ارتباطی بین آلیس به باب و چارلی به باب می‌پردازیم. چارلی از ترتیب درست کیوبیت‌ها اطلاع دارد و آنها را به هم ریخته است. کیوبیت‌های ارسالی چارلی به آلیس درهم‌تنیده هستند. به علت درهم‌تنیدگی جایگاه ذرات و درست‌نبودن ترتیب کیوبیت‌ها، اگر ایو به دنباله ارسالی آلیس به باب دست پیدا کند و هر تغییری در آن بدهد شناسایی می‌شود. پس از آن از فوتون‌های دام استفاده کرده‌ایم و ایو از جایگاه فوتون‌های رمزشده و دام اطلاعی ندارد و به علت اطلاع‌نداشتن از حالت اولیه و دنباله H نمی‌تواند پیام محرمانه را بازخوانی کند. ذرات درهم‌تنیده به صورت تصادفی در دنباله پخش شده‌اند و فقط چارلی از جایگاه کیوبیت‌ها اطلاع دارد. برای ارسال دنباله H به او از حالت Bell به عنوان فوتون دام استفاده شده است. ایو از جایگاه این ذرات اطلاعی ندارد و نمی‌تواند فوتون‌های کنترلی را از دام تشخیص دهد.

جدول ۲: پیشینه مخابره مستقیم نیمه‌کوانتومی.

شماره مرجع	سال	ژورنال	کنترلی	مراحل پروتکل‌ها	توضیحات
[۱۵]	۲۰۱۴	Science China Physics, Mechanics & Astronomy	*	پروتکل‌های ارتباط مستقیم نیمه‌کوانتومی ASQDC	دو پروتکل ASQDC مبتنی بر تصادف و اندازه‌گیری و ارسال مجدد
[۱۶]	۲۰۱۵	Quantum Information Processing	*	ارتباطات کوانتومی کنترل‌شده m-qubit	کنترل ارتباطات کوانتومی با استفاده از حالت Bell و جایگزینی ذرات
[۱۷]	۲۰۱۶	Quantum Information Processing	*	پروتکل مخابره مستقیم امن نیمه‌کوانتومی سه‌مرحله‌ای SQSDC	بررسی اختلال ایو پس از انتقال کوانتومی
[۱۸]	۲۰۱۷	Quantum Information Processing	*	پروتکل اول مخابره امن نیمه‌کوانتومی کنترل‌شده پنج‌مرحله‌ای	گفتگوی نیمه‌کوانتومی با امنیت بدون قید و شرط برای یک کاربر کلاسیک و یک کاربر کوانتومی
[۱۸]	۲۰۱۷	Quantum Information Processing	*	پروتکل دوم مخابره امن نیمه‌کوانتومی کنترل‌شده بر اساس سوئیچ رمزنگاری پنج‌مرحله‌ای	بررسی حالات کوانتومی برای جلوگیری از استراق سمع کننده
[۱۹]	۲۰۱۷	Globecom Workshops IEEE	*	پروتکل SQDC بدون کلید	ثابت نگه داشتن زمان نگهداری بیت‌های کوانتومی
[۲۰]	۲۰۱۸	Quantum Information Processing	*	دو حمله C-NOT برای دریافت پیام مخفی	فرایند انتقال اطلاعات کلاسیک برای رمزگذاری
[۲۱]	۲۰۱۸	International Journal of Theoretical Physics	*	پردازش اطلاعات کوانتومی با حداقل منابع ممکن	حفظ طرح رمزنگاری کلاسیک با استفاده از کوانتوم
[۲۲]	۲۰۱۸	Quantum Information Processing	*	یک حالت امنیتی بی‌قید و شرط برای پروتکل تک‌حالته SQKD	نرخ خطای کم
[۲۳]	۲۰۲۰	International Journal of Theoretical Physics	*	با هدف حداکثرکردن تأثیرگذاری ارتباطات کوانتومی	پروتکل می‌تواند به راحتی با وضعیت ارتباطات سه‌جانبه یا حتی ارتباطات طرف N ، تعمیم داد و کاملاً مستحکم هستند.

جدول ۳: رمزگشایی توسط باب.

مقدار اندازه‌گیری شده	بیت پیام محرمانه آلیس	کیوبیت ارسالی به باب
۰۰ یا ۱۱	۰	$\|0\rangle$
۰۰ یا ۱۱	۱	$\|1\rangle$
۱۰ یا ۰۱	۰	$\|1\rangle$
۱۰ یا ۰۱	۱	$\|0\rangle$

حال احتمال دسترسی ایو به هر بیت از پیام ۱/۲ است و احتمال شناسایی ایو $1-(1/2)^n$ است. تا زمانی که n به اندازه کافی بزرگ باشد احتمال تشخیص حدود ۱ است.

- حمله اندازه‌گیری و ارسال دوباره

در این مرحله اگر در دنباله ارسالی چارلی به آلیس، ایو نفوذ کند و ذرات آن دنباله را اندازه‌گیری کند، به علت آن که ذرات درهم‌تنیده هستند و ایو از آنها اطلاع ندارد، با هر اندازه‌گیری روی این ذرات، ذره دیگر تغییر می‌کند. درهم‌تنیدگی بین ذرات از بین می‌رود، سپس چارلی جایگاه اصلی کیوبیت‌ها را به آلیس اعلام می‌کند و ایو شناسایی می‌شود. سپس ایو در دنباله آلیس به باب نفوذ می‌کند. به دلیل اطلاع‌نداشتن از جایگاه ذرات رمزشده و فوتون‌های دام، احتمال این که با اندازه‌گیری ذرات به هر بیت پیام دسترسی پیدا کند ۱/۲ است. ایو برای بازخوانی پیام باید از دنباله H اطلاع داشته باشد و چون اطلاع ندارد نمی‌تواند آن را بازخوانی کند.

- حمله جعل هویت

در تمام مراحل پروتکل پیشنهادی از فوتون دام استفاده شده است و کیوبیت‌های اصلی به صورت تصادفی در دنباله قرار داده می‌شود. در این مرحله ایو نمی‌تواند هویت چارلی و آلیس را جعل کند. ایو از جایگاه ذرات اطلاعی ندارد، بنابراین اگر دنباله جدیدی بسازد در صورتی که یکی از دنباله‌ها را قطع کند، به علت اطلاع‌نداشتن شناسایی می‌شود. حال اگر شناسایی نشود و هویت چارلی و آلیس را جعل کند، برای دست‌یابی به هر بیت پیام می‌تواند با احتمال ۱/۲ به آن پیام برسد و احتمال شناسایی خودش $1-(1/2)^n$ می‌باشد. حال اگر n بزرگ باشد احتمال شناسایی ایو حدود ۱ است.

- حمله C-NOT

در مرحله کنترل امنیت کوانتومی، حمله استراق سمع کننده تشخیص داده می‌شود و در پایه اندازه‌گیری حضور ایو با احتمال ۱/۲ آشکار می‌شود. در این حمله، استراق سمع کننده کیوبیتی که خود تولید می‌کند و کیوبیت باب یا چارلی را از گیت C-NOT عبور می‌دهد تا درهم‌تنیدگی بین این دو کیوبیت ایجاد کند تا بتواند با اندازه‌گیری روی کیوبیت تولیدی‌اش پیام محرمانه را بازیابی کند.

۸- محاسبه بازدهی پروتکل پیشنهادی

برای محاسبه بازدهی، اول آلیس n حالت سه‌ذره‌ای را تولید می‌کند که دو ذره آن جهت رمزگذاری پیام‌های محرمانه مورد استفاده قرار می‌گیرد. آلیس جهت ارسال امن دنباله به باب فقط ترتیب کیوبیت‌ها را به هم می‌ریزد. جهت اعلام ترتیب درست کیوبیت‌ها در این مرحله یک بیت کلاسیک تولید می‌شود و برای رمزگذاری از n فوتون جهت کدگذاری پیام‌های محرمانه استفاده می‌گردد. برای ارسال دنباله امن رمزگذاری شده به چارلی تعدادی فوتون دام تولید می‌شود که تعداد فوتون‌های دام تولیدشده باید حداکثر نصف تعداد فوتون‌های کدگذاری شده باشد. برای هر دو بیت کلاسیک (یک حالت کوانتومی و یک جایگاه در دنباله آن) یک فوتون دام در نظر می‌گیریم. سپس در مرحله کنترل امنیت H بیت کلاسیک تولید خواهد شد که در مرحله کدگشایی توسط چارلی به دنباله نیاز خواهد داشت. از این میان آلیس برای ارسال امن این دنباله به چارلی

جدول ۴: مقایسه طرح پیشنهادی با طرح‌های پیشین.

نام پروتکل	m_t	q_c	q_t	b_c	$\eta_1\%$	$\eta_2\%$
پروتکل اول [۱۸]	n	$4n$	$21n$	$2n$	۴	۴٫۳۵
پروتکل دوم [۱۸]	n	$3n$	$3n$	$2n$	۶	۵٫۵۶
پروتکل [۲۳]	$4n$	n	$4n$	$4n$	۲۲	۵۰٫۰
پروتکل پیشنهادی	n	$2n$	n	$2n$	۵۰	۶۶٫۶

نیاز به تولید فوتون دام دارد، به دلیل این که تعداد فوتون دنباله اصلی n کیوبیت است و در نتیجه $n/2$ فوتون تولید خواهد شد. برای هر فوتون دام جهت اعلام جایگاه آن یک بیت کلاسیک تولید می‌شود و در نتیجه تعداد کل بیت کلاسیک آشکارشده به هنگام رمزبرداری $2n$ و در این حالت تعداد کل کیوبیت‌های استفاده‌شده $9n$ است. در طی پروتکل نیز فوتون دام تولیدشده نیاز به کدگذاری n کیوبیت دارد. بازده پیشنهادشده پروتکل به صورت (۷) می‌باشد. در صورت استفاده از بیت کلاسیک برای رمزبرداری پیام b_c را می‌گذاریم و بازده به صورت (۸) می‌باشد

$$h_1 = \frac{m_t}{q_t} = \frac{n}{2n} = \frac{1}{2} = 50\% \quad (۷)$$

$$h_2 = \frac{m_t}{q_t + b_c} = \frac{2n}{n + 2n} = \frac{2}{3} = 66/6\% \quad (۸)$$

۹- مقایسه پروتکل پیشنهادی با پروتکل‌های پیشین

در این مرحله طرح پیشنهادی را با طرح مشابه پیشین مقایسه می‌کنیم. برای بررسی امنیت کانال یک‌طرفه، تحلیل با [۲۳] صورت گرفته که در مقایسه با مقالات سال‌های اخیر به خوبی به موضوع امنیت کانال‌های یک‌طرفه اشاره کرده است. بخشی از کیوبیت‌های اولیه در پروتکل‌های پیشنهادی پیشین تولید شده که برای بررسی امنیت کانال ارسالی مورد استفاده قرار می‌گیرد و پس از تحلیل امنیت کنار گذاشته می‌شوند، ولی در طرح پیشنهادی از همه این کیوبیت‌های تولیدشده جهت ارسال پیام استفاده خواهد شد. گیرنده چارلی طبق مراحل پروتکل پیشنهادی و مرحله رمزگشایی می‌تواند کلاسیکی باشد. در نتیجه پروتکل با یک کاربر کوانتومی و دو کاربر کلاسیک قابل پیاده‌سازی می‌باشد که از لحاظ هزینه مقرون به صرفه است. طبق جدول ۴ طرح پیشنهادی نسبت به طرح‌های پیشین بازدهی قابل توجهی داشته است.

۱۰- نتیجه‌گیری

در بررسی‌های صورت‌گرفته پژوهش از طرح پیشنهادی توضیح داده شده می‌توان نتیجه گرفت که همه کیوبیت‌های تولیدشده برای ارسال پیام استفاده می‌شوند. اما در پروتکل [۲۳] تعدادی از کیوبیت‌های اولیه تولیدشده برای بررسی امنیت کانال ارسالی استفاده می‌شوند و پس از بررسی امنیت دور ریخته می‌شوند. به علت کلاسیکی‌بودن گیرنده (چارلی)، پروتکل با دو کاربر کلاسیکی و یک کاربر کوانتومی قابل پیاده‌سازی است و هزینه پیاده‌سازی آن مقرون به صرفه است. یک پروتکل مخابره امن نیمه‌کوانتومی کنترل‌شده با استفاده از حالت اولیه سه‌ذره‌ای ارائه شده و امنیت آن مورد بررسی قرار گرفته است. لذا در این پروتکل کنترل‌کننده حالت اولیه سه‌ذره‌ای را تولید می‌کند که ذره اول از کیوبیت‌ها را برای خود نگه می‌دارد و یک ذره را به فرستنده و ذره دیگر را به گیرنده ارسال می‌کند تا آنها بتوانند پیام محرمانه خود را به یکدیگر، ارسال و همچنین امنیت کانال را بررسی کنند. در این طرح اطلاعات به سادگی و بدون انجام عملیات پیچیده‌ای مخابره می‌شوند. گیرنده برای کدگشایی پیام خود به ذره نزد کنترل‌کننده نیاز دارد. تا زمانی که کنترل‌کننده این دنباله را به گیرنده ارسال نکند، کنترل‌کننده قادر به بازخوانی پیام نیست. سپس نشان دادیم که این پروتکل در برابر استراق سمع کننده امن است. پروتکل پیشنهادی کاملاً مقرون به صرفه و با هزینه پایین قابل اجرا است، زیرا فقط کنترل‌کننده نیاز به تجهیزات کوانتومی دارد و دو کاربر دیگر می‌توانند کلاسیک باشند. همچنین بازدهی طرح پیشنهادی نسبت به طرح‌های پیشین افزایش یافته است. لذا فاکتور مهمی که برای تحلیل عملکرد پروتکل‌های ارتباط مستقیم امن کوانتومی به کار گرفته می‌شود، بازدهی می‌باشد.

مراجع

[1] M. Boyer, D. Kenigsberg, and T. Mor, "Quantum key distribution with classical Bob," in *Proc. IEEE 1st Int. Conf. on Quantum, Nano, and Micro Technologies, ICQNM'07,* pp. 10-10, Guadeloupe, French, 2-6 Jan. 2007.

[۲] م. هوشمند و ش. حسن‌پور، "ارتباط مستقیم امن کوانتومی کنترل‌شده با هدف افزایش بازدهی،" *مجموعه مقالات یازدهمین کنفرانس بین‌المللی انجمن رمز ایران*، ۶ صص.، تهران، ایران، ۱۲-۱۱ شهریور ۱۳۹۳.

[3] G. E. Moore, "Cramming more components onto integrated circuits," *Proceedings of the IEEE*, vol. 86, no. 1, pp. 82-85, Jan. 1998.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2001.

[5] T. P. Spiller, W. J. Munro, S. D. Barrett, and P. Kok, "An introduction to quantum information processing: applications and realizations," *Contemporary Physics*, vol. 46, no. 6, pp. 407-436, 2005.

[6] D. C. Marinescu and G. M. Marinescu, *Approaching Quantum Computing*, pp. 1-41, Pearson/Prentice Hall, 2005.

[7] M. Nakahara and T. Ohmi, Quantum Computing: From Linear Algebra to Physical Realizations, CRC Press, 2008.

[8] R. P. Feynman, "Simulating physics with computers," *International J. of Theoretical Physics*, vol. 21, no. 6/7, pp. 467-488, 1982.

[9] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. of the 28th Annual ACM Symp. on Theory of Computing, STOC'96,* pp. 212-219, Philadelphia, PA, USA, 22-24 May 1996.

[10] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. IEEE 35th Annual Symp. on Foundations of Computer Science,* pp. 124-134, Santa Fe, NM, USA, 20-22 Nov. 1994.

[11] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78-88, Jan. 1983.

[12] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," *Advances in Cryptology: Proceedings of CRYPTO '82,* pp. 267-275, Santa Barbara, CA, USA, 23-25 Aug 1982.

[13] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7-11, 2014.

[۱۴] م. هوشمند، م. خرم‌پناه و ر. ساروقی، "ارسال محرمانه اطلاعات به کمک کیوبیت‌های درهم‌تنیده،" *مجموعه مقالات نهمین کنفرانس بین‌المللی رمز ایران*، ۵ صص. تبریز، ایران، ۲۴-۲۳ شهریور ۱۳۹۱.

[15] X. Zou and D. Qiu, "Three-step semiquantum secure direct communication protocol," *Science China Physics, Mechanics & Astronomy*, vol. 57, no. 9, pp. 1696-1702, 2014.

[16] K. Thapliyal and A. Pathak, "Applications of quantum cryptographic switch: various tasks related to controlled quantum communication can be performed using bell states and permutation of particles," *Quantum Information Processing*, vol. 14, no. 7, pp. 2599-2616, 2015.

[17] Y. P. Luo and T. Hwang, "Authenticated semi-quantum direct communication protocols using bell states," *Quantum Information Processing*, vol. 15, no. 2, pp. 947-958, 2016.

[18] C. Shukla, K. Thapliyal, and A. Pathak, "Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue," *Quantum Information Processing*, vol. 16, no. 12, Article No.: 295, 2017.

[19] H. Lu, M. Barbeau, and A. Nayak, "Economic no-key semi-quantum direct communication protocol," in *Proc. IEEE Globecom Workshops, GC Wkshps'2017,* 7 pp., Singapore, Singapore, 4-8 Dec. 2017.

[20] J. Gu, P. H. Lin, and T. Hwang, "Double C-NOT attack and counterattack on 'three-step semi-quantum secure direct communication protocol'," *Quantum Information Processing*, vol. 17, no. 7, Article No.: 182, 8 pp., Jul. 2018.

[21] C. Xie, L. Li, H. Situ, and J. He, "Semi-quantum secure direct communication scheme based on bell states," *International J. of Theoretical Physics*, vol. 57, no. 6, pp. 1881-1887, 2018.

[22] W. Zhang, D. Qiu, and P. Mateus, "Security of a single-state semi-quantum key distribution protocol," *Quantum Information Processing*, vol. 17, no. 4, Article No.: 2050013, 21 pp., 2018.

[23] L. C. Xu, H. Y. Chen, N. R. Zhou, and L. H. Gong, "Multi-party semi-quantum secure direct communication protocol with cluster states," *International J. of Theoretical Physics*, vol. 49, no. 1, Article No.: 1950004, 10 Jan. 2020.

[24] F. G. Deng and G. L. Long, "Controlled order rearrangement encryption for quantum key distribution," *Physical Review A*, vol. 68, no. 4, Article No.: 042315, Oct. 2003.

زینب رشیدی تحصیلات خود را در رشته مهندسی برق الکترونیک در مقطع کارشناسی و در رشته مهندسی برق مخابرات در مقطع کارشناسی ارشد به ترتیب در دانشگاه ازاد نایین و دانشگاه بین المللی امام رضا به پایان رسانده است. زمینه های پژوهشی مورد علاقه ایشان عبارتند از: مخابرات کوانتومی و نیمه کوانتومی.

منیره هوشمند تحصیلات خود در رشته مهندس برق الکترونیک را در مقاطع کارشناسی، کارشناسی ارشد و دکترا در دانشگاه فردوسی مشهد به پایان رسانده است. وی هم اکنون دانشیار گروه برق دانشگاه بین المللی امام رضا (ع) میباشد. زمینه های پژوهشی مورد علاقه ایشان عبارتند از: مخابرات کوانتومی و نیمه کوانتومی، رمزنگاری کوانتومی و نیمه کوانتومی، سنتز کوانتومی و تصحیح خطای کوانتومی.