پایداری حامل‌های درهم‌تنیده در برابر نوفه

شیما امامی‌پناه[۱]، مرضیه آسوده[۲]

تاریخ ارسال : ۱۴۰۰/۰۸/۰۲ تاریخ پذیرش: ۱۴۰۰/۰۸/۲۲

چکیده: مشابه نقشی که حامل‌ها در مکالمات کلاسیکی به عنوان محیط انتقال دهنده‌ی پیام دارند، حالت‌های درهم تنیده نیز می‌توانند به عنوان محیطی در نظر گرفته شوند که نقش حامل اطلاعات را داشته باشند. به این ترتیب می‌توانیم پروتکل‌هایی برای مخابرات کوانتومی تعریف کنیم که در آن‌ها حالت‌های کوانتومی در یک سو با حامل درهم‌تنیده می‌شوند (به حامل سوار می‌شوند) و در سوی دیگر توسط گیرندگان به فرم امن از آن جدا می‌شوند (از حامل پیاده می‌شوند) و حامل را به‌صورت دست نخورده برای استفاده‌ی مجدد باقی می‌گذارند. به‌علاوه این پروتکل‌ها می‌توانند برای اشتراک رمز کوانتومی مورد استفاده قرار گیرند. در این مقاله پایداری این پروتکل‌ها را در برابر نوفه‌ی میراکننده‌ی فاز و واقطبش بررسی می‌کنیم و نشان می‌دهیم که علی رغم اثر مستمر نوفه، حامل در دو نوع فضای مشخص با پایه‌های درهم‌تنیده که فضای کاملی برای کیوبیت‌های حامل هستند و با عملکرد پروتکل سازگاری دارند باقی می‌ماند.

واژه‌های کلیدی: "اشتراک رمز کوانتومی"، "درهم‌تنیدگی"، "حامل‌های قابل استفاده‌ی مجدد"

۱- مقدمه

در اغلب پروسه‌های اطلاعات کوانتومی [1-4] مانند فرابرد کوانتومی و توزیع کلید کوانتومی، درهم‌تنیدگی به عنوان یک منبع کوانتومی مورد استفاده قرار می‌گیرد. در طرح‌های اشتراک رمز [5-10] همبستگی‌های قوی غیر کلاسیکی موجود در حالت‌های درهم‌تنیده که بین کاربران قانونی به اشتراک گذاشته می‌شود به آن‌ها اجازه‌ی تولید یک کلید تصادفی را می‌دهد. البته پروتکل‌های رمزنگاری دیگری هم وجود دارند که در آن‌ها از درهم‌تنیدگی استفاده نمی‌شود [11-18]. کاربران قانونی که در این پروتکل‌ها وجود دارند آلیس[۱]، باب[۲] و چارلی[۳] نامیده می‌شوند.

۱- دانشکده فیزیک، دانشگاه آزاد اسلامی، واحد تهران شمال.
آدرس پست الکترونیک: Sh.emamipanah@gmail.com

۲- استادیار، دانشکده فیزیک، دانشگاه آزاد اسلامی، واحد تهران شمال.
آدرس پست الکترونیک:Marzieh.asoudeh@gmail.com

در پروتکل توزیع کلید کوانتومی، آلیس و باب می‌خواهند با استفاده از به اشتراک گذاشتن زوج‌های بیشینه گیری‌های مشخص بر درهم‌تنیده و انجام یک سری اندازه روی آن‌ها یک کلید رمزی را بین خود توزیع کنند. آن‌ها از طریق یک کانال مخابراتی پیام‌هایی را رد و بدل می‌کنند و در پایان علی رغم وجود استراق سمع کننده به یک کلید یکسان و امن دسترسی پیدا می‌کنند. در واقع امنیت و یکسان بودن کلیدهای توزیع شده بین آلیس و های منحصر به فردی باب در این پروتکل‌ها به علت ویژگی است که در زوج‌های بیشینه درهم‌تنیده وجود دارد.

علاوه بر پروتکل توزیع کلید کوانتومی می‌توانیم به پروتکل اشتراک رمز که مورد علاقه‌ی ما در این مقاله است اشاره کنیم. در مسئله‌ی اشتراک رمز آلیس می‌خواهد یک پیام را به گونه‌ای به باب و چارلی بفرستد که فقط با همکاری یکدیگر بتوانند آن را باز کنند. در این مقاله

[۱] Alice
[۲] Bob
[۳] Charlie

می‌خواهیم پروتکلی را توضیح دهیم که در آن از درهم‌تنیدگی به عنوان حامل امن اطلاعات برای فرستادن یک پیام استفاده می‌شود. ایده‌ی استفاده از حالت‌های درهم‌تنیده بین دو نقطه‌ی دور به عنوان حامل امن و قابل استفاده‌ی مجدد اطلاعات اولین بار در مقاله‌ی [۱۹] مطرح شد و سپس در مقاله‌ی[۲۰] به مسئله‌ی اشتراک رمز بسط یافت. این ایده در واقع بسط کوانتومی ایده‌ای است که در شبکه‌ی مخابرات کلاسیکی امروزی وجود دارد. در یک سو فرستنده پیام را به حامل سوار می‌کند و در سوی دیگر گیرندگان پیام را از آن پیاده می‌کنند و حامل را به صورت دست نخورده برای استفاده‌ی مجدد باقی می‌گذارند. امن بودن حامل به این معنا است که حالت پیام در حین انتقال از نقطه نظر استراق سمع کننده که آن را ایو[1] می‌نامیم پنهان است. در این پروتکل پیام می‌تواند کلاسیکی یا کوانتومی باشد. منظورمان از پیام کلاسیکی همان بیت‌های کلاسیکی است که در پایه‌های استاندارد $\{|0\rangle,|1\rangle\}$ کد شده‌اند و منظورمان از پیام کوانتومی حالتی است که در برهم‌نهی این پایه‌ها کد می‌شود $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$.

در این مقاله اثر دو نوع نوفه‌ی مهم به نام‌های میراکننده‌ی فاز[2] و واقطبش[3] را که به‌طور مستمر روی یک پروتکل اشتراک رمز اثر می‌کنند بررسی می‌کنیم. در مقاله‌ی [21] فرض ما بر این بود که قبل از شروع پروتکل حامل یک بار با نوفه مختل شده است و زمان اجرای پروتکل به گونه‌ای است که نوفه‌ی اضافه شده قابل چشم‌پوشی است. در این مقاله خواهیم دید که حتی اگر اثر نوفه را نه فقط یک بار بلکه به‌طور مستمر درنظر بگیریم، حامل در دو نوع فضای مشخص با پایه‌های درهم‌تنیده که فضای کاملی برای کیوبیت‌های حامل هستند و با عملکرد پروتکل سازگاری دارند باقی میماند.

مقاله را به این صورت پیش می‌بریم که در بخش دوم به معرفی یک پروتکل اشتراک رمز خواهیم پرداخت. در بخش سوم نوفه‌ی میراکننده‌ی فاز و واقطبش را معرفی می‌کنیم و اثر آن‌ها را بر روی این پروتکل بررسی می‌کنیم. در بخش چهارم خواهیم دید که اثر مستمر نوفه چه تاثیری بر روی پروتکل خواهد داشت. و در بخش پنجم با یک نتیجه گیری مقاله را به پایان خواهیم برد.

۲. پروتکل اشتراک رمز کوانتومی

برای شروع بحث ابتدا باید عملگر کنترلی[4] CNOT را معرفی کنیم. این عملگر روی یک حالت دو کیوبیتی اثر می‌کند که یکی از کیوبیت‌ها کنترلی و دیگری هدف است. اگر کیوبیت کنترلی $|0\rangle$ باشد اثر CNOT روی کیوبیت هدف مثل اثر عملگر واحد I است. (کاری انجام نمی‌دهد). اگر کیوبیت کنترلی $|1\rangle$ باشد اثر CNOT روی کیوبیت هدف مثل اثر اپراتور پاؤلی X است. (بیت را بر می‌گرداند).

استفاده از حالت‌های درهم‌تنیده به عنوان حامل امن اطلاعات بین دو نقطه به این صورت است که آلیس می‌خواهد با استفاده از حالت $|EPR\rangle_{AB}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ که به عنوان حامل بین خود و باب به اشتراک گذاشته است پیام q را به باب بفرستد. آلیس پیام q را در حالت $|q\rangle_1$ کد می‌کند (کیوبیت 1 مربوط به حالت پیام می‌باشد). سپس عملگر $C_{A,1}$ را روی حالت حامل و پیام اثر می‌دهد ($C_{A,1}$عملگر کنترلی CNOT است که کیوبیت کنترلی آن A و کیوبیت هدف آن 1 است). به این ترتیب پیام q با حامل درهم‌تنیده می‌شود:

$$C_{A,1}\left[\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}|q\rangle_1\right] = \frac{1}{\sqrt{2}}(|00q\rangle+|11\bar{q}\rangle)_{AB,1}. \quad (۱)$$

($\bar{q}$ برگردان شده‌ی q است : $\bar{1}=0$ و $\bar{0}=1$). آلیس کیوبیت 1 را به باب می‌فرستد. اگر در رابطه ی بالا نسبت به A و B رَدّ جزئی بگیریم می‌بینیم که کیوبیت 1 در حین انتقال در حالت بیشینه درهم‌آمیخته است یعنی از نقطه نظر ایو پیام یکنواخت و کاملا تصادفی است:

$$\rho_1=\frac{1}{2}(|q\rangle\langle q|+|\bar{q}\rangle\langle\bar{q}|)=\frac{I}{2} \quad (۲)$$

[1] Eve
[2] De-phasing
[3] Depolarizing
[4] Controlled Not

در مقصد باب کیوبیت 1 را دریافت می‌کند و عملگر $C_{B,1}$ را اثر می‌دهد:

$$\begin{aligned} & C_{B,1}\left[\frac{1}{\sqrt{2}}\left(|00q\rangle|00\bar{q}\rangle\right)_{AB,1}\right] \\ & =\frac{1}{\sqrt{2}}\left(|00q\rangle+|11q\rangle\right)_{AB,1} \\ & =\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{AB}|q\rangle_1 . \end{aligned} \quad (۳)$$

همان‌طور که می‌بینید پیام از حامل جدا شده است و باب به درستی پیام آلیس را دریافت کرده است. حامل نیز به صورت دست نخورده برای استفاده‌ی مجدد باقی مانده است.

در طرح‌های اشتراک رمز آلیس یک پیام را به گونه‌ای به باب و چارلی می‌فرستد که فقط با همکاری یکدیگر بتوانند آن‌را بخوانند. در اینجا می‌خواهیم پروتکلی را مطرح کنیم که از حالت‌های درهم‌تنیده به عنوان حاملی بین آلیس، باب و چارلی برای فرستادن پیام استفاده می‌کند. نقش حالت‌های درهم‌تنیده به عنوان حامل این است که آلیس با درهم‌تنیده کردن پیام با حامل می‌تواند حالت پیام را در حین انتقال به باب و چارلی از دید ایو پنهان کند. فرض بر این است که در مقصد باب و چارلی در یک مکان هستند تا بتوانند با همکاری یکدیگر پیام را بخوانند. قبل از اینکه نحوه‌ی اجرای پروتکل را بررسی کنیم ابتدا به بیان یک سری از قراردادها می‌پردازیم.

پاریته‌ی زوج و پاریته‌ی فرد برای دو کیوبیت را به‌صورت زیر می‌نویسیم:

$$\begin{aligned} & \left|\tilde{0}\right\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right), \\ & \left|\tilde{1}\right\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right). \end{aligned} \quad (۴)$$

روابط بالا را در رابطه‌ی زیر خلاصه می‌کنیم:

$$\left|\tilde{q}\right\rangle=\frac{1}{\sqrt{2}}\left(|0,q\rangle+|1,\bar{q}\rangle\right). \quad (۵)$$

گاهی اوقات از نوشتن ضرایب بهنجارش صرف نظر می‌کنیم. مثلاً هنگامی‌که می‌نویسیم $|000\rangle+|111\rangle$ منظورمان حالت بهنجار $\frac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right)$ است. پاریته‌ی زوج و پاریته‌ی فرد برای سه کیوبیت به‌صورت زیر نوشته می‌شوند:

$$\begin{aligned} & \left|\tilde{0}\right\rangle_{ABC}=|0\rangle_A\left|\tilde{0}\right\rangle_{BC}+|1\rangle_A\left|\tilde{1}\right\rangle_{BC} \\ & =|000\rangle+|011\rangle+|101\rangle+|110\rangle . \\ & \left|\tilde{1}\right\rangle_{ABC}=|0\rangle_A\left|\tilde{1}\right\rangle_{BC}+|1\rangle_A\left|\tilde{0}\right\rangle_{BC} \\ & =|001\rangle+|010\rangle+|100\rangle+|111\rangle . \end{aligned} \quad (۶)$$

اجرای پروتکل را با دورهای زوج (0,2,4,…) آغاز می‌کنیم: در این دورها آلیس، باب و چارلی حالت درهم‌تنیده‌ی $|GHZ\rangle_{ABC}=|000\rangle+|111\rangle$ را به عنوان حامل به اشتراک گذاشته‌اند. کیوبیت‌های A ، B و C به ترتیب کیوبیت‌های سهم آلیس، باب و چارلی از حامل هستند. در دورهای زوج آلیس پیام $|q\rangle$ را در حالت ضربی $|q,q\rangle_{1,2}$ کد می‌کند و آن‌را با عملگر $C_{A,1}C_{A,2}$ به حامل درهم‌تنیده می‌کند:

$$\begin{aligned} & \left(C_{A,1}C_{A,2}\right)\left[\left(|000\rangle+|111\rangle\right)_{ABC}|q,q\rangle_{1,2}\right] \\ & =\left(|000\rangle|q,q\rangle+|111\rangle|\bar{q},\bar{q}\rangle\right)_{ABC,1,2} \end{aligned} \quad (۷)$$

آلیس کیوبیت 1 را به باب و کیوبیت 2 را به چارلی می‌فرستد. این کیوبیت‌ها در حین انتقال در حالت بیشینه درهم‌آمیخته هستند، یعنی از نقطه نظر ایو کاملا تصادفی و یکنواخت هستند. در مقصد باب با اثر دادن عملگر $C_{B,1}$ می‌تواند مستقلاً $|q\rangle_1$ را از حامل جدا کرده و پیامی که آلیس فرستاده است را بخواند:

$$\begin{aligned} & C_{B,1}\left(|000\rangle|q,q\rangle+|111\rangle|\bar{q},\bar{q}\rangle\right)_{ABC,1,2} \\ & =\left(|000\rangle|q,q\rangle+|111\rangle|q,\bar{q}\rangle\right)_{ABC,1,2} \\ & =\left(|000\rangle|q\rangle+|111\rangle|\bar{q}\rangle\right)_{ABC,2}|q\rangle_1 . \end{aligned} \quad (۸)$$

چارلی نیز با اثر دادن عملگر $C_{C,2}$ می‌تواند مستقلاً $|q\rangle_2$ را از حامل جدا کرده و پیام را بخواند:

$$C_{C,2}\left(|000\rangle|q\rangle+|111\rangle|\bar{q}\rangle\right)_{ABC,2} = \left(|000\rangle+|111\rangle\right)_{ABC}|q\rangle_2 . \quad (۹)$$

در انتهای دورهای زوج آلیس، باب و چارلی هر کدام جداگانه روی سهم‌های خود از حامل عملگر هادامارد Hرا اثر می‌دهند و آنرا از حالت $|GHZ\rangle_{ABC}$ به حالت $|\tilde{0}\rangle_{ABC}$ تبدیل می‌کنند:

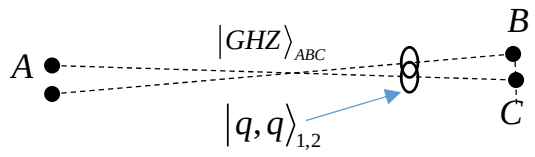
$$\left(H_A\otimes H_B\otimes H_C\right)|GHZ\rangle_{ABC}=|\tilde{0}\rangle_{ABC} \quad (۱۰)$$

در بدست آوردن رابطه‌ی بالا از روابط زیر و قراردادهایی که داشتیم استفاده کردیم:

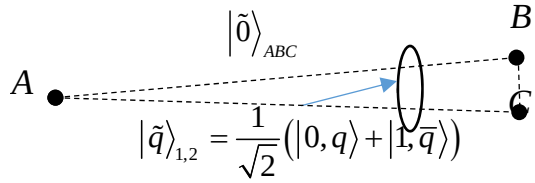
$$H|0\rangle=|+\rangle,\ H|1\rangle=|-\rangle.$$
$$|+\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right). \quad (۱۱)$$
$$|-\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right).$$

حامل دورهای فرد (1,3,5,…) حالت درهم‌تنیده‌ی $|\tilde{0}\rangle_{ABC}$ است. آلیس پیام $|q\rangle$ را در حالت درهم‌تنیده‌ی $|\tilde{q}\rangle_{1,2}$ کد می‌کند و آنرا با یکی از دو عملگر $C_{A,1}$ یا $C_{A,2}$ به حامل درهم‌تنیده می‌کند. (فرقی نمی‌کند که آلیس کدام عملگر را انتخاب کند):

$$C_{A,1}\left[|\tilde{0}\rangle_{ABC}|\tilde{q}\rangle_{1,2}\right] = |0\rangle_A|\tilde{0}\rangle_{BC}|\tilde{q}\rangle_{1,2}+|1\rangle_A|\tilde{1}\rangle_{BC}|\tilde{\bar{q}}\rangle_{1,2} \quad (۱۲)$$



الف) دورهای زوج



ب) دورهای فرد

شکل ۱. پروتکل اشتراک رمز با استفاده از حامل‌های درهم‌تنیده

آلیس کیوبیت 1 را به باب و کیوبیت 2 را به چارلی می‌فرستد. کیوبیت 1 و کیوبیت 2 در حین انتقال در حالت بیشینه درهم‌آمیخته هستند و از نقطه نظر ایو رندم و یکنواخت هستند. (مثلاً برای بدست آوردن حالت کیوبیت 1 کافی است که در رابطه‌ی بالا نسبت به ABC,2 رَدّ جزئی بگیرید، خواهید دید که $\rho_1=\frac{I}{2}$ می‌شود). در مقصد باب و چارلی پس از دریافت کیوبیت‌های 1 و 2 با همکاری یکدیگر عملگر $C_{B,1}C_{C,2}$ را اثر می‌دهند و پیام را از حامل جدا می‌کنند:

$$\left(C_{B,1}C_{C,2}\right)\left[|0\rangle_A|\tilde{0}\rangle_{BC}|\tilde{q}\rangle_{1,2}+|1\rangle_A|\tilde{1}\rangle_{BC}|\tilde{\bar{q}}\rangle_{1,2}\right] = |\tilde{0}\rangle_{ABC}|\tilde{q}\rangle_{1,2} \quad (۱۳)$$

در رابطه‌ی بالا فضای کنترلی عملگرهای CNOT روی کیوبیت‌های C،B و فضای هدف روی کیوبیت‌های 2،1 است. می‌دانیم که $|\tilde{0}\rangle_{BC}$ پاریته‌ی زوج دو کیوبیت و $|\tilde{1}\rangle_{BC}$ پاریته‌ی فرد دو کیوبیت است. هنگامی که $|\tilde{0}\rangle_{BC}$ کنترلی است $|\tilde{q}\rangle_{1,2}$ تغییری نمی‌کند، اما هنگامی‌که $|\tilde{1}\rangle_{BC}$ کنترلی است $|\tilde{\bar{q}}\rangle_{1,2}$ برگردان می‌شود و به $|\tilde{q}\rangle_{1,2}$ تبدیل می‌شود. از آنجائیکه $H^2=I$ است، در انتهای دورهای فرد آلیس، باب و چارلی با اثر دادن عملگر هادامارد روی سهم‌هایشان از حامل آن‌را از حالت $|\tilde{0}\rangle_{ABC}$ به حالت $|GHZ\rangle_{ABC}$ برمی‌گردانند.

به علت اینکه در دورهای زوج باب و چارلی مستقلاً می‌توانند پیام را بخوانند آلیس در این دورها کیوبیت‌های اضافی را که حاوی اطلاعات مهمی نیستند می‌فرستد. درعوض پیام‌های مهم را فقط در دورهای فرد که باب و چارلی برای خواندن پیام نیاز به همکاری یکدیگر دارند می‌فرستد. ممکن است این سوال پیش آید که چرا فقط از دورهای فرد استفاده نمی‌کنیم؟ پاسخ این است که وجود عملگر هادامارد که حامل دورهای زوج و فرد را به یکدیگر تبدیل می‌کند باعث می‌شود که اگر ایو بخواهد خودش را با حامل درهم‌تنیده کند در بین دورها از حامل جدا شود.

برای دیدن این مطلب فرض کنید که ایو به‌صورت زیر خود را با حامل دورهای زوج و فرد درهم‌تنیده کرده است:

$$\begin{aligned}&\left|\tilde{0}_{ABC},E\right\rangle\\&=\left|000\right\rangle\xi_{000}+\left|011\right\rangle\xi_{011}+\left|101\right\rangle\xi_{101}+\left|110\right\rangle\xi_{110}.\\&\left|GHZ,E\right\rangle=\left|000\right\rangle\eta_{000}+\left|111\right\rangle\eta_{111}.\end{aligned}\qquad(۱۴)$$

هنگامی‌که در انتهای دورهای زوج آلیس، باب و چارلی عملگرهای هادامارد را اعمال می‌کنند حامل به‌صورت زیر تبدیل می‌شود:

$$\begin{aligned}&H^{\otimes3}\left|GHZ,E\right\rangle\\&=\left|+++\right\rangle\eta_{000}+\left|---\right\rangle\eta_{111}\\&=\left(\left|\tilde{0}\right\rangle_{ABC}+\left|\tilde{1}\right\rangle_{ABC}\right)\eta_{000}+\left(\left|\tilde{0}\right\rangle_{ABC}-\left|\tilde{1}\right\rangle_{ABC}\right)\eta_{111}\\&=\left|\tilde{0}\right\rangle_{ABC}(\eta_{000}+\eta_{111})+\left|\tilde{1}\right\rangle_{ABC}(\eta_{000}-\eta_{111}).\end{aligned}\qquad(۱۵)$$

از آنجائیکه می‌بایست حامل دورهای زوج بعد از اثر دادن عملگرهای هادامارد به حالت $\left|\tilde{0}\right\rangle_{ABC}$ تبدیل شود بنابراین در رابطه‌ی بالا می‌بایست $\eta_{000}=\eta_{111}$ باشد، که این امر باعث جدا شدن ایو از حامل در دورهای زوج می‌شود. از طرفی دیگر برای تساوی روابط (۱۴) و (۱۵) می‌بایست $\xi_{110}=\xi_{101}=\xi_{011}=\xi_{000}$ باشد، که در این صورت ایو از حامل دورهای فرد نیز جدا می‌شود.

دیدیم که چگونه در این پروتکل آلیس می‌تواند پایه‌های استاندارد را برای باب و چارلی بفرستد. به علت خطی بودن این پروسه آلیس می‌تواند هر برهم‌نهی از حالت‌های پایه که به‌صورت پیام کوانتومی $\left|\varphi\right\rangle=\alpha\left|0\right\rangle+\beta\left|1\right\rangle$ است را در دورهای زوج به‌صورت $\left|\varphi'\right\rangle=\alpha\left|00\right\rangle+\beta\left|11\right\rangle$ و در دورهای فرد به‌صورت $\left|\varphi''\right\rangle=\alpha\left|\tilde{0}\right\rangle+\beta\left|\tilde{1}\right\rangle$ بفرستد.

۳. نوفه

۳-۱. کانال میراکننده‌ی فاز

در اطلاعات کوانتومی نوفه را به‌صورت یک کانال که روی حالت کوانتومی اثر می‌کند در نظر می‌گیریم. در بررسی کانال میراکننده‌ی فاز برای یک کیوبیت حالت خالص $\left|\psi\right\rangle=\alpha\left|0\right\rangle+\beta\left|1\right\rangle$ را در نظر می‌گیریم. در این ترکیب خطی حالت پایه‌ی $\left|0\right\rangle$ و $\left|1\right\rangle$ در یک فاز نسبی هستند. اثر کانال به این صورت است که فاز نسبی این دو حالت را به تدریج از بین می‌برد و در نهایت یک حالت مخلوط ایجاد می‌کند. برای مدل سازی این نوفه فرض می‌کنیم که عملگری مانند $R_Z(\theta)$ روی حالت‌های $\left|0\right\rangle$ و $\left|1\right\rangle$ اختلاف فاز θ ایجاد می‌کند و به‌طور نامنظم با یک توزیع گاؤسی روی حالت اولیه اثر می‌کند و آن را به‌صورت زیر تبدیل می‌کند:

$$\left|\psi\right\rangle\left\langle\psi\right|\to\int p(\theta)R_Z(\theta)\left|\psi\right\rangle\left\langle\psi\right|R_Z^{+}(\theta)d\theta\qquad(۱۶)$$

۳-۲. اثر نوفه‌ی میراکننده‌ی فاز بر عملکرد پروتکل

حالت خالص $\left|GHZ\right\rangle=\frac{1}{\sqrt{2}}\left(\left|000\right\rangle+\left|111\right\rangle\right)$ را که ترکیب خطی دو حالت پایه‌ی $\left|000\right\rangle$ و $\left|111\right\rangle$ با یک فاز نسبی مشخص است در نظر بگیرید. نوفه‌ی میراکننده‌ی فاز به‌صورت ضربه‌های رندم فاز روی کیوبیت‌ها اثر می‌کند و به تدریج فاز نسبی این دو حالت را از بین می‌برد و در نهایت یک حالت مخلوط ایجاد می‌کند. فرض کنید ضربه‌های نامنظم فاز روی کیوبیت j ام باعث ایجاد اختلاف فاز θ_j شود:

$$\begin{aligned}&Z\left|0\right\rangle=\left|0\right\rangle\to e^{i\theta_jZ}\left|0\right\rangle=e^{i\theta_j}\left|0\right\rangle,\\&Z\left|1\right\rangle=-\left|1\right\rangle\to e^{i\theta_jZ}\left|1\right\rangle=e^{-i\theta_j}\left|1\right\rangle.\end{aligned}\qquad(۱۷)$$

اثر ضربه‌های فاز روی سه کیوبیت به‌صورت زیر است:

$$\begin{aligned}&e^{i\theta_1Z}e^{i\theta_2Z}e^{i\theta_3Z}\left|000\right\rangle\\&=e^{i(\theta_1+\theta_2+\theta_3)}\left|000\right\rangle=e^{i\theta}\left|000\right\rangle.\\&e^{i\theta_1Z}e^{i\theta_2Z}e^{i\theta_3Z}\left|111\right\rangle\\&=e^{-i(\theta_1+\theta_2+\theta_3)}\left|111\right\rangle=e^{-i\theta}\left|111\right\rangle.\end{aligned}\qquad(۱۸)$$

اثر نوفه‌ی میراکننده‌ی فاز روی حالت $\left|GHZ\right\rangle\left\langle GHZ\right|$ به‌صورت زیر بدست می‌آید:

$$\frac{1}{2}\int p(\theta)\begin{bmatrix}\left|000\right\rangle\left\langle000\right|+e^{2i\theta}\left|000\right\rangle\left\langle111\right|\\+e^{-2i\theta}\left|111\right\rangle\left\langle000\right|+\left|000\right\rangle\left\langle000\right|\end{bmatrix}d\theta\qquad(۱۹)$$

در رابطه‌ی بالا فرض می‌کنیم ضربه‌های فاز حول صفر متقارن است و تابع توزیع احتمال زوج است. انتگرال این تابع را برابر با مقدار $(1-2P)$ قرار می‌دهیم:

$$\begin{aligned}&(1-2P)|GHZ\rangle\langle GHZ|\\&+P\left(|GHZ\rangle\langle GHZ|+|GHZ'\rangle\langle GHZ'|\right)\end{aligned} \qquad (۲۰)$$

در نوشتن رابطه‌ی بالا حالت $|GHZ'\rangle$ را به‌صورت $|GHZ'\rangle=\frac{1}{\sqrt{2}}\left(|000\rangle-|111\rangle\right)$ تعریف کردیم. حالت $|GHZ\rangle$ در اثر نوفه‌ی میرا کننده‌ی فاز با احتمال $(1-P)$ تغییری نمی‌کند اما با احتمال خطای P تبدیل به حالت $|GHZ'\rangle$ می‌شود:

$$\begin{aligned}&|GHZ\rangle\langle GHZ|_{ABC}\rightarrow\\&(1-P)|GHZ\rangle\langle GHZ|_{ABC}\\&+P|GHZ'\rangle\langle GHZ'|_{ABC}\end{aligned} \qquad (۲۱)$$

بنابراین حامل دورهای زوج در اثر نوفه‌ی میرا کننده‌ی فاز به‌صورت زیر نوشته می‌شود:

$$\begin{aligned}\rho^{even}&=(1-P)|GHZ\rangle\langle GHZ|_{ABC}\\&+P|GHZ'\rangle\langle GHZ'|_{ABC}.\end{aligned} \qquad (۲۲)$$

در پروتکل اشتراک رمز حامل مختل شده توسط نوفه در دورهای زوج به چه صورت عمل می‌کند؟ می‌دانیم که قسمت $|GHZ\rangle$ مانند گذشته به خوبی عمل می‌کند اما باید عملکرد قسمت $|GHZ'\rangle$ را بررسی کنیم. در دورهای زوج پیام در حالت ضربی $|q,q\rangle_{1,2}$ کد می‌شود و عملگرهای CNOT که توسط آلیس، باب و چارلی برای سوار کردن پیام به حامل و پیاده کردن پیام از حامل اعمال می‌شوند بصورت $\Omega^{even}=C_{B,2}C_{B,1}C_{A,2}C_{A,1}$ هستند. عملکرد قسمت $|GHZ'\rangle$ در تحویل دادن پیام به‌صورت زیر است:

$$\begin{aligned}&\Omega^{even}\left(|000\rangle-|111\rangle\right)_{ABC}|q,q\rangle_{1,2}\\&=\left(|000\rangle-|111\rangle\right)_{ABC}|q,q\rangle_{1,2}\end{aligned} \qquad (۲۳)$$

در رابطه ی بالا می‌بینیم که $|GHZ'\rangle$ به خوبی $|GHZ\rangle$ عمل کرده است زیرا در انتهای دور، پیام به همان صورتی که فرستاده شده از حامل جدا شده است.

در انتهای دورهای زوج آلیس، باب و چارلی عملگرهای هادامارد را روی حامل اثر می‌دهند و آنرا به حامل دورهای فرد تبدیل می‌کنند. از قبل می‌دانیم که $H^{\otimes 3}|GHZ\rangle_{ABC}=|\tilde{0}\rangle_{ABC}$ است، اما باید اثر عملگرهای هادامارد روی حالت $|GHZ'\rangle$ را بررسی کنیم:

$$\begin{aligned}&\left(H_A\otimes H_B\otimes H_C\right)\left(|000\rangle-|111\rangle\right)_{ABC}\\&=\left(|+++\rangle-|---\rangle\right)_{ABC}\\&=\left(|001\rangle+|010\rangle+|100\rangle+|111\rangle\right)_{ABC}\\&=|0\rangle_A|\tilde{1}\rangle_{BC}+|1\rangle_A|\tilde{0}\rangle_{BC}=|\tilde{1}\rangle_{ABC}.\end{aligned} \qquad (۲۴)$$

بنابراین حامل دورهای فرد به‌صورت زیر است:

$$\rho^{odd}=(1-P)|\tilde{0}\rangle\langle\tilde{0}|_{ABC}+P|\tilde{1}\rangle\langle\tilde{1}|_{ABC}. \qquad (۲۵)$$

در دورهای فرد پیام در حالت درهم‌تنیده‌ی $|\tilde{q}\rangle_{1,2}$ کد می‌شود. حامل دورهای فرد در تحویل دادن پیام به چه صورت عمل می‌کند؟ از قبل می‌دانیم که قسمت $|\tilde{0}\rangle_{ABC}$ از حامل به خوبی کار می‌کند اما باید عملکرد قسمت $|\tilde{1}\rangle_{ABC}$ را بررسی کنیم. آلیس پیام $|\tilde{q}\rangle_{1,2}$ را با عملگر $C_{A,1}$ یا $C_{A,2}$ به حامل سوار می‌کند:

$$\begin{aligned}&C_{A,1}\left(|\tilde{1}\rangle_{ABC}|\tilde{q}\rangle_{1,2}\right)\\&=C_{A,1}\left[\left(|0\rangle_A|\tilde{1}\rangle_{BC}+|1\rangle_A|\tilde{0}\rangle_{BC}\right)\left(|0,q\rangle+|1,\bar{q}\rangle\right)_{1,2}\right]\\&=|0\rangle_A|\tilde{1}\rangle_{BC}\underbrace{\left(|0,q\rangle+|1,\bar{q}\rangle\right)_{1,2}}_{|\tilde{q}\rangle_{1,2}}\\&+|1\rangle_A|\tilde{0}\rangle_{BC}\underbrace{\left(|1,q\rangle+|0,\bar{q}\rangle\right)_{1,2}}_{|\tilde{\bar{q}}\rangle_{1,2}}.\end{aligned} \qquad (۲۶)$$

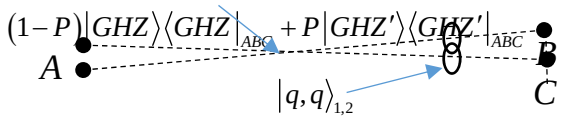
آلیس کیوبیت 1 را به باب و کیوبیت 2 را به چارلی می‌فرستد. از رابطه‌ی بالا مشخص است که این کیوبیت‌ها در حین انتقال در حالت بیشینه درهم‌آمیخته هستند. در مقصد باب و چارلی باید با همکاری یکدیگر پیام را از حامل جدا کنند:

$$\begin{aligned}&\left(C_{B,1}C_{C,2}\right)\left[|0\rangle_A|\tilde{1}\rangle_{BC}|\tilde{q}\rangle_{1,2}+|1\rangle_A|\tilde{0}\rangle_{BC}|\tilde{\bar{q}}\rangle_{1,2}\right]\\&=|0\rangle_A|\tilde{1}\rangle_{BC}|\tilde{q}\rangle_{1,2}+|1\rangle_A|\tilde{0}\rangle_{BC}|\tilde{\bar{q}}\rangle_{1,2}\\&=\underbrace{\left(|0\rangle_A|\tilde{1}\rangle_{BC}+|1\rangle_A|\tilde{0}\rangle_{BC}\right)}_{|\tilde{1}\rangle_{ABC}}|\tilde{\bar{q}}\rangle_{1,2}.\end{aligned}\qquad(۲۷)$$

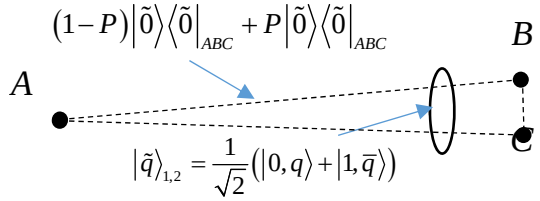
در رابطه‌ی بالا می‌بینیم که پیام از حامل جدا شده است اما به‌صورت برگردان تحویل داده شده است. کل عملگرهای CNOT در دورهای فرد $\Omega^{odd}=C_{B,1}C_{C,2}C_{A,1}$ است. بنابراین عملکرد قسمت $|\tilde{1}\rangle_{ABC}$ از حامل در تحویل دادن پیام به‌صورت زیر است:

$$\Omega^{odd}|\tilde{1}\rangle_{ABC}|\tilde{q}\rangle_{1,2}=|\tilde{1}\rangle_{ABC}|\tilde{\bar{q}}\rangle_{1,2}.\qquad(۲۸)$$

اثر نوفه‌ی میرا کننده‌ی فاز روی پروتکل اشتراک رمز را می‌توانیم به این صورت خلاصه کنیم: در دورهای زوج که پیام q در حالت ضربی $|q,q\rangle_{1,2}$ کد می‌شود، حامل در اثر نوفه با حالت $|GHZ'\rangle$ که در تحویل دادن پیام به خوبی حالت $|GHZ\rangle$ عمل می‌کند مخلوط می‌شود. در دورهای فرد که پیام q در حالت درهم‌تنیده‌ی $|\tilde{q}\rangle_{1,2}$ کد می‌شود، حامل $|\tilde{1}\rangle_{ABC}$ با حالت $|\tilde{0}\rangle_{ABC}$ که پیام را برگردان می‌کند مخلوط می‌شود. پیام $|\tilde{q}\rangle_{1,2}$ با احتمال $(1-P)$ درست دریافت می‌شود و با احتمال خطای P برگردان می‌شود.



الف) دورهای زوج



ب) دورهای فرد

شکل ۲. اثر نوفه‌ی میراکننده‌ی فاز در پروتکل اشتراک رمز با حامل‌های درهم‌تنیده

۳-۳. کانال واقطبش

کانال واقطبش با احتمال $(1-P)$ حالت کوانتومی اولیه‌ی ρ را حفظ میکند و با احتمال خطای P تمام اطلاعات موجود در آن را پاک می‌کند و به‌صورت حالت بیشینه درهم‌آمیخته که یک حالت کاملا تصادفی و یکنواخت است تبدیل می‌کند:

$$\rho\to(1-p)\rho+p\frac{I}{2}\qquad(۲۹)$$

رابطه‌ی بالا را برای کانال یک کیوبیت نوشتیم که حالت بیشینه درهم‌آمیخته برای آن $\frac{I}{2}$ است. می‌توانیم با استفاده از اتحاد زیر رابطه‌ی بالا را مرتب کنیم:

$$2I=\rho+X\rho X+Y\rho Y+Z\rho Z\qquad(۳۰)$$

X,Y,Z عملگرهای پاؤلی هستند. بنابراین کانال واقطبش حالت کوانتومی ρ را به‌صورت زیر متحول می‌کند:

$$\rho\to\frac{1-3P}{4}\rho+\frac{P}{4}X\rho X+\frac{P}{4}Y\rho Y+\frac{P}{4}Z\rho Z\qquad(۳۱)$$

از رابطه‌ی بالا مشخص است که در کانال واقطبش خطاهای X,Y,Z با احتمال یکسان رخ می‌دهند.

۴-۳. اثر نوفه‌ی واقطبش در عملکرد پروتکل

حامل $|GHZ\rangle_{ABC}$ در اثر نوفه‌ی واقطبش با احتمال $(1-P)$ تغییری نمی‌کند اما با احتمال P هر کدام از کیوبیت‌هایش در حالت بیشینه درهم‌آمیخته قرار می‌گیرد:

$$|GHZ\rangle\langle GHZ|_{ABC} \rightarrow (1-P)|GHZ\rangle\langle GHZ|_{ABC} + P\left(\frac{I_A}{2}\otimes\frac{I_B}{2}\otimes\frac{I_C}{2}\right). \quad (۳۲)$$

سه کیوبیت در یک فضای هشت بعدی قرار دارند. می‌توانیم حالت‌های درهم‌تنیده‌ی زیر را به‌عنوان پایه‌های فضای هشت بعدی در نظر بگیریم:

$$\begin{aligned}
|GHZ_1\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle).\\
|GHZ'_1\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|000\rangle-|111\rangle).\\
|GHZ_2\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|110\rangle+|001\rangle).\\
|GHZ'_2\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|110\rangle-|001\rangle).\\
|GHZ_3\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|101\rangle+|010\rangle).\\
|GHZ'_3\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|101\rangle-|010\rangle).\\
|GHZ_4\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|011\rangle+|100\rangle).\\
|GHZ'_4\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|011\rangle-|100\rangle).
\end{aligned} \quad (۳۳)$$

حالت‌های بالا یک فضای کامل برای کیوبیت‌های حامل هستند:

$$I_{ABC} = \sum_{i=1}^{4}|GHZ_i\rangle\langle GHZ_i|_{ABC} + |GHZ'_i\rangle\langle GHZ'_i|_{ABC}. \quad (۳۴)$$

توجه کنید که $|GHZ_1\rangle$ همان حالت $|GHZ\rangle$ است. بنابراین حامل دورهای زوج در اثر نوفه‌ی واقطبش به‌صورت زیر نوشته می‌شود:

$$\rho^{even} = (1-P)|GHZ_1\rangle\langle GHZ_1|_{ABC} + \frac{P}{8}\sum_{i=1}^{4}|GHZ_i\rangle\langle GHZ_i|_{ABC} + |GHZ'_i\rangle\langle GHZ'_i|_{ABC} \quad (۳۵)$$

$|GHZ_i\rangle$ها و $|GHZ'_i\rangle$ها اجزای تشکیل دهنده‌ی حامل مختل شده توسط نوفه در دورهای زوج هستند. برای اینکه عملکرد این حامل را بررسی کنیم باید عملکرد هر کدام از این اجزا را در تحویل دادن پیام بررسی کنیم. در دورهای زوج پیام در حالت $|q,q\rangle_{1,2}$ کد می‌شود و کل عملگرهای CNOT بصورت $\Omega^{even} = C_{C,2}C_{B,1}C_{A,2}C_{A,1}$ است:

$$\begin{aligned}
&\Omega^{even}|GHZ_1\rangle_{ABC}|q,q\rangle_{1,2} = |GHZ_1\rangle_{ABC}|q,q\rangle_{1,2}.\\
&\Omega^{even}|GHZ'_1\rangle_{ABC}|q,q\rangle_{1,2} = |GHZ'_1\rangle_{ABC}|q,q\rangle_{1,2}.\\
&\Omega^{even}|GHZ_2\rangle_{ABC}|q,q\rangle_{1,2} = |GHZ_2\rangle_{ABC}|q,\bar{q}\rangle_{1,2}.\\
&\Omega^{even}|GHZ'_2\rangle_{ABC}|q,q\rangle_{1,2} = |GHZ'_2\rangle_{ABC}|q,\bar{q}\rangle_{1,2}.\\
&\Omega^{even}|GHZ_3\rangle_{ABC}|q,q\rangle_{1,2} = |GHZ_3\rangle_{ABC}|\bar{q},q\rangle_{1,2}.\\
&\Omega^{even}|GHZ'_3\rangle_{ABC}|q,q\rangle_{1,2} = |GHZ'_3\rangle_{ABC}|\bar{q},q\rangle_{1,2}.\\
&\Omega^{even}|GHZ_4\rangle_{ABC}|q,q\rangle_{1,2} = |GHZ_4\rangle_{ABC}|\bar{q},\bar{q}\rangle_{1,2}.\\
&\Omega^{even}|GHZ'_4\rangle_{ABC}|q,q\rangle_{1,2} = |GHZ'_4\rangle_{ABC}|\bar{q},\bar{q}\rangle_{1,2}.
\end{aligned} \quad (۳۶)$$

در رابطه‌ی بالا می‌بینیم که در تمام حالت‌ها در انتهای دور، پیام از حامل جدا می‌شود. حالت $|q,q\rangle_{1,2}$ با احتمال $(1-P)+2\left(\frac{P}{8}\right)=1-\frac{3P}{4}$ به درستی تحویل داده می‌شود اما با احتمال خطای $\frac{3P}{4}$ یکی از کیوبیت‌ها یا هر دوی آنها بصورت برگردان شده تحویل داده می‌شود. (توجه کنید که در دورهای زوج پیام مهمی ارسال نمی‌شود).

در پایان دورهای زوج در اثر عملگرهای هادامارد حالت‌های $|GHZ_i\rangle_{ABC}$ به حالت‌های $|\tilde{0}_i\rangle_{ABC}$ و حالت‌های $|GHZ'_i\rangle_{ABC}$ به حالت‌های $|\tilde{1}_i\rangle_{ABC}$ تبدیل می‌شوند:

$$
\begin{aligned}
&\left|\tilde{0}_1\right\rangle_{ABC}=|000\rangle+|011\rangle+|101\rangle+|110\rangle.\\
&\left|\tilde{1}_1\right\rangle_{ABC}=|111\rangle+|100\rangle+|010\rangle+|001\rangle.\\
&\left|\tilde{0}_2\right\rangle_{ABC}=|000\rangle-|011\rangle-|101\rangle+|110\rangle.\\
&\left|\tilde{1}_2\right\rangle_{ABC}=|111\rangle-|100\rangle-|010\rangle+|001\rangle.\\
&\left|\tilde{0}_3\right\rangle_{ABC}=|000\rangle-|011\rangle+|101\rangle-|110\rangle.\\
&\left|\tilde{1}_3\right\rangle_{ABC}=|111\rangle-|100\rangle+|010\rangle-|001\rangle.\\
&\left|\tilde{0}_4\right\rangle_{ABC}=|000\rangle+|011\rangle-|101\rangle-|110\rangle.\\
&\left|\tilde{1}_4\right\rangle_{ABC}=|111\rangle+|100\rangle-|010\rangle-|001\rangle.
\end{aligned}
\qquad (۳۷)
$$

حالت‌های درهم‌تنیده‌ی بالا نیز برای سه کیوبیت حامل تشکیل یک فضای کامل می‌دهند. در واقع می‌دانیم که پایه‌های یک فضا می‌توانند با عملگرهای یونیتاری به یکدیگر تبدیل شوند که در اینجا عملگرهای هاداماردی که کاربران در انتهای دورها اعمال می‌کنند همین نقش را به عهده دارد :

$$
I_{ABC}=\sum_{i=1}^{4}\left|\tilde{0}_i\right\rangle\left\langle\tilde{0}_i\right|_{ABC}+\left|\tilde{1}_i\right\rangle\left\langle\tilde{1}_i\right|_{ABC}. \qquad (۳۸)
$$

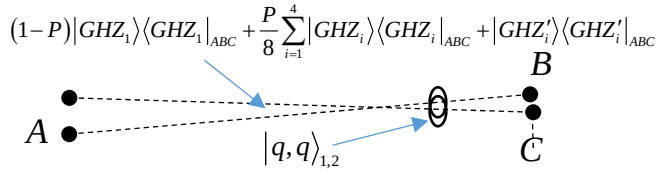
بنابراین حامل دورهای فرد به‌صورت زیر است:

$$
\begin{aligned}
\rho^{odd}&=(1-P)\left|\tilde{0}_1\right\rangle\left\langle\tilde{0}_1\right|_{ABC}\\
&+\frac{P}{8}\sum_{i=1}^{4}\left|\tilde{0}_i\right\rangle\left\langle\tilde{0}_i\right|_{ABC}+\left|\tilde{1}_i\right\rangle\left\langle\tilde{1}_i\right|_{ABC}.
\end{aligned}
\qquad (۳۹)
$$

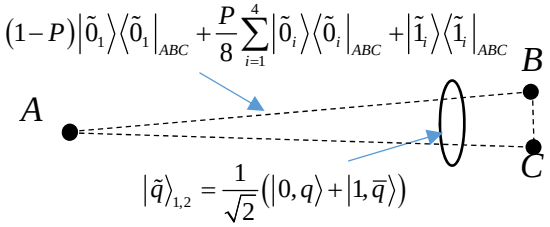
توجه کنید که $\left|\tilde{0}_1\right\rangle_{ABC}$ همان حالت $\left|\tilde{0}\right\rangle_{ABC}$ است، $\left|\tilde{1}_1\right\rangle_{ABC}$ نیز همان حالت $\left|\tilde{1}\right\rangle_{ABC}$ است. برای اینکه عملکرد حامل در دورهای فرد را بررسی کنیم می‌بایست عملکرد اجزای آن که شامل $\left|\tilde{0}_i\right\rangle_{ABC}$ها و $\left|\tilde{1}_i\right\rangle_{ABC}$ها است را بررسی کنیم. در دورهای فرد پیام در حالت $\left|\tilde{q}\right\rangle_{1,2}$ کد می‌شود و کل عملگرهای CNOT با عملگر $\Omega^{odd}=C_{B,1}C_{C,2}C_{A,1}$ داده می‌شود:

$$
\begin{aligned}
&\Omega^{odd}\left|\tilde{0}_1\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}=\left|\tilde{0}_1\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}.\\
&\Omega^{odd}\left|\tilde{1}_1\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}=\left|\tilde{1}_1\right\rangle_{ABC}\left|\tilde{\tilde{q}}\right\rangle_{1,2}.\\
&\Omega^{odd}\left|\tilde{0}_2\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}=\left|\tilde{0}_2\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}.\\
&\Omega^{odd}\left|\tilde{1}_2\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}=\left|\tilde{1}_2\right\rangle_{ABC}\left|\tilde{\tilde{q}}\right\rangle_{1,2}.\\
&\Omega^{odd}\left|\tilde{0}_3\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}=\left|\tilde{0}_3\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}.\\
&\Omega^{odd}\left|\tilde{1}_3\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}=\left|\tilde{1}_3\right\rangle_{ABC}\left|\tilde{\tilde{q}}\right\rangle_{1,2}.\\
&\Omega^{odd}\left|\tilde{0}_4\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}=\left|\tilde{0}_4\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}.\\
&\Omega^{odd}\left|\tilde{1}_4\right\rangle_{ABC}\left|\tilde{q}\right\rangle_{1,2}=\left|\tilde{1}_4\right\rangle_{ABC}\left|\tilde{\tilde{q}}\right\rangle_{1,2}.
\end{aligned}
\qquad (۴۰)
$$

در رابطه‌ی بالا می‌بینیم که در تمام حالت‌ها در انتهای دور حامل از پیام جدا شده است. در حالت‌های $\left|\tilde{0}_i\right\rangle$ (پاریته‌ی زوج سه کیوبیت) پیام به درستی دریافت شده است و در حالت‌های $\left|\tilde{1}_i\right\rangle$ (پاریته‌ی فرد سه کیوبیت) پیام بهصورت برگردان دریافت شده است. در دورهای فرد پیام با احتمال $(1-P)+4\left(\frac{P}{8}\right)=1-\frac{P}{2}$ به‌صورت درست $\left|\tilde{q}\right\rangle_{1,2}$ و با احتمال خطای $\frac{P}{2}$ به‌صورت برگردان شده $\left|\tilde{\tilde{q}}\right\rangle_{1,2}$ تحویل داده می‌شود.



الف) دورهای زوج



ب) دورهای فرد

شکل ۳. اثر نوفه‌ی واقطبش در پروتکل اشتراک رمز با حامل‌های درهم‌تنیده

۴. بررسی اثر نوفه به‌طور مستمر

برای بررسی اثر نوفه‌ی میراکننده‌ی فاز به‌طور مستمر می‌توانیم فرض کنیم که در دور 1 هستیم و نوفه یک بار اعمال شده است و حامل به‌صورت رابطه‌ی (۲۵) نوشته شده است. (می‌توانیم از رابطه‌ی (۲۲) نیز آغاز کنیم، درنهایت تاثیری در بحث ندارد). اگر بنا باشد که نوفه‌ی میراکننده‌ی فاز به‌طور مستمر به این حامل وارد شود باید اثر آن را برای تمام حالت‌های ممکن در حامل حساب کنیم. مطابق محاسباتی که در بخش ۲-۳ با جزئیات بیان کردیم خواهیم داشت:

$$\begin{aligned}&|\tilde{0}_i\rangle\langle\tilde{0}_i|\to(1-P)|\tilde{0}_i\rangle\langle\tilde{0}_i|+\frac{P}{3}\left[\sum_{j\neq i}|\tilde{0}_j\rangle\langle\tilde{0}_j|\right]\\&|\tilde{1}_i\rangle\langle\tilde{1}_i|\to(1-P)|\tilde{1}_i\rangle\langle\tilde{1}_i|+\frac{P}{3}\left[\sum_{j\neq i}|\tilde{1}_j\rangle\langle\tilde{1}_j|\right]\end{aligned}\qquad(۴۱)$$

در رابطه‌ی بالا می‌بینیم که اثر نوفه‌ی میراکننده‌ی فاز بر روی هر کدام از $|\tilde{0}_i\rangle$ها به این صورت است که با احتمال $(1-P)$ خودش حفظ می‌شود و با احتمال خطای $\frac{P}{3}$ ترکیب خطی سه نوع دیگر می‌شود. (مشابه همین بحث برای $|\tilde{1}_i\rangle$ها هم برقرار است). در واقع نوفه هر تعداد باری که اعمال شود حامل را از فضای $|\tilde{0}_i\rangle$ها و $|\tilde{1}_i\rangle$ها خارج نمی‌کند و از آنجائیکه عملکرد پروتکل با این فضا سازگاری دارد، اختلال اضافه شده پروتکل را از عملکرد تعریف شده اش خارج نمی‌کند.

برای ورود به دور بعدی که کاربران عملگرهای هادامارد را اثر می‌دهند حامل به ترکیب خطی از $|GHZ_i\rangle$ها و $|GHZ_i'\rangle$ها تبدیل می‌شود. بنابراین می‌بایست نوفه‌ی میراکننده‌ی فاز را به همان روش توضیح داده شده در بخش ۲-۳ برای $|GHZ_i\rangle$ها و $|GHZ'_i\rangle$ها محاسبه کنیم:

$$\begin{aligned}&|GHZ_i\rangle\langle GHZ_i|\to\\&(1-P)|GHZ_i\rangle\langle GHZ_i|+P|GHZ'_i\rangle\langle GHZ'_i|.\\&|GHZ'_i\rangle\langle GHZ'_i|\to\\&(1-P)|GHZ'_i\rangle\langle GHZ'_i|+P|GHZ_i\rangle\langle GHZ_i|.\end{aligned}\qquad(۴۲)$$

در رابطه‌ی بالا مشخص است که نوفه‌ی میراکننده‌ی فاز با احتمال $(1-P)$ حالت های $|GHZ_i\rangle$ را حفظ می‌کند و با احتمال خطای P حالت $|GHZ'_i\rangle$ متناظر با آن را تحویل می‌دهد. (مشابه همین بحث برای $|GHZ'_i\rangle$ برقرار است). از آنجائیکه نوفه هر تعداد باری که اثر کند حامل را از فضای $|GHZ_i\rangle$ها و $|GHZ'_i\rangle$ها خارج نمی‌کند و عملکرد پروتکل با این فضا سازگاری دارد، اختلال اضافه شده پروتکل را از عملکرد تعریف شده اش خارج نمی‌کند.

برای اینکه اثر مستمر نوفه‌ی واقطبش را بر روی حامل بررسی کنیم، هر بار که می‌خواهیم نوفه را لحاظ کنیم می‌بایست ترکیب خطی حالت حامل و حالت بیشینه

درهم‌آمیخته‌ی سه کیوبیت را در نظر بگیریم. زیرا اثر کانال واقطبش به این صورت است که با احتمال $(1-P)$ حالت اولیه را حفظ میکند و با احتمال خطای P تمام اطلاعات آن را از بین می‌برد و به حالت یکنواخت و کاملا تصادفی تبدیل می‌کند. در اینجا چون حامل سه کیوبیتی است پس به حالت بیشینه درهم آمیخته برای سه کیوبیت تبدیل می‌شود. اگر در حالتی باشیم که حامل در فضای $|GHZ_i\rangle$ها و $|GHZ'_i\rangle$ها نوشته شده باشد، بسط I را برحسب رابطه‌ی (۳۴) می‌نویسیم. اما اگر در حالتی باشیم که حامل در فضای $|\tilde{0}_i\rangle$ها و $|\tilde{1}_i\rangle$ها نوشته شده باشد، بسط I را برحسب رابطه‌ی (۳۸) می‌نویسیم. با این حساب حامل هم‌چنان در فضای $|GHZ_i\rangle$ها و $|GHZ'_i\rangle$ها، یا در فضای $|\tilde{0}_i\rangle$ها و $|\tilde{1}_i\rangle$ها نوشته می‌شود و می‌دانیم که باقی ماندن حامل در این فضاها با عملکرد پروتکل سازگاری دارد.

۵. نتیجه‌گیری

در این مقاله پایداری پروتکل اشتراک رمز با حامل‌های درهم‌تنیده را در برابر نوفه‌ی میراکننده‌ی فاز و نوفه‌ی واقطبش که به‌طور مستمر اثر می‌کند بررسی کردیم. در این پروتکل حالت‌های درهم‌تنیده به عنوان حامل بین فرستنده و گیرندگان به اشتراک گذاشته می‌شوند و مانند محیطی عمل می‌کنند که در یک سو فرستنده پیام را به آن‌ها سوار می‌کند و در سوی دیگر گیرندگان پیام را از آن‌ها پیاده می‌کنند. پیام در حین انتقال در حالت بیشینه درهم‌آمیخته قرار می‌گیرد و از دید استراق سمع کننده پنهان می‌ماند. نشان دادیم که حتی اگر نوفه به‌طور مستمر بر حامل وارد شود، حامل به‌طور کل از فرم خارج نمی‌شود بلکه در دو نوع فضای مشخص با پایه‌های درهم‌تنیده که فضای کاملی برای کیوبیت‌های حامل هستند و با عملکرد پروتکل سازگاری دارند باقی می‌ماند.

مراجع

1. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 70, 1895–1899 (1993)
2. Bennett, C., Wiesner, S.: Communication via one and two-particle operators on Einstein-Podolsky Rosen states. Phys. Rev. Lett. 69(20), 2881 (1992)
3. Raussendorf, R., Briegel, H.-J.: A one-way quantum computer. Phys. Rev. Lett. 86, 5188 (2001)
4. Broadbent, A., Fitzsimons, J., Kashefi, E.: Universal blind quantum computation. In: Proceedings of the 50th Annual Symposium on Foundations of Computer Science, 517-526 (2009)
5. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A 59, 1829 (1999)
6. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A 59, 162 (1999)
7. Xgiao, Li, Long, Gui Lu, Deng, Fu-Guo, Pan, Jian-Wei: Efficient multi-party quantum secret sharing schemes. Phys. Rev. A 59, 1829 (1999)
8. Xiao, Li, Long, Gui Lu, Deng, Fu-Guo, Pan, Jian-Wei: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A 69,052307 (2004)
9. Zhang, Zhan-jun, Man, Zhong-xiao: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A 72,022303 (2005)
10. Wu, Y., Zhou, J., Gong, X., Guo, Y., Zhang, Z.-M., He, G.: Continuous-variable measurement-device independent multipartite quantum communication. Phys. Rev. A 93, 022325 (2016)
11. Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, p. 8. New York (1984)
12. Ekert, A.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67, 661-663 (1991)
13. Bechmann-Pasquinucci, H., Gisin, N.: Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography. Phys. Rev. A 59, 4238–4248 (1999)
14. Bruss, D., Macchiavello, C.: Optimal eavesdropping in cryptography with three-dimensional quantum states. Phys. Rev. Lett. 88(12), 127901 (2002) .
15. Schmid, C., Trojek, P., Bourennane, M., Kurtsiefer, C., Zukowski, M., Weinfurter, H.:

Experimental single qubit quantum secret sharing. Phys. Rev. Lett. 95, 230505 (2005)
16. Zhang, Zhan-jun, Li, Yong, Man, Zhong-xiao: Multiparty quantum secret sharing. Phys. Rev. A 71, 044301 (2005)
17. Tavakoli, A., Herbauts, I., Zukowski, M., Bourennane, M.: Secret sharing with a single d-level quantum system. Phys. Rev. A Rapid Commun. 92, 030302 (2015)
18. Karimipour, Vahid, Asoudeh, Marzieh: Quantum secret sharing and random hopping: using single states instead of entanglement. Phys. Rev. A Rapid Commun. 92, 030301 (2015)
19. Zhang, Y.S., Li, C.F., Guo, G.C.: Quantum key distribution via quantum encryption. Phys. Rev. A 64,024302 (2001)
20. Bagherinezhad, S., Karimipour, V.: Quantum secret sharing based on reusable GHZ states as secure carriers. Phys. Rev. A 67,044302 (2003)
21. Emamipanah, sh., Asoudeh, M., Karimipour, V.: Entangled states as robust and re-usable carriers of information. Quantum information processing (2020)

Robustness of Entangled Carriers to Noise

Shima Emamipanah, Marzieh Asodeh

Abstract

Similar to the role that carriers play in classical conversations as a medium for transmitting messages, entangled states can also be considered as a medium that plays the role of a carrier for information. In this way, we can define protocols for quantum communications in which quantum states are entangled with the carrier on one side (embedded in the carrier) and on the other side are safely separated from it by the receivers (embedded in the carrier), leaving the carrier intact for reuse. In addition, these protocols can be used for quantum cryptography. In this paper, we investigate the robustness of these protocols against phase and polarization damping noise and show that despite the continuous effect of noise, the carrier remains in two distinct types of spaces with entangled bases that are complete spaces for the carrier qubits and are consistent with the protocol performance.

Keywords: "Quantum code sharing", "entanglement", "reusable carriers"