دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۲ (۱-۱۰)
https://monadi.isc.org.ir

ارائه‌شده در نوزدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه گیلان، ۹ و ۱۰ شهریور ۱۴۰۱

پروتکل چندکاربره گفت‌وگوی کوانتومی با قابلیت گسترش تعداد کاربران در زمان اجرا★

علی خزائی[۱،*]، حسین همائی[۱] و منیره هوشمند[۲]

[۱]دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران
[۲]گروه مهندسی برق، دانشگاه بین المللی امام رضا (ع)، مشهد، ایران

اطلاعات مقاله

کلمات کلیدی:
پروتکل‌های امنیتی
امنیت کوانتوم
گفت‌وگوی کوانتومی چند کاربره

dor: 20.1001.1.24763047.1401.11.2.1.0

نوع مقاله: پژوهشی

چکیده

گفت‌وگوی کوانتومی به نوعی از ارتباطات کوانتومی گفته می‌شود که در آن کاربران می‌توانند به صورت همزمان برای یکدیگر پیام ارسال کنند. اولین نمونه‌های پروتکل‌های گفت‌وگوی کوانتومی با مشکلات امنیتی نظیر نشت اطلاعات و آسیب‌پذیری‌هایی همچون دریافت و ارسال مجدد روبرو بودند. از این رو، پروتکل‌های متعددی ارائه شده که سعی در برطرف نمودن این نواقص دارند. با وجود این پیشرفت‌ها، گفت‌وگوهای کوانتومی همچنان با چالش‌هایی روبرو هستند. در حال حاضر، محدود بودن تعداد شرکت‌کنندگان و عدم امکان گسترش کاربران در زمان گفت‌وگو از جمله مهم‌ترین چالش‌های این نوع پروتکل‌ها محسوب می‌شود. در این پژوهش یک پروتکل گفت‌وگوی کوانتومی چندکاربره طراحی کرده‌ایم که چالش‌های فوق را برطرف نماید. پروتکل پیشنهادی حالت تعمیم یافته گفت‌وگوی کوانتومی است که در آن هر کاربر می‌تواند به صورت همزمان با کاربران دیگر ارتباط برقرار کند. تعداد کاربران شرکت‌کننده محدود نیست و به صورت پویا (یعنی بدون نیاز به راه‌اندازی مجدد پروتکل) نیز قابل تغییر است. بنابراین، در زمان اجرای پروتکل، یک کاربر می‌تواند گفت‌وگو را ترک کند و یا کاربری جدید می‌تواند به آن ملحق شود. ارتباط میان کاربران از طریق یک سرور نیمه‌صادق مرکزی برقرار می‌شود. بررسی‌های انجام شده نشان می‌دهد که پروتکل پیشنهادی نسبت به نشت اطلاعات مقاوم است. یعنی، هیچ کاربر غیرمجازی (حتی سرور مرکزی) نمی‌تواند به داده‌های خام مبادله شده میان افراد دسترسی پیدا کند.

© ۱۴۰۱ انجمن رمز ایران

۱ مقدمه

با ظهور کامپیوترها و الگوریتم‌های کوانتومی، روش‌های رمزنگاری نامتقارن کلاسیک که بر سختی حل یک مسئله ریاضی مانند فاکتورگیری بنا شده بودند با چالش جدی روبه‌رو شدند [۱-۳]. از سوی دیگر، رمزنگاری کوانتومی با تکیه بر قوانین فیزیک کوانتومی، امنیت بدون قید و شرط [۱] را فراهم می‌کند. به همین دلیل رمزنگاری کوانتومی یکی از موضوعات مورد توجه محققان در سال‌های اخیر بوده است [۴].

در حوزه مخابره کوانتومی، انواع مختلفی از پروتکل‌های کوانتومی معرفی شده‌اند که با تکیه بر اصول فیزیک کوانتوم سعی در افزایش امنیت ارتباطات دارند. از جمله مهم‌ترین دسته پروتکل‌هایی که در سال‌های اخیر

[1] unconditional security

★از کمیته علمی نوزدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: a.khazaei@modares.ac.ir (علی خزائی)، homaei@modares.ac.ir (حسین همائی)، m.hooshmand@imamreza.ac.ir (منیره هوشمند)
© ۱۴۰۱ تمامی حقوق متعلق به انجمن رمز ایران است.

مورد توجه محققان این حوزه قرار گرفته‌اند می‌توان به پروتکل‌های توزیع کلید کوانتومی [1] [۵–۸] و ارتباط مستقیم امن کوانتومی [2] [۷–۱۰] اشاره کرد. توزیع کلید کوانتومی، از قواعد فیزیک کوانتوم برای به اشتراک گذاشتن کلید متقارن بین دو کاربر استفاده می‌کند. سپس با استفاده از این کلید و الگوریتم‌های رمزنگاری کلاسیک، امنیت ارتباط را تضمین می‌کند. اما در ارتباط مستقیم امن کوانتومی، اطلاعات به صورت امن بر روی کیوبیت‌ها [3] کدگذاری شده و از طریق یک کانال امن کوانتومی منتقل می‌شوند و نیازی به اشتراک کلید اولیه وجود ندارد [۱۱].

مشکل نسخه‌های اولیه پروتکل‌های ارتباط مستقیم امن کوانتومی، یک طرفه بودن این پروتکل‌ها بود. به این معنی که در هر لحظه فقط یک کاربر قادر به ارسال اطلاعات به کاربر دیگر بود. در سال ۲۰۰۴، برای اولین بار، Nguyen یک پروتکل گفت‌وگوی کوانتومی (QD [4]) مبتنی بر ارتباط مستقیم امن کوانتومی ارائه داد که در آن، دو کاربر به صورت همزمان قادر به ارسال اطلاعات بودند [۱۲]. از آن پس پروتکل‌های گفت‌وگوی کوانتومی متعددی ارائه شده‌اند. برخی از این پروتکل‌ها از طریق ذرات کوانتومی منفرد [۱۳–۱۵] و برخی بر مبنای درهم‌تنیدگی [5] [۱۶، ۱۷] اطلاعات را ارسال می‌کنند.

باید توجه داشت که صرف استفاده از فیزیک کوانتوم در طراحی یک پروتکل به این معنا نیست که آن پروتکل خالی از نقص خواهد بود. فرضیات اولیه‌ای نظیر ایده‌آل بودن کانال‌های ارتباطی و همچنین مورد اعتماد بودن دستگاه‌های کوانتومی باعث به وجود آمدن مشکلات امنیتی در این پروتکل‌ها شده است. در سال‌های اخیر، پژوهشگران تلاش کرده‌اند تا انواع نقص‌ها و ضعف‌هایی که ممکن است در این پروتکل‌ها وجود داشته باشند را شناسایی و برطرف نمایند. به عنوان مثال، در [۱۸] مشخص شد که [۱۲] دارای آسیب‌پذیری دریافت و ارسال مجدد [6] است و راه‌کاری برای اصلاح پروتکل مطرح گردید. اما این پروتکل نیز خالی از نقص نبود. در [۱۹] پروتکل‌های [۱۲، ۱۸] بررسی شدند و نشان داده شد که نفوذگر با دانستن حالت اولیه و اعلام نهایی در کانال عمومی، می‌تواند به بخشی از اطلاعات دسترسی پیدا کند. در واقع، در این پروتکل‌ها امکان نشت اطلاعات وجود داشت.

در [۱۶] با استفاده از یک پروتکل ارتباط مستقیم امن نیمه کوانتومی (SQSDC [7]) یک پروتکل گفت‌وگوی نیمه کوانتومی (SQD [8]) چند کاربره با استفاده از حالت اولیه خوشه‌ای چهار ذره، طراحی شده است که در آن دو فرستنده کلاسیک می‌توانند به صورت همزمان پیام را برای گیرنده کوانتومی ارسال نمایند. SQD به دسته‌ای از پروتکل‌های گفت‌وگوی کوانتومی گفته می‌شود که در آن یک کاربر یا سرور مرکزی کوانتومی وجود دارد و سایر کاربران کلاسیک هستند.

در [۲۰] یک پروتکل QD پیاده‌سازی شده است که پیام‌ها را بر روی حالت‌های در هم تنیده رمز می‌کند. این پروتکل در برابر حمله اسب تروا [9] و نویزهای جمعی مقاوم است.

در سال ۲۰۱۷ اولین پروتکل چند کاربره [۲۱] با استفاده از کیودیت [10] طراحی شد. در این پروتکل، n کاربر از طریق یک بخش قابل اعتماد [11] با هم ارتباط برقرار می‌کنند. کیودیت به حالت تعمیم یافته یک کیوبیت با d بُعد اشاره دارد. از مزایای استفاده از کیودیت در ارتباطات، می‌توان به پایداری بالاتر در برابر نویز و نیز انتقال حجم اطلاعات بیشتر در قالب یک ذره اشاره کرد؛ با این وجود، باید توجه داشت که پیچیدگی پیاده‌سازی کیودیت بیشتر از کیوبیت است [۲۲].

ما در این مقاله قصد داریم یک پروتکل گفت‌وگوی چند کاربره با استفاده از کیوبیت معرفی کنیم که دو ویژگی زیر را برآورده می‌سازد:

(۱) عدم محدودیت تعداد کاربران در ارتباط و همچنین عدم محدودیت در تعداد ارتباطات کاربران با یکدیگر و
(۲) قابلیت گسترش تعداد کاربران در زمان اجرای پروتکل، بدون نیاز به اجرای دوباره پروتکل و قطع اتصال سایر کاربران.

بر اساس ویژگی اول، هر تعداد کاربر دلخواهی که قابلیت برقراری ارتباط کوانتومی را داشته باشند، می‌توانند از طریق سرور مرکزی یک ارتباط اولیه دوطرفه را شکل داده و با یکدیگر گفت‌وگو نمایند. بر مبنای ویژگی دوم، در هر زمانی کاربران جدیدی می‌توانند به پروتکل اضافه شوند یا کاربران قبلی قادرند گفت‌وگو را ترک کنند، بدون آنکه خللی در ارتباطات سایر کاربران ایجاد شود.

در ادامه این مقاله، ابتدا مدل پیشنهادی توضیح داده شده است. به این منظور، فرضیات مسئله بیان شده و گام‌های اجرای پروتکل توضیح داده شده است. سپس، روشی برای گسترش تعداد کاربران در زمان اجرای پروتکل پیشنهاد شده است. در ادامه، مثالی از نحوه اجرای پروتکل ذکر شده است تا به درک بهتر مراحل کار کمک نماید. بخش ۳ به بررسی پروتکل از نظر امنیتی و کارایی پرداخته است. در نهایت، مطالب جمع‌بندی شده و در آخرین بخش از مقاله ارائه شده است.

۲ مدل پیشنهادی

در پروتکل پیشنهادی از توپولوژی ستاره در شبکه‌های کامپیوتری استفاده شده است. یعنی، یک سرور مرکزی ارتباط بین کاربران را برقرار می‌کند. وظیفه اصلی سرور مرکزی تولید ذرات درهم‌تنیده کوانتومی و نیز هدایت پیام‌های ارسالی کاربران به یکدیگر است. هدف نهایی از اجرای پروتکل آن است که مجموعه‌ای از کاربران از طریق این سرور مرکزی، به صورت امن و همزمان، دوبه‌دو با یکدیگر به گفتگو بپردازند. برای این کار روش‌های متفاوتی وجود دارد که از جمله می‌تواند به حالت‌های درهم‌تنیده اشاره کرد. ما در این مقاله از حالت GHZ [۲۳] برای دستیابی به این هدف استفاده کرده‌ایم. دلیل این کار، وجود حالت عمومی GHZ و نیز امکان استفاده

[1] Quantum Key Distribution (QKD) [2] Quantum Secure Direct Communication (QSDC) [3] qubit [4] Quantum Dialogue [5] entanglement [6] intercept and resend [7] Semi-Quantum Secure Direct Communication [8] Semi-Quantum Dialogue [9] Trojan horse [10] qudit [11] trusted party

از عملگرهای تصادفی برای کدگذاری حالت‌های کوانتومی آن است. در این بخش، ابتدا فرضیاتی که برای به‌کارگیری پروتکل در نظر گرفته‌ایم را بیان می‌کنیم. سپس، گام‌های اجرای پروتکل را تشریح خواهیم کرد.

۱.۲ فرضیات

فرضیات موجود در پروتکل پیشنهادی به شرح زیر هستند:

- سرور مرکزی و کاربران قابلیت تولید ذرات درهم‌تنیده کوانتومی را دارند. همچنین، همه کاربران در پروتکل دارای قابلیت اندازه‌گیری کوانتومی هستند.
- سرور مرکزی نیمه‌صادق [1] است. به این معنی که از اجرای درست گام‌های پروتکل توسط آن مطمئن هستیم اما می‌دانیم که در مورد اطلاعات و پیام‌های کاربران کنجکاو است.
- با توجه به اینکه هدف از اجرای پروتکل گفت‌وگوی کوانتومی مبادله دو طرفه پیام‌ها میان کاربران است، پیش از شروع کار لازم است که هر کاربر زیرمجموعه‌ای از کاربرانی که می‌خواهد با آن‌ها گفت‌وگو نماید را مشخص کند. به عبارت دیگر، لازم است که هر کاربر برای مشارکت در گفت‌وگو اعلام آمادگی کرده باشد. به این منظور، هر کاربر درخواستی برای سرور ارسال نموده و در آن مشخص می‌کند که در ادامه می‌خواهد با کدام کاربران گفت‌وگو نماید. در اینجا فرض شده که این کار قبلاً انجام شده و در حال حاضر قرار است که n کاربر با شماره‌های $1, 2, 3, \ldots, n$ با یکدیگر گفت‌وگو نمایند. این n کاربر پیش از این احراز اصالت شده‌اند و هویت آن‌ها برای سرور مشخص شده است. در ادامه، کاربری با شماره i را با نماد p_i نشان خواهیم داد. همچنین، فرض می‌کنیم که یک کانال احراز اصالت شده میان سرور و هر یک از کاربران برقرار شده است. مقصود از کانال احراز اصالت شده، یک کانال ارتباطی رمزگذاری شده است که در آن آغازگر اتصال (یعنی سرویس گیرنده)، طرف مقابل (یعنی سرور) را احراز اصالت کرده است.
- حجم اطلاعاتی که کاربر می‌تواند در قالب یک پیام به سرور ارسال کند m بیت است. یعنی، در هر بار ارسال اطلاعات، دقیقا m بیت داده منتقل می‌شود. بدیهی است که در صورتی که طول پیغام کمتر از m بیت باشد از یک مکانیزم لایه‌گذاری [2] توافقی برای افزایش طول پیام استفاده می‌شود. همچنین در هر دور از ارسال اطلاعات، کاربر یک پیام مشخص را می‌تواند به کاربران دیگر ارسال کند.
- میان سرور و هر یک از کاربران یک کلید متقارن به اشتراک گذاشته شده است. (در ادامه مراحل اجرای پروتکل، از این کلید برای رمز کردن پیام ارسالی کاربران به سرور استفاده خواهد شد.) پیشنهاد می‌شود که از یک پروتکل توزیع کلید کوانتومی نظیر [۲۴] برای این منظور استفاده شود. کلید مشترک میان p_i و سرور را به صورت k_{is} نام‌گذاری می‌کنیم.

[1] semi-honest [2] padding

۲.۲ گام‌های اجرای پروتکل

گام ۱. ابتدا سرور یک حالت اولیه n ذره‌ای GHZ تولید می‌کند:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|\underbrace{00\cdots0}_{n}\rangle + |\underbrace{11\cdots1}_{n}\rangle\right) \quad (1)$$

سپس دنباله مرتبی از دنباله‌های تصادفی باینری به شکل کلی زیر را تولید می‌نماید (در ادامه مقاله، برای نمایش دنباله‌های مرتب، آن‌ها را میان دو پرانتز قرار می‌دهیم.):

$$R = (Q_2 \cdots Q_n) \quad (2)$$

در عبارت فوق، هر کدام از Q_iها دنباله‌ای باینری به طول $m^* = \lceil m + \Delta m \rceil$ هستند (علت استفاده از Δm حالت اضافه در گام ۴ توضیح داده شده است) که به صورت تصادفی تولید شده‌اند. مثلاً دنباله تصادفی kاُم در دنباله R به فرم کلی $Q_k = q_k^1, q_k^2, \ldots, q_k^{m^*}$ است. توجه داشته باشید که در ترتیب فوق، فقط دنباله‌های تصادفی را نام برده‌ایم. لذا، به دلیل آنکه Q_1 همواره مقدار صفر را اختیار می‌کند از ذکر آن خودداری شده است. در حقیقت، n دنباله داریم که دنباله اول صفر و بقیه دنباله‌ها تصادفی هستند.

دنباله‌های تصادفی فوق برای ساخت دنباله‌ای از عملگرها (U) به کار گرفته می‌شوند. مثلاً، اگر bاُمین بیت از رشته‌های تصادفی Q_2 تا Q_n در کنار هم قرار گیرند عملگر bاُم را تشکیل می‌دهند که به صورت $U_{q_2^b q_3^b \cdots q_n^b}$ نمایش داده می‌شود. از این عملگرها برای کدگذاری حالت اولیه استفاده خواهد شد. دنباله عملگرهای تولید شده عبارتند از:

$$\ddot{U} = \left(U_{q_2^1 q_3^1 \cdots q_n^1}, U_{q_2^2 q_3^2 \cdots q_n^2}, \ldots, U_{q_2^{m^*} q_3^{m^*} \cdots q_n^{m^*}}\right) \quad (3)$$

گام ۲. سرور به تعداد m^* حالت اولیه تولید می‌کند. سپس، با استفاده از عملگرها، حالت اولیه را کدگذاری می‌کند:

$$U_{Q_2 Q_3 \cdots Q_n} = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} |j\rangle\langle j| \otimes \left(\prod_{k=2}^{n} |j \oplus Q_k\rangle\langle j|\right) \quad (4)$$

پس از اعمال عملگرها، نتیجه زیر حاصل می‌شود:

$$|GHZ\rangle'_{Q_2 Q_3 \cdots Q_n} = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} \left(|j\rangle |j \oplus q_2\rangle \cdots |j \oplus Q_n\rangle\right) \quad (5)$$

که با بسط آن به فرم زیر خواهیم رسید:

$$|GHZ\rangle^1_{q_2^1 q_3^1 \cdots q_n^1} = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} \left(|j\rangle |j \oplus q_2^1\rangle \cdots |j \oplus q_n^1\rangle\right)$$

$$|GHZ\rangle^2_{q_2^2 q_3^2 \cdots q_n^2} = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} \left(|j\rangle |j \oplus q_2^2\rangle \cdots |j \oplus q_n^2\rangle\right)$$

$$\vdots$$

$$|GHZ\rangle^{m^*}_{q_2^{m^*} q_3^{m^*} \cdots q_n^{m^*}} = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} \left(|j\rangle \, |j \oplus q_2^{m^*}\rangle \cdots |j \oplus q_n^{m^*}\rangle \right) \qquad (۶)$$

گام ۳. سرور m^* حالت را به n دنباله‌ی کوانتومی $S_1, S_2, \ldots, S_n$ تقسیم می‌کند؛ هر یک از S_iها به شکل $S_i = \{S_i^1 S_i^2 \cdots S_i^{m^*}\}$ است، به گونه‌ای که اولین ذره در هر GHZ را در S_1، دومین ذره در S_2، ... و nامین ذره در S_n قرار می‌گیرد. در گام بعد، سرور تعدادی فوتون دام[1] را در پایه‌های Z و X آماده کرده و به صورت تصادفی در دنباله‌های $S_1, S_2, \ldots, S_n$ قرار می‌دهد و هر دنباله S_i را به p_i ارسال می‌کند.

گام ۴. سرور محل و همچنین پایه فوتون‌های دام را از طریق کانال کلاسیک به هر کاربر اعلام می‌کند. کاربران این فوتون‌ها را اندازه‌گیری کرده و نتیجه اندازه‌گیری را به سرور ارسال می‌کنند. سرور با بررسی نتیجه اندازه‌گیری، وجود یا عدم وجود شنودگر را بررسی می‌کند. در صورتی که میزان خطا از مقدار تعیین شده (آستانه خطا) کمتر باشد، پروتکل ادامه پیدا می‌کند؛ در غیر این صورت، پروتکل باز راه‌اندازی خواهد شد. در اینجا، آستانه خطا، متغیری است که با توافق طرفین و بسته به شرایط فیزیکی و خطای اندازه‌گیری دستگاه‌های موجود در ارتباط اندازه‌گیری شده و به عنوان پارامتر اولیه بین سرور و کاربران توافق می‌شود.

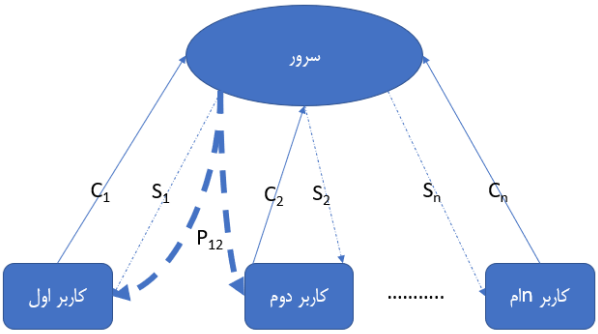
به طور همزمان، کاربران با استفاده از Δm حالت اضافه به بررسی سرور خواهند پرداخت. به این صورت که با انتخاب ذرات مشخص و با استفاده از خاصیت درهم‌تنیدگی، نتایج اندازه‌گیری را مقایسه خواهند کرد [۲۵]. در صورتی که میزان خطا از یک مقدار از پیش تعیین شده بیشتر باشد، سرور قابل اعتماد نیست و پروتکل متوقف خواهد شد.

گام ۵. هر کاربر بعد از حذف فوتون‌های دام و فوتون‌های بررسی سرور، به دنباله اصلی حاوی اطلاعات دسترسی پیدا می‌کند. سپس، با استفاده از پایه Z روی دنباله خود اندازه‌گیری را انجام می‌دهد. در صورتی که نتیجه اندازه‌گیری شده برابر $|1\rangle$ باشد مقدار ۱ و در صورتی که نتیجه اندازه گیری شده $|0\rangle$ باشد مقدار ۰ را در دنباله k_i قرار می‌دهد.

گام ۶. فرض کنید p_i بخواهد پیام سرّی I_i را برای p_j ارسال کند. برای این کار، ابتدا مقدار $C_i = k_i \oplus I_i$ را محاسبه می‌کند؛ سپس با استفاده از کلید به اشتراک گذاشته شده k_{is} مقدار C_i را رمز کرده و برای سرور ارسال می‌نماید. توجه داشته باشید که پیام ارسالی کاربر در ابتدا با کلید اختصاصی خودش (k_i) XOR شده و سپس با کلید به اشتراک گذاشته شده با سرور رمز می شود. رمز کردن داده‌ها، می‌تواند از طریق یک پروتکل رمزنگاری متقارن استاندارد نظیر AES [۲۶] صورت پذیرد.

گام ۷. سرور با استفاده از کلید k_{is} پیام دریافتی از p_i را رمزگشایی می‌کند. سپس، مقدار C_{ij} را به صورت زیر محاسبه می‌نماید:

[1] decoy photon



$S_1 \Rightarrow k_1$ $\quad C_1 = k_1 \oplus I_1$ $\quad P_{12} = C_{12} \oplus C_1 \oplus C_2$

$S_2 \Rightarrow k_2$ $\quad C_2 = k_2 \oplus I_2$ $\quad P_{1n} = C_{1n} \oplus C_1 \oplus C_n$

$S_n \Rightarrow k_n$ $\quad C_n = k_n \oplus I_n$ $\quad P_{2n} = C_{2n} \oplus C_2 \oplus C_n$

شکل ۱. شمای کلی پروتکل

$$C_{ij} = |j \oplus Q_i\rangle \oplus |j \oplus Q_j\rangle \qquad (۷)$$

در حقیقت، سرور با اطلاع از ترتیب دنباله‌های ارسالی مقدار C_{ij} را به دست می‌آورد که برابر با $k_i \oplus k_j$ است.

در ادامه، سرور مقدار p_{ij} را به صورت زیر تولید کرده، با استفاده از k_{is} آن را رمز کرده و برای دو کاربری که خواهان برقراری ارتباط با هم هستند ارسال می‌کند:

$$P_{ij} = C_{ij} \oplus C_i \oplus C_j \qquad (۸)$$

این کار از طریق یک کانال احراز اصالت شده صورت می‌گیرد. چرا که، در صورت عدم استفاده از کانال احراز اصالت شده کاربر یا شخص دیگری می‌تواند خود را به عنوان سرور معرفی کند و داده‌های ارسالی را دریافت کند. توجه داشته باشید که وجود چنین کانالی جزء فرضیات اولیه پروتکل در نظر گرفته شده است. یعنی، تشکیل این کانال نیازمند اجرای پروتکلی مستقل است که بررسی آن خارج از محدوده این مقاله قرار می‌گیرد.

گام ۸. کاربران ابتدا پیام را رمزگشایی می‌کنند و در نهایت، مقدار دریافتی هر کاربر برابر $I_i \oplus I_j$ خواهد بود؛ زیرا، با XOR شدن مقدار C_{ij} با پیام‌های کاربران، مقدارهای k_i و k_j حذف می‌شوند و تنها $I_i \oplus I_j$ باقی می‌ماند. بنابراین، هر کاربر با XOR کردن مقدار p_{ij} با پیام سری خود، به پیام سری کاربر مقابل دست پیدا می‌کند.

شمای کلی پروتکل پیشنهادی در شکل شماره ۱ نمایش داده شده است.

۳.۲ گسترش کاربران در زمان اجرا

در صورتی که در زمان اجرای پروتکل کاربری بخواهد به مجموعه کاربران اضافه شود، ابتدا یک درخواست برقراری ارتباط به سرور ارسال می‌کند. سپس، کاربر m حالت Φ^+ بل را آماده کرده و ذره‌های اول را برای سرور ارسال می‌کند. سرور بعد از دریافت این ذره‌ها یک دنباله‌ی باینری تصادفی جدید (Q_{n+1}) به طول m ایجاد نموده و به لیست دنباله‌هایی که قبلا تولید کرده بود اضافه می‌کند:

$$R = (Q_2, Q_3, \ldots, Q_n, Q_{n+1}) \qquad (۹)$$

دلیل استفاده از m بیت (به جای m^* بیت) در دنباله Q_{n+1} این است که کاربر جدید از روشی متفاوت برای سنجش درستی سرور استفاده می‌کند. یعنی، کاربر جدید نیازی به Δm بیت اضافی برای سنجش صحت عملکرد سرور ندارد. سرور با استفاده از دنباله‌ی فوق دنباله عملگرهای کدگذاری جدید را تولید می‌کند:

$$\ddot{U} = \left(U_{q_1^1 q_2^1 \cdots q_n^1 q_{n+1}^1}, U_{q_1^2 q_2^2 \cdots q_n^2 q_{n+1}^2}, \ldots, U_{q_1^{m^*} q_2^{m^*} \cdots q_n^{m^*}}\right) \quad (۱۰)$$

چون q_{n+1} روی عملیات سایر عملگرها اثر ندارد، در نتیجه، کدگذاری و عملگرهای کاربران دیگر ثابت خواهند ماند.

سرور ذره‌های دریافتی را با عملگر تولید شده کدگذاری می‌کند:

$$U_{Q_{n+1}} = \left(\frac{1}{\sqrt{2}}\sum_{j=0}^{1} |j\rangle\langle j| \left(|j \oplus Q_{n+1}\rangle\langle j|\right)\right) \otimes I \quad (۱۱)$$

و آن را در دنباله S_{n+1} قرار داده، سپس فوتون‌های دام را به این دنباله اضافه کرده و برای p_{n+1} ارسال می‌کند.

کاربر پس از دریافت محل و پایه اندازه‌گیری فوتون‌های دام، در پایه‌های اعلام شده اندازه‌گیری می‌کند و نتیجه را برای سرور ارسال می‌کند. در صورتی که سرور متوجه حضور شنودگر شود ارتباط باز راه‌اندازی می‌شود. کاربر فوتون‌های دام را از دنباله S_{n+1} حذف کرده، سپس بررسی می‌کند در صورتی که حالت بعد از اندازه‌گیری $|00\rangle$ و یا $|01\rangle$ باشد مقدار ۰ را و در صورتی که حالت نهایی $|11\rangle$ و یا $|10\rangle$ باشد مقدار ۱ را در k_{i+1} قرار می‌دهد. همچنین، اگر سرور بر روی ذرات اندازه‌گیری انجام داده باشد، کاربر ارتباط را باز راه‌اندازی می‌کند. به این ترتیب، کاربر جدید هم کلید مورد نیاز برای رمز کردن اطلاعات خود را در اختیار خواهد داشت.

حال فرض کنید که یکی از کاربران فعال در پروتکل بخواهد فرایند ارسال و دریافت خود را متوقف نموده و از گفت‌وگو خارج شود. برای این کار کافی است که یک پیام به سرور ارسال نموده و خروج خود را اعلام نماید. سرور با دریافت چنین پیامی باید کلید کاربر مورد نظر را تغییر دهد که از این به بعد قابل استفاده نباشد. برای انجام این کار، سرور دنباله‌ی تصادفی آن کاربر را تغییر می‌دهد. از آنجا که مقدار کلید به مقدار دنباله تصادفی وابسته است، با تغییر دنباله، کلید نیز تغییر می‌کند. لذا، از این پس کلید قبلی کاربرد نخواهد داشت.

۴.۲ مثال

برای واضح شدن نحوه کار پروتکل، یک مثال از گفت‌وگوی کوانتومی میان چهار کاربر را بررسی می‌کنیم. A، B، C و D چهار کاربری هستند که قصد گفت‌وگوی کوانتومی دارند. به این صورت که p_A و p_B، p_C و p_D، p_D و p_B قصد برقراری ارتباط را دارند. فرض کنید پیام‌های ارسالی هر کاربر به صورت زیر باشد:

$$I_A = 011 \qquad I_B = 111$$
$$I_c = 000 \qquad I_D = 110 \quad (۱۲)$$

در ابتدا به دلیل وجود چهار کاربر، سرور یک حالت اولیه GHZ چهار ذره‌ای را تولید می‌کند:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \quad (۱۳)$$

سپس سرور با فرض $\Delta m = 1$ دنباله‌ای چهار عضوی (تعداد کاربران) از دنباله‌های چهاربیتی (۳+۱) تصادفی تولید می‌کند. فرض کنید دنباله‌های تولید شده توسط سرور به شرح زیر باشند:

$$R = (0100, 1011, 1110, 0011) \quad (۱۴)$$

سرور با استفاده از این دنباله‌ها، عملگرها را آماده می‌کند. بنابراین، دنباله‌ای مشابه با $\ddot{U}$ به دست خواهد آمد:

$$\ddot{U} = (U_{0100}, U_{1011}, U_{1110}, U_{0011}) \quad (۱۵)$$

در این مرحله، سرور با استفاده از عملگرهای فوق، حالت اولیه را با استفاده از رابطه (۴) کدگذاری می‌کند. همچنین، بررسی می‌کند که کاربران از پروتکل خارج نشده باشند و نیز تقاضای برقراری ارتباط میان کاربران به صورت دو طرفه باشد (یعنی هر دو طرف بخواهند با یکدیگر گفت‌وگو نمایند). در صورتی که شرایط مورد نظر برقرار بود، سرور دنباله‌های S_i که شامل ذره‌های iام هر GHZ است را تولید و با اضافه کردن فوتون‌های دام به آن، برای هر p_i ارسال می‌نماید:

$$|GHZ\rangle^1_{0110} = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle)$$
$$|GHZ\rangle^2_{1010} = \frac{1}{\sqrt{2}}(|0010\rangle + |1101\rangle)$$
$$|GHZ\rangle^3_{0111} = \frac{1}{\sqrt{2}}(|0111\rangle + |1000\rangle)$$
$$|GHZ\rangle^4_{0101} = \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle) \quad (۱۶)$$

کاربران فوتون‌های دام را در پایه‌های ارسالی توسط سرور اندازه‌گیری کرده و نتیجه را به سرور ارسال می‌کنند. به این ترتیب، سرور قادر خواهد بود وجود شنودگر را بررسی نماید. از سوی دیگر، کاربران با بررسی Δm فوتون‌های اضافه صحت عملکرد سرور را بررسی می‌کنند.

اگر صحت عملیات فوق تأیید شد، کاربران در پایه Z، دنباله دریافتی را اندازه‌گیری کرده و نتیجه را در k_i قرار می‌دهند:

$$k_A = 111 \qquad k_B = 010$$
$$k_C = 000 \qquad k_D = 110 \quad (۱۷)$$

پس از آن، هر کاربر مقدار C_i را محاسبه می‌کند:

$$C_A = k_A \oplus I_A = 111 \oplus 011 = 100$$
$$C_B = k_B \oplus I_B = 010 \oplus 111 = 101$$
$$C_C = k_C \oplus I_C = 000 \oplus 000 = 000$$
$$C_D = k_D \oplus I_D = 110 \oplus 110 = 000 \quad (۱۸)$$

هر کاربر، C_i مربوط به خود را با استفاده از کلید متقارنی که قبلا میان او و سرور به اشتراک گذاشته شده است (k_{is})، رمز کرده و برای سرور ارسال می‌کند.

با توجه به اینکه سرور از رابطه بین k_iها مطلع است، مقادیر C_{ij} را بر اساس گام‌های بیان شده محاسبه می‌کند:

$$C_{AB} = ۱۰۱ \quad C_{BD} = ۱۰۰ \quad C_{CD} = ۱۱۰ \tag{۱۹}$$

سپس، سرور مقدار p_{ij} را محاسبه کرده و برای طرفین هر ارتباط ارسال می‌کند:

$$\begin{aligned} P_{AB} &= C_{AB} \oplus C_A \oplus C_B = ۱۰۱ \oplus ۱۰۰ \oplus ۱۰۱ = ۱۰۰ \\ P_{BD} &= C_{BD} \oplus C_B \oplus C_D = ۱۰۰ \oplus ۱۰۱ \oplus ۰۰۰ = ۰۰۱ \\ P_{CD} &= C_{CD} \oplus C_C \oplus C_D = ۱۱۰ \oplus ۰۰۰ \oplus ۰۰۰ = ۱۱۰ \end{aligned} \tag{۲۰}$$

در نهایت، هر کاربر p_{ij} دریافتی را با پیام سری خود XOR کرده و به این ترتیب پیام ارسالی طرف مقابل را استخراج می‌کند. به عنوان نمونه، کاربر A می‌تواند پیام کاربر B را به صورت زیر محاسبه کند:

$$P_{AB} \oplus I_A = ۱۰۰ \oplus ۰۱۱ = ۱۱۱ \tag{۲۱}$$

کاربر B نیز به صورت مشابه می‌تواند پیام ارسالی از سمت کاربر A را به صورت زیر محاسبه کند:

$$P_{AB} \oplus I_B = I_A = ۱۰۰ \oplus ۱۱۱ = ۰۱۱ \tag{۲۲}$$

حال فرض می‌کنیم p_E قصد دارد به پروتکل ملحق شده و با p_B گفت‌وگو کند. به این منظور، p_E، m حالت بل را ایجاد می‌کند:

$$\text{Bell state} = \frac{۱}{\sqrt{۲}}(|۰۰\rangle + |۱۱\rangle) \tag{۲۳}$$

سپس، ذره اول را به سرور ارسال می‌کند. سرور دنباله تصادفی $Q_{۴+۱} = \{۰۱۱\}$ را تولید کرده و عملگر $U_{۰۱۱}$ را تولید می‌کند:

$$U_{۰۱۱} = \left(\frac{۱}{\sqrt{۲}} \sum_{j=۰}^{۱} |j\rangle \langle j| \left(|j \oplus Q_۵\rangle \langle j| \right) \right) \otimes I \tag{۲۴}$$

سرور عملگر $U_{۰۱۱}$ را بر روی کیوبیت اول اعمال می‌کند. پس از اعمال عملگر، حالت کلی سیستم به شکل زیر خواهد بود:

$$\begin{aligned} |\text{Bell state}\rangle^۱ &= \frac{۱}{\sqrt{۲}}(|۰۰\rangle + |۱۱\rangle) \\ |\text{Bell state}\rangle^۲ &= \frac{۱}{\sqrt{۲}}(|۰۱\rangle + |۱۰\rangle) \\ |\text{Bell state}\rangle^۳ &= \frac{۱}{\sqrt{۲}}(|۰۱\rangle + |۱۰\rangle) \end{aligned} \tag{۲۵}$$

سرور فوتون‌های دام را به همراه ذرات دریافتی برای p_E ارسال می‌کند. سپس p_E فوتون‌های دام را در پایه‌های اعلام شده توسط سرور اندازه‌گیری کرده و نتیجه را برای سرور ارسال می‌کند. سرور با بررسی نتیجه دریافتی وجود شنودگر را بررسی می‌کند.

p_E فوتون‌های دام را از دنباله دریافتی حذف کرده و با اندازه‌گیری بر روی دنباله دریافتی مقدار $k_E = ۱۰۰$ را محاسبه می‌کند. فرض کنید که $I_E = ۰۰۱$ باشد. برای ارسال این پیام، p_E مقدار $C_E = ۱۰۱$ را محاسبه و برای سرور ارسال می‌کند. سرور با XOR کردن مقدار $C_{BE} = ۱۱۰$ با CE و CB، $P_{BE} = ۱۱۰$ را محاسبه می‌کند و برای p_E و p_B ارسال می‌کند. به این ترتیب، هر یک از این دو کاربر به پیام کاربر مقابل دسترسی پیدا می‌کند:

$$\begin{aligned} I_B &= ۱۱۰ \oplus ۰۰۱ = ۱۱۱ \\ I_E &= ۱۱۰ \oplus ۱۱۱ = ۰۰۱ \end{aligned} \tag{۲۶}$$

۳ ارزیابی پروتکل

۱.۳ ارزیابی امنیتی پروتکل

در این بخش، مقاومت پروتکل پیشنهادی خود را در برابر چند حمله مهم بررسی می‌کنیم. این حملات عبارتند از شنود یا ایجاد اختلال توسط مهاجمین بیرونی (حمله شماره ۱)، شنود داده‌ها توسط سرور (حمله شماره ۲) و نیز نشت داده‌ها به کاربران غیرمجاز داخلی (حمله شماره ۳). علت انتخاب این حملات، آن است که امنیت پروتکل‌های ارتباطی کوانتومی معمولاً از طریق بررسی مقاومت آن‌ها در برابر این حملات سنجیده می‌شود.

(حمله شماره ۱)- فرض کنید در هنگامی که سرور دنباله S_i را برای p_i ارسال می‌کند شنودگر این دنباله را دریافت و روی آن اندازه‌گیری کند و سپس با ساخت فوتون‌های تقلبی در حالت اندازه‌گیری شده آن را برای p_i ارسال نماید. حملاتی نظیر دریافت و ارسال مجدد، درهم‌تنیدگی-اندازه‌گیری و حمله اختلال از این نوع هستند. در پروتکل پیشنهادی، به دلیل آن‌که در دنباله S_i از فوتون‌های دام استفاده شده، هیچ فرد بیرونی از محل و همچنین حالت پایه‌ای این فوتون‌ها اطلاع ندارد. لذا اگر مهاجم بیرونی این دنباله‌ها را شنود کند، با اندازه‌گیری این فوتون‌ها باعث از بین رفتن حالت اولیه می‌شود. لذا، کاربر با استفاده از اندازه‌گیری بر روی این فوتون‌ها و ارسال آن به سرور می‌تواند حمله را شناسایی نماید.

همچنین در صورتی که شنودگر بخواهد از حمله تکرار در کانال‌های احراز اصالت شده استفاده کند با شکست روبه‌رو خواهد شد؛ زیرا در هر دور از پروتکل پیام دریافتی از سمت سرور با پیام جدید کاربر کدگشایی می‌شود. به عبارت دیگر، در صورتی که یک پیام تکراری با پیام جدید کاربر مقابل رمزگشایی شود، حاصل یک مقدار بی‌معنی خواهد شد.

(حمله شماره ۲)- همان گونه که پیشتر اشاره شد، در این پروتکل فرض شده که سرور نیمه‌صادق است؛ به این معنا که از اجرای درست پروتکل توسط آن مطمئن هستیم، اما سرور نسبت به اطلاعات کاربران کنجکاو است. همان طور که در گام‌های اجرای پروتکل بیان شد، کاربران با استفاده از خواص درهم‌تنیدگی GHZ می‌توانند از مورد اعتماد بودن سرور اطمینان حاصل کنند. یعنی، در صورتی که سرور روی حالات ارسالی اندازه‌گیری انجام دهد، کاربران متوجه اندازه‌گیری شده و پروتکل

را بازنشانی می‌کنند. همچنین در صورتی که سرور حالت‌های تک فوتون را به جای حالت GHZ ارسال کند کاربران با اندازه‌گیری حالات ارسالی، متوجه عدم ارتباط بین حالات شده و پروتکل را بازنشانی می‌کنند. در زمان اضافه شدن کاربر جدید، به دلیل استفاده از حالت بل، در صورتی که سرور اندازه‌گیری روی حالت ارسالی انجام دهد کاربر متوجه خواهد شد. بنابراین، به طور کلی، شنود اطلاعات از سوی سرور توسط کاربران تشخیص داده خواهد شد.

(حمله شماره ۳)- به دلیل آن‌که ما از اجرای درست پروتکل توسط سرور اطمینان داریم سرور اجازه سرقت اطلاعات سایر کاربران به کاربر دیگر را نمی‌دهد. در واقع سرور تنها به کاربری اطلاعات کاربر دیگر را ارسال می‌کند که از ارسال دنباله C_i توسط آن کاربر مطمئن شود.

۲.۳ ارزیابی کارایی پروتکل

بر اساس فرمول کارایی Cabello [۲۷]، میزان کارایی از رابطه زیر محاسبه می شود.

$$\eta = b_s/(q_t + b_t) \qquad (۲۷)$$

که در آن b_s میزان اطلاعات سری مبادله شده، q_t میزان کیوبیت‌های استفاده شده و b_t میزان اطلاعات کلاسیک استفاده شده است. طبق این رابطه، میزان کارایی پروتکل پیشنهادی در این مقاله به صورت زیر محاسبه می‌شود:

$$\eta = \frac{n \times m}{m^* + y + n \times m} = \frac{n \times m}{m + \Delta m + y + n \times m} \qquad (۲۸)$$

که در آن، y، تعداد فوتون‌های دام است.

در بدترین حالت $y = m$ خواهد بود. به این معنا که به تعداد بیت‌های پیام، فوتون دام در دنباله قرار می‌گیرد. توجه داشته باشید که این یک فرض بسیار بدبینانه است و در عمل مقدار y همواره کمتر از m خواهد بود. همچنین Δm کسری از m است. یعنی می‌توان آن را به صورت یک مقدار کوچکتر از ۱ ضرب در m در نظر گرفت. فرض کنید، این ضریب برابر با $d < ۱$ باشد. بنابراین، Δm به صورت $d \times m$ قابل نمایش است. با توجه به توضیحات فوق، در بدترین حالت، رابطه فوق به صورت زیر ساده‌سازی خواهد شد:

$$\eta = \frac{n \times m}{m + d \times m + m + n \times m} = \frac{n}{۲ + d + n} \qquad (۲۹)$$

در رابطه فوق، با توجه به ناچیز بودن مقدار d می‌توان از آن صرف نظر کرد. در نتیجه، کارایی پروتکل پیشنهادی در بدترین حالت از رابطه زیر به دست می‌آید:

$$\eta = \frac{n}{۲ + n} \qquad (۳۰)$$

با توجه به رابطه فوق، در صورتی که تعداد کاربران افزایش یابد، کارایی نیز بیشتر خواهد شد. به عبارت دیگر، مزیت استفاده از پروتکل پیشنهادی مخصوصا زمانی نمایان خواهد شد که تعداد کاربران زیاد باشد.

جدول ۱. مقایسه کارایی پروتکل پیشنهادی با پروتکل‌های مشابه

پروتکل	تعداد کاربر	کارایی (درصد)
Shi et al. [۲۸]	۲	۶۶٫۷
Wang et al. [۲۹]	۲	۶۶٫۷
Zhou et al. [۳۰]	۲	۸۰
Yang et al. [۳۱]	۲	۶۶٫۷
پروتکل پیشنهادی	۲	۵۰
	۳	۶۰
	۴	۶۶٫۷
	۵	۷۱٫۴
	⋮	⋮
	n	$\frac{n}{۲+n} \times ۱۰۰$

به گونه‌ای که با افزایش کاربران، کارایی هر چه بیشتر به یک نزدیک خواهد شد. در جدول شماره ۱ کارایی پروتکل پیشنهادی با سایر پروتکل‌های گفت‌وگوی کوانتومی مقایسه شده است. توجه داشته باشید که پروتکل‌های پیشین تنها برای استفاده دو کاربر طراحی شده بودند. لذا در جدول ۱، کارایی آن‌ها تنها برای حالت دو–کاربره ذکر شده است. بدیهی است که در این حالت خاص، پروتکل پیشنهادی نسبت به پروتکل‌های پیشین از کارایی پایین‌تری برخوردار است. اما همان گونه که توضیح داده شد، با افزایش تعداد کاربران کارایی افزایش یافته و به ۱۰۰ درصد نزدیک خواهد شد. جهت بیشتر نمایان شدن این موضوع، در جدول ۱، کارایی روش پیشنهادی را برای ۲، ۳، ۴، ۵ و n کاربر نمایش داده‌ایم.

۴ جمع‌بندی

ما یک پروتکل جدید گفت‌وگوی کوانتومی را ارائه دادیم که در آن n کاربر می‌توانند از طریق یک سرور نیمه صادق مرکزی، پیام‌هایی را به صورت سرّی به یکدیگر ارسال نمایند. در این پروتکل، برای اولین بار، قابلیت اضافه یا کم شدن کاربران در زمان اجرای پروتکل و بدون نیاز به اجرای دوباره آن ارائه شد. بررسی‌های انجام شده نشان داد که این پروتکل در مقابل شنود داخلی که ممکن است از طریق سرور و یا یک کاربر روی دهد و نیز در برابر شنود خارجی مقاوم است. به دلیل محدودیت حجم مقاله از بررسی کامل حملات پرهیز شده است و در مقالات آینده به آن پرداخته خواهد شد.

مراجع

[1] Hwang, Won-Young. Quantum key distribution with high loss: toward global secure communication. *Physical review letters*, 91(5):057901, 2003.

[2] Shor, Peter W. Polynomial-time algorithms for prime

factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[3] Grover, Lov K. A fast quantum mechanical algorithm for database search. in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[4] Kumar, Ajay and Garhwal, Sunita. State-of-the-art survey of quantum cryptography. *Archives of Computational Methods in Engineering*, 28:3831–3868, 2021.

[5] Bennett, Charles H and Brassard, Gilles. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[6] Bennett, Charles H. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.

[7] Deng, Fu-Guo and Long, Gui Lu. Bidirectional quantum key distribution protocol with practical faint laser pulses. *Physical Review A*, 70(1):012311, 2004.

[8] Lo, Hoi-Kwong, Ma, Xiongfeng, and Chen, Kai. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[9] Deng, Fu-Guo and Long, Gui Lu. Secure direct communication with a quantum one-time pad. *Physical Review A*, 69(5):052319, 2004.

[10] Beige, Almut, Englert, Berthold-Georg, Kurtsiefer, Christian, and Weinfurter, Harald. Secure communication with a publicly known key. *arXiv preprint quant-ph/0111106*, 2001.

[11] Deng, Fu-Guo, Long, Gui Lu, and Liu, Xiao-Shu. Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. *Physical Review A*, 68(4):042317, 2003.

[12] Nguyen, Ba An. Quantum dialogue. *Physics Letters A*, 328(1):6–10, 2004.

[13] Ye, Tian-Yu and Ye, Chong-Qiang. Semi-quantum dialogue based on single photons. *International Journal of Theoretical Physics*, 57:1440–1454, 2018.

[14] Yin-Ju, Lu. Quantum dialogue protocol based on bell entangled states and single photons. *International Journal of Theoretical Physics*, 60:3815–3821, 2021.

[15] Ye, Tian-Yu, Li, Hong-Kun, and Hu, Jia-Li. Information leakage resistant quantum dialogue with single photons in both polarization and spatial-mode degrees of freedom. *Quantum Information Processing*, 20(6):209, 2021.

[16] Xu, Liang-Chao, Chen, Hua-Ying, Zhou, Nan-Run, and Gong, Li-Hua. Multi-party semi-quantum secure direct communication protocol with cluster states. *International Journal of Theoretical Physics*, 59:2175–2186, 2020.

[17] Ye, Tian-Yu. Quantum secure direct dialogue over collective noise channels based on logical bell states. *Quantum Information Processing*, 14:1487–1499, 2015.

[18] Zhong-Xiao, Man, Zhan-Jun, Zhang, and Yong, Li. Quantum dialogue revisited. *Chinese Physics Letters*, 22(1):22, 2005.

[19] Gao, Fei, Guo, FenZhuo, Wen, QiaoYan, and Zhu, FuChen. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Science in China Series G: Physics, Mechanics and Astronomy*, 51(5):559–566, 2008.

[20] Huang, Dazu, Chen, Zhigang, Xie, Jianquan, and Guo, Ying. Bidirectional quantum secure direct communication based on entanglement. in *Advances in Security Technology: International Conference, SecTech 2008, and Its Special Sessions, Sanya, Hainan Island, China, December 13-15, 2008. Revised Selected Papers*, pp. 40–49. Springer, 2009.

[21] Cao, Gang and Jiang, Min. Multi-party quantum dialogue protocol based on multi-particle ghz states. in *2017 Chinese Automation Congress (CAC)*, pp. 1614–1618. IEEE, 2017.

[22] Bechmann-Pasquinucci, Helle and Tittel, Wolfgang. Quantum cryptography using larger alphabets. *Physical Review A*, 61(6):062308, 2000.

[23] Greenberger, Daniel M, Horne, Michael A, and Zeilinger, Anton. Going beyond bell's theorem. *Bell's theorem, quantum theory and conceptions of the universe*, pp. 69–72, 1989.

[24] Wang, Weilong, Tamaki, Kiyoshi, and Curty, Marcos. Measurement-device-independent quantum key distribution with leaky sources. *Scientific reports*, 11(1):1678, 2021.

[25] Zhang, Wei-Wei and Zhang, Ke-Jia. Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. *Quantum information processing*, 12:1981–1990, 2013.

[26] Dworkin, Morris J, Barker, Elaine B, Nechvatal, James R,

Foti, James, Bassham, Lawrence E, Roback, E, and Dray Jr, James F. Advanced encryption standard (aes). 2001.

[27] Cabello, Adán. Quantum key distribution in the holevo limit. *Physical Review Letters*, 85(26):5635, 2000.

[28] Shi, Guo-Fang, Xi, Xiao-Qiang, Hu, Ming-Liang, and Yue, Rui-Hong. Quantum secure dialogue by using single photons. *Optics communications*, 283(9):1984–1986, 2010.

[29] Wang, He, Zhang, Yuqing, Hu, Yupu, Tian, Yangli, and Zhu, Zhenchao. Two quantum dialogue schemes based on bell states and two-qutrit entangled states without information leakage. *Journal of National University of Defense Technology*, 34(2):10–13, 2012.

[30] Zhou, Nan-Run, Wu, Gui-Tong, Gong, Li-Hua, and Liu, San-Qiu. Secure quantum dialogue protocol based on w states without information leakage. *International Journal of Theoretical Physics*, 52:3204–3211, 2013.

[31] Yang, Chun-Wei and Hwang, Tzonelih. Quantum dialogue protocols immune to collective noise. *Quantum information processing*, 12:2131–2142, 2013.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 20, Number 2 (pp. 1–10)
https://monadi.isc.org.ir

Presented at the ISCISC 2022 in University of Giulan, Rasht, Iran

Multi-Party Quantum Dialogue with the Capability to Expand the Number of Users at Runtime★

Ali Khazaei *,[1], Hossein Homaei [1] and Monireh Houshmand [2]

[1] *Faculty of Electrical and Computer Engineering, Tarbiat Modares university, Tehran, Iran*
[2] *Faculty of Electrical Engineering, Imam Reza International university, Mashhad, Iran*

ARTICLE INFO.

Keywords:
Security protocols
quantum security
multi-user quantum dialogue

dor: 20.1001.1.24763047.1401.11.2.1.0

Type: research paper

ABSTRACT

Quantum dialogue is a type of quantum communication in which users can simultaneously send messages to each other. The earliest instances of quantum dialogue protocols faced security problems such as information leakage and were vulnerable to intercept and resend attacks. Therefore, several protocols have been presented that try to solve these defects. Despite these improvements, the quantum dialogue still faces some challenges. Currently, the limited number of participants and the impossibility of expanding users during the conversation are among the most important challenges of this kind of protocol. In this research, we have designed a multi-user quantum dialogue protocol that solves the mentioned challenges. The proposed protocol is a generalized type of quantum dialogue in which users can communicate simultaneously. The number of participating users is not limited and can be changed dynamically (i.e. without the need to restart the protocol). It means that, during the execution of the protocol, a user can leave the conversation, or a new user can join it. Communication between users is established through a central semi-trusted server. The investigations show that the proposed protocol does not have information leakage. In other words, no unauthorized entity (not even the intermediate server) can access the raw data exchanged between users.

© 2022 ISC

★ The ISCISC 2022 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: a.khazaei@modares.ac.ir (Ali Khazaei), homaei@modares.ac.ir (Hossein Homaei), m.hooshmand@imamreza.ac.ir (Monireh Houshmand)
© 2022 ISC. All rights reserved.