چهارمین کنفرانس ملی ایده های نوین مهندسی برق
۲۰و۲۱ آبان ماه ۱۳۹۴ - دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)

روشی برای نهان‌نگاری کوانتومی عکس FRQI در یک پروتکل دیالوگ کوانتومی

شاهرخ حیدری[۱]، مصیب ناصری[۲]
[۱]گروه مهندسی کامپیوتر، واحد کرمانشاه، دانشگاه آزاد اسلامی ،کرمانشاه، ایران، shahrokh.heidari@outlook.com
[۲] گروه فیزیک، واحد کرمانشاه ، دانشگاه آزاد اسلامی ، کرمانشاه ، ایران،m.naseri@iauksh.ac.ir

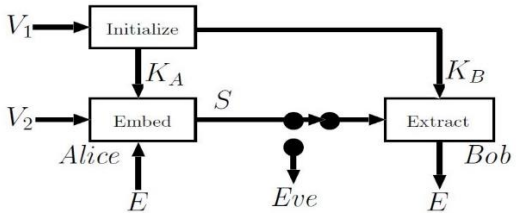
چکیده - منظور از نهان‌نگاری، پنهان کردن اطلاعات در قالب یک کاور است، به طوری که تنها برای گیرنده قابل رؤیت باشد. این کاور می‌تواند عکس، صدا، متن، فیلم و یا هر چیز دیگر باشد، به طوری که اطلاعات در این کاور نهان‌نگاری شده و تنها گیرنده قادر به دریافت این اطلاعات است. در این مقاله یک پروتکل برای دیالوگ کوانتومی بیان می‌شود به طوری که یک سرویس‌دهنده ارتباط بین گیرنده و فرستنده را فراهم می-کند. این پروتکل بر اساس ذرات درهم‌تنیده دوگانه بل می‌باشد. نهان‌نگاری که در این پروتکل پیشنهاد می‌شود دارای کاور عکس کوانتومی است. بنابراین هنگام ارسال عکس کوانتومی فرستنده اطلاعات خود را در این کاور طبق پروتکل دیالوگ کوانتومی موجود نهان‌نگاری می‌کند و از طریق کانال کوانتومی برای گیرنده ارسال می‌کند. این اطلاعات را تنها گیرنده می‌تواند استخراج کند.

کلید واژه- دیالوگ کوانتومی، نهان‌نگاری کوانتومی، درهم‌تنیدگی، درهم‌تنیدگی دوگانه بل، عکس کوانتومی FRQI

۱- مقدمه

ادبیات نهان‌نگاری را می‌توان از دید Simmons نگاه کرد که در سال ۱۹۸۳ آن را به‌عنوان مشکل زندانیان مطرح کرد. در این مدل، آلیس و باب به زندان افتاده و در دو سلول متفاوت هستند. آن‌ها می‌خواهند به کمک یک نقشه از زندان فرار کنند، اما تمام ارتباطات آن‌ها توسط شخصی به نام Eve کنترل می‌شود. اگر Eve، هرگونه اطلاعات پنهان و مضمونی را در ارتباط آن‌ها که نشان دهد قصد فرار دارند، تشخیص دهد، تمام ارتباطات بین آن دو را قطع کرده و آن‌ها را به سلول انفرادی می‌اندازد. بنابراین آلیس و باب باید راهی پیدا کنند که اطلاعات خود را در یک کاور مخفی کنند. این امنیت به کلید رمزی وابسته است که آلیس و باب به طریقی برای ارسال به یکدیگر، تنظیم کرده‌اند. سپس آن‌ها از این کلید برای بهره‌برداری از اطلاعات مخفی شده در کاور استفاده می‌کنند. آیا آلیس و باب می‌توانند یک نقشه فرار بدون اینکه Eve متوجه شود، طرح کنند؟بله. آن‌ها می‌توانند با استفاده از نهان‌نگاری، یک ارتباط پنهانی را باهم برقرار کنند[۱].

نهان‌نگاری روشی برای پنهان کردن اطلاعات است که تنها برای گیرنده مشخص، قابل رؤیت است. با توجه به ضرورت به-وجود آمدن کامپیوترهای کوانتومی بر اساس پیش‌بینی گوردن مور[۲] و مطرح شدن نظریه اطلاعات کوانتومی، نهان‌نگاری کوانتومی نیز به عنوان شاخه‌ای از مخفی‌سازی اطلاعات کوانتومی مطرح شد. نهان‌نگاری از طریق یک کاور یا به‌اصطلاح پوشش انجام می‌گیرد که این پوشش سبب مخفی ماندن پیام اصلی می‌شود. نهان‌نگاری کوانتومی، انتقال پیام مورد نظر به طور مخفیانه به همراه کاور اطلاعات از طریق کانال کوانتومی است[۳]. شکل ۱ مدلی برای نهان‌نگاری کوانتومی را نشان می-دهد که در سال ۲۰۰۶ توسط ناتوری بیان شد[۴]. همان‌طور که می‌بینید V_1 ابتدا به عنوان کلید اولیه به فرستنده و گیرنده داده می‌شود. از این V_1 فرستنده برای تعبیه کردن اطلاعات در کاور و گیرنده برای استخراج اطلاعات استفاده می‌کند. آلیس از طریق V_1 و V_2 که در اختیار دارد، اطلاعات E را در کاور نهان‌نگاری می‌کند و برای باب ارسال می‌کند. باب پس از دریافت با توجه به V_1 که در اختیار دارد، می‌تواند به‌راحتی E را از کاور استخراج کند. در این بین، فرض بر این است که Eve به کانال کوانتومی دسترسی دارد.



شکل ۱: یک مدل نهان‌نگاری کوانتومی در یک کانال کوانتومی[۴]

ما در این مقاله پروتکلی را برای دیالوگ کوانتومی پیشنهاد می‌کنیم و از این مدل نهان‌نگاری بیان شده برای ارسال عکس کوانتومی در این پروتکل استفاده می‌کنیم. در دیالوگ کوانتومی یک سرویس‌دهنده، ارتباط بین فرستنده و گیرنده را فراهم می‌کند. ارتباط امن و مخابرات امن یکی از مهمترین موضوعاتی است که امروزه زندگی بشر را به شدت تحت تأثیر قرار داده است. مخابرات، ارتباط و انتقال داده کلاسیک با دو چالش مهم روبروست: امنیت و کارایی. سیستم‌های کلاسیک، معمولا یکی از این دو نیاز را تأمین می‌کنند و در تأمین هردو نیاز با هم با مشکل روبرو هستند. مخابرات کوانتومی و نظریه اطلاعات کوانتومی از جمله زمینه های جدیدی است که در آن می‌توان به رفع مشکلات ارتباط امن کلاسیک امیدوار بود. انتقال حالت کوانتومی از یک نقطه به نقطه دیگر را مخابرات کوانتومی می‌گویند. در مخابرات کوانتومی، اطلاعاتی که باید مخابره شوند، روی فوتون‌هایی سوار می‌شوند که هم می‌توانند در فضای آزاد و هم از طریق فیبرهای نوری کم تلف ارسال شوند[۵]. این ارتباط کوانتومی می‌تواند به منظور ایجاد یک مکالمه تلفنی بین دو شخص مورد استفاده قرار گیرد. در این حالت یک شخص سوم باید وجود داشته باشد که به عنوان سرویس‌دهنده، امکان برقراری ارتباط بین فرستنده و گیرنده را توسط کدهای شناسایی آن‌ها، فراهم می‌کند. در ادامه یک پروتکل امن تلفن کوانتومی با استفاده از ذرات درهم‌تنیده دوگانه بل پیشنهاد می‌شود.

در بخش دوم ذرات درهم‌تنیده و ذرات درهم‌تنیده دوگانه بل معرفی می‌شود. بخش بعد پروتکل پیشنهادی برای دیالوگ کوانتومی مطرح می‌شود. بخش چهارم به معرفی عکس‌های کوانتومی FRQI می‌پردازد. بخش پنجم روش نهان‌نگاری کوانتومی برای این پروتکل را بیان می‌کند و در بخش آخر نتیجه‌گیری بیان می‌شود.

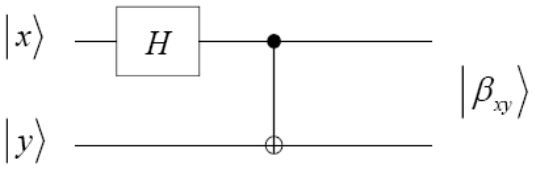
در بخش دوم ذرات درهم‌تنیده و ذرات درهم‌تنیده دوگانه بل معرفی می‌شود. بخش بعد پروتکل پیشنهادی برای دیالوگ کوانتومی مطرح می‌شود. بخش چهارم به معرفی عکس‌های کوانتومی FRQI می‌پردازد. بخش پنجم روش نهان‌نگاری کوانتومی برای این پروتکل را بیان می‌کند و در بخش آخر نتیجه‌گیری بیان می‌شود.

۲- ذرات درهم‌تنیده و ذرات درهم‌تنیده دوگانه بل

انیشتن در سال ۱۹۳۵ به منظور ناقص نشان دادن توانایی واقع‌نمایی نظریه مکانیک کوانتومی با کمک دو تن از شاگردان خود، آزمایش مشهوری که به EPR معروف شد را طراحی کرد[۶]. این آزمایش در تحولات بعدی فیزیک جدید در قرن بیستم تأثیر بسزایی داشت. در این آزمایش فرض می‌شد که دو سیستم کوانتومی نظیر دو فوتون در یک محیط ایزوله و مجزا از تأثیرات بیرونی با هم اندرکنش انجام می‌دهند و سپس ازهم دور می‌شوند. تا زمانی که این دو فوتون در شرایط انزوا از محیط بیرون باقی بمانند، هر اندازه هم که فاصله میان آن دو زیاد باشد باز هم یک سیستم واحد به‌شمار می‌آیند به‌طوری که اگر یکی از دو فوتون‌ها اندازه‌گیری شود تا برخی از مشخصه‌های آن شناسایی شود، آزمایشگر می‌تواند اطلاعات مشابهی را در مورد فوتون دوم کسب کند بدون آنکه به آن دسترسی مستقیم داشته باشد.هر اصلاح یا تغییری که به ذره شماره یک اعمال شود، زوج آن یعنی ذره شماره دو نیز دچار تغییرات می‌شود. تغییرات ذره دو که ناشی از تغییرات اعمال شده به ذره یک است،وابسته به فاصله میان آن‌ها نیست. ذره دو به طور همزمان تغییرات ذره یک را حس می‌کند.

با استفاده از گیت‌های کوانتومی می‌توان همانند شکل ۲ یک زوج فوتون درهم‌تنیده را به صورت ریاضی مدل کرد. این مدار با سری کردن گیت هادامارد و CNOT بدست می‌آید. اگر ورودی این مدار را یکی از حالات $|00\rangle,|01\rangle,|10\rangle,|11\rangle$ در نظر بگیریم، چهار حالت درهم‌تنیده متفاوت با عنوان Bell states بدست خواهد آمد.

$$|\Phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),|\Psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle) \quad (۱)$$



شکل ۲: ایجاد یک زوج فوتون درهم‌تنیده

حال اگر دومین ذره از هر حالت را از یک گیت کوانتومی هادامارد عبور دهیم حالات دوگانه بل یا Bell dual basis بدست خواهند آمد.

$$|\chi^+\rangle=\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle-|11\rangle) \quad (۲)$$

$$|\chi^-\rangle=\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle) \quad (۳)$$

$$|\omega^+\rangle=\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle+|11\rangle) \quad (۴)$$

$$|\omega^-\rangle=\frac{1}{2}(|00\rangle-|01\rangle-|10\rangle-|11\rangle) \quad (۵)$$

۳- پروتکل دیالوگ کوانتومی مبتنی بر ذرات درهم‌تنیده دوگانه بل

فرض می‌کنیم فرستنده، آلیس و گیرنده، باب باشد. در این صورت یک سرور به عنوان سرویس‌دهنده امکان برقراری ارتباط بین آلیس و باب را توسط کدهای شناسایی آن‌ها فراهم می‌کند. سپس با در اختیار گذاشتن کانال کوانتومی لازم برای مکالمه زمینه لازم را برای مراسله اطلاعات رمز شده بین آن‌ها محیا می‌کند. برخلاف خطوط تلفنی ناامن معمولی که امروزه استفاده می‌شود، روش حاضر دستیابی به نوعی از خطوط امن تلفنی را میسر می‌سازد. این پروتکل از دو فاز تشکیل شده است، فاز احراز هویت و فاز نحوه ارتباط امن، که در ادامه بررسی می‌شوند.

در فاز احراز هویت، تعداد L کیوبیت رشته احراز هویت را بااستفاده از پایه های Z و X فراهم می‌شود و برای کاربر ارسال می‌شود. به این ترتیب که اگر بیت iام از بیت های شناسایی یا احراز هویت 1 باشد، S از پایه های Z و اگر اگر بیت iام از بیت های شناسایی یا احراز هویت 0 باشد، S از پایه های X استفاده می‌کند. که S همان رشته احراز هویت کوانتومی ست. و پایه‌های X, Z برابر است با :

$$X=\{|0\rangle,|1\rangle\},Z=\{|+\rangle,|-\rangle\} \quad (۶)$$

از آنجایی که کاربر بیت های صحیح احراز هویت خود را می داند، لذا می‌تواند برای اندازه گیری رشته از پایه های درستی استفاده نماید و درنتیجه کیوبیت های ارسالی از سرور را به خوبی تشخیص دهد. لذا سرور می‌تواند با دریافت نتیجه اندازه-گیری کاربر از اصالت و قانونی بودن وی اطمینان حاصل کند.

در فاز ارتباط امن، این پروتکل از ذرات درهم‌تنیده دوگانه بل استفاده می‌کند. قبل از هرچیز، ذرات درهم‌تنیده دوگانه بل را می‌توان به صورت زیر نیز نشان داد[۵]:

$$|\chi^+\rangle=\frac{1}{2}(|++\rangle+|+-\rangle+|-+\rangle-|--\rangle) \quad (۷)$$

$$|\chi^-\rangle=\frac{1}{2}(|++\rangle-|+-\rangle+|-+\rangle+|--\rangle) \quad (۸)$$

$$|\omega^+\rangle=\frac{1}{2}(|++\rangle+|+-\rangle-|-+\rangle+|--\rangle) \quad (۹)$$

$$|\omega^-\rangle=\frac{1}{2}(|+-\rangle-|++\rangle+|-+\rangle+|--\rangle) \quad (۱۰)$$

که + و - برابر است با : $|+\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ و $|-\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

در هر یک از چهار حالت فوق ذره اول را با مقدار آن جایگزین خواهیم کرد. به طور مثال برای χ^+ خواهیم داشت :

$$|\chi^+\rangle=\frac{1}{2}(|++\rangle+|+-\rangle+|-+\rangle-|--\rangle)$$

$$\frac{1}{2}\left(\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}|+\rangle\right]+\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}|-\rangle\right]+\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}|+\rangle\right]-\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}|-\rangle\right]\right)$$

$$\frac{1}{2\sqrt{2}}\left[|0+\rangle+|1+\rangle+|0-\rangle+|1-\rangle+|0+\rangle-|1+\rangle-|0-\rangle+|1-\rangle\right]$$

$$\frac{1}{2\sqrt{2}}\left[2|0+\rangle+2|1-\rangle\right]=\frac{1}{\sqrt{2}}\left[|0+\rangle+|1-\rangle\right]=$$

$$|\chi^+\rangle=\frac{|0+\rangle+|1-\rangle}{\sqrt{2}} \quad (۱۱)$$

و به همین صورت برای حالت‌های دیگر ذرات درهم‌تنیده دوگانه بل خواهیم داشت:

$$|\chi^+\rangle=\frac{|0+\rangle+|1-\rangle}{\sqrt{2}},|\chi^-\rangle=\frac{|0+\rangle-|1-\rangle}{\sqrt{2}} \quad (۱۲)$$

$$|\omega^+\rangle=\frac{|0-\rangle+|1+\rangle}{\sqrt{2}},|\omega^-\rangle=\frac{|0-\rangle-|1+\rangle}{\sqrt{2}} \quad (۱۳)$$

در این پروتکل پیشنهادی از عملگرهای کوانتومی σ_x ،

I ، $i\sigma_y$ و σ_z استفاده می‌شود که تعریف ریاضی هرکدام از این عملگرها به صورت زیر است و همچنین $|0\rangle$ و $|1\rangle$ را نیز به صورت ماتریسی زیر نمایش می‌دهیم :

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},i\sigma_y=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$$
$$\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\ |0\rangle=\begin{pmatrix}1\\0\end{pmatrix},|1\rangle=\begin{pmatrix}0\\1\end{pmatrix} \qquad (۱۴)$$

گفتیم که سرور شرایط لازم برای ارتباط آلیس و باب را فراهم می‌کند. سرور یکی از حالت های دوگانه بل را در نظر می‌گیرد و ذره اول را برای آلیس و همچنین ذره دوم را برای باب ارسال می‌کند. آلیس بر حسب نیاز خود یکی از عملگرهای گفته شده را بروی ذره اول اعمال می‌کند و برای باب از طریق کانال کوانتومی می‌فرستد. باب ذره اول را که عملگر بروی آن اعمال شده است را دریافت می‌کند همچنین ذره دوم را هم در اختیار دارد بنابراین باب هم یکی از عملگرهای یگانه را بروی ذره دوم اعمال می‌کند باتوجه به جداولی که در ادامه گفته می‌شود و نتیجه حاصله، باب می‌تواند بیت‌های ارسالی آلیس را متوجه شود. در ادامه چگونگی عملکرد پروتکل با مثال توضیح داده می‌شود.

آلیس با توجه به بیت هایی که قرار است ارسال کند، یکی از عملگرهای زیر را بر روی ذره اول اعمال می‌کند. همان‌طور که در جدول ۱ می‌بینید.

جدول ۱: بیت‌های معادل با عملگرهای یگانی در این پروتکل

I	σ_x	$i\sigma_y$	σ_z
00	01	10	11

حال ببینیم نتیجه هر یک از این عملگرها بر روی ذره اول هریک از چهار حالت ذرات درهم‌تنیده دوگانه بل چه خواهد بود. ابتدا با χ^+ شروع خواهیم کرد.

$$|\chi^+\rangle=\frac{|0+\rangle+|1-\rangle}{\sqrt{2}}$$
$$\sigma_{x_1}\chi^+=\begin{pmatrix}0&1\\1&0\end{pmatrix}\frac{|0+\rangle+|1-\rangle}{\sqrt{2}}$$
$$\begin{pmatrix}0&1\\1&0\end{pmatrix}|0\rangle=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}=|1\rangle$$
$$\begin{pmatrix}0&1\\1&0\end{pmatrix}|1\rangle=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}=|0\rangle$$
$$\frac{|1+\rangle+|0-\rangle}{\sqrt{2}}=\frac{|0-\rangle+|1+\rangle}{\sqrt{2}}=\omega^+$$
$$\rightarrow\sigma_{x_1}\chi^+=\omega^+ \qquad (۱۵)$$

به همین ترتیب سایر عملگرها و حالات را نیز می‌توان محاسبه کرد که جدول ۲ برای ذره اول نشان داده شده است.

جدول۲: نتیجه عملگرهای یکانی بروی ذره اول از حالات درهم‌تنیده دوگانه.

	χ^+	χ^-	ω^+	ω^-
I_1	χ^+	χ^-	ω^+	ω^-
σ_{x_1}	ω^+	ω^-	χ^+	χ^-
$i\sigma_{y_1}$	ω^-	ω^+	χ^-	χ^+
σ_{z_1}	χ^-	χ^+	ω^-	ω^+

همچنین هنگامی که عملگرهای یکانی را بروی ذره دوم اثر می‌دهیم نتایجی حاصل می‌شود که در جدول ۳ مشاهده می‌کنید:

جدول۳: نتیجه عملگرهای یکانی بروی ذره دوم از حالات درهم‌تنیده دوگانه.

	χ^+	χ^-	ω^+	ω^-
I_2	χ^+	χ^-	ω^+	ω^-
σ_{x_2}	χ^-	χ^+	ω^-	ω^+
$i\sigma_{y_2}$	ω^-	ω^+	χ^-	χ^+
σ_{z_2}	ω^+	ω^-	χ^+	χ^-

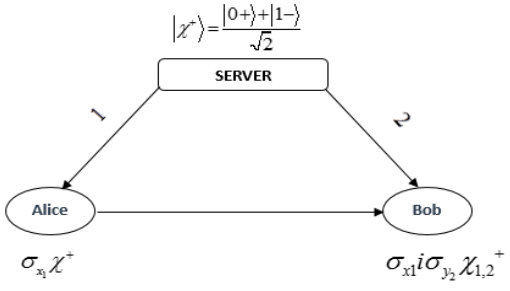
با توجه به اینکه آلیس بروی ذره اول، عملگر خود را اعمال می‌کند و برای باب می‌فرستد، بنابراین باب با توجه به جدول ۴ که از جدول‌های ۲ و ۳ بدست می‌آید، عملگر استفاده شده آلیس را تشخیص می‌دهد. هنگامی که عملگر استفاده شده آلیس را

تشخیص دهد یعنی به بیت هایی که آلیس قصد ارسال آن را داشته، پی برده است.

جدول ۴: نتیجه عملگرهای یکانی که آلیس و باب به ترتیب بروی ذره اول و دوم اعمال می‌کنند.

	χ^+	χ^-	ω^+	ω^-
$I_1 I_2$	χ^+	χ^-	ω^+	ω^-
$I_1 \sigma_{x_2}$	χ^-	χ^+	ω^-	ω^+
$I_1 i\sigma_{y_2}$	ω^-	ω^+	χ^-	χ^+
$I_1 \sigma_{z_2}$	ω^+	ω^-	χ^+	χ^-
$\sigma_{x_1} I_2$	ω^+	ω^-	χ^+	χ^-
$\sigma_{x_1} \sigma_{x_2}$	ω^-	ω^+	χ^-	χ^+
$\sigma_{x_1} i\sigma_{y_2}$	χ^-	χ^+	ω^-	ω^+
$\sigma_{x_1} \sigma_{z_2}$	χ^+	χ^-	ω^+	ω^-
$i\sigma_{y_1} I_2$	ω^-	ω^+	χ^-	χ^+
$i\sigma_{y_1} \sigma_{x_2}$	ω^+	ω^-	χ^+	χ^-
$i\sigma_{y_1} i\sigma_{y_2}$	χ^+	χ^-	ω^+	ω^-
$i\sigma_{y_1} \sigma_{z2}$	χ^-	χ^+	ω^-	ω^+
$\sigma_{z_1} I_2$	χ^-	χ^+	ω^-	ω^+
$\sigma_{z_1} \sigma_{x_2}$	χ^+	χ^-	ω^+	ω^-
$\sigma_{z_1} i\sigma_{y_2}$	ω^+	ω^-	χ^+	χ^-
$\sigma_{z_1} \sigma_{z_2}$	ω^-	ω^+	χ^-	χ^+

آلیس می‌خواهد با باب ارتباط برقرار کند بنابراین سرور شرایط لازم را باید فراهم کند. فرض می‌کنیم که سرور χ^+ را از بین حالات درهم‌تنیده بل انتخاب می‌کند. همان‌طور که در شکل ۳ می‌بینید ذره اول از χ^+را برای آلیس و ذره دوم آن را برای باب ارسال می‌کند. فرض می‌کنیم که آلیس بخواهد بیت‌های 01 را ارسال کند. بنابراین طبق جدول ۱ باید عملگر σ_x را بروی ذره اول اعمال کند. پس از اعمال، آلیس نتیجه خود را برای باب ارسال می‌کند. باب هم عملگر خود را بروی ذره دوم اعمال می‌کند. فرض که $i\sigma_{y_2}$ را اثر دهد. تا به اینجا باب از عملگری که آلیس استفاده کرده خبر ندارد. اما چیزی که در دست دارد χ^-خواهد بود چرا که داریم: $\sigma_{x_1} i\sigma_{y_2} \chi^+ = \chi^-$ اما باب با استفاده از جدول۴ می‌تواند به عملگر استفاده شده آلیس پی ببرد بدین صورت که، حالت درهم‌تنیده مورد استفاده سرور χ^+ بوده است(سرور قبلا از طریق کانال کلاسیک به باب اطلاع داده است). پس به ستون χ^+ در جدول ۴ مراجعه خواهد کرد. در این ستون به دنبال ایتمی می‌گردد که نتیجه نهایی χ^- و عملگر استفاده شده برا ذره دوم $i\sigma_{y_2}$ (که خود استفاده کرده)باشد. طبق جدول۴ تنها سطر هفت با این مشخصات مطاقبت دارد. بنابراین در اینجا پی خواهد برد که آلیس عملگر σ_x را اعمال کرده است. طبق جدول ۱ ، σ_x برابر خواهد بود با 01 بنابراین باب پی برد که آلیس قصد ارسال 01 را داشته است. این مثال برای دو بیت بود به همین طریق آلیس می‌تواند رشته‌ای از بیت‌ها را ارسال کند.به طریقی که در بالا گفته شد، باب، به منظور آلیس در یک ارتباط کوانتومی امن پی می‌برد. به طریقی مشابه باب هم می‌تواند پاسخ آلیس را بدهد.



شکل۳: نحوه ارتباط آلیس و باب با استفاده از ذرات درهم‌تنیده دوگانه

۴- نمایش انعطاف‌پذیر عکس کوانتومی (FRQI)

نمایش انعطاف‌پذیر برای تصاویر کوانتومی، یک نمایش برای تصویر کوانتومی است که مبتنی بر نمایش پیکسل‌ها پیشنهاد

شده است[۷]. FRQI، شامل اطلاعات رنگ و موقعیت دقیق مربوط به هر پیکسل در عکس می‌باشد. بر اساس FRQI ، نمایش تصاویر کوانتومی می‌تواند طبق نمایش زیر نوشته شود:

$$I(\theta)=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle \qquad (۱۶)$$

$$|c_i\rangle=\cos\theta_i|0\rangle+\sin\theta_i|1\rangle$$

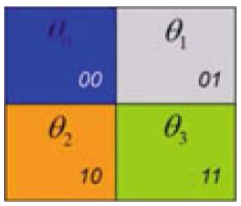
$$\theta_i\in\left[0,\frac{\pi}{2}\right], i=0,1,...,2^{2n}-1$$

$(\theta_0,\theta_1,\theta_2,...,\theta_{2n-1})$ وضعیت‌های کوانتومی پایه، $|0\rangle,|1\rangle$ بردار زاویه‌های رنگ‌های کد شده هستند و $|i\rangle$ برای $i=0,1,...,2^{2n}-1$ پایه های محاسباتی $2^{2n}-1$ بعدی می‌باشد. دو قسمت FRQI یعنی $|c_i\rangle$ و $|i\rangle$ اطلاعاتی در مورد رنگ و موقعیت آن‌ها در تصویر را به ترتیب کد می‌کنند. در تصاویر کوانتومی دو بعدی، اطلاعات موقعیت $|i\rangle$ شامل دو قسمت زیر می‌شود: مختصات عمودی و افقی[۸].

(۱۷)

$$|i\rangle=|y\rangle|x\rangle=|y_{n-1}y_{n-2}...y_0\rangle|x_{n-1}x_{n-2}...x_0\rangle$$

که در آن $|y_i\rangle|x_i\rangle\in\{0,1\}$. به ازای $|y_{n-1}y_{n-2}...y_0\rangle$ اطلاعات موقعیت عمودی را با استفاده از n کیوبیت اول کد می‌کند و $|x_{n-1}x_{n-2}...x_0\rangle$ اطلاعات موقعیت افقی را با استفاده از n کیوبیت دوم کد می‌کند. به طور مثال، معادله ۱۸، نمایش FRQI را برای یک تصویر ۲×۲ که در شکل ۳ نشان داده شده است، را نشان می‌دهد.



شکل۴: یک تصویر ساده و وضعیت FRQI مربوط به آن[۷].

$$|I\rangle=\frac{1}{2}\begin{bmatrix}(\cos\theta_0|0\rangle+\sin\theta_0|1\rangle)\otimes|00\rangle+\\(\cos\theta_1|0\rangle+\sin\theta_1|1\rangle)\otimes|01\rangle+\\(\cos\theta_2|0\rangle+\sin\theta_2|1\rangle)\otimes|10\rangle+\\(\cos\theta_3|0\rangle+\sin\theta_3|1\rangle)\otimes|11\rangle\end{bmatrix} \qquad (۱۸)$$

۵- روش نهان‌نگاری پیشنهادی

در پروتکلی که برای دیالوگ کوانتومی پیشنهاد شد، سرویس دهنده یا سرور ملزومات لازم برای ارتباط بین آلیس و باب را فراهم می‌کند. در این بخش هدف این است که در کاور تصویر کوانتومی FRQI ، یک سری اطلاعات را در این پروتکل نهان‌نگاری کنیم طوری که هنگامی که آلیس تصویر نهان‌نگاری شده را برای باب ارسال می‌کند تنها باب قادر به استخراج اطلاعات مخفی شده باشد. حتی سرور هم قادر به تشخیص اطلاعات در این حالت نخواهد بود. مراحل الگوریتم پیشنهادی به‌صورت زیر است:

گام اول: طبق مدل نهان‌نگاری که در شکل ۱ بیان شد. ابتدا آلیس و باب باید بر سر یک کلید به توافق برسند. طول کلید را برابر با تعداد تتاهای تصویر مورد نظر در نظر می‌گیریم. طبق آن‌چه که در بخش ۳ گفته شد آلیس می‌تواند یک رشته کیوبیت را که نمایان‌گر کلید مورد نظر است، با عملگرهای یکانی کد کند و برای باب ارسال کند و باب هم با توجه به اندازگیری ذره‌های دریافتی و استفاده از جدول ۴ می‌تواند رشته کیوبیت کد شده را دیکد و تشخیص دهد. بنابراین آلیس و باب بر سر یک کلید به طول تتاهای تصویر کوانتومی مورد نظر، به توافق می‌رسند. در این گام آلیس به تعداد نصف بیت‌های اطلاعات خود که قرار است پنهان شود، در کلید به طور تصادفی ۱ می‌گذارد. چرا که همانطور که در ادامه هم خواهیم گفت، هر عملگر یکانی می‌تواند طبق جدول ۱، دو بیت را کد کند.

گام دوم: سرور رشته‌ای به طول n (تعداد تتاهای تصویر کوانتومی) از حالات درهم‌تنیده دوگانه بل ایجاد می‌کند:

(۱۹)

$$Q=\{|\beta_1\rangle|\beta_2\rangle|\beta_3\rangle...|\beta_n\rangle\},\beta_i\in\{\chi^{\pm},\omega^{\pm}\}$$

سپس سرور از این رشته، دو زیر رشته ایجاد می‌کند. که رشته

اول شامل ذره اول و رشته دوم شامل ذره دوم از رشته Q می‌باشد. a را برای نشان دادن ذره اول و b را برای نشان دادن ذره دوم استفاده می‌کنیم. بنابراین خواهیم داشت:

$$Q_a = \{|\beta_{1a}\rangle|\beta_{2a}\rangle|\beta_{3a}\rangle...|\beta_{na}\rangle\}, \beta_i \in \{\chi^{\pm}, \omega^{\pm}\} \quad (۲۰)$$

$$Q_b = \{|\beta_{1b}\rangle|\beta_{2b}\rangle|\beta_{3b}\rangle...|\beta_{nb}\rangle\}, \beta_{ib} \in \{\chi^{\pm}, \omega^{\pm}\} \quad (۲۱)$$

در این حالت سرور رشته Q_a را برای آلیس و رشته Q_b را از طریق کانال کوانتومی برای باب می‌فرستد.

گام سوم: این گام شامل دو فاز است. فاز ارسال و فاز دریافت.

فاز ارسال: آلیس هنگام ارسال تصویر کوانتومی خود که به شکل FRQI می‌باشد بدین طریق عمل می‌کند: اگر iامین بیت از کلید 0 باشد، آلیس تتای iام از تصویر را به صورت زیر از طریق کانال کوانتومی ارسال می‌کند.

$$I(\theta_i) = \frac{1}{2}\cos\theta_i|0\rangle + \sin\theta_i|1\rangle \otimes |i\rangle \quad (۲۲)$$

اگر iامین بیت از کلید 1 باشد آلیس تتای iام را به صورت زیر ارسال خواهد کرد.

$$I(\theta_i) = \frac{1}{2}\cos\theta_i|0\rangle + \sin\theta_i|1\rangle \otimes |i\rangle \otimes |\delta\rangle \quad (۲۳)$$

که $|\delta\rangle$ بدین شکل ایجاد می‌شود. آلیس طبق جدول ۱ متناظر با بیت‌هایی که قرار است پنهان کند، عملگر یکانی خود را انتخاب و بروی iامین ذره اول، از رشته Q_a اثر می‌دهد. در نتیجه $|\delta\rangle$ ایجاد می‌شود. و طبق معادله ۲۲ پیکسل مورد نظر به شکل FRQI ارسال خواهد شد.

فاز دریافت: باب هنگام دریافت، کلید در دست خود را چک می‌کند. اگر هنگام دریافت پیکسل iام، iامین بیت از کلید 0 باشد، بنابراین باب می‌فهمد که در این پیکسل نهان‌نگاری صورت نگرفته است و پیکسل را به همان صورت دریافت می‌کند. اما اگر هنگام دریافت پیکسل iام، iامین بیت کلید را 1 ببیند بنابراین متوجه نهان‌نگاری در این پیکسل خواهد شد. در نتیجه ذره $|\delta\rangle$ را جدا کرده. یک عملگر یکانی بروی iامین ذره دوم، از رشته Qb انجام می‌دهد. در نتیجه با استفاده از جدول ۴ و آنچه که در بخش ۳ گفته شد، به بیت‌های نهان شده آلیس پی خواهد برد.

گام چهارم: در اینجا گام سوم انقدر تکرار می‌شود که آلیس تمام پیکسل‌های خود را که به صورت FRQI هستند برای باب ارسال کند.

گام پنجم: در آخر باب با کنارهم قرار دادن بیت‌های استخراجی اطلاعات نهان شده را بدست خواهد آورد.

۶- نتیجه گیری

به منظور ایجاد یک ارتباط امن کوانتومی، در این مقاله، نخست یک پروتکل دیالوگ کوانتومی که یک سرور واسط ارتباطی بین فرستنده و گیرنده است، پیشنهاد شد. در این پروتکل از یک روش نهان‌نگاری طبق مدلی که در شکل ۱ بیان شد، پیشنهاد شد. کاور این نهان‌نهان نگاری یک عکس کوانتومی به شیوه نمایش FRQI است. از جمله کارهای آتی که می‌توان در این زمینه انجام داد، استفاده از روشی برای نهان‌نگاری صوت کوانتومی در این پروتکل اشاره کرد.

مراجع

[1] Simmons, G.J.:Advances in Cryptology: Proceedings of Crypto 83. Plenum Press, New York, pp. 51–67 (1984).
[2] S.Imr, “Quantum computing and communications – Introduction and challenges” Computer and Electrical Engineering, Vol. 40, No.1, pp. 134-141, 2014
[3] Wei, Z.-H., et al. (2015). "The Quantum Steganography Protocol via Quantum Noisy Channels." International Journal of Theoretical Physics: 1-11.
[4] Natori, S. (2006). Why Quantum Steganography Can Be Stronger Than Classical.
[۵] شهرام محمدنژاد، ۱۳۸۵، مخابرات کوانتومی و چشم انداز آن در شبکه های مخابرات نوری، سیزدهمین کنفرانس اپتیک و فوتونیک ایران، تهران، انجمن اپتیک و فتونیک ایران، مرکز تحقیقات مخابرات ایران.
[6] Einstein A, Podolsky B, Rosen N; Podolsky; Rosen (1935). "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" Phys. Rev. 47 (10): 777–780.
[7] Phuc Q. Le, Fangyan Dong, Kaoru Hirota, A flexible representation of quantum images for polynomial preparation, image compression, and processing operations, 2010.
[8] Zhang, W.-W., et al. (2013). "A Quantum Watermark Protocol." International Journal of Theoretical Physics 52(2): 504-513.