دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۴، جلد ۲۳، شماره ۲ (۱۳–۲۸)
https://monadi.isc.org.ir

ارائه‌شده در بیست و دومین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه شهید بهشتی، ۱۶ و ۱۷ مهرماه ۱۴۰۴

طرح نوین تسهیم راز نیمه‌کوانتومی مقاوم بدون تبادل مستقیم کیوبیت حاوی پیام

محمد بلوکیان*[۱،۲] و منیره هوشمند[۲]

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

اطلاعات مقاله

کلمات کلیدی:
کیوبیت
برهم‌نهی کوانتومی
رمزنگاری کوانتومی
مخابره از راه دور کوانتومی
رمزنگاری نیمه‌کوانتومی
تسهیم راز کوانتومی
تسهیم راز نیمه‌کوانتومی

نوع مقاله: پژوهشی

چکیده

نظریه اطلاعات و محاسبات کوانتومی یکی از مهم‌ترین شاخه‌های مورد توجه در سال‌های اخیر است که در ابعاد اتمی و زیراتمی کاربرد دارد. برخلاف رمزنگاری کلاسیک که دارای امنیت مبتنی بر پیچیدگی محاسبات است، رمزنگاری کوانتومی امنیت بی‌قید و شرط داشته و امنیت آن مبتنی بر محدودیت‌های فیزیکی است. در رمزنگاری نیمه‌کوانتومی یکی از کاربران مجهز به عملیات کاملاً کوانتومی و کاربر دیگر تنها محدود به انجام عملیات کاملاً کلاسیکی است. در رمزنگاری نیمه‌کوانتومی نسبت به رمزنگاری کوانتومی بار محاسباتی کاربران و همچنین هزینه دستگاه‌های سخت‌افزاری کوانتومی در پیاده‌سازی عملی کاهش می‌یابد. در این مقاله یک طرح تسهیم راز نیمه‌کوانتومی ارائه شده است که کاربر کوانتومی (فرستنده) آلیس می‌خواهد یک پیام معین را با دو کاربر کلاسیکی (گیرنده) باب و چارلی به اشتراک بگذارد. کاربران به تنهایی نمی‌توانند به پیام معین دسترسی پیدا کنند و باید برای دسترسی به آن با یکدیگر همکاری کنند. در پروتکل‌های تسهیم راز نیمه‌کوانتومی گیرنده‌ها معمولا نیاز به اندازه‌گیری و ساخت کیوبیت جدید در پایه کلاسیک $\{|0\rangle, |1\rangle\}$ دارند و فرستنده معمولا نیاز به حافظه کوانتومی دارد. در این مقاله یک پروتکل تسهیم راز نیمه‌کوانتومی با استفاده از مخابره از راه دور کوانتومی پیشنهاد شده و امنیت آن در برابر انواع حمله‌های دشمن بررسی شده است. بر خلاف پروتکل‌های قبلی تسهیم راز نیمه‌کوانتومی، در پروتکل پیشنهادی، فرستنده نیاز به حافظه کوانتومی و گیرنده‌ها نیاز به تولید کیوبیت جدید ندارند. همچنین از آنجا که پروتکل پیشنهادی مبتنی بر مخابره از راه دور کوانتومی است، کیوبیت حامل اطلاعات بر روی کانال ارسال نمی‌گردد.

۱ مقدمه

تسهیم راز[1] یک ابزار مفید در ارتباطات امن کلاسیک است. در تسهیم راز، فرستنده یک پیام مخفی را میان n گیرنده توزیع می‌کند، بطوریکه گیرنده‌ها فقط با همکاری همدیگر می‌توانند آن پیام مخفی را بازیابی کنند. در تسهیم راز، فرستنده نگران است که یکی از گیرنده‌ها ناصادق باشد. به همین دلیل پیام‌ها را به طور مستقیم برای گیرنده‌ها نمی‌فرستد،

[1] Secret Sharing

★داوری اولیه‌ی این مقاله توسط کمیته علمی بیست و دومین کنفرانس بین‌المللی انجمن رمز و داوری نهایی آن توسط گروه دبیران دوفصل‌نامه علمی منادی افتا انجام شده است.

*نویسنده مسئول.
آدرس‌های رایانامه: mohammad.bolokian@semnan.ac.ir (محمد بلوکیان)، m.hooshmand@imamreza.ac.ir (منیره هوشمند)

بلکه آن را به چند قسمت رمزشده تقسیم کرده، هر یک از آن قسمت‌های رمزشده را برای یکی از گیرنده‌ها ارسال می‌کند. گیرنده‌ها فقط در صورتی که با هم همکاری کنند می‌توانند به پیام محرمانه دست یابند [۱–۳]. یکی از پراهمیت‌ترین شاخه‌های رمزنگاری [۱] کوانتومی، تسهیم راز کوانتومی [۲] است که مکانیک کوانتومی را با رمزنگاری کلاسیک ترکیب می‌کند.

۲ پیشینه تحقیق

هیلری [۳] و همکاران، اولین پروتکل تسهیم راز کوانتومی را با استفاده از حالات سه کیوبیتی [۴] درهم‌تنیده [۵] GHZ [۶] در سال ۱۹۹۹ ارائه دادند [۴]. کارلسون [۷] و همکاران، یک طرح تسهیم راز کوانتومی مبتنی بر حالات Bell [۸] [۵] و گائو [۹] و همکاران، یک طرح تسهیم راز بدون حالت درهم‌تنیده را ارائه کردند [۶]. شیئو [۱۰] و همکاران، طرح هیلاری را به n نفر گسترش دادند و کارایی و بازدهی آن را بهبود بخشیدند [۷]. زانگ [۱۱] و همکاران، یک طرح تسهیم راز کوانتومی مبتنی بر جابه‌جایی درهم‌تنیدگی حالات Bell پیشنهاد دادند [۸].

به طور کلی پژوهش‌های انجام شده در زمینه تسهیم راز کوانتومی را می‌توان به دو گروه عمده تقسیم کرد: گروهی که به تسهیم راز کوانتومی پیام‌های کلاسیک پرداخته‌اند و گروهی که به تسهیم راز کوانتومی اطلاعات کوانتومی پرداخته‌اند و در آن‌ها راز، یک حالت نامعلوم دلخواه به صورت کیوبیت می‌باشد [۹–۱۹].

در پروتکل‌های تسهیم راز کوانتومی، تمام کاربران باید دارای قابلیت انجام عملیات کوانتومی و مجهز به منابع کوانتومی باشند. اگرچه همیشه لازم نیست که هر کاربر مجهز به قابلیت‌های تمام‌کوانتومی برای پردازش اطلاعات باشد. در سال ۲۰۰۷، بویر [۱۲] و همکاران، اولین پروتکل توزیع کلید نیمه‌کوانتومی [۱۳] که در آن گیرنده دارای قابلیت کلاسیک یا نیمه‌کوانتومی [۱۴] است را ارائه کرد. اصطلاح نیمه‌کوانتومی بیان می‌کند که یکی از کاربران قانونی محدود به انجام عملیات کاملاً کلاسیک شامل آماده کردن و اندازه‌گیری کیوبیت‌ها در پایه کلاسیک $\{|0\rangle, |1\rangle\}$ می‌باشد [۲۰]. در پروتکل‌های تسهیم راز نیمه‌کوانتومی [۱۵] (SQSS)، راز می‌تواند به دو صورت نامعین (از پیش تعریف نشده) و معین (از پیش تعریف شده) باشد.

در سال ۲۰۱۰، لی [۱۶] و همکاران اولین پروتکل تسهیم راز نیمه‌کوانتومی را با استفاده از حالات سه کیوبیتی درهم‌تنیده GHZ-LIKE پیشنهاد کردند [۲۱]. در سال ۲۰۱۱، لین [۱۷] و همکاران نشان دادند در مرحله بررسی استراق سمع طرح ارائه شده در مرجع [۲۱] دام‌های امنیتی وجود دارد که می‌تواند منجر به حمله قطع و ارسال مجدد [۱۸] و حمله‌ی اسب تروجان [۱۹] شده و باعث فاش شدن کلید شود که این با الزامات امنیتی تسهیم راز تناقض دارد. همچنین دو راه حل برای پیشگیری از این حادثه امنیتی پیشنهاد شده و همچنین یک طرح بهبود یافته ارائه دادند [۲۲].

در سال ۲۰۱۲، Wang و همکاران یک پروتکل تسهیم راز نیمه‌کوانتومی سه کاربره با استفاده از حالات دو کیوبیتی درهم‌تنیده ارائه کردند که به یک کاربر کوانتومی اجازه می‌دهد یک راز را با دو کاربر کلاسیک به اشتراک بگذارد [۲۳]. در سال ۲۰۱۳، Li و همکاران یک پروتکل تسهیم راز نیمه‌کوانتومی سه کاربره پیشنهاد دادند که به جای استفاده از حالات درهم‌تنیده از حالت‌های غیر درهم‌تنیده استفاده می‌کند و همچنین یک طرح چند کاربره از طرح مرجع [۲۱] ارائه کردند [۲۴]. همچنین در سال ۲۰۱۳، Yang و همکاران طرح ارائه شده در مرجع [۲۴] را بهبود دادند و نشان دادند بازدهی کیوبیت‌ها در پروتکل ارائه شده بیشتر از طرح مرجع [۲۴] می‌باشد [۲۵].

در سال ۲۰۱۷، Yu و همکاران یک طرح تسهیم راز نیمه‌کوانتومی چند کاربره پیشنهاد دادند که به یک کاربر کوانتومی (مدیر) اجازه می‌دهد یک راز را میان چندین کاربر کلاسیکی بر اساس حالت‌های GHZ-LIKE به اشتراک بگذارد [۲۶]. در سال ۲۰۱۷، Wang و همکاران یک طرح تسهیم راز نیمه‌کوانتومی مبتنی بر حالات Bell ارائه کردند [۲۷]. در سال ۲۰۱۸، Gao و همکاران طرح ارائه شده در مرجع [۲۷] را بررسی کردند و دو مشکل از طرح ارائه شده گرفتند: اول اینکه این طرح نمی‌تواند وظیفه تسهیم راز نیمه‌کوانتومی را به سرانجام برساند و دوم اینکه در آن طرح حفره امنیتی وجود دارد و این بدین معنی نیست که نمی‌تواند شرکت کننده متقلب را تشخیص دهد، بلکه بدین معنی است که یکی از گیرنده‌ها برروی کانال کوانتومی حمله می‌کند و سعی بر تنهایی به دست آوردن راز آلیس دارد [۲۸]. در سال ۲۰۱۸، Chen و همکاران طرح ارائه شده در مرجع [۲۷] را بررسی کردند و دریافتند که این طرح امن نیست و از حمله قطع و ارسال مجدد رنج می‌برد. آنها یک طرح بهبود یافته را ارائه دادند و همچنین آن طرح را به چند کاربره گسترش دادند و سپس یک استراتژی بهبود یافته مبتنی بر توزیع کلید نیمه‌کوانتومی ارائه کردند برای اینکه تضمین کند که طرح جدید مقاوم است در برابر حمله‌ای که پیشنهاد کرده بودند [۲۹].

در سال ۲۰۱۸، Yin و همکاران یک طرح جدید از تسهیم راز نیمه‌کوانتومی ارائه دادند که از حالت درهم‌تنیده دوذره‌ای

$$|\phi\rangle = X_i(|{+}{+}\rangle + |{-}{-}\rangle) + Y_i(|{+}{+}\rangle - |{-}{-}\rangle)$$

که $X_i^2 + Y_i^2 = \frac{1}{2}$، برای به اشتراک گذاری یک پیام نامعین استفاده می‌کند و همچنین در این مرجع ثابت شد که طرح ارائه شده می‌تواند در برابر انواع استراق سمع کننده [۲۰] مقاومت کند [۳۰]. همچنین در سال ۲۰۱۸، Li و همکاران یه طرح جدید تسهیم راز نیمه‌کوانتومی با استفاده از منبع محدود ارائه کردند [۳۱]، که تفاوت این طرح‌ها در مرحله بررسی استراق سمع و امنیت آنها و همچنین استفاده از حالت‌های درهم‌تنیده متفاوت برای اشتراک‌گذاری راز نامشخص می‌باشد.

[1] Cryptography [2] Quantum secret sharing [3] Hillery [4] Qubit [5] Entanglened [6] Greenberger–Horne–Zeilinger [7] Karlsson [8] Bell State [9] Guo [10] Xiao [11] Zhang [12] Boyer [13] Quantum Key Distribution [14] Semi Quantum [15] Quntum Secret Sharing [16] Li [17] Lin [18] Intercept-resend attack [19] Trojan horse attack

[20] Eve

در پروتکل‌های تسهیم راز همانطور که گفتیم راز می‌تواند معین و قبل از انجام پروتکل مشخص شده باشد که یا صفر است یا یک و آخر پروتکل گیرنده‌ها به این صفر یا یک که از قبل تعیین شده دسترسی پیدا می‌کنند. اولین پروتکل در سال ۲۰۱۵، توسط Xie و همکاران با استفاده از حالت‌های سه کیوبیتی درهم‌تنیده که یک پیام معین را بین گیرنده‌ها به اشتراک می‌گذارد پیشنهاد شد [۳۲]. در سال ۲۰۱۶، Yin و همکاران با استفاده از استراتژی حمله قطع و ارسال مجدد ثابت کردند طرح ارائه شده در مرجع [۳۲]، برای یک شرکت‌کننده متقلب امن نیست و همچنین یک طرح بهبود یافته مبتنی بر حالات GHZ پیشنهاد کردند. که این طرح بهبود یافته امن می‌باشد [۳۳]. همچنین در سال ۲۰۱۷، Gao و همکاران مرجع [۳۳] را آنالیز کردند و اثبات کردند که دارای مشکلات زیادی است و همچنین یک طرح تسهیم راز نیمه‌کوانتومی بهبود یافته ارائه کردند که امن‌تر و کاراتر می‌باشد [۳۴]. تفاوت این طرح‌ها در مرحله بررسی استراق سمع و امنیت آنها می‌باشد. در سال ۲۰۲۰، Zhou با هدف کاهش مصرف منابع و ساده‌سازی اجرای عملی، پروتکلی بهینه‌سازی‌شده برای تسهیم راز نیمه‌کوانتومی ارائه داد که تنها بر روی بیت‌های خاص اعمال عملیات کوانتومی می‌کرد و با حفظ امنیت در برابر حملات رایج، بازده عملیاتی بالایی را ممکن ساخت [۳۵].

در سال ۲۰۲۱، Tian و همکاران پروتکلی کارآمد برای تسهیم راز نیمه‌کوانتومی ارائه دادند که با بهره‌گیری از بیت‌های خاص انتخاب‌شده، توانست بازده کوبیتی را افزایش داده و با حفظ سادگی عملیاتی، امنیت پروتکل را در برابر حملات متداول تضمین کند [۳۶]. در یکی از جدیدترین مطالعات، He و همکاران در سال ۲۰۲۴ با تمرکز بر تحلیل امنیتی پروتکل‌های SQSS مبتنی بر بیت‌های خاص، نشان دادند که برخی از طرح‌های موجود در برابر حملات پیشرفته مانند جایگزینی تطبیقی و دستکاری شرکت‌کننده مخرب آسیب‌پذیرند. آن‌ها با بررسی دقیق پروتکل Tian [۳۶] و سایر ساختارهای مشابه، نقاط ضعف عملی را استخراج کرده و نسخه‌ای بهبودیافته با سازوکارهای تشخیص خطا، رمزگذاری تقویتی، و کنترل پایه‌ای تصادفی پیشنهاد دادند. نتایج تحلیل نشان داد که طرح پیشنهادی نه‌تنها امنیت بالاتری دارد، بلکه با حفظ محدودیت‌های نیمه‌کوانتومی، کارایی عملیاتی آن نیز قابل قبول باقی مانده است [۳۷].

در سال ۲۰۲۳، Xing و همکاران پروتکلی کارآمد برای اشتراک‌گذاری راز نیمه‌کوانتومی مبتنی بر حالات تک ذره‌ای پیشنهاد دادند که علاوه بر سادگی اجرا، کارایی بالایی در انتقال اطلاعات محرمانه دارد [۳۸]. Gao در سال ۲۰۲۴ با تحلیل رمزنگاری پروتکل ارائه شده توسط Xing و همکاران [۳۸]، آسیب‌پذیری‌ها و نقاط ضعف امنیتی آن را شناسایی کرد و نشان داد که این پروتکل نیازمند بهبودهایی برای تضمین امنیت کامل است [۳۹].

Zhou و همکاران در سال ۲۰۲۳، پروتکل آستانه‌ای (t,n) برای اشتراک‌گذاری راز نیمه‌کوانتومی بر پایه ذرات تک را معرفی کردند که امکان تعیین تعداد مشارکت‌کنندگان برای بازسازی راز را فراهم می‌کند و انعطاف‌پذیری پروتکل را افزایش می‌دهد [۴۰]. Li و همکاران در سال ۲۰۲۴، پروتکل نوین SQSS چندطرفه‌ای مبتنی بر حالات درهم‌تنیده M-ذره‌ای پیشنهاد دادند که شرکت‌کنندگان کلاسیک تنها به اندازه‌گیری در مبنای Z و انجام عملیات هادامارد محدود هستند. با بهره‌گیری از ویژگی کوانتومی بین حالات Bell و عملیات هادامارد[1] برای شناسایی جاسوس‌ها، پروتکل در برابر حملات CNOT دوگانه و Trojan horse مقاوم بوده و ساختاری کاملاً یک‌طرفه، بهره‌وری کوبیت بالا و کنترل محتوای راز توسط Alice را فراهم می‌کند [۴۱].

He و همکاران در سال ۲۰۲۵، یک پروتکل چندطرفه[2] SQSS مبتنی بر حالات تک ذره‌ای ارائه شده است که ذرات فریب‌دهنده همزمان برای حمل اطلاعات محرمانه و تشخیص جاسوسی استفاده می‌شوند، بهره‌وری کیوبیت آن ۱۰۰٪ است و اطلاعات محرمانه به صورت مشترک توسط همه شرکت‌کنندگان تعیین می‌شود، که امنیت و کارایی بالایی را نسبت به پروتکل‌های پیشین فراهم می‌کند [۴۲].

در این مقاله، با استفاده از مخابره از راه دور کوانتومی یک پروتکل SQSS جدید با استفاده از حالت چهار کیوبیتی متقارن با حداکثر درهم‌تنیدگی ارائه شده است که در آن کاربر کوانتومی یک پیام معین را بین دو کاربر کلاسیک به اشتراک می‌گذارد. در این طرح، فرستنده نیاز به حافظه کوانتومی و گیرنده‌ها نیاز به تولید کیوبیت جدید ندارند. همچنین از آنجا که طرح پیشنهادی مبتنی بر مخابره از راه دور کوانتومی است، کیوبیت حامل اطلاعات بر روی کانال ارسال نمی‌گردد و با استفاده از قاعده درهم‌تنیدگی و مخابره از راه دور کوانتومی به تسهیم راز پرداخته می‌شود.

۳ شرح پروتکل

در پروتکل تسهیم راز نیمه‌کوانتومی ارائه شده، سه شرکت‌کننده به نام‌های آلیس، باب و چارلی حضور دارند. در این پروتکل، آلیس، به عنوان فرستنده، دارای قابلیت کوانتومی است و باب و چارلی به عنوان دو گیرنده فقط محدود به انجام عملیات کلاسیک هستند. طبق پروتکل، آلیس می‌خواهد یک راز یک بیتی را بین دو گیرنده به اشتراک بگذارد، به گونه‌ای که کاربران با همکاری یکدیگر بتوانند این راز را آشکار کنند و به تنهایی نتوانند به راز دسترسی پیدا کنند.

در این پروتکل به هیچ وجه اطلاعات اصلی منتقل نمی‌شود و با استفاده از قاعده درهم‌تنیدگی و مخابره از راه دور کوانتومی به انتقال راز پرداخته می‌شود. همین موضوع بر اهمیت و امنیت آن پروتکل می‌افزاید.

۱.۳ تعیین راز

در این مرحله، آلیس راز یک بیتی خود را مشخص می‌کند، که می‌تواند صفر یا یک باشد. بر اساس راز تعیین شده توسط آلیس، این کاربر بر اساس جدول ۱، یک حالت دو کیوبیتی که شامل کیوبیت‌های a_1 و a_2 هستند تولید می‌کند. این حالات به هیچ وجه ارسال نمی‌شوند و در دست

[1] Hadamard [2] Multi-party

آلیس باقی می‌مانند.

جدول ۱. اطلاعات کلید آلیس

راز تعیین شده آلیس	حالت ساخته شده توسط آلیس
K_A	$\|\phi\rangle_{a_1a_2}$
۰	$\|00\rangle$
	$\|11\rangle$
۱	$\|01\rangle$
	$\|10\rangle$

۲.۳ تشکیل کانال

در این مرحله، آلیس کانال مورد استفاده در این پروتکل را تشکیل می‌دهد. این کانال ۴ کیوبیتی به صورت زیر است:

$$|\phi\rangle_{A_1A_2BC} = \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle) \quad (1)$$

که در آن، کیوبیت‌های A_1 و A_2 متعلق به آلیس و کیوبیت‌های B و C به ترتیب متعلق به باب و چارلی هستند. به عبارت دیگر، قرار است کیوبیت‌های B و C در ابتدای پروتکل برای باب و چارلی ارسال شوند. پس از آن، آلیس یک رشته n-تایی از کانال ۴ کیوبیتی بالا را تولید می‌کند که همانند قبل آلیس دو کیوبیت اول هرکدام از این کانال‌ها را برای خودش نگه می‌دارد و کیوبیت‌های سوم و چهارم را به صورت رشته کیوبیت‌های با نام‌های S_B و S_C به ترتیب برای باب و چارلی ارسال می‌کند.

حال به بررسی حالت کامل سیستم در انتشار یک حالت از n حالت کانال مورد نظر پرداخته می‌شود. با توجه به انتخاب راز توسط آلیس و تعیین کیوبیت‌های a_1 و a_2 بر اساس راز انتخابی، حالت کامل سیستم به صورت زیر خواهد بود:

$$|\phi\rangle_{a_1a_2A_1A_2BC} = |\phi\rangle_{a_1a_2} \otimes |\phi\rangle_{A_1A_2BC} \quad (2)$$
$$|\phi\rangle_{a_1a_2} = |00\rangle \Rightarrow |\phi\rangle_{a_1a_2A_1A_2BC} = |000000\rangle + |000101\rangle + |001010\rangle + |001111\rangle$$
$$|\phi\rangle_{a_1a_2} = |11\rangle \Rightarrow |\phi\rangle_{a_1a_2A_1A_2BC} = |110000\rangle + |110101\rangle + |111010\rangle + |111111\rangle$$
$$|\phi\rangle_{a_1a_2} = |01\rangle \Rightarrow |\phi\rangle_{a_1a_2A_1A_2BC} = |010000\rangle + |010101\rangle + |011010\rangle + |011111\rangle$$
$$|\phi\rangle_{a_1a_2} = |10\rangle \Rightarrow |\phi\rangle_{a_1a_2A_1A_2BC} = |100000\rangle + |100101\rangle + |101010\rangle + |101111\rangle$$

۳.۳ اعمال CNOT

پس از ارسال کیوبیت‌ها توسط آلیس به سمت باب و چارلی و تعیین راز، آلیس بر روی کیوبیت‌های a_1، a_2، A_1 و A_2 عملگر CNOT را اعمال می‌کند، به این صورت که در آن، کیوبیت‌های a_1 و a_2 به عنوان کیوبیت‌های کنترل و A_1 و A_2 به عنوان کیوبیت‌های هدف هستند.

$$a_1 \xrightarrow{\text{CNOT}} A_1, \qquad a_2 \xrightarrow{\text{CNOT}} A_2 \quad (3)$$

هدف از اعمال CNOT، درهم‌تنیده کردن کیوبیت‌های a_1 و a_2 به ترتیب با کیوبیت‌های A_1 و A_2 است. با این کار، بین کیوبیت‌ها، ارتباطی پدید می‌آید که در ادامه از آن برای انتقال راز استفاده می‌شود.

حالت کل سیستم بعد از اعمال CNOT به شرح زیر است:

$$|\phi\rangle_{a_1a_2A_1A_2BC} = |000000\rangle + |000101\rangle + |001010\rangle + |001111\rangle$$
$$|\phi\rangle_{a_1a_2A_1A_2BC} = |111100\rangle + |111001\rangle + |110110\rangle + |110011\rangle$$
$$|\phi\rangle_{a_1a_2A_1A_2BC} = |010100\rangle + |010001\rangle + |011110\rangle + |011011\rangle$$
$$|\phi\rangle_{a_1a_2A_1A_2BC} = |101000\rangle + |101101\rangle + |100010\rangle + |100111\rangle \quad (4)$$

۴.۳ اندازه‌گیری Z روی A_1 و A_2

پس از اعمال CNOT توسط آلیس، روی کیوبیت‌های دست خودش، آلیس یک اندازه‌گیری دو کیوبیتی در پایه Z روی کیوبیت‌های A_1 و A_2 انجام می‌دهد. نتایج این اندازه‌گیری در جدول ۲ قابل مشاهده است. هدف از این اندازه‌گیری، شکسته شدن تمامی درهم‌تنیدگی‌های موجود در کیوبیت‌ها است. همچنین اطلاعات کیوبیت‌ها به نحوی جابجا می‌شود که در مراحل بعد بتوان به راز اصلی دست پیدا کرد.

۵.۳ اندازه‌گیری در پایه محاسباتی

همه کاربران روی کیوبیت‌های در دست خود در پایه محاسباتی اندازه‌گیری می‌کنند. بدین منظور، آلیس روی کیوبیت‌های a_1 و a_2 و باب و چارلی به ترتیب روی کیوبیت‌های B و C اندازه‌گیری می‌کنند. بدین ترتیب همه کیوبیت‌ها به بیت تبدیل شده و کاربران می‌توانند آن‌ها را خوانده و در کانال کلاسیک ایمن به اشتراک بگذارند.

۶.۳ انتشار اطلاعات کلاسیک

در این مرحله، آلیس، باب و چارلی، بیت‌های کلاسیک خود که از اندازه‌گیری در پایه محاسباتی روی کیوبیت‌های در دست خودشان به دست آورده‌اند، را در کانال کلاسیک ایمن به اشتراک می‌گذارند. پس از اشتراک‌گذاری این بیت‌های کلاسیک، طرفین می‌توانند با XOR کردن تمامی این بیت‌ها به راز آلیس دست پیدا کنند. این مرحله به طور کامل در جدول ۳ قابل مشاهده است.

$$\text{راز} = \text{بیت‌های آلیس} \oplus \text{بیت باب} \oplus \text{بیت چارلی} \quad (5)$$

جدول ۲. اطلاعات کلید آلیس

حالت پس از اندازه‌گیری آلیس روی A_1 و A_2	حالت a_1 و a_2 بر اساس راز انتخابی آلیس	حالت فروپاشی شده کیوبیت‌های B و C
$\|00\rangle$	$\|00\rangle$	$\|00\rangle$
	$\|11\rangle$	$\|11\rangle$
	$\|01\rangle$	$\|01\rangle$
	$\|10\rangle$	$\|10\rangle$
$\|01\rangle$	$\|00\rangle$	$\|01\rangle$
	$\|11\rangle$	$\|10\rangle$
	$\|01\rangle$	$\|11\rangle$
	$\|10\rangle$	$\|11\rangle$
$\|10\rangle$	$\|00\rangle$	$\|01\rangle$
	$\|11\rangle$	$\|01\rangle$
	$\|01\rangle$	$\|11\rangle$
	$\|11\rangle$	$\|01\rangle$
$\|11\rangle$	$\|00\rangle$	$\|11\rangle$
	$\|11\rangle$	$\|00\rangle$
	$\|01\rangle$	$\|10\rangle$
	$\|10\rangle$	$\|01\rangle$

طبق جدول ۳ راز آلیس به درستی و با همکاری تمام کاربران به دست گیرنده‌ها رسیده است.

۴ بررسی امنیت

در پروتکل مطرح شده، چون کیوبیت‌های حامل اطلاعات در کانال به صورت مستقیم منتقل نمی‌شوند، غیرممکن است که استراق سمع کننده (ایو [1]) بتواند کیوبیت‌های مذکور را در فرایند انتقال پیام جدا کند. ایو تنها در زمان ایجاد کانال کوانتومی و توزیع کانال بین کاربران می‌تواند حمله کند. و این یعنی اگر کانال امن باشد، اطلاعات با امنیت بی قید و شرط مبادله می‌شوند و نشت اطلاعاتی صورت نخواهد گرفت. بر همین اساس، برای اثبات امنیت این پروتکل کافی است، تنها امنیت کانال کوانتومی بررسی شود. حملاتی که در اینجا مد نظر قرارگرفته است، شامل حمله قطع و ارسال کیوبیت جدید [2]، حمله قطع و اندازه‌گیری کیوبیت [3] و حمله دستکاری پیام [4] می‌باشد.

آلیس یک جدول نشانی برای باب و چارلی ارسال کرده تا پس از شروع پروتکل، باب و چارلی هر عملی که روی کیوبیت خود انجام می‌دهند را طبق آن جدول با ارسال تنها یک بیت کلاسیک برای هر کیوبیت به آلیس اعلام کنند (جدول ۴).

زمانی که باب و چارلی بیت ۰ را ارسال می‌کنند، یعنی کیوبیت را

جدول ۳. بیت‌های به اشتراک گذاشته شده کاربران و تشکیل راز اولیه

راز آلیس	حالت a_1 و a_2 بر اساس راز	بیت‌های آلیس	بیت باب	بیت چارلی	نتیجه XOR
۰	$\|00\rangle$	۰, ۰	۰	۰	۰
		۰, ۱	۰	۱	۰
		۱, ۰	۱	۰	۰
		۱, ۱	۱	۱	۰
	$\|11\rangle$	۰, ۰	۱	۱	۰
		۰, ۱	۱	۰	۰
		۱, ۰	۰	۱	۰
		۱, ۱	۰	۰	۰
۱	$\|01\rangle$	۰, ۰	۰	۱	۱
		۰, ۱	۰	۰	۱
		۱, ۰	۱	۱	۱
		۱, ۱	۱	۰	۱
	$\|10\rangle$	۰, ۰	۱	۰	۱
		۰, ۱	۱	۱	۱
		۱, ۰	۰	۰	۱
		۱, ۱	۰	۱	۱

جدول ۴. اقدامات آلیس بر اساس بیت‌های ارسالی باب و چارلی

بیت ارسالی باب	بیت ارسالی چارلی	عمل باب	عمل چارلی	عمل آلیس بر اساس بیت‌های دریافتی
۰	۰	بازتاب	بازتاب	چک کردن کیوبیت‌ها
۰	۱	بازتاب	اندازه‌گیری	اندازه‌گیری کیوبیت چارلی و چک کردن کیوبیت‌ها
۱	۰	اندازه‌گیری	بازتاب	اندازه‌گیری کیوبیت باب چک کردن کیوبیت‌ها
۱	۱	اندازه‌گیری کیوبیت در پایه محاسباتی	اندازه‌گیری کیوبیت در پایه محاسباتی	اشتراک گذاری راز

بدون اعمال اندازه‌گیری بازتاب کرده‌اند و زمانی که بیت ۱ را ارسال می‌کنند، یعنی در پایه محاسباتی اندازه‌گیری کرده‌اند.

آلیس برای چک کردن کانال دو عمل را انجام می‌دهد، که این دو عمل

[1] Eve [2] Intercept-and-replace attack [3] Intercept-and-measure attack
[4] Message modification attack

به صورت تصادفی بر روی رشته کیوبیت‌های S_{CH} انجام می‌شود. از ۳ حالت اول جدول ۴، آلیس برای چک کردن کانال و از حالت آخر برای اشتراک گذاری راز استفاده می‌کند. زمانی‌که کاربران حالت ۰۱، یعنی حالت بازتاب، اندازه‌گیری را انجام می‌دهند کیوبیتی که بر پایه محاسباتی اندازه‌گیری شده، به همراه کیوبیت متناظر با آن که در دست آلیس است، تنها می‌توانند در پایه Z چک شوند. کیوبیت‌های A_1 با B و A_2 با C متناظر هستند. به عبارتی این کیوبیت‌ها با هم درهم تنیده هستند. حال فرض می‌کنیم که کاربران هر دو کیوبیت خود را بازتاب کرده و به آلیس بیت صفر را اعلام می‌کنند.

روش اول: آلیس بر روی کیوبیت‌های A_1 و A_2 اندازه‌گیری در پایه محاسباتی انجام می‌دهد. نتایج این اندازه‌گیری به صورت جدول ۵ است.

جدول ۵. اندازه‌گیری آلیس روی A_1 و A_2 در پایه Z

نتیجه اندازه‌گیری آلیس روی A_1 و A_2	حالت فروپاشی شده کیوبیت‌های B و C
۰۰	$\|۰۰\rangle$
۰۱	$\|۰۱\rangle$
۱۰	$\|۱۰\rangle$
۱۱	$\|۱۱\rangle$

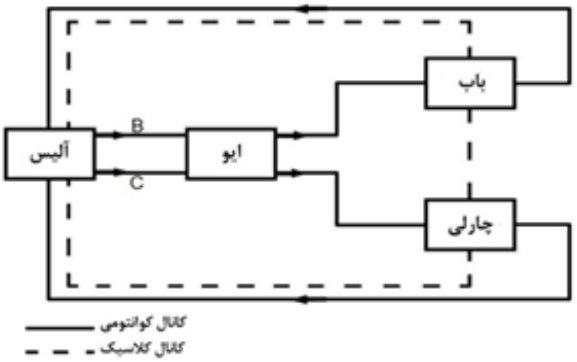
همانطور که در جدول ۵ مشاهده می‌شود، پس از اندازه‌گیری آلیس بر روی کیوبیت‌های A_1 و A_2 در پایه محاسباتی، کیوبیت‌های B و C به یک حالت خاص تغییر پیدا می‌کنند. پس از آن آلیس روی کیوبیت‌های B و C یک اندازه‌گیری در پایه محاسباتی انجام می‌دهد، آنگاه آلیس به نتایج دو اندازه‌گیری می‌نگرد. اگر نتیجه اندازه‌گیری همان حالت خاصی که در جدول آمده شد، کانال از حمله در امان بوده است، در غیر این صورت حمله ای رخ داده است.

روش دوم: آلیس کیوبیت‌های A_1 و A_2 را در پایه X، $\{|+\rangle, |-\rangle\}$ اندازه‌گیری می‌کند. نتایج اندازه‌گیری به صورت جدول ۶ است.

جدول ۶. اندازه‌گیری آلیس روی A_1 و A_2 در پایه X

نتیجه اندازه‌گیری آلیس روی A_1 و A_2	حالت فروپاشی شده کیوبیت‌های B و C
++	$\|++\rangle$
+−	$\|+-\rangle$
−+	$\|-+\rangle$
−−	$\|--\rangle$

همانطور که در جدول ۶ مشاهده می‌شود، همانند حالت اول، پس از اندازه‌گیری آلیس بر روی کیوبیت‌های B و C در پایه X، کیوبیت‌های B و C به یک حالت خاص تغییر پیدا می‌کنند. پس از آن آلیس روی کیوبیت‌های B و C یک اندازه‌گیری در پایه X انجام می‌دهد، آنگاه آلیس به نتایج دو اندازه‌گیری می‌نگرد. اگر نتیجه اندازه‌گیری همان حالت خاصی که در جدول آمده شد، کانال از حمله در امان بوده است در غیر این صورت حمله ای رخ داده است.



شکل ۱. نحوه دخالت دشمن در پروتکل

حال به بررسی امنیت با وجود دشمن می‌پردازیم. حضور دشمن در این پروتکل به صورت شکل ۱ است، چون حمله دشمن در مسیر برگشت کیوبیت‌ها مانند حمله دشمن در مسیر رفت کیوبیت‌ها از آلیس به باب و چارلی می‌باشد از بررسی آن صرف نظر کردیم.

انواع حملاتی که بررسی کردیم به صورت جدول ۷ می‌باشد.

جدول ۷. اندازه‌گیری آلیس روی A_1 و A_2 در پایه X

حمله مرد میانی	حمله قطع و اندازه‌گیری کیوبیت‌ها	حمله قطع و ارسال کیوبیت جدید
		اندازه‌گیری دشمن در پایه Z و Z
		اندازه‌گیری دشمن در پایه X و X
		اندازه‌گیری دشمن در پایه Bell
		اندازه‌گیری دشمن در پایه X و Z
		اندازه‌گیری دشمن در پایه Z و X
حمله پیام دستکاری		اعمال CNOT از روی کیوبیت‌های دشمن
		اعمال CNOT از روی کیوبیت‌های کاربران

۱.۴ حمله قطع و ارسال کیوبیت جدید

در این نوع حمله با توجه به اینکه کیوبیت‌های آلیس، باب و چارلی در کانال متقارن هستند، هرگونه تغییر در کیوبیت‌ها توسط دشمن به راحتی با چک کردن کانال به دو روش مشخص می‌شود. فرض می‌کنیم که کیوبیت‌های جدید دشمن به صورت زیر می‌باشد.

$$|\phi\rangle = a_0 |۰۰\rangle + a_1 |۰۱\rangle + a_2 |۱۰\rangle + a_3 |۱۱\rangle \qquad (۶)$$

۱.۱.۴ بازتاب-بازتاب

در این حالت دو گیرنده کیوبیت‌های در دست خود را بدون هیچ گونه دستکاری به آلیس بازتاب کردند. در ابتدا فرض می‌کنیم آلیس امنیت کانال را به روش اول چک کند یعنی آلیس روی کیوبیت‌های A_1 و A_2 اندازه‌گیری در پایه محاسباتی انجام می‌دهد و یکی از ۴ حالت ۰۰، ۰۱، ۱۰ و ۱۱ را به دست می‌آورد. و در هر یک از این حالات کیوبیت‌های B و C به $|۰۰\rangle$، $|۰۱\rangle$، $|۱۰\rangle$ و $|۱۱\rangle$

تغییر حالت می‌دهد. سپس آلیس کیوبیت‌های B و C را در پایه کلاسیک اندازه‌گیری می‌کند و این حالات به ترتیب با احتمال $|a_0|^2$، $|a_1|^2$، $|a_2|^2$ و $|a_3|^2$ رخ می‌دهند. اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2، ۰۰ و روی کیوبیت‌های B و C، ۰۰ باشد در اینصورت دشمن آشکار نمی‌شود و احتمال پی بردن به وجود دشمن در این حالت $1-|a_0|^2$ می‌باشد، ولی اگر نتیجه اندازه گیری آلیس روی کیوبیت‌های B و C یکی از ۳ حالت ۰۱، ۱۰، ۱۱ باشد دشمن آشکار می‌شود. در بقیه نتایج اندازه‌گیری آلیس مشابه همین حالت دشمن آشکار می‌شود. در این حمله اگر ضریب کیوبیت‌های دشمن متقارن باشد، دشمن با احتمال ٪۷۵ آشکار می‌شود. اگر آلیس امنیت کانال را به روش دوم چک کند، یعنی آلیس روی کیوبیت‌های A_1 و A_2 در پایه X، $\{|+\rangle, |-\rangle\}$ اندازه‌گیری انجام دهد، یکی از ۴ حالت $++$، $+-$، $-+$ و $--$ را به دست می‌آورد. و در هر یک از این حالات کیوبیت‌های B و C به $|++\rangle$، $|+-\rangle$، $|-+\rangle$ و $|--\rangle$ تغییر حالت می‌دهد. در این حالت مشابه حالت قبل اگر ضریب کیوبیت‌های دشمن متقارن باشد دشمن با احتمال ٪۷۵ آشکار می‌شود.

۲.۱.۴ بازتاب-اندازه‌گیری

در این حالت باب کیوبیت خود را بازتاب کرده و چارلی کیوبیت خود را در پایه کلاسیک اندازه‌گیری می‌کند. کیوبیتی که در پایه محاسباتی اندازه‌گیری شده، به همراه کیوبیت متناظر در دست آلیس، تنها می‌توانند در پایه Z چک شوند. کیوبیت‌های A_1 با B و A_2 با C متناظر هستند. در این حالت اگر آلیس کانال را به روش اول چک کند چون کیوبیت B و کیوبیت متناظر با آن یعنی A_1 در پایه کلاسیک اندازه‌گیری شدند آلیس روی کیوبیت A_2 و C در پایه کلاسیک اندازه‌گیری می‌کند. پس این حالت مشابه حالت بازتاب بازتاب زمانی که آلیس کانال را به روش اول چک کرده بود. پس در این هم اگر ضریب کیوبیت‌های دشمن متقارن باشد، دشمن با احتمال ٪۷۵ آشکار می‌شود. حال فرض می‌کنیم آلیس امنیت کانال را به روش دوم چک کند. چون کیوبیت B توسط باب و کیوبیت متناظر با آن یعنی A_1 در پایه کلاسیک اندازه‌گیری شدند، در این حالت آلیس کیوبیت‌های A_2 و C را در پایه X اندازه‌گیری می‌کند. نتایج اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+0$، $+1$، -0 و -1 می‌باشد. و در هر یک از این نتیجه اندازه‌گیری روی کیوبیت‌های B و C به صورت $+0$، $+1$، -0 و -1 می‌شود و این حالات به ترتیب با احتمال $|a_0|^2$، $|a_1|^2$، $|a_2|^2$ و $|a_3|^2$ رخ می‌دهند. اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2، $+0$ و روی کیوبیت‌های B و C، $+0$ باشد، در این صورت دشمن آشکار نمی‌شود و احتمال پی بردن به وجود دشمن در این حالت $1-|a_0|^2$ می‌باشد؛ ولی اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C یکی از ۳ حالت $+1$، -0 و -1 باشد دشمن آشکار می‌شود. در بقیه نتایج اندازه‌گیری آلیس مشابه همین حالت دشمن آشکار می‌شود. در این حمله اگر ضریب کیوبیت‌های دشمن متقارن باشد دشمن با احتمال ٪۷۵ آشکار می‌شود.

حالت اندازه‌گیری، بازتاب کاملا مشابه حالت بازتاب، اندازه‌گیری است.

پس اگر ضرایب حالت دشمن را متقارن فرض کنیم، در حمله قطع و ارسال کیوبیت جدید، احتمال آشکارسازی دشمن در تمامی حالات ٪۷۵ می‌باشد.

$$P_1 = \frac{1}{6}(0.75+0.75+0.75+0.75+0.75+0.75) = 0.75 \quad (7)$$

۲.۴ حمله قطع و اندازه‌گیری کیوبیت‌ها

دشمن کیوبیت‌های ارسالی آلیس به باب و چارلی را قطع می‌کند و آن کیوبیت‌ها را در پایه‌های ZZ، XX، ZX، XZ و Bell اندازه‌گیری می‌کند و بعد از اندازه‌گیری، کیوبیت‌ها را برای باب و چارلی می‌فرستد. اندازه‌گیری دشمن در تمام پایه‌ها در ادامه بررسی شده است.

۱.۲.۴ اندازه‌گیری دشمن در پایه Z

دشمن کیوبیت‌های ارسالی آلیس به باب و چارلی را قطع می‌کند و آن کیوبیت‌ها را در پایه محاسباتی اندازه‌گیری می‌کند و سپس آن‌ها را برای باب و چارلی می‌فرستد. اقدام دشمن به صورت جدول ۸ است.

جدول ۸. اندازه‌گیری دشمن در پایه Z

نتیجه اندازه‌گیری دشمن روی B و C	حالت فروپاشی شده کیوبیت‌های A_1 و A_2
۰۰	$\|00\rangle$
۰۱	$\|01\rangle$
۱۰	$\|10\rangle$
۱۱	$\|11\rangle$

الف- بازتاب بازتاب: در این حالت هر دو کاربر کلاسیک کیوبیت را بازتاب کرده‌اند. اگر آلیس کانال را به روش اول چک کند، چون نتایج اندازه‌گیری دشمن روی کیوبیت‌های B و C به صورت ۰۰، ۰۱، ۱۰ و ۱۱ می‌باشد و چون در هر یک از حالات نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 و همچنین B و C هم مانند اندازه‌گیری دشمن است، آلیس متوجه حضور دشمن نمی‌شود؛ چرا که کیوبیت‌ها پس از اندازه‌گیری توسط دشمن به یکی از نتایج مورد دلخواه آلیس تغییر می‌کنند و نتایج اندازه‌گیری آلیس هم همین حالات هستند. به عنوان نمونه، زمانی که نتیجه اندازه‌گیری دشمن روی کیوبیت‌های B و C، ۰۰ باشد، نتیجه اندازه‌گیری آلیس هم روی کیوبیت‌های A_1 و A_2 با احتمال ٪۱۰۰، ۰۰ می‌باشد و همچنین نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C هم ۰۰ می‌باشد. پس در این حالت کانال را نمی‌توان به روش اول چک کرد. حال به بررسی کانال به روش دوم می‌پردازیم. چون دشمن در پایه محاسباتی روی کیوبیت‌های باب و چارلی اندازه‌گیری کرده و سپس آن کیوبیت‌ها را برای آن‌ها می‌فرستد؛ باب و چارلی هم عینا آن کیوبیت‌ها را برای آلیس می‌فرستند. اگر آلیس کانال را به روش دوم چک کند، یعنی روی کیوبیت‌های A_1 و A_2 در پایه X، اندازه‌گیری انجام دهد در این

حالت آلیس با احتمال ٪۷۵ به وجود دشمن پی می‌برد. به عنوان نمونه، زمانی که نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2، $|{++}\rangle$ باشد، نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C احتمالاتی و با احتمال ٪۲۵ یکی از حالات $++$، $-+$، $+-$ و $--$ می‌شود و از این ۴ حالت تنها زمانی که نتیجه $++$ باشد حضور دشمن آشکار نمی‌شود. پس با احتمال ٪۷۵ حضور دشمن آشکار می‌شود.

ب- بازتاب اندازه‌گیری: باب کیوبیت خود را بازتاب و چارلی کیوبیت خود را اندازه‌گیری می‌کند. در این حالت آلیس پس از دریافت کیوبیت‌ها از باب و چارلی، روی کیوبیت A_1 با B اندازه‌گیری Z انجام می‌دهد. ابتدا به روش اول کانال چک می‌شود، در این حالت آلیس نمی‌تواند به وجود دشمن پی ببرد چرا که نتایج اندازه‌گیری دشمن زیر مجموعه نتایج دلخواه آلیس است. این حالت کاملا مشابه حالت چک کردن آلیس به روش اول در حالت بازتاب بازتاب می‌باشد. اگر آلیس کانال را به روش دوم چک کند، می‌تواند روی کیوبیت‌های A_1 و B کانال در پایه X و روی A_2 و C در پایه Z اندازه‌گیری کند. در این حالت نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+۰$، $+۱$، -۰ و -۱ و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های A_1 و A_2 می‌باشد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+۰$ باشد نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، $+۰$ و -۰ می‌باشد و حالات $+۱$ و -۱ اتفاق نمی‌افتد. پس احتمال رخداد نتیجه اندازه‌گیری روی کیوبیت‌های B و C در حالات $+۰$ و -۰، ٪۵۰ می‌باشد و فقط در حالت -۰، دشمن آشکار می‌شود پس احتمال پی بردن به وجود دشمن در این بخش ٪۵۰ می‌باشد.

احتمال کلی آشکارسازی دشمن در حمله اندازه‌گیری در پایه برابر است با:

$$P_2 = \frac{1}{6}(0 + 0.75 + 0.5 + 0 + 0 + 0.5) = 0.2916 \quad (8)$$

حالت اندازه‌گیری-بازتاب کاملا مشابه حالت بازتاب-اندازه‌گیری است.

۲.۲.۴ اندازه‌گیری دشمن در پایه X

دشمن کیوبیت‌های ارسالی آلیس به باب و چارلی را قطع می‌کند و آن کیوبیت‌ها را در پایه X اندازه‌گیری می‌کند و سپس آن‌ها را برای باب و چارلی می‌فرستد. اقدام دشمن به صورت جدول ۹ است.

جدول ۹. اندازه‌گیری دشمن در پایه X

حالت فروپاشی شده کیوبیت‌های A_1 و A_2	نتیجه اندازه‌گیری دشمن روی B و C
$\|{++}\rangle$	$++$
$\|{+-}\rangle$	$+-$
$\|{-+}\rangle$	$-+$
$\|{--}\rangle$	$--$

الف- بازتاب بازتاب: در این حالت هر دو کاربر کلاسیک کیوبیت را بازتاب کرده‌اند. دشمن در پایه X روی کیوبیت‌های باب و چارلی اندازه‌گیری کرده و سپس آن کیوبیت‌ها را به باب و چارلی می‌فرستد. باب و چارلی هم عیناً آن کیوبیت‌ها را برای آلیس می‌فرستند. اگر آلیس کانال را به روش اول چک کند چون نتایج اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت ۰۰، ۰۱، ۱۰ و ۱۱ و در هر یک از این حالات نتیجه اندازه‌گیری روی کیوبیت‌های B و C احتمالاتی و هر یک از نتایج ۰۰، ۰۱، ۱۰ و ۱۱ با احتمال ٪۲۵ رخ می‌دهد، پس در حالاتی که نتایج اندازه‌گیری یکسان است دشمن آشکار نمی‌شود و در بقیه حالات آشکار می‌شود. به عنوان نمونه، زمانی که نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2، ۰۰ باشد، اگر آلیس روی کیوبیت‌های B و C اندازه‌گیری کند با احتمال ٪۲۵ هر یک از نتایج ۰۰، ۰۱، ۱۰ و ۱۱ رخ می‌دهد. اگر نتیجه اندازه‌گیری روی B و C، ۰۰ باشد در این حالت دشمن آشکار نمی‌شود و اگر نتیجه اندازه‌گیری ۰۱، ۱۰ و ۱۱ شود آلیس به وجود دشمن پی می‌برد. پس در این حالت آلیس با احتمال ٪۷۵ به وجود دشمن پی می‌برد. حال به بررسی کانال به روش دوم می‌پردازیم. در این حالت آلیس متوجه حضور دشمن نمی‌شود، چرا که کیوبیت‌ها پس از اندازه‌گیری توسط دشمن به یکی از نتایج مورد دلخواه آلیس تغییر می‌کنند و نتایج اندازه‌گیری آلیس هم همین حالات هستند. به عنوان نمونه، زمانی که نتیجه اندازه‌گیری دشمن روی کیوبیت‌های B و C، $++$ باشد نتیجه اندازه‌گیری آلیس هم روی کیوبیت‌های A_1 و A_2 با احتمال ٪۱۰۰، $++$ می‌باشد و همچنین نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C هم $++$ می‌باشد پس در این حالت وجود دشمن آشکار نمی‌شود.

ب- بازتاب اندازه‌گیری: در این حالت باب کیوبیت خود را بازتاب کرده و چارلی کیوبیت خود را در پایه کلاسیک اندازه‌گیری می‌کند. کیوبیتی که در پایه محاسباتی اندازه‌گیری شده، به همراه کیوبیت متناظر در دست آلیس، تنها می‌توانند در پایه Z چک شوند. کیوبیت‌های A_1 با B و A_2 با C متناظر هستند. در این حالت اگر آلیس کانال را به روش اول چک کند، همانند چک کردن آلیس به روش اول در حالت بازتاب-بازتاب، آلیس با احتمال ٪۷۵ به وجود دشمن پی می‌برد. اگر آلیس کانال را با روش دوم چک کند، می‌تواند روی کیوبیت‌های A_1 با B کانال در پایه X و روی A_2 و C در پایه Z اندازه‌گیری کند. در این حالت نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+۰$، $+۱$، -۰ و -۱ خواهد بود و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های A_1 و A_2 می‌باشد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+۰$ باشد، نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، $+۰$ و $+۱$ می‌باشد و حالات -۰ و -۱ اتفاق نمی‌افتند. احتمال رخداد نتیجه اندازه‌گیری روی کیوبیت‌های B و C در حالات $+۰$ و $+۱$، ٪۵۰ می‌باشد و در حالت $+۱$، دشمن آشکار می‌شود. پس احتمال پی بردن به وجود دشمن در این بخش ٪۵۰ می‌باشد.

حال به محاسبه احتمال کلی آشکارسازی دشمن در حمله اندازه‌گیری

دشمن در پایه X می‌پردازیم.

$$P_{۳}=\frac{۱}{۶}(۰+۰/۷۵+۰/۷۵+۰/۵+۰/۷۵+۰/۵)=۰/۵۴۱۶ \quad (۹)$$

حالت اندازه‌گیری-بازتاب کاملا مشابه حالت بازتاب-اندازه‌گیری است.

۳.۲.۴ اندازه‌گیری دشمن در پایه X و پایه Z

در این حالت دشمن کیوبیت‌ها را گرفته و کیوبیت‌های باب را در پایه X و کیوبیت‌های چارلی را در پایه Z اندازه‌گیری می‌کند و سپس آن‌ها را برای باب و چارلی می‌فرستد. اقدام دشمن در این نوع حمله به صورت جدول ۱۰ است.

جدول ۱۰. اندازه‌گیری دشمن در پایه Z و X

نتیجه اندازه‌گیری دشمن روی B و C	حالت فروپاشی شده کیوبیت‌های $A_۱$ و $A_۲$
$+۰$	$\|+۰\rangle$
$+۱$	$\|+۰\rangle$
-۰	$\|-۰\rangle$
-۱	$\|-۱\rangle$

الف- بازتاب بازتاب: در این حالت هر دو کاربر کلاسیک کیوبیت را بازتاب کرده‌اند. اگر آلیس کانال را به روش اول چک کند نتایج اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۲$ به صورت ۰۰، ۰۱، ۱۰ و ۱۱ و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های $A_۱$ و $A_۲$ می‌باشد. با توجه به اندازه‌گیری دشمن روی کیوبیت‌های باب در پایه X و کیوبیت‌های چارلی در پایه Z، زمانی که نتایج اندازه‌گیری آلیس روی کیوبیت های $A_۱$ و C یکسان است آن حالت با احتمال ۵۰٪ رخ می‌دهد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۲$ به صورت ۰۰ باشد نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، ۰۰ و ۱۰ می‌باشد که احتمال رخداد هر کدام ۵۰٪ می‌شود و حالات ۰۱ و ۱۱ اتفاق نمی‌افتد. زمانی که نتیجه اندازه‌گیری کیوبیت‌های B و C، ۰۰ باشد دشمن آشکار نمی‌شود و زمانی که ۱۰ باشد دشمن اشکار می‌شود؛ پس احتمال پی بردن به وجود دشمن در این حالت ۵۰٪ می‌باشد. اگر آلیس کانال را با روش دوم چک کند، نتایج اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۲$ به صورت $++$، $-+$، $+-$ و $--$ و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های $A_۱$ و $A_۲$ می‌باشد. با توجه به اندازه‌گیری دشمن روی کیوبیت‌های باب در پایه X و کیوبیت‌های چارلی در پایه Z، زمانی که نتایج اندازه‌گیری آلیس روی کیوبیت های $A_۲$ و C یکسان است آن حالت با احتمال ۵۰٪ رخ می‌دهد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۲$ به صورت $++$ باشد، نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، $++$ و $-+$ می‌باشد که احتمال رخداد هرکدام ۵۰٪ می‌شود و حالات $+-$ و $--$ اتفاق نمی‌افتد. زمانی که نتیجه اندازه‌گیری کیوبیت‌های B و C، $++$ باشد دشمن آشکار نمی‌شود و زمانی که نتیجه اندازه‌گیری $+-$ باشد دشمن آشکار می‌شود؛ پس احتمال پی بردن به وجود دشمن در این حالت ۵۰٪ می‌باشد.

ب- بازتاب اندازه‌گیری: در این حالت باب کیوبیت خود را بازتاب کرده و چارلی کیوبیت خود را در پایه کلاسیک اندازه‌گیری می‌کند. کیوبیتی که در پایه محاسباتی اندازه‌گیری شده، به همراه کیوبیت متناظر در دست آلیس، تنها می‌توانند در پایه Z چک شوند. کیوبیت‌های $A_۱$ با B و $A_۲$ با C متناظر هستند. در این حالت اگر آلیس کانال را به روش اول چک کند، هیچ فرقی نمی‌کند که کیوبیتی که دشمن در پایه X یا Z اندازه‌گیری کرده، کدام کیوبیت باشد. فرض می‌کنیم کیوبیت دوم در پایه X توسط دشمن اندازه‌گیری شده باشد. نتایج اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۱$، ۰۰، ۰۱ ، ۱۰ و ۱۱ و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های $A_۱$ و $A_۲$ می‌باشد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۲$ به صورت ۰۰ باشد نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، ۰۰ و ۰۱ می‌باشد که احتمال رخداد این دو حالت یکسان و برابر ۵۰٪ می‌باشد و حالات ۱۰ و ۱۱ اتفاق نمی‌افتد. فقط در حالت ۰۱ حضور دشمن آشکار می‌شود پس احتمال پی بردن به وجود دشمن در این حالت ۵۰٪ می‌باشد. اگر آلیس کانال را با روش دوم چک کند، در این قسمت دو حالت به وجود می‌آید. اگر کیوبیتی که یکی از کاربران اندازه‌گیری کرده همان کیوبیتی باشد که دشمن نیز در پایه اندازه‌گیری کرده باشد، احتمال پی بردن به حضور دشمن امکان‌پذیر نمی‌باشد. اما اگر کیوبیتی که یکی از کاربران اندازه‌گیری کرده همان کیوبیتی باشد که دشمن در پایه اندازه‌گیری کرده باشد. حضورش با احتمال ۷۵٪ آشکار می‌شود. برای نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۱$، از ۴ نتیجه $+۰$، -۰، $+۱$ و -۱، نتیجه $+۰$ شود، دشمن آشکار نمی‌شود؛ ولی در ۳ حالت دیگر دشمن حضورش آشکار می‌شود. پس در این حالت احتمال پی بردن به وجود دشمن ۷۵٪ می‌باشد.

ج- اندازه‌گیری بازتاب: در این حالت باب کیوبیت خود را در پایه کلاسیک اندازه‌گیری کرده و چارلی کیوبیت خود را بازتاب می‌کند. کیوبیتی که در پایه محاسباتی اندازه‌گیری شده، به همراه کیوبیت متناظر در دست آلیس، تنها می‌توانند در پایه Z چک شوند. کیوبیت‌های $A_۱$ با B و $A_۲$ با C متناظر هستند. در این حالت اگر آلیس کانال را به روش اول چک کند، هیچ فرقی نمی‌کند که کیوبیتی که دشمن در پایه Z یا X اندازه‌گیری کرده، کدام کیوبیت باشد. فرض می‌کنیم کیوبیت اول در پایه X توسط دشمن اندازه‌گیری شده باشد. نتایج اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۲$، ۰۰، ۰۱، ۱۰ و ۱۱ و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های $A_۱$ و $A_۲$ می‌باشد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های $A_۱$ و $A_۲$ به صورت ۰۰ باشد، نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، ۰۰ و ۱۰ می‌باشد که احتمال رخداد این دو حالت یکسان و برابر ۵۰٪ می‌باشد و حالات ۰۱ و ۱۱ اتفاق نمی‌افتد. فقط در حالت ۱۰ حضور دشمن آشکار می‌شود؛ پس احتمال پی بردن به وجود دشمن در این حالت

۵۰٪ می‌باشد. اگر آلیس کانال را با روش دوم چک کند، احتمال پی بردن به حضور دشمن امکان‌پذیر نمی‌باشد. نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2، $+0$، -0، $+1$ و -1 و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های A_1 و A_2 می‌باشد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+0$ باشد نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، با احتمال ۱۰۰٪ فقط $+0$ می‌باشد و حالات -0، $+1$ و -1 اتفاق نمی‌افتد. پس در این حالت وجود دشمن آشکار نمی‌شود.

حال به محاسبه احتمال آشکارسازی دشمن در این نوع حمله می‌پردازیم.

$$P_4 = \frac{1}{6}(0.5 + 0.5 + 0.75 + 0.5 + 0.5 + 0) = 0.4583 \quad (10)$$

۴.۲.۴ اندازه‌گیری دشمن در پایه Z و پایه X

در این حالت احتمال آشکارسازی دشمن کاملا مشابه حالت، اندازه‌گیری دشمن در پایه X و پایه Z می‌باشد؛ پس احتمال آشکار سازی دشمن در این نوع حمله به صورت زیر است.

$$P_5 = 0.4583 \quad (11)$$

۵.۲.۴ اندازه‌گیری دشمن در پایه Bell

دشمن در این حالت کیوبیت‌ها را در پایه Bell اندازه‌گیری می‌کند. اقدام دشمن به صورت جدول ۱۱ است، که حالات بل به صورت زیر می‌باشند:

$$\begin{aligned}
\beta_{00} &= |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
\beta_{01} &= |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
\beta_{10} &= |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
\beta_{11} &= |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned} \quad (12)$$

جدول ۱۱. اندازه‌گیری دشمن در پایه Bell

نتیجه اندازه‌گیری دشمن روی B و C	حالت فروپاشی شده کیوبیت‌های A_1 و A_2
β_{00}	$\|\beta_{00}\rangle$
β_{01}	$\|\beta_{01}\rangle$
β_{10}	$\|\beta_{10}\rangle$
β_{11}	$\|\beta_{11}\rangle$

الف- بازتاب بازتاب: در این حالت هر دو کاربر کلاسیک کیوبیت را بازتاب کرده‌اند، نتایج اندازه‌گیری دشمن روی کیوبیت‌های B و C به صورت β_{00}، β_{01}، β_{10} و β_{11} می‌باشد. اگر آلیس کانال را به روش اول چک کند، نتایج اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت ۰۰، ۰۱، ۱۰ و ۱۱ و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های A_1 و A_2 می‌باشد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت ۰۰ باشد نتیجه اندازه‌گیری B و C، ۰۰ و ۱۱ می‌باشد که احتمال رخداد این دو حالت یکسان و برابر ۵۰٪ می‌باشد و حالات ۰۱ و ۱۰ اتفاق نمی‌افتد. فقط در حالت ۱۱ حضور دشمن آشکار می‌شود؛ پس احتمال پی‌بردن به وجود دشمن در این حالت ۵۰٪ می‌باشد. در حالتی که نتیجه اندازه‌گیری ۰۰ باشد، دشمن آشکار نمی‌شود و در حالتی که نتیجه اندازه‌گیری ۱۱ باشد، دشمن با احتمال ۵۰٪ آشکار می‌شود. اگر آلیس کانال را با روش دوم چک کند، نتایج اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $++$، $-+$، $+-$ و $--$ و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های A_1 و A_2 می‌باشد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $++$ باشد، نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، $++$ و $--$ می‌باشد، که احتمال رخداد این دو حالت یکسان و برابر ۵۰٪ می‌باشد و حالات $-+$ و $+-$ اتفاق نمی‌افتد. در حالتی که نتیجه اندازه‌گیری $++$ باشد دشمن آشکار نمی‌شود و در حالتی که نتیجه اندازه‌گیری $--$ باشد، دشمن با احتمال ۵۰٪ آشکار می‌شود. پس در این حالت احتمال پی‌بردن به وجود دشمن ۵۰٪ می‌باشد.

ب- بازتاب اندازه‌گیری: در این حالت باب کیوبیت خود را بازتاب کرده و چارلی کیوبیت خود را در پایه کلاسیک اندازه‌گیری می‌کند. کیوبیتی که در پایه محاسباتی اندازه‌گیری شده، به همراه کیوبیت متناظر در دست آلیس، تنها می‌توانند در پایه Z چک شوند. کیوبیت‌های A_1 با B و A_2 با C متناظر هستند. در این حالت اگر آلیس کانال را به روش اول چک کند، مانند حالتی است که کاربران بازتاب بازتاب کردند و آلیس از روش اول برای چک کردن استفاده کرده است. اگر آلیس کانال را با روش دوم چک کند، نتایج اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+0$، -1، $+1$ و -0 و نتیجه اندازه‌گیری روی کیوبیت‌های B و C وابسته به نتیجه اندازه‌گیری روی کیوبیت‌های A_1 و A_2 می‌باشد. به عنوان نمونه اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+0$ باشد، نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C، $+0$ و -1 می‌باشد که احتمال رخداد این دو حالت یکسان و برابر ۵۰٪ می‌باشد و حالات -0 و $+1$ اتفاق نمی‌افتد. حالتی که نتیجه اندازه‌گیری $+0$ باشد دشمن آشکار نمی‌شود و در حالتی که نتیجه اندازه‌گیری -1 باشد دشمن با احتمال ۵۰٪ آشکار می‌شود. پس در این حالت احتمال پی‌بردن به وجود دشمن ۵۰٪ می‌باشد. بدین ترتیب اگر دشمن روی کیوبیت‌های باب و چارلی اندازه‌گیری Bell انجام دهد، در هر صورت با احتمال ۵۰٪ حضورش آشکار می‌شود. حالت اندازه‌گیری، بازتاب کاملا مشابه حالت بازتاب، اندازه‌گیری است.

حال به محاسبه احتمال آشکارسازی دشمن در این نوع حمله می‌پردازیم.

$$P_6 = \frac{1}{6}(0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5) = 0.5 \quad (13)$$

۳.۴ حمله دستکاری پیام

در این نوع حمله، دشمن می‌تواند انواع عملگرها را بر روی دو کیوبیت باب و چارلی اعمال کند و آن دو کیوبیت را تغییر دهد. کوچکترین تغییر در کیوبیت‌های باب و چارلی باعث آشکار شدن دشمن می‌شود؛ چرا که کانال متقارن بوده و در هر صورت به هر دو روش چک کردن کانال می‌توان به وجود دشمن پی برد. پس این نوع حمله نیز وجود دشمن را آشکارکرده و خللی در امنیت پروتکل ایجاد نمی‌کند. فرض می‌کنیم دشمن روی کیوبیت‌های باب و چارلی CNOT اعمال کرده و سپس برای باب و چارلی ارسال می‌کند، که دو حالت زیربخش‌های زیر به وجود می‌آید.

۱.۳.۴ اعمال CNOT از روی کیوبیت دشمن

در این حالت، دشمن از روی دو کیوبیت خودش بر روی دو کیوبیت باب و چارلی CNOT اعمال کند، که کیوبیت‌های دشمن به صورت زیر است:

$$|\psi\rangle_E = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle \quad (۱۴)$$

حالت کامل سیستم به صورت زیر می‌شود:

$$\begin{aligned}|\psi\rangle_E \otimes |\phi\rangle_{A_1A_2BC} = \frac{1}{2}(&\alpha_0 |000000\rangle + \alpha_0 |000101\rangle \\ &+ \alpha_0 |001010\rangle + \alpha_0 |001111\rangle + \alpha_1 |010000\rangle \\ &+ \alpha_1 |010101\rangle + \alpha_1 |011010\rangle + \alpha_1 |011111\rangle \\ &+ \alpha_2 |100000\rangle + \alpha_2 |100101\rangle + \alpha_2 |101010\rangle \\ &+ \alpha_2 |101111\rangle + \alpha_3 |110000\rangle + \alpha_2 |110101\rangle \\ &+ \alpha_2 |111010\rangle + \alpha_3 |111111\rangle) \end{aligned} \quad (۱۵)$$

پس از اعمال CNOT از کیوبیت‌های دشمن به کیوبیت‌های باب و چارلی، حالت کامل سیستم به صورت زیر می‌شود:

$$\begin{aligned}|\psi\rangle_E \otimes |\phi\rangle_{A_1A_2BC} = \frac{1}{2}(&\alpha_0 |000000\rangle + \alpha_0 |000101\rangle \\ &+ \alpha_0 |001010\rangle + \alpha_0 |001111\rangle + \alpha_1 |010001\rangle \\ &+ \alpha_1 |010100\rangle + \alpha_1 |011011\rangle + \alpha_1 |011110\rangle \\ &+ \alpha_2 |100010\rangle + \alpha_2 |100111\rangle + \alpha_2 |101000\rangle \\ &+ \alpha_2 |101101\rangle + \alpha_3 |110011\rangle + \alpha_2 |110110\rangle \\ &+ \alpha_2 |111001\rangle + \alpha_3 |111100\rangle) \end{aligned} \quad (۱۶)$$

الف- بازتاب بازتاب: در این حالت، هر دو کاربر کلاسیک کیوبیت را بازتاب کرده‌اند. آلیس ابتدا به روش اول کانال را چک می‌کند. نتایج اندازه‌گیری آلیس در پایه Z روی کیوبیت‌های A_1 و A_2، به صورت جدول ۱۲ است.

سپس آلیس کیوبیت‌های B و C را در پایه کلاسیک اندازه‌گیری می‌کند و نتیجه آن به صورت ۰۰، ۰۱، ۱۰ و ۱۱ می‌باشد و این نتایج به ترتیب با احتمال $|a_0|^2$، $|a_1|^2$، $|a_2|^2$ و $|a_3|^2$ رخ می‌دهند. اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2، ۰۰ و روی کیوبیت‌های B و C، هم ۰۰ باشد در این صورت دشمن آشکار نمی‌شود و احتمال پی بردن به وجود دشمن در این حالت $1-|a_0|^2$ می‌باشد؛ ولی اگر نتیجه اندازه‌گیری آلیس، روی کیوبیت‌های B و C یکی از ۳ حالت ۰۱، ۱۰ و ۱۱ باشد دشمن آشکار می‌شود. در بقیه نتایج اندازه‌گیری آلیس مشابه همین حالت دشمن آشکار می‌شود. در این حمله اگر ضریب کیوبیت‌های دشمن متقارن باشد دشمن با احتمال ۷۵٪ آشکار می‌شود. اگر آلیس امنیت کانال را به روش دوم چک کند، یعنی آلیس روی کیوبیت‌های A_1 و A_2 در پایه X، اندازه‌گیری انجام دهد، یکی از ۴ حالت $++$، $-+$، $+-$ و $--$ را به دست می‌آورد. سپس آلیس کیوبیت‌های B و C را در پایه کلاسیک اندازه‌گیری می‌کند و نتیجه آن به صورت $++$، $-+$، $+-$ و $--$ می‌باشد و این نتایج به ترتیب با احتمال $|a_0|^2$، $|a_1|^2$، $|a_2|^2$ و $|a_3|^2$ رخ می‌دهند. اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2، $++$ و روی کیوبیت‌های B و C هم $++$ باشد، در این صورت دشمن آشکار نمی‌شود و احتمال پی‌بردن به وجود دشمن در این حالت $1-|a_0|^2$ می‌باشد؛ ولی اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C یکی از ۳ حالت $-+$، $+-$ و $--$ باشد دشمن آشکار می‌شود. در بقیه نتایج اندازه‌گیری آلیس، مشابه همین حالت دشمن آشکار می‌شود. در این حمله اگر ضریب کیوبیت‌های دشمن متقارن باشد، دشمن با احتمال ۷۵٪ آشکار می‌شود.

جدول ۱۲. اندازه‌گیری آلیس روی A_1 و A_2 در پایه Z

نتیجه اندازه‌گیری آلیس روی A_1 و A_2	حالت فروپاشی شده کیوبیت‌های دیگر
۰۰	$\alpha_0 \|0000\rangle + \alpha_1 \|0101\rangle + \alpha_2 \|1010\rangle + \alpha_3 \|1111\rangle$
۰۱	$\alpha_0 \|0000\rangle + \alpha_1 \|0101\rangle + \alpha_2 \|1010\rangle + \alpha_3 \|1111\rangle$
۱۰	$\alpha_0 \|0000\rangle + \alpha_1 \|0101\rangle + \alpha_2 \|1010\rangle + \alpha_3 \|1111\rangle$
۱۱	$\alpha_0 \|0000\rangle + \alpha_1 \|0101\rangle + \alpha_2 \|1010\rangle + \alpha_3 \|1111\rangle$

ب- بازتاب اندازه‌گیری: در این حالت باب کیوبیت خود را بازتاب کرده و چارلی کیوبیت خود را در پایه کلاسیک اندازه‌گیری می‌کند. کیوبیتی که در پایه محاسباتی اندازه‌گیری شده، به همراه کیوبیت متناظر در دست آلیس، تنها می‌توانند در پایه Z چک شوند. کیوبیت‌های A_1 با B و A_2 با C متناظر هستند. در این حالت اگر آلیس کانال را به روش اول چک کند، مانند حالتی است که کاربران بازتاب بازتاب کردند و آلیس از روش اول برای چک کردن استفاده کرده است. اگر آلیس کانال را با روش دوم چک کند، نتایج اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2 به صورت $+0$، -1، $+1$ و -0 و نتیجه اندازه‌گیری روی کیوبیت‌های B و C هم $+0$، -1، $+1$ و -0 می‌باشد و این نتایج به ترتیب با احتمال $|a_0|^2$، $|a_1|^2$، $|a_2|^2$ و $|a_3|^2$ رخ می‌دهند. اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های A_1 و A_2، $+0$ و روی کیوبیت‌های B و C، هم $+0$ باشد، در این صورت دشمن آشکار نمی‌شود و احتمال پی‌بردن به وجود دشمن در این حالت می‌باشد؛ ولی اگر نتیجه اندازه‌گیری آلیس روی کیوبیت‌های B و C یکی از ۳ حالت -1، $+1$ و -0 باشد، دشمن آشکار می‌شود. در

بقیه نتایج اندازه‌گیری آلیس، مشابه همین حالت دشمن آشکار می‌شود. در این حمله، اگر ضریب کیوبیت‌های دشمن متقارن باشد، دشمن با احتمال ۷۵٪ آشکار می‌شود.

همانطور که مشاهده شد، در همه حالات اگر دشمن از روی کیوبیت‌های خود روی کیوبیت باب و چارلی CNOT اعمال کند، وجود دشمن آشکار خواهد شد. در صورت تقارن بین ضریب‌های کیوبیت‌های دشمن احتمال آشکارسازی دشمن ۷۵٪ است. حالت اندازه‌گیری–بازتاب کاملا مشابه حالت بازتاب–اندازه‌گیری است.

$$P_{\text{۷}} = \frac{\text{۱}}{\text{۶}}(\text{۰٫۷۵}+\text{۰٫۷۵}+\text{۰٫۷۵}+\text{۰٫۷۵}+\text{۰٫۷۵}+\text{۰٫۷۵}) = \text{۰٫۷۵} \quad (۱۷)$$

۲.۳.۴ اعمال CNOT از روی کیوبیت‌های باب و چارلی

دشمن از روی دو کیوبیت باب و چارلی بر روی کیوبیت خود CNOT اعمال کند. در این حالت، کیوبیت‌های دشمن همانند حالت قبل است. پس از اعمال CNOT از کیوبیت‌های دشمن به کیوبیت‌های باب و چارلی، حالت کامل سیستم به صورت زیر می‌شود:

$$\begin{aligned}|\psi\rangle_E \otimes |\phi\rangle_{A_1A_2BC} = \frac{\text{۱}}{\text{۲}}(&\alpha_\text{۰}|\text{۰۰۰۰۰۰}\rangle + \alpha_\text{۰}|\text{۰۱۰۱۰۱}\rangle \\ &+ \alpha_\text{۰}|\text{۱۰۱۰۱۰}\rangle + \alpha_\text{۰}|\text{۱۱۱۱۱۱}\rangle + \alpha_\text{۱}|\text{۰۱۰۰۰۰}\rangle \\ &+ \alpha_\text{۱}|\text{۰۰۰۱۰۱}\rangle + \alpha_\text{۱}|\text{۱۱۱۰۱۰}\rangle + \alpha_\text{۱}|\text{۱۰۱۱۱۱}\rangle \\ &+ \alpha_\text{۲}|\text{۱۰۰۰۰۰}\rangle + \alpha_\text{۲}|\text{۱۱۰۱۰۱}\rangle + \alpha_\text{۲}|\text{۰۰۱۰۱۰}\rangle \\ &+ \alpha_\text{۲}|\text{۰۱۱۱۱۱}\rangle + \alpha_\text{۳}|\text{۱۱۰۰۰۰}\rangle + \alpha_\text{۲}|\text{۱۰۰۱۰۱}\rangle \\ &+ \alpha_\text{۲}|\text{۰۱۱۰۱۰}\rangle + \alpha_\text{۳}|\text{۰۰۱۱۱۱}\rangle)\end{aligned} \quad (۱۸)$$

همانطور که مشاهده می‌شود، روی کیوبیت‌های آلیس، باب و چارلی هیچ تغییری ایجاد نمی‌شود. پس اینکار دشمن هیچ تأثیری روی فرآیند پروتکل ندارد. همچنین پس از انجام پروتکل، دشمن عیناً کیوبیت‌های اولیه خودش به دستش می‌رسد. پس این حمله حمله‌ای بیهوده از طرف دشمن می‌باشد. احتمال آشکارسازی دشمن در این حالت صفر است و این صفر بودن به این معنی نیست که پروتکل ناامن است، بلکه به این معناست که دشمن حمله‌ای انجام نداده است که کیوبیت‌ها را دستکاری کند یا به راز دست پیدا کند.

بنابراین احتمال کلی آشکارسازی دشمن در برابر تمام حملات به صورت زیر است:

$$P = \frac{\text{۱}}{\text{۷}}(P_\text{۱}+P_\text{۲}+P_\text{۳}+P_\text{۴}+P_\text{۵}+P_\text{۶}+P_\text{۷}) = \text{۰٫۵۴} \quad (۱۹)$$

بدین ترتیب مشاهده شد که در تمام حالت‌ها احتمال آشکار شدن دشمن وجود دارد. در کارهای قبلی، در مقابل بعضی حملات دشمن، حضور دشمن برای کاربران آشکار نمی‌شد، اما در طرح ارائه شده محدودیتی در این زمینه وجود ندارد. همچنین در طرح‌های قبلی به تمام حالات حمله دشمن اشاره نشده بود که در این طرح تمام حملات مورد بررسی قرار گرفته است.

پس از چک کردن کانال به دو روش ذکر شده، در رشته کیوبیت‌های کانال و مطمئن شدن از عدم وجود دشمن، آلیس زمانی‌که باب و چارلی هر دو بیت کلاسیک ۱ را فرستاده باشند، یعنی زمانی که اندازه‌گیری اندازه‌گیری کرده باشند، راز K_A را بین کاربران به اشتراک می‌گذارد.

۵ ارزیابی

در طرح ارائه شده، کیوبیت‌های حامل اطلاعات به صورت مستقیم از طریق کانال‌های ارتباطی به کاربران ارسال نمی‌شود و اطلاعات از طریق مخابره از راه دور کوانتومی از فرستنده به گیرنده‌ها منتقل می‌شود. در اکثر طرح های قبلی، رازی که بین کاربران به اشتراک گذاشته می‌شود راز معینی نیست و گیرنده‌ها با همکاری همدیگر می‌توانند به کلید دسترسی پیدا کنند. ولی در طرح ارائه شده، راز از اول پروتکل معین می‌باشد. یعنی فرستنده به تسهیم راز با گیرنده‌ها پرداخته و همه کاربران با همکاری همدیگر می‌توانند به راز فرستنده پی ببرند. در طرح‌های قبلی، فرستنده نیاز به حافظه کوانتومی و گیرنده‌ها نیاز به اندازه‌گیری در پایه محاسباتی و تولید کیوبیت جدید دارند، ولی در طرح پیشنهادی، فرستنده نیاز به ذخیره سازی کیوبیت‌ها ندارد. پس نیاز به حافظه کوانتومی ندارد. گیرنده‌ها نیز فقط در پایه محاسباتی اندازه‌گیری می‌کنند و نیاز به تولید کیوبیت جدید ندارند. در پروتکل پیشنهادی، چون کیوبیت‌های حامل اطلاعات در کانال به صورت مستقیم منتقل نمی‌شوند، بنابراین استراق سمع‌کننده نمی‌تواند کیوبیت‌های مذکور را در طی فرایند انتقال پیام جدا کند، بلکه تنها در زمان ایجاد کانال کوانتومی می‌تواند حمله کند که تحلیل آن در بخش سوم ارائه شد.

۶ نتیجه‌گیری

در این مقاله، یک پروتکل جدید تسهیم راز نیمه‌کوانتومی با استفاده از مخابره از راه دور کوانتومی ارائه شد. با توجه به طرح‌های پیشین و طرح جدید ارائه شده، مشاهده می‌شود که در چند سال اخیر، شاخه‌های رمزنگاری نیمه‌کوانتومی به خصوص تسهیم راز نیمه‌کوانتومی نسبت به رمزنگاری کوانتومی، به دلیل کاهش بار محاسباتی کاربران و هزینه دستگاه‌های سخت‌افزاری کوانتومی مورد نیاز جهت پیاده‌سازی عملی، مورد توجه جدی بوده است.

مراجع

[1] Adi, Shamir. How to share a secret. *Commun. ACM*, 22:612–613, 1979.

[2] Blakley, George Robert. Safeguarding cryptographic keys. in *Managing requirements knowledge, international workshop on*, pp. 313–313. IEEE Computer Society, 1979.

[3] Gruska, Jozef. *Foundations of computing*. International

[15] Wu, Yadong, Cai, Runze, He, Guangqiang, and Zhang, Jun. Quantum secret sharing with continuous variable graph state. *Quantum information processing*, 13(5):1085–1102, 2014.

[16] Qin, Huawang and Dai, Yuewei. Efficient quantum secret sharing. *Quantum Information Processing*, 15(5):2091–2100, 2016.

[17] Zhou, Jian and Guo, Ying. Continuous-variable measurement-device-independent multipartite quantum communication using coherent states. *Journal of the Physical Society of Japan*, 86(2):024003, 2017.

[18] Qin, Huawang, Zhu, Xiaohua, and Dai, Yuewei. (t, n) threshold quantum secret sharing using the phase shift operation. *Quantum Information Processing*, 14(8):2997–3004, 2015.

[19] Song, Xiuli and Liu, Yanbing. Cryptanalysis and improvement of verifiable quantum (k, n) secret sharing. *Quantum Information Processing*, 15(2):851–868, 2016.

[20] Boyer, Michel, Kenigsberg, Dan, and Mor, Tal. Quantum key distribution with classical bob. in *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*, pp. 10–10. IEEE, 2007.

[21] Li, Qin, Chan, Wai Hong, and Long, Dong-Yang. Semiquantum secret sharing using entangled states. *Physical Review A—Atomic, Molecular, and Optical Physics*, 82(2):022303, 2010.

[22] Lin, Jason, Yang, Chun-Wei, Tsai, Chia-Wei, and Hwang, Tzonelih. Intercept-resend attacks on semi-quantum secret sharing and the improvements. *International Journal of Theoretical Physics*, 52(1):156–162, 2013.

[23] Wang, Jian, Zhang, Sheng, Zhang, Quan, and Tang, Chao-Jing. Semiquantum secret sharing using two-particle entangled state. *International Journal of Quantum Information*, 10(05):1250050, 2012.

[24] Li, Lvzhou, Qiu, Daowen, and Mateus, Paulo. Quantum secret sharing with classical bobs. *Journal of Physics A: Mathematical and Theoretical*, 46(4):045304, 2013.

[25] Yang, Chun-Wei and Hwang, Tzonelih. Efficient key construction on semi-quantum secret sharing protocols. *International Journal of Quantum Information*, 11(05):1350052, 2013.

[26] Yu, Kun-Fei, Gu, Jun, Hwang, Tzonelih, and Gope, Prosanta. Multi-party semi-quantum key distribution-Thomson Computer Press, 1997.

[4] Hillery, Mark, Bužek, Vladimír, and Berthiaume, André. Quantum secret sharing. *Physical Review A*, 59(3):1829, 1999.

[5] Karlsson, Anders, Koashi, Masato, and Imoto, Nobuyuki. Quantum entanglement for secret sharing and secret splitting. *Physical Review A*, 59(1):162, 1999.

[6] Guo, Guo-Ping and Guo, Guang-Can. Quantum secret sharing without entanglement. *Physics Letters A*, 310(4):247–251, 2003.

[7] Xiao, Li, Lu Long, Gui, Deng, Fu-Guo, and Pan, Jian-Wei. Efficient multiparty quantum-secret-sharing schemes. *Physical Review A—Atomic, Molecular, and Optical Physics*, 69(5):052307, 2004.

[8] Zhang, Zhan-jun and Man, Zhong-xiao. Multiparty quantum secret sharing of classical messages based on entanglement swapping. *Physical Review A—Atomic, Molecular, and Optical Physics*, 72(2):022303, 2005.

[9] Wang, Ming-Ming, Wang, Wei, Chen, Jin-Guang, and Farouk, Ahmed. Secret sharing of a known arbitrary quantum state with noisy environment. *Quantum Information Processing*, 14(11):4211–4224, 2015.

[10] Zhu, Zhen-Chao, Hu, Ai-Qun, and Fu, An-Min. Cryptanalysis of a new circular quantum secret sharing protocol for remote agents. *Quantum information processing*, 12(2):1173–1183, 2013.

[11] Qin, Su-Juan, Gao, Fei, Wen, Qiao-Yan, and Zhu, Fu-Chen. Cryptanalysis of the hillery-bužek-berthiaume quantum secret-sharing protocol. *Physical Review A—Atomic, Molecular, and Optical Physics*, 76(6):062324, 2007.

[12] Long, Yinxiang, Qiu, Daowen, and Long, Dongyang. Quantum secret sharing of multi-bits by an entangled six-qubit state. *Journal of Physics A: Mathematical and Theoretical*, 45(19):195303, 2012.

[13] Jia, Heng-Yue, Wen, Qiao-Yan, Gao, Fei, Qin, Su-Juan, and Guo, Fen-Zhuo. Dynamic quantum secret sharing. *Physics Letters A*, 376(10-11):1035–1041, 2012.

[14] Liu, Zhi-Hao, Chen, Han-Wu, Xu, Juan, Liu, Wen-Jie, and Li, Zhi-Qiang. High-dimensional deterministic multiparty quantum secret sharing without unitary operations. *Quantum Information Processing*, 11(6):1785–1795, 2012.

convertible multi-party semi-quantum secret sharing. *Quantum Information Processing*, 16(8):194, 2017.

[27] Yin, Aihan, Wang, Zefan, and Fu, Fangbo. A novel semi-quantum secret sharing scheme based on bell states. *Modern Physics Letters B*, 31(13):1750150, 2017.

[28] Gao, Gan, Wang, Yue, and Wang, Dong. Cryptanalysis of a semi-quantum secret sharing scheme based on bell states. *Modern Physics Letters B*, 32(09):1850117, 2018.

[29] Chen, Bingren, Yang, Wei, and Huang, Liusheng. Cryptanalysis and improvement of the novel semi-quantum secret sharing scheme based on bell states. *Modern Physics Letters B*, 32(25):1850294, 2018.

[30] Yin, Ai Han and Tong, Yan. A novel semi-quantum secret sharing scheme using entangled states. *Modern Physics Letters B*, 32(22):1850256, 2018.

[31] Li, Zhulin, Li, Qin, Liu, Chengdong, Peng, Yu, Chan, Wai Hong, and Li, Lvzhou. Limited resource semiquantum secret sharing. *Quantum Information Processing*, 17(10), 2018.

[32] Xie, Chen, Li, Lvzhou, and Qiu, Daowen. A novel semi-quantum secret sharing scheme of specific bits. *International Journal of Theoretical Physics*, 54(10):3819–3824, 2015.

[33] Yin, Aihan and Fu, Fangbo. Eavesdropping on semi-quantum secret sharing scheme of specific bits. *International Journal of Theoretical Physics*, 55(9):4027–4035, 2016.

[34] Gao, Xiang, Zhang, Shibin, and Chang, Yan. Cryptanalysis and improvement of the semi-quantum secret sharing protocol. *International Journal of Theoretical Physics*, 56(8):2512–2520, 2017.

[35] Ming-Kuai, Zhou. Improvement of the semi-quantum secret sharing protocol of specific bits. *International Journal of Theoretical Physics*, 59(6):1772–1776, 2020.

[36] Tian, Yuan, Li, Jian, Chen, Xiu-Bo, Ye, Chong-Qiang, and Li, Heng-Ji. An efficient semi-quantum secret sharing protocol of specific bits. *Quantum Information Processing*, 20(6):217, 2021.

[37] Xing, Ding, Wang, Yifei, Dou, Zhao, Li, Jian, Chen, Xiubo, and Li, Lixiang. Efficient semi-quantum secret sharing protocol using single particles. *Chinese Physics B*, 32(7):070308, 2023.

[38] Gao, Gan. Cryptanalysis of efficient semi-quantum secret sharing protocol using single particles. *Chinese Physics B*, 33(4):040301, 2024.

[39] Zhou, Ziyi, Wang, Yifei, Dou, Zhao, Li, Jian, Chen, Xiubo, and Li, Lixiang. A (t, n) threshold protocol of semi-quantum secret sharing based on single particles. *Frontiers in Physics*, 11:1225059, 2023.

[40] Li, Jing, Liu, Jiaming, and Wang, Xianmin. A (4, 4) threshold protocol of semi-quantum secret sharing using entangled state. *Laser Physics Letters*, 22(1):015208, 2024.

[41] He, Fan, Xin, Xiangjun, Li, Chaoyang, and Li, Fagen. Semi-quantum secret sharing protocol based on decoy particles carrying secret information. *Quantum Information Processing*, 24(8):258, 2025.

[42] He, Fan, Xin, Xiangjun, Li, Chaoyang, and Li, Fagen. Security analysis of the semi-quantum secret-sharing protocol of specific bits and its improvement. *Quantum Information Processing*, 23(2):51, 2024.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2026, Volume 23, Number 2 (pp. 13–28)
https://monadi.isc.org.ir

Presented at the ISCISC 2025 in Shahid Beheshti University, Tehran, Iran

A novel semi-quantum secret sharing scheme secure against eavesdropping without direct transmission of message-carrying qubits★

Mohammad Bolokian *,[1] and Monireh Houshmand [2]

[1] *Electrical Engineering Department, Semnan University, Semnan, Iran*
[2] *Electrical Engineering Department, Imam Reza International University, Mashhad, Iran*

EXTENDED ABSTRACT

Keywords:
Quantum cryptography, Semi-quantum cryptography, Quantum teleportation, Quantum secret sharing, Qubit

Type: Research paper

Semi-quantum cryptography has emerged as an important research direction that bridges the gap between classical and fully quantum cryptographic systems. In semi-quantum protocols, one party is assumed to have full quantum capabilities, while the remaining participants are restricted to classical operations such as measuring and preparing qubits in the computational basis or reflecting qubits without disturbance. This asymmetric setting significantly reduces the technological requirements for end users and makes semi-quantum schemes more suitable for near-term practical deployment. Among various cryptographic primitives, secret sharing plays a fundamental role in secure multi-party communication, access control, and distributed trust management. In a secret sharing protocol, a secret message is divided among multiple participants in such a way that only authorized subsets of users can reconstruct the secret through cooperation.

In the context of semi-quantum secret sharing (SQSS), the challenge lies in achieving unconditional security while simultaneously minimizing quantum resource consumption. Many existing SQSS protocols require classical participants to perform measurements and re-prepare qubits, while the quantum party must maintain quantum memory to store qubits during the protocol execution. These requirements increase implementation complexity and introduce additional security vulnerabilities, particularly in noisy or imperfect quantum channels. Furthermore, in a large class of traditional SQSS schemes, the message-carrying qubits are directly transmitted through the quantum channel, making them susceptible to eavesdropping, intercept-resend attacks, and entanglement-based adversarial strategies.

In this work, we propose a novel semi-quantum secret sharing protocol that overcomes the aforementioned limitations by leveraging the principles of quantum teleportation. In the proposed scheme, a fully quantum user, Alice, aims to share a secret classical message with two classical users, Bob and Charlie. Neither Bob nor Charlie can independently reconstruct the secret; only through cooperation can the original message be recovered. The key innovation of our protocol is that the secret message is encoded into local quantum operations rather than being carried by traveling qubits. As a result, message-carrying qubits are never transmitted through the quantum channel, which significantly enhances security against external eavesdroppers.

★ The ISCISC 2025 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: mohammad.bolokian@semnan.ac.ir (Mohammad Bolokian), m.hooshmand@imamreza.ac.ir (Monireh Houshmand)

The protocol begins with the distribution of entangled quantum states between Alice and the classical users. These entangled pairs serve as the quantum channel required for teleportation-based operations. Unlike conventional SQSS protocols, Bob and Charlie are not required to generate new qubits or possess quantum memory. Their role is limited to performing classical operations, such as reflecting incoming qubits or measuring them in the computational basis when instructed. Alice, on the other hand, performs local quantum operations and Bell-state measurements to encode the secret information into the correlations of the shared entangled states.

After Alice completes the teleportation-based encoding process, she broadcasts classical information that enables Bob and Charlie to collaboratively reconstruct the secret. Individually, the classical information available to each receiver is insufficient to reveal any meaningful information about the secret message. Only by combining their respective classical outcomes can the receivers successfully recover the shared secret. This collaborative requirement ensures the fundamental security property of secret sharing and prevents dishonest participants from gaining unilateral access to the message. From a security perspective, the proposed SQSS protocol exhibits strong resistance against common quantum attacks. Since message-carrying qubits are never transmitted, an external eavesdropper cannot directly intercept the encoded information. Any attempt to tamper with the quantum channel inevitably introduces detectable disturbances due to the properties of quantum entanglement and teleportation. Moreover, because the protocol does not rely on quantum memory at the sender's side, it reduces vulnerability to memory-based attacks and decoherence effects. The absence of qubit re-preparation by classical users further minimizes the attack surface and simplifies the security analysis.

In addition to its security advantages, the proposed protocol offers notable practical benefits. By eliminating the need for quantum memory and qubit preparation at the receivers' side, the overall hardware requirements are significantly reduced. This makes the protocol particularly attractive for real-world scenarios in which only a limited number of trusted nodes possess full quantum capabilities, while the majority of users operate with classical or semi-classical devices. The teleportation-based structure of the protocol also allows it to be naturally integrated into larger quantum communication networks and combined with other quantum cryptographic primitives.

A comparison with existing semi-quantum secret sharing schemes highlights the efficiency and robustness of the proposed approach. Traditional protocols often require additional quantum resources, such as auxiliary qubits or repeated measurement rounds, to achieve comparable security guarantees. In contrast, our scheme achieves secure secret sharing with fewer quantum operations and without direct transmission of sensitive quantum states. These features collectively contribute to improved scalability and feasibility for near-term implementation.

In conclusion, this paper presents a new semi-quantum secret sharing protocol that is secure against eavesdropping and does not require direct transmission of message- carrying qubits. By exploiting quantum teleportation, the proposed scheme achieves strong security guarantees while significantly reducing quantum resource requirements for both the sender and receivers. The protocol is well-suited for practical quantum communication environments where full quantum capabilities are not universally available. Future work will focus on extending the scheme to support more participants, analyzing its performance under noisy quantum channels, and implementing the protocol within quantum simulation frameworks such as Qiskit to further validate its practicality and robustness.