گفتگوی امن کوانتومی مصون در برابر نویز فازجمعی با افزایش بازدهی

بتول فرقانی[۱] منیره هوشمند[۲] محمد بلوکیان[۳]

۱- گروه برق - دانشگاه بین‌المللی امام رضا (ع) – مشهد – ایران
forghany_el_1@yahoo.com

۲- گروه برق - دانشگاه بین‌المللی امام رضا (ع) – مشهد – ایران
m.hooshmand@imamreza.ac.ir

۳- گروه برق - دانشگاه بین‌المللی امام رضا (ع) – مشهد – ایران
mohammad.bolokian@yahoo.com

چکیده: در گفتگوی امن کوانتومی که همان مخابره مستقیم امن کوانتومی دوطرفه است، کاربران به‌صورت همزمان و دو طرفه تبادل اطلاعات دارند. در این مقاله، یک پروتکل گفتگوی امن کوانتومی که مصون در برابر نویز فاز جمعی است، ارائه شده است. در این پروتکل اطلاعات هر دو کاربر به دسته‌های سه بیتی تقسیم شده و به کمک دو حالت GHZ به طور همزمان به همدیگر منتقل می‌شود. در این طرح از جابجایی در هم‌تنیدگی برای تولید حالت اولیه استفاده می‌شود. در این روش، حمله‌های استراق‌سمع کننده آشکار شده و نشت اطلاعات ندارد. بازدهی این طرح نسبت به پروتکل‌های پیشین افزایش‌یافته است. بهترین بازده پروتکل‌های پیشین ۲۵٪ بوده است اما پروتکل پیشنهادی به ۴۲/۸۵٪ رسیده است.

واژه‌های کلیدی: رمزنگاری کوانتومی، جابجایی درهم‌تنیدگی، گفتگوی امن کوانتومی، نویز فاز جمعی، نشت اطلاعات، حالت GHZ

نوع مقاله: پژوهشی

DOI: 10.52547/jiaeee.20.3.67

تاریخ ارسال مقاله: ۱۴۰۰/۱۰/۲۵
تاریخ پذیرش مشروط مقاله: ۲۲ / ۴ /۱۴۰۱
تاریخ پذیرش مقاله: ۵ / ۶ /۱۴۰۱
نام نویسنده مسئول: منیره هوشمند
نشانی نویسنده مسئول: ایران - مشهد – خیابان اسرار - دانشگاه بین‌المللی امام رضا (ع) - دانشکده مهندسی برق

۱- مقدمه

مخابره مستقیم امن کوانتومی[۱] (QSDC) [۱] به‌عنوان یکی از مهم‌ترین شاخه‌های رمزنگاری، موردتوجه جمعی از محققان در سال های اخیر قرارگرفته است[۵-۲]. QSDC به ارسال مستقیم پیام محرمانه می‌پردازد. به‌طوری‌که، ارسال پیام به کمک ایجاد یک کانال کوانتومی و بدون نیاز به توزیع کلید بین کاربرها صورت می‌پذیرد. مسئله اصلی در طراحی پروتکل‌های QSDC این است که طرح ارائه شده در برابر انواع حمله‌های استراق‌سمع کننده امن باشد.

در گفتگوی امن کوانتومی[۲] (QSD) که همان مخابره مستقیم امن کوانتومی دوطرفه[۳] (BQSDC) است، کاربران به‌صورت هم‌زمان تبادل اطلاعات دارند [۱۰-۶]. در این نوع از پروتکل، پیام امن در دو مسیر، از آلیس به باب و باب به آلیس هم‌زمان انتقال پیدا می‌کند. در پروتکل‌های QSD امکان نشت اطلاعات بر روی کانال عمومی کلاسیک و نویز بر روی کانال کوانتومی وجود دارد[۱۳،۱۲،۱۱].

در سال ۲۰۰۴، اولین پروتکل QSD بر پایه حالت‌های بل[۳] (Bell) ارائه شده است [۱۴]. بعدازآن، در سال ۲۰۰۸، Gao, et al. به بررسی نشت اطلاعات در پروتکل‌های ارائه شده پیشین پرداختند [۱۵]. سپس پروتکل‌های دیگری برای QSD ارائه شد که در همگی سعی بر امنیت در برابر استراق‌سمع کننده داشتند و نشت اطلاعات نیز ندارند [۲۴،۲۳،۲۲،۲۰-۱۶].

پژوهش‌های اخیر درزمینه‌ی محاسبات کوانتومی، بر روی حفاظت یا بازیابی حالات کوانتومی که در معرض نویزهای خارجی یا داخلی قرار دارند، متمرکزشده‌اند. یکی از مهم‌ترین و متداول‌ترین انواع نویز، نویز جمعی[۴] است [۲۵]، دو نویز جمعی وجود دارد: نویز فاز جمعی[۵] و نویز چرخش جمعی[۶].

به دلیل تابع‌های گرمایی، نوسان و معیوب بودن فیبر نوری، نویز در کانال کوانتومی همیشه وجود دارد که باعث تغییر حالت‌ها در کانال کوانتومی می‌شود [۲۶]. تمام کیوبیت‌ها[۷] در یک پنجره زمانی به‌صورت جمعی تحت تأثیر یک نویز یکسان قرار می‌گیرند. بنابراین به این نوع نویز، نویز جمعی گفته می‌شود [۲۷]. نویز کانال به دلیل تغییراتی که در کیوبیت‌های حمل‌کننده پیام ایجاد می‌کند، مضر است و کاربران متوجه نمی‌شوند که این تغییرات را نویز کانال ایجاد کرده یا استراق‌سمع کننده (ایو[۸]) باعث آن بوده است [۲۸]. وجود نویز در کانال باعث انجام حمله‌های فعال بدون شناسایی استراق‌سمع کننده می‌شود و امنیت را بسیار به خطر می‌اندازد. گفتگوی امن کوانتومی تحت نویز جمعی، گفتگوی دو کاربر به‌صورت هم‌زمان یا پی‌درپی در یک کانال کوانتومی دارای نویز جمعی است.

در سال‌های اخیر بر روی نویز جمعی در QSD تحقیق و بررسی انجام شده است و پروتکل‌هایی ارائه شده است که با نویز در کانال مقابله می‌کند[۱۸]. در [۲۹] دو پروتکل QSD ارائه شده است که هرکدام با دو نوع نویز جمعی قدرتمند مقابله می‌کنند. این دو پروتکل QSD از حالت‌های چهار کیوبیتی مصون در برابر نویز که متشکل از دو جفت حالت Bell است، ساخته شده‌اند. گیرنده با دو اندازه‌گیری در پایه Bell به پیام امن دست پیدا می‌کند. علاوه بر این، به دلیل به اشتراک‌گذاری امن حالت‌های کوانتومی در ابتدای پروتکل این دو پروتکل عاری از هرگونه نشت اطلاعات هستند.

در [۳۰] دو پروتکل QSD مقاوم در برابر نویز جمعی ارائه شده است. زیر فضای بدون نویز برای بی‌اثر کردن دو نوع نویز جمعی استفاده می‌شود. در هر دو پروتکل، پیام امن بر روی کیوبیت منطقی اولیه توسط دو عملگر یکانی رمز می‌شود. علاوه بر این، اندازه‌گیری تک کیوبیت به اندازه‌گیری بر پایه Bell یا اندازه‌گیری‌های پیچیده برای رمزگشایی ترجیح داده می‌شود. برای اجتناب از نشت اطلاعات در هر دو پروتکل حالت اولیه کیوبیت منطقی به‌صورت خصوصی بین دو کاربر تأیید شده به اشتراک گذاشته می‌شود.

در [۳۱] دو پروتکل QSD دریک کانال رمزگذاری شده دارای نویز جمعی ارائه شده است. حالت‌های بدون نویز، از دو کیوبیت به‌عنوان حالت حامل پیام برای مبارزه با نویز جمعی تشکیل شده است. جفت‌های Bell، نقش کلید کوانتومی خصوصی را بازی می‌کنند، که بین دو کاربر توسط کانال کوانتومی دارای نویز جمعی به اشتراک گذاشته می‌شود. در [۳۲] دو پروتکل QSD ضد نویز بدون نشت اطلاعات با استفاده از فن‌آوری جابجایی درهم‌تنیدگی[۹] بین دو حالت Bell منطقی ارائه شده است. تأثیر منفی نویز با استفاده از حالت Bell منطقی به‌عنوان حالت کوانتومی حامل پیام، پاک شده است. از نشت اطلاعات به خاطر استفاده از جابجایی درهم‌تنیدگی بین دو حالت Bell منطقی اجتناب شده است. اندازه‌گیری چهار کیوبیتی حالت Bell برای رمزگشایی استفاده می‌شود.

در [۳۳] با استفاده از فن‌آوری درهم‌تنیدگی کوانتومی تحت نویز فاز جمعی و نویز چرخش جمعی دو پروتکل QSD ارائه شده است. حالت‌های Bell منطقی به‌عنوان حالات حامل پیام برای مقابله با نویز جمعی استفاده می‌شوند. حالت‌های Bell منطقی کمکی به‌طور خصوصی بین دو کاربر به اشتراک گذاشته می‌شوند. پیام امن گیرنده بر روی حالت Bell منطقی حاصل از جابجایی درهم‌تنیدگی رمز می‌شود. استراق‌سمع کننده به‌وسیله فوتون دام در حمله‌های فعال خود آشکار می‌شود. برای رمزگشایی در این پروتکل‌ها اندازه‌گیری چهار کیوبیتی در پایه Bell موردنیاز است. در [۳۴] دو طرح برای پروتکل‌های گفتگوی مستقیم امن کوانتومی که با نویز فاز جمعی و نویز چرخش جمعی سازگار است، ارائه شده است. در این مقاله با استفاده از حالت‌ها Bell منطقی به‌عنوان منتقل‌کننده پیام با نویز جمعی مقابله می‌شود. تمام حالت‌های Bell منطقی برای انتقال پیام امن بین دو کاربر قانونی استفاده می‌شود. اندازه‌گیری بر پایه Bell برای رمزگشایی چهار کیوبیت استفاده می‌شود. دو کاربر بدون انتقال پیام کلاسیک اضافی برای رمزگشایی، ارتباط مستقیم دارند. نشت اطلاعات با دو گام انتقال حل شده است.

در [۲۷] دو پروتکل QSD بر پایه حالت درهم‌تنیده[۱۰] GHZ ارائه شده است که با نویز جمعی مقابله می‌کنند. از طرفی برای پروتکل‌های ارائه شده، دو تابع رمزنگاری جدید طراحی شده است که با دو نوع نویز جمعی مقابله می‌کنند. این طرح‌ها در برابر حمله اسب تروجان[۱۱] مصون هستند و نشت اطلاعات ندارند. در [۳۵] دو پروتکل گفتگوی کوانتومی نامتقارن ارائه شده است. کارکرد هر دو پروتکل در مقابله با نویز جمعی بررسی شده است. برای مقابله در برابر نویز جمعی از کیوبیت‌های مصون در برابر نویز استفاده شده است. در سال‌های اخیر در زمینه گفتگوی امن کوانتومی تصدیق شده در کانال دارای نویز جمعی پژوهش‌هایی صورت گرفته است[۳۷،۳۶،۱۶]. تصدیق شده به‌معنای احراز هویت کاربر مقابل است تا از تعدادی از حملات استراق‌سمع کننده جلوگیری کنند.

در مراجع مختلف درمورد امنیت پروتکل ارائه شده یا پروتکل‌های مراجع دیگر بحث شده است[۱۶-۱۲]. در[۱۶] بعداز ارائه یک پروتکل گفتگوی امن کوانتومی تحت کانال‌های دارای نویز جمعی، تحلیل امنیت پروتکل خود را برای چند نوع حمله، اسب تروجان، درهم‌تنیدگی-اندازه‌گیری، رهگیری-ارسال مجدد و نوعی از حمله غیرفعال از استراق‌سمع کننده بیرونی بررسی کرده است.

در [۲۱] دو نوع پروتکل QSD تحت نویز جمعی ارائه شده است. در این مقاله نشت اطلاعات و تحلیل امنیت در برابر حمله‌های فعال استراق‌سمع کننده انجام شده است. این مرجع دو نوع حمله را بررسی کرده است ۱- حمله اندازه گیری-رهگیری-ارسال مجدد و ۲- حمله همبستگی-استخراج.

در این مقاله یک پروتکل جدید QSD تحت نویز فاز جمعی باهدف بهبود بازدهی ارائه شده است. در این پروتکل از حالت GHZ استفاده شده است و بازدهی نسبت به کارهای پیشین افزایش‌یافته و به ۴۲/۸۵٪ رسیده است. امنیت این پروتکل از چند منظر قابل اعتماد است. به‌دلیل استفاده از اشتراک‌گذاری محرمانه حالت اولیه نشت اطلاعات وجود ندارد. از حالت‌هایی برای انتقال اطلاعات محرمانه استفاده شده است که ماکسیمم درهم‌تنیدگی را دارند و اطلاعات در کانال کلاسیک نشت پیدا نمی‌کنند. به دلیل وجود نویز فاز جمعی در کانال به‌راحتی نمی‌توان از حالت GHZ استفاده کرد و برای حالت‌هایی از حالت GHZ که مقاوم در برابر نویز نیستند از عملگر یکانی محلی σ_X برای تبدیل آن به حالت‌های مقاوم در برابر نویز فاز جمعی استفاده شود. از یک دنباله کلاسیک به‌عنوان دنباله کمکی استفاده می‌شود. برای اینکه نشت اطلاعات وجود نداشته باشد، حالات اولیه به‌صورت تصادفی از بین چهار حالت عاری از نویز حالت GHZ انتخاب می‌شود. تک‌کیوبیت منطقی به‌عنوان کیوبیت دام استفاده می‌شود.

در این مقاله، در بخش ۲ مفاهیم مقدماتی موردنیاز این پروتکل ارائه شده است و بعد در بخش ۳ مراحل پروتکل QSD تحت نویز فاز جمعی به‌تفصیل توضیح داده شده است. در بخش ۴ امنیت پروتکل پیشنهادی بررسی شده است. در بخش ۵ بازدهی پروتکل پیشنهادی محاسبه شده است و در بخش ۶ مقایسه با پروتکل‌های پیشین انجام شده است. در بخش ۷ نتیجه‌گیری کوتاه از مقاله و پروتکل ارائه شده بیان شده است.

۲- مفاهیم مقدماتی

در این بخش ابتدا گذری کوتاه بر مکانیک کوانتومی و عملکرد نویز فاز جمعی خواهیم داشت، سپس روابط آنتروپی و اطلاعات متقابل شانون که در تحلیل امنیت پروتکل پیشنهادی مورد استفاده قرار می‌گیرند ارائه می‌گردد.

۲-۱- گذری بر مکانیک کوانتومی

واحد ذخیره‌سازی اطلاعات کوانتومی با بیت کوانتومی یا کیوبیت نامیده می‌شود. مدل ریاضی کیوبیت بردار یکه دو بعدی است که بردارهای پایه $|0\rangle$ و $|1\rangle$، تعریف شده در معادله (۱)، برای این فضا انتخاب شده است. تفاوت اصلی بین فیزیک کلاسیک و فیزیک کوانتوم برهم‌نهی[۱۲] است. بدین معنا که نه تنها $|0\rangle$ و $|1\rangle$ بلکه هر برهم‌نهی (ترکیب خطی) از آنها طبق معادله (۱) که $|\alpha|^2+|\beta|^2=1$ است، نیز یک حالت کوانتومی معتبر است. علاوه بر این، بردارهای $|\phi\rangle$ و $e^{i\theta}|\phi\rangle$ توصیف‌گر یک حالت کوانتومی هستند [۳۹،۳۸].

عملگر[۱۳] کوانتومی با یک ماتریس یکانی توصیف می‌گردد. ماتریس یکانی، ماتریسی است که ترانهاده-مزدوج آن برابر با معکوس آن باشد[۳۸]. از جمله مهمترین عملگرهای تک‌کیوبیتی، عملگرهای پائولی هستند که در معادلات (۲) توصیف شده‌اند. عملگرهای پائولی به‌صورت معادله (۳) برروی تک‌کیوبیت‌ها اثر می‌گذارند.

$$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix},|1\rangle=\begin{pmatrix}0\\1\end{pmatrix},\alpha|0\rangle+\beta|1\rangle=\begin{pmatrix}\alpha\\\beta\end{pmatrix}.$$
$$(\alpha=a_1+b_1i),(\beta=a_2+b_2i),0\le\alpha,\beta\le1 \quad (۱)$$

$$\sigma_I=|0\rangle\langle0|+|1\rangle\langle1|,$$
$$\sigma_X=|1\rangle\langle0|+|0\rangle\langle1|,$$
$$\sigma_Z=|0\rangle\langle0|-|1\rangle\langle1|. \quad (۲)$$

$$\sigma_I|0\rangle=|0\rangle,\sigma_I|1\rangle=|1\rangle,$$
$$\sigma_X|0\rangle=|1\rangle,\sigma_X|1\rangle=|0\rangle,$$
$$\sigma_Z|0\rangle=|0\rangle,\sigma_Z|1\rangle=-|1\rangle. \quad (۳)$$

نویز محیط بر روی تمام کیوبیت‌های گذر کرده از کانال کوانتومی تأثیر می‌گذارد. دو نوع نویز فاز جمعی و چرخش جمعی حائز اهمیت بیشتری هستند [۴۳-۴۰]. عملکرد نویز فاز جمعی (U_{dp}) بر روی تک‌کیوبیت‌ها با معادله (۴) توصیف می‌شود[۲۹].

$$U_{dp}|0\rangle=|0\rangle,U_{dp}|1\rangle=e^{i\varphi}|1\rangle,$$
$$U_{dp}(\alpha|0\rangle+\beta|1\rangle)=\alpha|0\rangle+\beta e^{i\varphi}|1\rangle, \quad (۴)$$

که φ پارامتر نویز و متغیر بازمان است.

حالت مقاوم در برابر نویز فاز جمعی را حالت منطقی نامیده و با زیرنویس "dp" نشان می‌دهیم. پایه‌های Z_{dp} و X_{dp} حالات تک‌کیوبیتی

منطقی مقاوم در برابر نویز فاز جمعی را نشان می‌دهند. این حالات به ترتیب در معادلات (۵) و (۶) معرفی شده‌اند.

$$|0\rangle_{dp}=|01\rangle,|1\rangle_{dp}=|10\rangle. \quad (۵)$$

$$|+\rangle_{dp}=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),|-\rangle_{dp}=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle). \quad (۶)$$

در این مقاله به هر کیوبیت از مجموعه $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ تک-کیوبیت فیزیکی و به هرکیوبیت از مجموعه $\{|0\rangle_{dp},|1\rangle_{dp},|+\rangle_{dp},|-\rangle_{dp}\}$، که مصون در برابر نویز فاز جمعی هستند، تک‌کیوبیت منطقی گفته می‌شود. حالات بل، حالات دوکیوبیتی هستند و به‌خاطر ویژگی‌های خود بعنوان پایه اندازه‌گیری از آن‌ها استفاده می‌شود. پایه‌های اندازه-گیری تک کیوبیتی در معادلات (۷) معرفی شده است[۳۸]. حالت بل منطقی نیز همان حالات بل است که بجای تک‌کیوبیت‌های $|0\rangle$ و $|1\rangle$ تک‌کیوبیت‌های منطقی $|0\rangle_{dp}$ و $|1\rangle_{dp}$ جایگزین شده است. پایه‌های اندازه‌گیری بل منطقی در معادلات (۸) معرفی شده است[۳۸].

$$\{|0\rangle,|1\rangle\} \quad (۷)$$

$$\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\} \quad (۸)$$

حالات GHZ که حالت‌هایی سه‌کیوبیتی هستند و بعنوان پایه-اندازه‌گیری سه‌کیوبیتی نیز از آنها استفاده می‌شود، این حالات در معادلات (۹) معرفی شده‌است. حالات Bell و حالات GHZ بیشینه درهم‌تنیدگی را دارند [۳۸]. کیوبیت‌های دوم و سوم حالات $|G_2\rangle$ و $|G_3\rangle$ و $|G_4\rangle$ و $|G_5\rangle$ طبق معادلات (۱۰) مقاوم در برابر نویز فاز جمعی هستند.

$$\begin{aligned}
&|G_0\rangle_{123}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle),|G_1\rangle_{123}=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle),\\
&|G_2\rangle_{123}=\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle),|G_3\rangle_{123}=\frac{1}{\sqrt{2}}(|001\rangle-|110\rangle),\\
&|G_4\rangle_{123}=\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle),|G_5\rangle_{123}=\frac{1}{\sqrt{2}}(|010\rangle-|101\rangle),\\
&|G_6\rangle_{123}=\frac{1}{\sqrt{2}}(|011\rangle+|100\rangle),|G_7\rangle_{123}=\frac{1}{\sqrt{2}}(|010\rangle-|101\rangle).
\end{aligned} \quad (۹)$$

$$\begin{aligned}
&(I\otimes U_{dp}\otimes U_{dp})|G_2\rangle_{123}=\frac{1}{\sqrt{2}}(|00e^{i\phi}1\rangle+|1e^{i\phi}10\rangle)\\
&=\frac{e^{i\phi}}{\sqrt{2}}(|001\rangle+|110\rangle)\cong\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle),\\
&(I\otimes U_{dp}\otimes U_{dp})|G_3\rangle_{123}=\frac{1}{\sqrt{2}}(|00e^{i\phi}1\rangle-|1e^{i\phi}10\rangle)\\
&=\frac{e^{i\phi}}{\sqrt{2}}(|001\rangle-|110\rangle)\cong\frac{1}{\sqrt{2}}(|001\rangle-|110\rangle),\\
&(I\otimes U_{dp}\otimes U_{dp})|G_4\rangle_{123}=\frac{1}{\sqrt{2}}(|0e^{i\phi}10\rangle+|10e^{i\phi}1\rangle)\\
&=\frac{e^{i\phi}}{\sqrt{2}}(|010\rangle+|101\rangle)\cong\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle),\\
&(I\otimes U_{dp}\otimes U_{dp})|G_5\rangle_{123}=\frac{1}{\sqrt{2}}(|0e^{i\phi}10\rangle-|10e^{i\phi}1\rangle)\\
&=\frac{e^{i\phi}}{\sqrt{2}}(|010\rangle-|101\rangle)\cong\frac{1}{\sqrt{2}}(|010\rangle-|101\rangle).
\end{aligned} \quad (۱۰)$$

۲-۲- آنتروپی شانون[۱۴]

میزان ابهام یک فرآیند تصادفی مانند $X=\{x_1,x_2,...,x_n\}$ را با آنتروپی ($H(X)$) نشان می‌دهند[۴۴] که در معادله (۱۱) معرفی شده است. در این رابطه، $P_X(x_i)$ احتمال وقوع x_i است.

$$H(X)=-\sum_{i=1}^{n}P_X(x_i)\log P_X(x_i), \quad (۱۱)$$

آنتروپی شرطی بین دو فرآیند تصادفی X و Y بدین معناست که اگر Yرخ دهد، ابهام درمورد X چقدر است. اگر X و Y مستقل باشند آنتروپی شرطی برابر با $H(X)$ می‌شود[۴۴]. آنتروپی شرطی در معادله (۱۲) معرفی شده است.

که $P_{X|Y}(x_i|y_i)$ احتمال شرطی بین x_i و y_i است. احتمال شرطی بدین معناست که احتمال وقوع x_i در صورت اینکه y_iرخداده باشد، چه میزان است.

میزان اطلاعات متقابل بین دو فرآیند تصادفی X و Y بدین معنا است که X و Y از هم چه میزان اطلاعات دارند. زمانی که X و Y مستقل از هم باشند، یعنی وقوع یکی به دیگری وابسته نباشد، میزان اطلاعات متقابل صفر است. اطلاعات متقابل ($I(X;Y)$) در معادله (۱۳) معرفی شده است [۴۴].

$$H(X|Y)=-\sum_{i=1}^{n}P_{X|Y}(x_i|y_i)\log P_{X|Y}(x_i|y_i), \quad (۱۲)$$

$$I(X;Y)=H(X)-H(X|Y), \quad (۱۳)$$

۳- پروتکل گفتگوی امن کوانتومی تحت نویز فاز جمعی

در این قسمت پروتکل جدیدی با هدف بهبود بازدهی ارائه شده است. در این پروتکل با استفاده از حالت‌های عاری از نویز GHZ می‌توان اثر نویز فاز جمعی و حملات استراق‌سمع کننده را از بین برد و یک گفتگوی امن کوانتومی عاری از نویز داشت. این پروتکل به‌صورت کاملا جدیدی سازماندهی شده است. انتخاب حالات اولیه، روش به اشتراک-گذاری آن‌ها، نحوه استفاده از کانال کلاسیک و امنیت روش استفاده شده کاملا جدید است.

در قسمت‌هایی از پروتکل به آستانه‌گذاری اشاره شده است. آستانه در هر بار استفاده از پروتکل توسط کاربران و با توجه به شرایط محیطی، نویزهای موجود، درصد امنیت مورد نیاز و هزینه اجرای پروتکل انتخاب می‌شود.

در این پروتکل آلیس و باب می‌توانند $m=3$ بیت پیام امن خود را به-صورت محرمانه و هم‌زمان مبادله کنند. پیام امن آلیس را m_Aو پیام امن باب را m_Bنام‌گذاری می‌کنیم. در ابتدای پروتکل، کاربران از جابجایی درهم‌تنیدگی برای اشتراک‌گذاری محرمانه حالات اولیه استفاده می‌کنند که این امر باعث جلوگیری از نشت اطلاعات می‌شود. سپس آن‌ها ابتدا m بیت پیام امن را به n بسته سه بیتی تقسیم می-

کنند. هر سه بیت از m_A و m_B بر روی کیوبیت‌های دوم و سوم یک حالت GHZ مقاوم در برابر نویز فاز جمعی کد شده و بر روی کانال دارای نویز فاز جمعی ارسال می‌شود. جزئیات مراحل پروتکل به شرح زیر است. در پایان در شکل ۱ بلوک دیاگرامی از اجرای پروتکل رسم شده است. برای بهتر مفهوم شدن مثالی از اجرای پروتکل را مرحله به مرحله پیش می‌بریم. فرض کنید در این مثال، $m_A=101$ و $m_B=011$ می‌باشد.

مرحله۱- اشتراک‌گذاری محرمانه حالات اولیه: آلیس تعداد $2n$ از حالات $|G_2\rangle$ تولید می‌کند که دنباله I نامیده می‌شود. او دو حالت مجاور از حالات $|G_2\rangle$ را در یک بسته قرار می‌دهد. مانند معادله (۱۴) کیوبیت فیزیکی اول از این بسته ۶ کیوبیتی را کیوبیت ۱ و دوکیوبیت فیزیکی بعدی که یک کیوبیت منطقی را می‌سازند را کیوبیت ۲ منطقی (2_{dp})، کیوبیت فیزیکی بعدی را کیوبیت ۳ و دو کیوبیت فیزیکی آخر را کیوبیت ۴ منطقی (4_{dp}) می‌نامیم. آلیس دنباله I را به دو دنباله I_A و I_B تقسیم می‌کند که I_A حاوی کیوبیت‌های فیزیکی ۱ و ۳ و I_B حاوی کیوبیت‌های منطقی ۲ و ۴ از هر دسته است. آلیس I_A را نزد خود نگه‌داشته و دنباله I_B را که مصون در برابر نویز فاز جمعی است را با فن‌آوری کیوبیت دام [۴۶,۴۵] برای باب ارسال می‌کند. دراین‌جا به دلیل حضور نویز فاز جمعی در کانال کوانتومی، از تک‌کیوبیت‌های منطقی برای فن‌آوری کیوبیت دام استفاده می‌شود.

$$
\begin{aligned}
&|G_2\rangle_{123}\otimes|G_2\rangle_{456}=\frac{1}{2}(|001\rangle+|110\rangle)_{123}\\
&\otimes(|001\rangle+|110\rangle)_{456}\\
&=\frac{1}{2}(|001001\rangle+|001110\rangle+|110001\rangle+|110110\rangle)_{123456}\\
&=\frac{1}{2}(|0\rangle|01\rangle|0\rangle|01\rangle+|0\rangle|01\rangle|1\rangle|10\rangle\\
&+|1\rangle|10\rangle|0\rangle|01\rangle+|1\rangle|10\rangle|1\rangle|10\rangle)_{1,2_{dp},3,4_{dp}}\\
&=\frac{1}{2}(|000101\rangle+|010110\rangle+|101001\rangle+|111010\rangle)_{1,3,2_{dp},4_{dp}}\\
&=\frac{1}{2}(|00\rangle|00\rangle+|01\rangle|01\rangle+|10\rangle|10\rangle+|11\rangle|11\rangle)_{1,3,2_{dp},4_{dp}}
\end{aligned}
\qquad (۱۴)
$$

مرحله۲- بررسی حضور استراق‌سمع کننده: باب بعد از دریافت دنباله I_B، دریافت آن را به آلیس اطلاع می‌دهد. سپس آلیس موقعیت قرار گرفتن کیوبیت‌های دام و پایه اندازه‌گیری و نتیجه اندازه-گیری در دنباله را به باب گزارش می‌دهد. اکنون باب کیوبیت‌های دام منطقی را از دنباله اصلی جدا کرده و آن‌ها را در پایه اعلامی آلیس اندازه‌گیری می‌کند و نتیجه اندازه‌گیری را با نتیجه اعلامی آلیس مقایسه کرده و در مورد حضور استراق‌سمع کننده تصمیم می‌گیرد و نتیجه را اعلام می‌کند. اگر استراق‌سمع کننده حضور داشته باشد مخابره قطع می‌شود درغیر این‌صورت مخابره ادامه پیدا کرده و به مرحله بعدی می‌رود [۲۶].

مرحله۳- جابجایی درهم‌تنیدگی: آلیس دنباله I_A را در پایه Bell اندازه‌گیری می‌کند و باب نیز دنباله I_B را در پایه Bell منطقی اندازه‌گیری می‌کند. با این اندازه‌گیری بین آلیس و باب جابجایی درهم‌تنیدگی اتفاق می‌افتد[۴۷]. جدول۱، طبق معادله (۱۵)، نتیجه اندازه‌گیری را نشان می‌دهد. احتمال مشاهده هرکدام از حالات Bell برای آلیس و حالات Bell منطقی برای باب $\frac{1}{4}$ است. از طرفی باب و آلیس به ازای نتیجه اندازه‌گیری $\{|\psi^+\rangle,|\psi^+\rangle_{dp}\}$ یا $\{|\varphi^+\rangle,|\varphi^+\rangle_{dp}\}$ بیت 0 و به ازای نتیجه اندازه‌گیری $\{|\psi^-\rangle,|\psi^-\rangle_{dp}\}$ یا $\{|\varphi^-\rangle,|\varphi^-\rangle_{dp}\}$ بیت 1 را تولید می‌کنند و دنباله کلاسیک n بیتی حاصل را A_{AB} می‌نامند و هر بیت از آن را a_{AB} می-نامند.

در مثال مفروض، فرض می‌کنیم آلیس و باب در اندازه‌گیری برای جابجایی درهم‌تنیدگی به ترتیب $|\psi^+\rangle$ و $|\psi_{dp}^+\rangle$ را مشاهده کرده‌اند. بنابراین بیت کلاسیک کمکی حاصل در دنباله $a_{AB}=0$ است.

$$
\begin{aligned}
&|G_2\rangle_{1,2_{dp}}\otimes|G_2\rangle_{3,4_{dp}}=\frac{1}{2}(|0\rangle|0\rangle+|1\rangle|1\rangle)_{1,2_{dp}}\\
&\otimes(|0\rangle|0\rangle+|1\rangle|1\rangle)_{3,4_{dp}}=\frac{1}{2}(|0\rangle|0\rangle|0\rangle|0\rangle\\
&+|0\rangle|0\rangle|1\rangle|1\rangle+|1\rangle|1\rangle|0\rangle|0\rangle\\
&+|1\rangle|1\rangle|1\rangle|1\rangle)_{1,2_{dp},3,4_{dp}}=\frac{1}{2}(|0\rangle|0\rangle|0\rangle|0\rangle\\
&+|0\rangle|1\rangle|0\rangle|1\rangle+|1\rangle|0\rangle|1\rangle|0\rangle\\
&+|1\rangle|1\rangle|1\rangle|1\rangle)_{1,3,2_{dp},4_{dp}}=\frac{1}{2}(|\varphi^+\rangle|\varphi^+\rangle_{dp}\\
&+|\varphi^-\rangle|\varphi^-\rangle_{dp}+|\psi^+\rangle|\psi^+\rangle_{dp}+|\psi^-\rangle|\psi^-\rangle_{dp})_{1,3,2_{dp},4_{dp}}
\end{aligned}
\qquad (۱۵)
$$

جدول (۱): نتایج اندازه‌گیری مرحله ۲

احتمال	حالت پس از اندازه-گیری آلیس	حالت پس از اندازه-گیری باب	بیت کلاسیک در دنباله A_{AB}
$\frac{1}{4}$	$\|\varphi^+\rangle$	$\|\varphi^+\rangle_{dp}$	0
$\frac{1}{4}$	$\|\varphi^-\rangle$	$\|\varphi^-\rangle_{dp}$	0
$\frac{1}{4}$	$\|\psi^+\rangle$	$\|\psi^+\rangle_{dp}$	1
$\frac{1}{4}$	$\|\psi^-\rangle$	$\|\psi^-\rangle_{dp}$	1

مرحله۴- تولید حالت اولیه: باب سه کیوبیت فیزیکی آخر از حالات Bell منطقی خودش را در پایه GHZ اندازه‌گیری می‌کند و طبق معادلات (۱۶) یکی از چهار حالت GHZ مقاوم در برابر نویز فاز جمعی را با احتمال $\frac{1}{2}$ به‌دست می‌آورد. باب با اعمال عملگر محلی بر

روی کیوبیت سوم طبق جدول ۲ حالت GHZ حاصل از اندازه‌گیری را به حالات GHZ مورد توافق با آلیس تبدیل می‌کند. او دنباله حاوی حالات اولیه را S می‌نامد. در مثال ذکر شده فرض کنید حالت پس از اندازه‌گیری باب $|G_2\rangle$ است.

$$|\varphi^+\rangle_{dp}=\frac{1}{\sqrt{2}}\left(|00\rangle_{dp}+|11\rangle_{dp}\right)=\frac{1}{\sqrt{2}}(|+\rangle|G_4\rangle_{123}-|-\rangle|G_5\rangle_{123}),$$
$$|\varphi^-\rangle_{dp}=\frac{1}{\sqrt{2}}\left(|00\rangle_{dp}-|11\rangle_{dp}\right)=\frac{1}{\sqrt{2}}(|-\rangle|G_4\rangle_{123}-|+\rangle|G_5\rangle_{123}),$$
$$|\psi^+\rangle_{dp}=\frac{1}{\sqrt{2}}\left(|01\rangle_{dp}+|10\rangle_{dp}\right)=\frac{1}{\sqrt{2}}(|+\rangle|G_2\rangle_{123}-|-\rangle|G_3\rangle_{123}),$$
$$|\psi^-\rangle_{dp}=\frac{1}{\sqrt{2}}\left(|01\rangle_{dp}-|10\rangle_{dp}\right)=\frac{1}{\sqrt{2}}(|-\rangle|G_2\rangle_{123}-|+\rangle|G_3\rangle_{123}).\quad(16)$$

جدول(۲): حالات اولیه GHZ متناظر با حالات بل منطقی

حالات Bell منطقی	احتمال	حالت GHZ حاصل از اندازه‌گیری باب	عملگر مورداستفاده بر روی کیوبیت دوم	حالت پس‌از اعمال عملگر
$\|\varphi^+\rangle_{dp}$	$1/2$	$\|G_4\rangle$	σ_I	$\|G_4\rangle$
	$1/2$	$\|G_5\rangle$	σ_Z	
$\|\varphi^-\rangle_{dp}$	$1/2$	$\|G_4\rangle$	σ_Z	$\|G_5\rangle$
	$1/2$	$\|G_5\rangle$	σ_I	
$\|\psi^+\rangle_{dp}$	$1/2$	$\|G_2\rangle$	σ_I	$\|G_2\rangle$
	$1/2$	$\|G_3\rangle$	σ_Z	
$\|\psi^-\rangle_{dp}$	$1/2$	$\|G_2\rangle$	σ_Z	$\|G_3\rangle$
	$1/2$	$\|G_3\rangle$	σ_I	

مرحله۵- رمزنگاری پیام امن باب: باب دنباله S را به دو دنباله با نام‌های S_1 و S_{23} تقسیم می‌کند. دنباله S_1 شامل ذره 1 و دنباله S_{23} شامل ذرات 2 و 3 از هر حالت GHZ مقاوم در برابر نویز فاز جمعی است. باب S_1 را برای خود نگه‌داشته و هر نمونه سه بیتی از m_B را بر روی یک بسته دو کیوبیتی در دنباله S_{23} طبق جدول ۳ رمز می‌کند. از آنجا که طبق این جدول، دو پیام مختلف به یک حالت GHZ کد شده است برای ایجاد امکان کدبرداری باب، به ازای بیت‌های پیام 000، 001، 010 و 011 بیت 0 و به ازای بیت‌های پیام 100، 101، 110 و 111 بیت 1 قرار می‌دهد. این دنباله کلاسیک را A_B و هر بیت از آن را a_B می‌نامیم. سپس او برای عدم افشای دنباله A_B بین بیت‌های دنباله کلاسیک A_{AB} و A_B عملگر کلاسیک XOR اعمال کرده و دنباله حاصل $(A_B^{'})$ را برای آلیس از طریق کانال کلاسیک عمومی ارسال می‌کند. باب همچنین دنباله $S_{23,B}$ را با فن‌آوری کیوبیت دام [۴۶,۴۵] برای آلیس ارسال می‌کند.

برای رمزگذاری پیام امن ابتدا طبق جدول ۳ مطابق با هر پیام امن سه‌بیتی عملگرهای محلی و بیت کلاسیک مناسب را در نظر انتخاب کردیم. عملگرها طوری انتخاب شده‌اند تا یک حالت GHZ مقاوم در برابر نویز فاز جمعی را به یک حالت دیگر مقاوم در برابر نویز فاز جمعی تبدیل می‌کنند. از آنجا که هشت پیام امن متمایز و تنها چهار حالت GHZ مقاوم در برابر نویز داریم، برای متمایز کردن هردو حالت مقاوم در برابر نویز تکرار شده از بیت کلاسیک استفاده می‌کنیم. در مثال مطرح‌شده، باب $m_B=011$ را برروی حالت اولیه $|G_2\rangle$ طبق جدول ۳ رمز می‌کند ($\sigma_X\otimes\sigma_Z\sigma_X$) و a_B مناسب با m_B را طبق جدول ۳ انتخاب می‌کند ($a_B=0$). او طبق معادله (۱۷) حالت $|G_5\rangle$ را با فن‌آوری کیوبیت دام [۴۶, ۴۵] با استفاده از کانال کوانتومی و $a_B^{'}=a_B\oplus a_{AB}=0\oplus 0=0$ را از طریق کانال کلاسیک برای آلیس ارسال می‌کند.

$$|G_2\rangle\xrightarrow{\sigma_X\otimes\sigma_Z\sigma_X}|G_5\rangle\quad(17)$$

مرحله۶- بررسی حضور استراق‌سمع کننده: آلیس مانند مرحله ۲ عمل می‌کند و در مورد حضور استراق‌سمع کننده تصمیم می‌گیرد و نتیجه را اعلام می‌کند. اگر استراق‌سمع کننده حضورداشته باشد مخابره قطع می‌شود درغیر این‌صورت مخابره ادامه پیدا کرده و به مرحله بعدی می‌روند.

مرحله۷- رمزنگاری پیام امن آلیس: آلیس نیز، پیام m_A را به دسته‌های سه بیتی تقسیم می‌کند. هر نمونه سه بیتی از m_A را بر روی کیوبیت‌ها در دنباله $S_{23,B}$ که از باب دریافت کرده با اعمال عملگرهای پائولی طبق جدول ۳ رمز می‌کند. حالت‌های پس از اعمال عملگرها، با توجه به حالت اولیه، نیز در جدول نشان داده شده است که GHZهای مصون در برابر نویز جمعی می‌باشند. از آنجا که در هر ستون، هر حالت GHZ دو بار تکرار شده است، برای ایجاد تمایز بین آنها و امکان کدبرداری، آلیس یک دنباله کلاسیک به نام A_A تولید می‌کند که به ازای بیت‌های پیام 000، 001، 010 و 011 بیت $a_A=0$ و به ازای بیت‌های پیام 100، 101، 110 و 111 بیت $a_A=1$ قرار می‌دهد. سپس آلیس برای عدم افشای اطلاعات دنباله A_A، بین بیت‌های متناظر دنباله کلاسیک A_{AB} و A_A عملگر کلاسیک XOR اعمال می‌کند و دنباله کلاسیک حاصل $(A_A^{'})$ را برای باب از طریق کانال کلاسیک عمومی ارسال می‌کند. آلیس همچنین دنباله $S_{23,BA}$ را با فن‌آوری کیوبیت دام [۴۶, ۴۵] برای باب ارسال می‌کند.

در مثال مطرح‌شده، $m_A=101$ است، بنابراین در این مرحله آلیس طبق جدول۳ عملگر مناسب را برروی حالت اولیه $|G_5\rangle$ دریافتی از باب اعمال می‌کند و a_A مناسب با m_A را طبق جدول ۳ انتخاب می‌کند ($a_A=1$). او طبق معادله (۱۸) حالت $|G_2\rangle$ را با فن‌آوری کیوبیت دام [۴۵,۴۴] با استفاده از کانال کوانتومی و

$a_A^{'} = a_A \oplus a_{AB} = 1 \oplus 0 = 1$ را از طریق کانال کلاسیک برای باب ارسال می‌کند.

$$|G_5\rangle \xrightarrow{\sigma_X \otimes \sigma_Z \sigma_X} |G_2\rangle \quad (18)$$

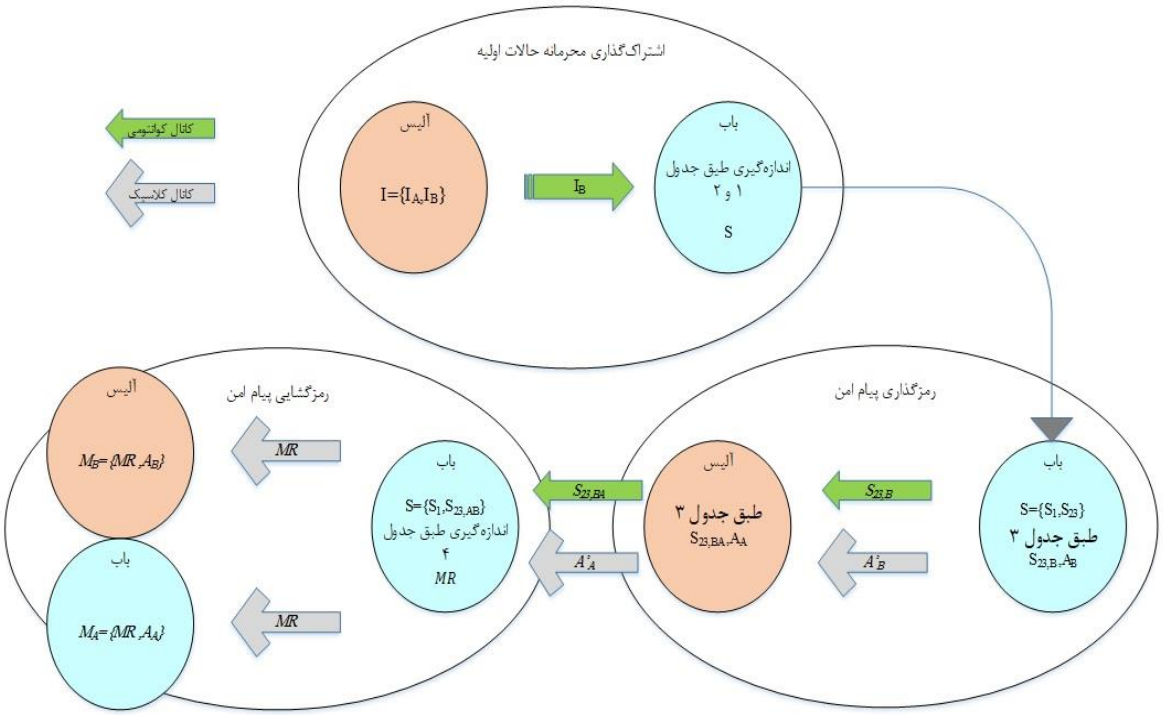
مرحله۸- بررسی دائم حضور استراق‌سمع کننده: باب مانند مرحله ۲ عمل می‌کند و در مورد حضور استراق‌سمع کننده تصمیم می‌گیرد و نتیجه را اعلام می‌کند. اگر استراق‌سمع کننده حضورداشته باشد مخابره قطع می‌شود، درغیر این‌صورت مخابره ادامه پیدا می‌کند و به مرحله بعدی می‌روند.

مرحله۹- رمز برداری پیام امن آلیس و باب: باب با ترکیب n حالت در دو دنباله S_1 و $S_{23,BA}$، دنباله S_{BA} را تولید کرده و هر بسته سه کیوبیتی از این دنباله را در پایه GHZ اندازه‌گیری می‌کند و نتیجه اندازه‌گیری (MR) را از طریق کانال کلاسیک عمومی به آلیس اعلام می‌کند. اکنون آلیس و باب بین بیت‌های دنباله $A_A^{'}$ و $A_B^{'}$ دریافتی و A_{AB} دست خود عملگر کلاسیک XOR اعمال می‌کنند و به ترتیب به دنباله‌های A_A و A_B دست می‌یابند. سپس آلیس و باب طبق بیت‌های پیام محرمانه خود، بیت‌های کمکی، حالت اولیه و حالت نهایی اندازه‌گیری‌شده، به بیت‌های پیام محرمانه کاربر دیگر طبق جدول ۴، دسترسی پیدا می‌کنند. جدول ۴ بدین صورت به دست آمده‌است که با توجه به حالت اولیه، پیام محرمانه هر کاربر، A_A و A_B دست خود و حالت نهایی، طبق جدول ۳، می‌توان به عملگر اعمالی و پیام امن کاربر دیگر پی‌برد.

در این مرحله از مثال حالت نهایی توسط باب در پایه GHZ اندازه‌گیری می‌شود و باب نتیجه اندازه‌گیری را بر روی کانال کلاسیک عمومی اعلام می‌کند. حالت نهایی در این مثال $|G_2\rangle$ است و a_B و a_A نیز مشخص است. آلیس برای خواندن پیام امن باب مانند معادله (۱۹) عمل می‌کند. باب نیز برای خواندن پیام امن آلیس مانند معادله (۲۰) عمل می‌کند. آلیس و باب پیام امن یکدیگر را طبق جدول ۴ می‌خوانند.

$$a_B = a_B^{'} \oplus a_{AB} = 0 \oplus 0 = 0$$
$$|G_2\rangle \xrightarrow{\sigma_X \otimes \sigma_Z \sigma_X} |G_5\rangle \rightarrow m_B = 011 \quad (19)$$

$$a_A = a_A^{'} \oplus a_{AB} = 1 \oplus 0 = 1$$
$$|G_2\rangle \xrightarrow{\sigma_X \otimes \sigma_Z \sigma_X} |G_5\rangle \rightarrow m_A = 101 \quad (20)$$



شکل (۱): بلوک دیاگرام مراحل پروتکل پیشنهادی

۴- تحلیل امنیت پروتکل پیشنهادی

در این بخش برای تحلیل امنیت پروتکل پیشنهادی سه معیار مهم که امنیت بدون قید و شرط را به همراه می‌آورد بررسی می‌شود. در بخش ۴-۱ عدم نشت اطلاعات در بیت‌های کلاسیک اعلامی در کانال کلاسیک عمومی در پروتکل پیشنهادی بررسی شده است. در بخش ۴-۲ شناسایی ایو در حمله‌های فعال او در پروتکل پیشنهادی بررسی شده است. در بخش ۴-۳ عدم افشای اطلاعات به وسیله استفاده از حالت درهم‌تنیده اثبات شده است. در بخش ۴-۴ مقابله پروتکل پیشنهادی با حمله اسب تروجان بررسی شده است.

$$p(mr_B = 00 \mid m_A = ijk, m_B = i'j'k') = \frac{1}{4},$$
$$p(mr_B = 01 \mid m_A = ijk, m_B = i'j'k') = \frac{1}{4},$$
$$p(mr_B = 10 \mid m_A = ijk, m_B = i'j'k') = \frac{1}{4},$$
$$P(mr_B = 11 \mid m_A = ijk, m_B = i'j'k') = \frac{1}{4},$$
$$i, j, k, i', j', k' \in \{0,1\}. \quad (۲۳)$$

۴-۱- عدم نشت اطلاعات در کانال کلاسیک

نشت اطلاعات بدین معناست که استراق‌سمع کننده بدون انجام هیچ نوع حمله فعالی به کیوبیت‌های ارسالی و صرفا توسط اطلاعات کلاسیک آشکار شده در کانال عمومی به بخشی از اطلاعات امن دست پیدا می‌کند [۴۸]. در این بخش از فرمول آنتروپی شانون [۴۴] برای پیدا کردن میزان اطلاعات متقابل ایو و کاربران استفاده شده‌است.

در پروتکل پیشنهادی دو دسته داده کلاسیک آشکار می‌شود: ۱) بیت‌های کمکی A'_A و A'_B و ۲) نتیجه اندازه‌گیری حالت نهایی در پایه GHZ.

در ادامه به ترتیب ثابت می‌کنیم که در دو حالت اطلاعاتی از پیام امن برای ایو آشکار نمی‌شود.

۱) از آنجا که طبق مراحل پروتکل، A'_A و A'_B حاصل XOR نتایج دو متغیر کاملا تصادفی است، معادلات (۲۰)، احتمال وقوع و احتمال وقوع شرطی a'_A را نشان می‌دهد. احتمال وقوع و احتمال وقوع شرطی a'_B به طرز مشابه به‌دست می‌آید. از معادلات (۲۰) می‌توان معادلات (۲۱) را نتیجه گرفت که در آن M_A و M_B به ترتیب متغیرهای تصادفی پیام امن آلیس و باب می‌باشد. از معادلات (۲۱) مشخص است که اطلاعات متقابل صفر است.

$$p(a'_A = l \mid m_A = ijk) = \frac{1}{2}, \qquad l, i, j, k \in \{0,1\}$$
$$p(a'_A = l) = \sum_{i,j,k \in \{0,1\}} p(a'_A = l \mid m_A = ijk)$$
$$= 8 \times \frac{1}{8} \times \frac{1}{2} = \frac{1}{2}. \quad (۲۱)$$

$$H(A'_A \mid M_A) = H(A'_A) \rightarrow I(A'_A; M_A) = 0,$$
$$H(A'_B \mid M_B) = H(A'_B) \rightarrow I(A'_B; M_B) = 0, \quad (۲۲)$$

۲) چنانچه متغیر تصادفی مرتبط با نتیجه اندازه‌گیری حالت نهایی در پایه GHZ، را با MR_B و هر نمونه از آن را با متغیر mr_B نشان دهیم و نتیجه کلاسیک مشاهده شده وقتی که حالت $|G_2\rangle$، $|G_3\rangle$، $|G_4\rangle$ و $|G_5\rangle$ را به ترتیب با 00، 01، 10 و 11 نام‌گذاری کنیم، طبق جدول ۴ معادلات (۲۲) بدست می آید. از معادلات (۲۲) می‌توان معادلات (۲۳) را نتیجه گرفت و در نهایت معادله (۲۴) حاصل می‌شود که دلالت بر اطلاعات متقابل صفر دارد.

$$p(mr_B = 00) = \sum p(mr_B = 00 \mid m_A = ijk, m_B = i'j'k')$$
$$\times p(m_A = ijk, m_B = i'j'k') = \frac{1}{4},$$
$$p(mr_B = 01) = p(mr_B = 10) = p(mr_B = 11) = \frac{1}{4}. \quad (۲۴)$$

$$H(MR_B) = H(MR_B \mid M_A, M_B)$$
$$\rightarrow I(MR_B; (M_A, M_B)) = 0. \quad (۲۵)$$

۴-۲- شناسایی ایو در حمله‌های فعال

فن‌آوری کیوبیت دام [۴۶،۴۵] برای آشکارسازی استراق‌سمع کننده و ارسال امن کیوبیت‌های حاوی پیام، بین فرستنده و گیرنده استفاده می‌شود. برای بررسی حضور استراق‌سمع کننده در کانال دارای نویز فاز جمعی، در جایگاه‌های تصادفی در دنباله کیوبیت‌های ارسالی، تک‌کیوبیت منطقی دام که حالت آن از بین چهار حالت $\{|0\rangle_{dp}, |1\rangle_{dp}, |+\rangle_{dp}, |-\rangle_{dp}\}$ تصادفی انتخاب می‌شود، قرار داده می‌شود. بعد از دریافت دنباله توسط گیرنده، گیرنده ابتدا دریافت دنباله را به فرستنده اطلاع می‌دهد و فرستنده موقعیت و نتیجه اندازه‌گیری کیوبیت‌های دام را به گیرنده اطلاع می‌دهد. گیرنده در موقعیت‌های اعلامی با پایه اندازه‌گیری گفته شده، اندازه‌گیری انجام می‌دهد و نتیجه اندازه‌گیری را با نتیجه اعلامی فرستنده مقایسه می‌کند. اگر نتایج یکسان باشد پروتکل ادامه یافته و در غیر اینصورت به دلیل تشخیص حضور ایو، پروتکل قطع می‌شود. تعداد کیوبیت‌های دام، برابر با تعداد کیوبیت‌های پیام (m) در نظر گرفته می‌شود. در این صورت احتمال تشخیص ایو برابر با $1-\left(\frac{1}{2}\right)^m$ خواهد بود. زمانی که m عدد بزرگی باشد، احتمال آشکار شدن حضور ایو نزدیک به یک می‌شود.

۴-۳- عدم نشت اطلاعات در حمله‌های فعال

در بخش ۴-۲ ثابت کردیم که حمله فعال توسط ایو، آشکار می‌شود. در این بخش ثابت می‌کنیم که ایو به هیچ میزان از پیام امن نیز دست نخواهد یافت. در ادامه ثابت می‌کنیم به خاطر استفاده از حالت درهم‌تنیده GHZ و ارسال دو کیوبیت از آن، حتی اگر ایو در هر پایه متعامد دلخواه $B = \{|b_{00}\rangle, |b_{01}\rangle, |b_{10}\rangle, |b_{11}\rangle\}$ اندازه‌گیری کند اطلاعاتی از پیام امن نخواهد داشت.

جدول (۳): عملگرهای رمزنگاری پیام امن سه بیتی

۳ بیت پیام امن	عملگر یکانی روی کیوبیت-های B و C	بیت کلاسیک a متناظر با پیام امن	حالت GHZ متناظر با پیام امن، با فرض حالت اولیه $\|G_2\rangle$	حالت GHZ متناظر با پیام امن، با فرض حالت اولیه $\|G_3\rangle$	حالت GHZ متناظر با پیام امن، با فرض حالت اولیه $\|G_4\rangle$	حالت GHZ متناظر با پیام امن، با فرض حالت اولیه $\|G_5\rangle$
000	$\sigma_I \otimes \sigma_I$	0	$\|G_2\rangle$	$\|G_3\rangle$	$\|G_4\rangle$	$\|G_5\rangle$
001	$\sigma_Z \otimes \sigma_I$	0	$\|G_3\rangle$	$\|G_2\rangle$	$\|G_5\rangle$	$\|G_4\rangle$
010	$\sigma_X \otimes \sigma_X$	0	$\|G_4\rangle$	$\|G_5\rangle$	$\|G_2\rangle$	$\|G_3\rangle$
011	$\sigma_X \otimes \sigma_Z\sigma_X$	0	$\|G_5\rangle$	$\|G_4\rangle$	$\|G_3\rangle$	$\|G_2\rangle$
100	$\sigma_X \otimes \sigma_X$	1	$\|G_4\rangle$	$\|G_5\rangle$	$\|G_2\rangle$	$\|G_3\rangle$
101	$\sigma_X \otimes \sigma_Z\sigma_X$	1	$\|G_5\rangle$	$\|G_4\rangle$	$\|G_3\rangle$	$\|G_2\rangle$
110	$\sigma_I \otimes \sigma_I$	1	$\|G_2\rangle$	$\|G_3\rangle$	$\|G_4\rangle$	$\|G_5\rangle$
111	$\sigma_Z \otimes \sigma_I$	1	$\|G_3\rangle$	$\|G_2\rangle$	$\|G_5\rangle$	$\|G_4\rangle$

جدول (۴): کدبرداری پیام امن سه بیتی

		کدبرداری با حالت اولیه $\|G_2\rangle$				کدبرداری با حالت اولیه $\|G_3\rangle$			
a کاربر دیگر	بیت محرمانه خود کاربر	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_2\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_3\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_4\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_5\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_2\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_3\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_4\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_5\rangle$
0	000	000	001	010	011	001	000	011	010
1	000	110	111	100	101	111	110	101	100
0	001	001	000	011	001	000	001	010	011
1	001	111	110	101	111	110	111	100	101
0	010	010	011	000	010	010	010	001	000
1	010	100	101	110	100	101	100	111	110
0	011	011	010	001	000	011	011	000	001
1	011	101	100	**111**	110	101	101	110	111
0	100	100	011	000	001	010	010	001	001
1	100	010	101	110	111	100	101	**111**	111
0	101	011	010	001	000	011	010	000	000
1	101	101	100	111	110	101	100	110	110
0	110	000	001	010	011	000	001	011	011
1	110	110	111	100	101	110	111	101	101
0	111	001	000	011	010	011	000	010	010
1	111	111	110	101	100	111	110	111	110
		کدبرداری با حالت اولیه $\|G_4\rangle$				کدبرداری با حالت اولیه $\|G_5\rangle$			
a کاربر دیگر	بیت محرمانه خود کاربر	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_2\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_3\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_4\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_5\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_2\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_3\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_4\rangle$	بیت‌های محرمانه کاربر دیگر با فرض حالت نهایی $\|G_5\rangle$
0	000	010	011	000	001	011	010	001	000
1	000	100	101	110	111	101	100	111	110
0	001	011	010	001	000	010	011	000	001
1	001	101	100	111	110	100	101	110	111
0	010	000	001	010	011	001	000	011	010
1	010	110	111	100	101	111	110	101	100

011	010	001	000	010	011	000	001	011	0
101	100	111	110	100	101	110	111	011	1
010	011	000	001	011	010	001	000	100	0
100	101	110	111	101	100	111	110	100	1
011	010	001	000	010	011	000	001	101	0
101	100	111	110	100	101	110	111	101	1
000	001	010	011	001	000	011	010	110	0
110	111	100	101	111	110	101	100	110	1
001	000	011	010	000	001	010	011	111	0
111	110	101	100	110	111	100	101	111	1

فرض کنید حالات $|01\rangle$ و $|10\rangle$ برحسب پایه B طبق معادلات (۲۵) نوشته‌شود.

$$|01\rangle = \alpha_{00}|b_{00}\rangle + \alpha_{01}|b_{01}\rangle + \alpha_{10}|b_{10}\rangle + \alpha_{11}|b_{11}\rangle,$$
$$|10\rangle = \beta_{00}|b_{00}\rangle + \beta_{01}|b_{01}\rangle + \beta_{10}|b_{10}\rangle + \beta_{11}|b_{11}\rangle, \quad (۲۶)$$

که $|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2=1$ و $|\beta_{00}|^2+|\beta_{01}|^2+|\beta_{10}|^2+|\beta_{11}|^2=1$ است.

در این صورت حالات $|G_2\rangle$ و $|G_3\rangle$ و $|G_4\rangle$ و $|G_5\rangle$ بر حسب پایه B به صورت معادلات (۲۶) نوشته می‌شوند.

طبق معادلات (۲۶) چناچه ایو در پایه B اندازه‌گیری انجام دهد، به ازای هر پایه دلخواه اولیه، احتمال وقوع مقادیر مشاهده‌شده هرکدام از حالات مقاوم در برابر نویز فاز جمعی GHZ برابر هم و طبق جدول ۵ است. می‌توان جدول ۵ را با معادلات (۲۷) نیز نشان داد.

جدول (۵): نتیجه اندازه‌گیری در پایه دلخواه B

حالت اولیه	احتمال وقوع	مقدار مشاهده شده mr_E
$\|G_2\rangle$، $\|G_3\rangle$ و $\|G_4\rangle$ و $\|G_5\rangle$	$\|\alpha_{00}\|^2+\|\beta_{00}\|^2$	00
$\|G_2\rangle$، $\|G_3\rangle$ و $\|G_4\rangle$ و $\|G_5\rangle$	$\|\alpha_{01}\|^2+\|\beta_{01}\|^2$	01
$\|G_2\rangle$، $\|G_3\rangle$ و $\|G_4\rangle$ و $\|G_5\rangle$	$\|\alpha_{10}\|^2+\|\beta_{10}\|^2$	10
$\|G_2\rangle$، $\|G_3\rangle$ و $\|G_4\rangle$ و $\|G_5\rangle$	$\|\alpha_{11}\|^2+\|\beta_{11}\|^2$	11

$$|G_2\rangle = \frac{1}{\sqrt{2}}(|001\rangle+|110\rangle) = \frac{1}{\sqrt{2}}(|0\rangle(\alpha_{00}|b_{00}\rangle+\alpha_{01}|b_{01}\rangle$$
$$+\alpha_{10}|b_{10}\rangle+\alpha_{11}|b_{11}\rangle)+|1\rangle(\beta_{00}|b_{00}\rangle+\beta_{01}|b_{01}\rangle+\beta_{10}|b_{10}\rangle$$
$$+\beta_{11}|b_{11}\rangle)) = \frac{1}{\sqrt{2}}((\alpha_{00}|0\rangle+\beta_{00}|1\rangle)|b_1\rangle+(\alpha_{01}|0\rangle$$
$$+\beta_{01}|1\rangle)|b_{01}\rangle+(\alpha_{10}|0\rangle+\beta_{10}|1\rangle)|b_{10}\rangle+(\alpha_{11}|0\rangle$$
$$+\beta_{11}|1\rangle)|b_{11}\rangle),$$
$$|G_3\rangle = \frac{1}{\sqrt{2}}(|001\rangle-|110\rangle) = \frac{1}{\sqrt{2}}(|0\rangle(\alpha_{00}|b_{00}\rangle+\alpha_{01}|b_{01}\rangle$$
$$+\alpha_{10}|b_{10}\rangle+\alpha_{11}|b_{11}\rangle)-|1\rangle(\beta_{00}|b_{00}\rangle+\beta_{01}|b_{01}\rangle$$
$$+\beta_{10}|b_{10}\rangle+\beta_{11}|b_{11}\rangle)) = \frac{1}{\sqrt{2}}((\alpha_{00}|0\rangle-\beta_{00}|1\rangle)|b_{00}\rangle$$
$$+(\alpha_{01}|0\rangle-\beta_{01}|1\rangle)|b_{01}\rangle+(\alpha_{10}|0\rangle-\beta_{10}|1\rangle)|b_{10}\rangle$$
$$+(\alpha_{11}|0\rangle-\beta_{11}|1\rangle)|b_{11}\rangle),$$
$$|G_4\rangle = \frac{1}{\sqrt{2}}(|010\rangle+|101\rangle) = \frac{1}{\sqrt{2}}(|0\rangle(\beta_{00}|b_{00}\rangle+\beta_{00}|b_{00}\rangle$$
$$+\beta_{01}|b_{01}\rangle+\beta_{11}|b_{11}\rangle)+|1\rangle(\alpha_{00}|b_{00}\rangle+\alpha_{01}|b_{01}\rangle+\alpha_{10}|b_{10}\rangle$$
$$+\alpha_{11}|b_{11}\rangle)) = \frac{1}{\sqrt{2}}((\beta_{00}|0\rangle+\alpha_{00}|1\rangle)|b_{00}\rangle+(\beta_{01}|0\rangle \quad (۲۷)$$
$$+\alpha_{01}|1\rangle)|b_{01}\rangle+(\beta_{10}|0\rangle+\alpha_{10}|1\rangle)|b_{10}\rangle+(\beta_{11}|0\rangle$$
$$+\alpha_{11}|1\rangle)|b_{11}\rangle),$$
$$|G_5\rangle = \frac{1}{\sqrt{2}}(|010\rangle-|101\rangle) = \frac{1}{\sqrt{2}}(|0\rangle(\beta_{00}|b_{00}\rangle+\beta_{00}|b_{00}\rangle$$
$$+\beta_{01}|b_{01}\rangle+\beta_{11}|b_{11}\rangle)-|1\rangle(\alpha_{00}|b_{00}\rangle+\alpha_{01}|b_{01}\rangle+\alpha_{10}|b_{10}\rangle$$
$$+\alpha_{11}|b_{11}\rangle)) = \frac{1}{\sqrt{2}}((\beta_{00}|0\rangle-\alpha_{00}|1\rangle)|b_{00}\rangle+(\beta_{01}|0\rangle$$
$$-\alpha_{01}|1\rangle)|b_{01}\rangle+(\beta_{10}|0\rangle-\alpha_{10}|1\rangle)|b_{10}\rangle+(\beta_{11}|0\rangle$$
$$-\alpha_{11}|1\rangle)|b_{11}\rangle).$$

$$p(mr_E = 00 \mid m_A = ijk) = |\alpha_{00}|^2 + |\beta_{00}|^2,$$
$$p(mr_E = 01 \mid m_A = ijk) = |\alpha_{01}|^2 + |\beta_{01}|^2,$$
$$p(mr_E = 10 \mid m_A = ijk) = |\alpha_{10}|^2 + |\beta_{10}|^2,$$
$$p(mr_E = 11 \mid m_A = ijk) = |\alpha_{11}|^2 + |\beta_{11}|^2,$$
$$i, j, k \in \{0,1\}, \quad (۲۸)$$

در رابطه (۲۸) mr_E نتیجه اندازه‌گیری ایو و $p(mr_E)$ احتمال وقوع آن در اندازه‌گیری ایو را نشان می‌دهد. اکنون احتمال اینکه متغیر mr_E برابر با ll' باشد را در معادله (۲۹) محاسبه می‌کنیم.

$$p(mr_E = ll') = \sum p(mr_E = ll' \mid x = ijk)P(x = ijk)$$
$$= |\alpha_{ll'}|^2 + |\beta_{ll'}|^2, l, l' \in \{0,1\} \quad (۲۹)$$

فرض کنید M_A متغیر تصادفی پیام امن آلیس و MR_E دنباله حاوی متغیر تصادفی نتیجه اندازه‌گیری ایو باشد. از معادله (۲۹) معادله (۳۰) را می‌توان نتیجه گرفت.

$$H(MR_E \mid M_A) = H(MR_E) \qquad (۳۰)$$

با توجه به معادله (۲۹) معادله (۳۰) حاصل شده که نشان‌دهنده استقلال دو متغیر M_A و MR_E از یکدیگر است. به روش مشابه می‌توان استقلال M_B از MR_E را طبق معادله (۳۲) نشان داد.

$$I(M_A, MR_E) = 0 \qquad (۳۱)$$

$$H(MR_E \mid M_B) = H(MR_E) \rightarrow I(M_B; R_E) = 0 \qquad (۳۲)$$

۴-۴- مقابله با حمله اسب تروجان

دو نوع حمله اسب تروجان وجود دارد: ۱- طرح مخفی کردن کیوبیت نامرئی [۴۹] ۲- اسب تروجان با فوتون تاخیر یافته [۵۰]. از روش مقابله در مرجع [۵۱] برای مقاومت در برابر حمله‌های اسب تروجان در اینجا به‌کار گرفته می‌شود. برای مقابله با نوع اول حمله اسب تروجان، باب و آلیس هنگام دریافت دنباله از کاربر مقابل در مرحله ۲ و مرحله ۶ در جلوی تجهیزات خود از یک فیلتر برای خارج کردن سیگنال فوتون با طول موج غیر مجاز استفاده می‌کنند.

برای مقابله با نوع دوم حمله اسب تروجان آلیس و باب هر سیگنال نمونه را با یک شکافنده تعداد فوتون (۵۰/۵۰) دو نیم کرده و دو سیگنال خروجی را در پایه مناسب اندازه‌گیری می‌کنند. اگر نرخ . در مرحله۱ آلیس یک دنباله ۶ کیوبیتی از حالت $|G_2\rangle$ به‌نام دنباله I آماده می‌کند و دنباله I را به دو دنباله I_A و I_B تقسیم می‌کند که I_A حاوی کیوبیت‌های فیزیکی ۱ و ۳ و I_B حاوی کیوبیت‌های منطقی ۲ و ۴ از هر دسته است (دنباله I_A حاوی ۲ کیوبیت و دنباله I_B حاوی ۴ کیوبیت منطقی است) پس $q_i = 6$ است. او I_A را برای خود نگه‌داشته و I_B را با فن‌آوری کیوبیت دام [۳۴, ۳۵] برای باب ارسال می‌کند، پس در اولین بررسی حضور استراق‌سمع کننده $q_{d_1} = 4$ است (تعداد کیوبیت‌های دام برابر با تعداد کیوبیت ارسالی است.) در مرحله ۲ آلیس و باب مقایسه‌ای کلاسیک برای کیوبیت‌های دام و شناسایی حضور استراق‌سمع کننده انجام می‌دهند. در مرحله ۳ آلیس و باب جابجایی درهم‌تنیدگی انجام می‌دهند. در مرحله ۴ باب حالات اولیه را تولید می‌کند و طبق جدول ۱ یک دنباله کلاسیک متناسب با آن‌ها نیز تولید می‌کند. در مرحله ۵ باب پیام امن خود را بر روی دنباله حاوی حالت اولیه، به‌وسیله عملگرهای یکانی رمز می‌کند و دنباله کلاسیک A'_B را برای آلیس ارسال می‌کند. سپس برای بررسی حضور استراق سمع کننده در دنباله حاوی پیام امن تعدادی تک‌کیوبیت منطقی دام می‌افزاید، که در این مرحله $q_{d_5} = 2$ است.

در مرحله ۶ مانند مرحله ۲ عمل می‌کنند. در مرحله ۷ آلیس پیام امن خود را بر روی دو کیوبیت ارسالی از باب، به‌وسیله عملگرهای چند فوتونی از آستانه مشخص شده توسط آلیس و باب بالاتر باشد مخابره متوقف می‌شود. درغیراین‌صورت مخابره ادامه میابد. در این حالت هر دو نوع حمله اسب تروجان شکست خواهند خورد.

۵- تحلیل بازدهی پروتکل پیشنهادی

ارزیابی هزینه اجرای پروتکل، با معیار بازدهی سنجیده می‌شود. بازدهی از فرمول $\eta = \frac{c}{q_{all}}$ محاسبه می‌شود که در آن c مجموع بیت‌های پیام امن آلیس و باب و q_{all}کیوبیت‌های تولید شده برای اجرای پروتکل است. $q_{all} = q_i + q_d$ است که q_i کیوبیت‌های تولید شده برای انتقال پیام و q_d کیوبیت‌های دام منطقی هستند [۲۷]. به‌طور طبیعی زمانی‌که نویز جمعی در کانال کوانتومی وجود دارد و می‌خواهیم آن را بی‌اثر کنیم، از دو کیوبیت برای انتقال یک بیت از اطلاعات استفاده می‌کنیم. از طرفی به‌خاطر برقراری امنیت در پروتکل‌های رمزنگاری و استفاده از کیوبیت‌های اضافه، بازده کاهش پیدا می‌کند. در بهترین حالت، در مقالات پیشین بازدهی پروتکل گفتگوی امن کوانتومی مصون در برابر نویز جمعی به ۲۵٪ رسیده است[۳۲،۳۳،۲۱].

برای محاسبه بازدهی فرض می‌کنیم سه بیت پیام امن آلیس و سه بیت پیام امن باب قرار است مبادله شود، پس مقدار $c = 6$ است

یکانی رمز می‌کند و به همراه کیوبیت دام برای باب ارسال می‌کند. بنابراین $q_{d_7} = 2$ است. دنباله کلاسیک A'_A را برای آلیس ارسال می‌کند. در مرحله ۸ مانند مرحله ۲ عمل می‌کنند. در مرحله آخر (مرحله ۹)، باب نتیجه اندازه‌گیری را برای خواندن پیام امن خود توسط آلیس بر روی کانال کلاسیک عمومی منتشر می‌کند. با این توضیحات مقدار هر متغیر $c = 6$، $q_{all} = q_i + q_d = 6 + 8 = 14$و درنتیجه $\eta = \frac{6}{14} = \%42.85$ است.

۶- مقایسه با پروتکل‌های پیشین

برای مقایسه هزینه پروتکل پیشنهادی با طرح‌های پیشین باید بازدهی طرح‌های پیشین را با روش پروتکل پیشنهادی محاسبه کرد، تا بتوان یک مقایسه عادلانه و درست انجام داد. در جدول ۶ مقایسه‌ای بین طرح‌های پیشین و طرح پیشنهادی صورت گرفته است. همان‌طور که در جدول ۶ مشخص است، بازدهی در پروتکل پیشنهادی افزایش مورد توجهی داشته است.

۷- نتیجه‌گیری

در این مقاله پروتکل جدید گفتگوی کوانتومی تحت نویز فاز جمعی ارائه شده است. امنیت این پروتکل ثابت شده‌است. بازدهی در این

پروتکل نسبت به پروتکل‌های پیشین افزایش‌یافته است. به عنوان کارهای آتی می‌توان پروتکل را برای کانالی با نویز چرخش جمعی تغییر داد. گفتگوی امن کوانتومی تحت نویز جمعی با تشخیص هویت یا نامتقارن نیز می توانند از مواردی باشند که در کارهای آتی می توان بر روی آن‌ها تحقیق کرد.

مراجع

[1] Sadeghzadeh S, houshmand M, Aghababa H, Koochakzadeh M. "Quantum Controlled Teleportation of three-qubit GHZ states using Ten-Qubit Channel". Journal of Iranian Association of Electrical and Electronics Engineers; 17 (1) :103-114, URL: http://jiaeee.com/article-1-500-fa.html (2020).

[2] Z. rashidi, M. hooshmand, "Improved Semi-Quantum Direct Communication Protocol", Iranian Journal of Electrical and ComputerEngineering, 19(2), 136142. magiran.com/p2357726 (2021).

[3] SS. Chen, L. Zhou, W. Zhong, "Three-step three party quantum secure direct communication". Science China Physics. Mech. Astron. 61, 90312 (2018).

[4] Y. B. Sheng, L. Zhou, G. L. Long, "One-step quantum secure direct communication", Science Bulletin, Volume 67, Issue 4 , Pages 367-374, ISSN 2095-9273 (2022).

[5] A. Sadeghi-zadeh.S. and B. Houshmand.M., "Bidirectional teleportation of a Two-qubit State by Using Eight-qubit Entangled State as a quantum Channel" Journal of Theoretical Physics, vol.56, no. 7, , pp. 21012112, 2017.

[6] Sh. Hassanpour, M. Houshmand, "Bidirectional quantum controlled teleportation by using EPR states and entanglement swapping", In 23th Iranian Conference on Electrical Engineering (ICEE), 2015.

[7] F. Zarmehi, M. H. Kochakzadeh, D. A. Moghadam, S. Talebi, " Efficient circular controlled quantum teleportation and broadcast schemes in the presence of quantum noises" quantum Information Processing 20:175, 2021.

[8] A. Sadeghi-zadeh.S. and B. Houshmand.M., "Bidirectional quantum teleportation of a Class of n-qubit States by Using (2n + 2)-qubit Entangled States as quantum Channel" Journal of Theoretical Physics, vol.57, no. 1, , pp. 175183, 2017.

[9] Bolokian, M., Houshmand, M., Sadeghizadeh, MS. et al. , "Multi-Party Quantum Teleportation with Selective Receiver", International Journal of Theoretical Physics, 60, 828–837, 2021.

[10] Sadeghi-Zadeh, M.S., Houshmand, M., Aghababa, H. et al. , "Bidirectional quantum teleportation of an arbitrary number of qubits over noisy channel", Quantum Inf Process 18, 353, 2019.

[11] L. Yin-Ju, "Quantum Dialogue Protocol Based on Bell Entangled States and Single Photons, " International Journal of Theoretical Physics, vol. 60, no. 10, pp. 3815–3821, 2021.

[12] Z. Liu and H. Chen, "Analyzing and Improving the Secure Quantum Dialogue Protocol Based on Four-Qubit Cluster State, " International Journal of Theoretical Physics, vol. 59, no. 7, pp. 2120–2126, 2020.

[13] B.-X. Liu and X.-Q. Liang, "Novel Controlled Quantum Dialogue Protocols Without Information Leakage, " International Journal of Theoretical Physics, vol. 61, no. 3, pp. 1–17, 2022.

[14] B. A. Nguyen, "Quantum dialogue," Physics Letters A, vol. 328, pp. 6-10, 2004.

[15] F. Gao, F. Guo, Q. Wen, and F. Zhu, "Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication," Science in China Series G: Physics, Mechanics and Astronomy, vol. 51, pp. 559-566, 2008.

[16] M. H. Zhang, Z. W. Cao, and J. Y. Peng, "Fault-tolerant asymmetric quantum dialogue protocols against collective noise," quantum Information Processing, vol. 17, no. 8, pp. 1–16, 2018.

[17] Y. G. Yang, S. Gao, Y. H. Zhou, and W. M. Shi, "New Secure Quantum Dialogue Protocols over Collective Noisy Channels," International Journal of Theoretical Physics, vol. 58, no. 9, pp. 2810–2822, 2019.

[18] L. Chang, Y. Zhang, X. Tian, Y. Qian, Zeng-liang Bai, and Y. Liu, "Fault Tolerant Controlled Quantum Dialogue with Logical Brown States Against Collective Noise," International Journal of Theoretical Physics, vol. 59, no. 7, pp. 2155–2174, 2020.

[19] W. Li, X.-W. Zha, and Y. Yu, "Secure quantum dialogue protocol based on four-qubit cluster state," International Journal of Theoretical Physics, vol. 57, no. 2, pp. 371–380, 2018.

[20] Z. Liu and H. Chen, "Analyzing and revising quantum dialogue without information leakage based on the entanglement swapping between any two bell states and the shared secret bell state, " International Journal of Theoretical Physics, vol. 58, no. 2, pp. 575–583, 2019.

[21] S. Ramachandran, Meera Balakrishnan, "Effect of Noise in the Quantum Bidirectional Direct Communication Protocol Using Non-maximally Entangled States, " International Journal of Theoretical Physics, vol. 61, no. 5, pp. 1–14, 2022.

[22] M.-H. Zhang, Z.-W. Cao, J.-Y. Peng, and G. Chai, "Fault tolerant quantum dialogue protocol over a collective noise channel, " The European Physical Journal D, vol. 73, no. 3, pp. 1–8, 2019.

[23] Z.-X. Man, Z.-J. Zhang, and Y. Li, "Quantum dialogue revisited," Chinese Physics Letters, vol. 22, pp. 22-24, 2005.

[24] Y. Yang and Q. Wen, "Quasi-secure quantum dialogue using single photons," Science in China Series G: Physics, Mechanics and Astronomy, vol. 50, pp. 558-562, 2007.

[25] V. Sharma, K. Thapliyal, A. Pathak, and S. Banerjee, "A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols," Quantum Information Processing, vol. 15, pp. 4681-4710, 2016.

[26] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Efficient quantum key distribution over a collective noise channel," Physical Review A, vol. 78, p. 022321, 2008.

[27] C.-H. Chang, C.-W. Yang, G.-R. Hzu, T. Hwang, and S.-H. Kao, "Quantum dialogue protocols over

collective noise using entanglement of GHZ state," Quantum Information Processing, pp. 1-21, 2016.
[28] D. Wu, H.-J. Lv, and G.-J. Xie, "Robust anti-collective noise quantum secure direct dialogue using logical bell states," International Journal of Theoretical Physics, vol. 55, pp. 457-469, 2016.
[29] C.-W. Yang and T. Hwang, "Quantum dialogue protocols immune to collective noise," Quantum Information Processing, vol. 12, pp. 2131-2142, 2013.
[30] T. Ye, "Information leakage resistant quantum dialogue against collective noise," SCIENCE CHINA Physics, Mechanics & Astronomy, vol. 57, pp. 2266-2275, 2014.
[31] T. Ye, "Fault tolerant channel-encrypting quantum dialogue against collective noise," SCIENCE CHINA Physics, Mechanics & Astronomy, vol. 58, pp. 1-10, 2015.
[32] Y. Tian-Yu, "Fault-Tolerant Quantum Dialogue Without Information Leakage Based on Entanglement Swapping between Two Logical Bell StatesSupported by the National Natural Science Foundation of China under Grant Nos. 61402407 and 11375152," Communications in Theoretical Physics, vol. 63, p. 431, 2015.
[33] T.-Y. Ye, "Robust quantum dialogue based on the entanglement swapping between any two logical Bell states and the shared auxiliary logical Bell state," Quantum Information Processing, vol. 14, pp. 1469-1486, 2015.
[34] T.-Y. Ye, "Quantum secure direct dialogue over collective noise channels based on logical Bell states," Quantum Information Processing, vol. 14, pp. 1487-1499, 2015.
[35] M.-H. Zhang, Z.-W. Cao, and J.-Y. Peng, "Fault-tolerant asymmetric quantum dialogue protocols against collective noise," Quantum Information Processing, vol. 17, p. 204, 2018.
[36] M. Xiao, Y.-R. Cao, and X.-L. Song, "Efficient and Secure Authenticated Quantum Dialogue Protocols over Collective-Noise Channels," Chinese Physics Letters, vol. 34, p. 030302, 2017.
[37] T.-Y. Ye, "Fault-tolerant authenticated quantum dialogue using logical Bell states," Quantum Information Processing, vol. 14, pp. 3499-3514, 2015.
[38] M. Nakahara and T. Ohmi, Quantum computing: from linear algebra to physical realizations: CRC press, 2008.
[39] Daeichian A. "State estimation of a quantum cavity driven by vacuum state". Journal of Iranian Association of Electrical and Electronics Engineers; 19 (3) :153-162 URL: http://jiaeee.com/article-1-1203-fa.html (2022).
[40] J. Lin and T. Hwang, "Bell state entanglement swappings over collective noises and their applications on quantum cryptography," Quantum Information Processing, vol. 12, pp. 1089-1107, 2013.
[41] X.-H. Li, B.-K. Zhao, Y.-B. Sheng, F.-G. Deng, and H.-Y. Zhou, "Fault tolerant quantum key distribution based on quantum dense coding with collective noise," International Journal of Quantum Information, vol. 7, pp. 1479-1489, 2009.
[42] P. Zanardi and M. Rasetti, "Noiseless quantum codes," Physical Review Letters, vol. 79, p. 3306, 1997.
[43] C.-W. Yang and T. Hwang, "Fault tolerant quantum key distributions using entanglement swapping of GHZ states over collective-noise channels," Quantum Information Processing, vol. 12, pp. 3207-3222, 2013.
[44] C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Technical Journal, vol. 28, pp. 656-715, 1949.
[45] L. Chun-Yan, L. Xi-Han, D. Fu-Guo, Z. Ping, L. Yu-Jie, and Z. Hong-Yu, "Efficient quantum cryptography network without entanglement and quantum memory," Chinese Physics Letters, vol. 23, p. 2896, 2006.
[46] L. Chun-Yan, Z. Hong-Yu, W. Yan, and D. Fu-Guo, "Secure quantum key distribution network with Bell states and local unitary operations," Chinese Physics Letters, vol. 22, p. 1049, 2005.
[47] S. Hassanpour and M. Houshmand, "Bidirectional teleportation of a pure EPR state by using GHZ states," Quantum Information Processing, vol. 15, pp. 905-912, 2016.
[48] W. Dong, C. Xu-Chao, Z. Xin-Wei, and N. Min, "Bidirectional quantum secure communication based on cluster state," in 2010 Third International Symposium on Information Science and Engineering, 2010.
[49] Q.-Y. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," Physics Letters A, vol. 351, pp. 23-25, 2006.
[50] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of Modern Physics, vol. 74, p. 145, 2002.
[51] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Improving the security of secure direct communication based on the secret transmitting order of particles," Physical Review A, vol. 74, p. 054302, 2006.

زیرنویس‌ها

[1] Quantum secure direct communication
[2] Quantum secure dialogue
[3] Bell state quantum
[4] Collective noise
[5] Collective-dephasing noise
[6] Collective-rotation noise
[7] Qubit
[8] Eve
[9] Entanglement swapping
[10] Greenberger–Horne–Zeilinger state quantum
[11] Trojan horse attak
[12] Superposition
[13] Gate
[14] Shannon entropy