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

یک پروتکل امن تلفن کوانتومی با استفاده از ذرات درهم‌تنیده دوگانه بل

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 - ارتباط امن بین فرستنده و گیرنده از جمله مسائلی است که امروزه بسیار حائز اهمیت است. هنگامی که فرستنده قصد ارتباط با گیرنده را دارد هر چه روش انتقال داده خود را ایمن‌تر ببیند، بیشتر به راه ارتباطی اعتماد دارد. با توجه به ناامن بودن سیستم‌های کلاسیک، پیشنهاد روشی امن برای مکالمه بین دوشخص می‌تواند بسیار کاربردی و قابل اعتماد باشد. در این مقاله یک پروتکل امن تلفن کوانتومی پیشنهاد می‌شود که مبتنی بر ذرات درهم‌تنیده دوگانه بل است. یک سرویس‌دهنده یا سرور کانال ارتباطی لازم برای ارتباط بین فرستنده و گیرنده را فراهم می-کند و فرستده با توجه به ذره دریافتی از سرور و ارسالی به باب، می‌تواند مکالمه را در کانالی امن انجام دهد.

کلید واژه- تلفن کوانتومی، مخابرات کوانتومی، ذرات درهم‌تنیده، ذرات درهم‌تنیده دوگانه بل

۱- مقدمه

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 می-گویند. 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[۱]. 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.

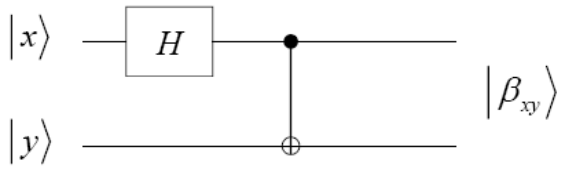
دربخش دوم ذرات درهم‌تنیده و ذرات درهم‌تنیده دوگانه بل توضیح داده شده است. بخش بعد پروتکل پیشنهادی برای تلفن کوانتومی مبتنی بر ذرات درهم‌تنیده دوگانه بل بیان می‌شود. بخش چهارم امنیت پروتکل را مورد بررسی قرار می‌دهد، و در آخر نتیجه‌گیری انجام شده است.

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[۲]. 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 ۱ 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.



شکل ۱: استفاده از گیت‌های هادامارد و CNOT برای ایجاد یک زوج فوتون درهم‌تنیده

در حالت اول هنگامی که ورودی مدار را $|00\rangle$ فرض کرده و خروجی مدار را محاسبه می‌کنیم. حالت $|0\rangle$ پس از عبور از گیت هادامارد به حالت زیر تبدیل می‌شود:

$$|0\rangle \underline{H} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \qquad (۱)$$

در نتیجه قبل از گیت CNOT حالت کوانتومی ترکیبی به صورت زیر خواهد بود:

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle) \qquad (۲)$$

در اثر عبور این حالت کوانتومی از گیت CNOT حالت زیر حاصل می‌شود:

$$\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)\underline{_{CNOT}}\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=|\Phi^+\rangle \qquad (۳)$$

اگر ورودی های دیگر را نیز در نظر بگیریم چهار حالت بل بدست خواهد آمد که به صورت زیر می‌باشند:

$$|\Phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),|\Psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle) \qquad (۴)$$

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.

$$|\chi^{+}\rangle=\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle-|11\rangle) \qquad (۵)$$

$$|\chi^{-}\rangle=\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle) \qquad (۶)$$

$$|\omega^{+}\rangle=\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle+|11\rangle) \qquad (۷)$$

$$|\omega^{-}\rangle=\frac{1}{2}(|00\rangle-|01\rangle-|10\rangle-|11\rangle) \qquad (۸)$$

۳- پروتکل تلفن 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 $X=\{|0\rangle,|1\rangle\}, Z=\{|+\rangle,|-\rangle\}$.

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[۳]:

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

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

$$|\omega^+\rangle=\frac{1}{2}\left(|++\rangle+|+-\rangle-|-+\rangle+|--\rangle\right) \quad (۱۱)$$

$$|\omega^-\rangle=\frac{1}{2}\left(|+-\rangle-|++\rangle+|-+\rangle+|--\rangle\right) \quad (۱۲)$$

که در این حالت + 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 :

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

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

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

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

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

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

$$|\chi^+\rangle=\frac{|0+\rangle+|1-\rangle}{\sqrt{2}},|\chi^-\rangle=\frac{|0+\rangle-|1-\rangle}{\sqrt{2}} \quad (۱۴)$$

$$|\omega^+\rangle=\frac{|0-\rangle+|1+\rangle}{\sqrt{2}},|\omega^-\rangle=\frac{|0-\rangle-|1+\rangle}{\sqrt{2}} \quad (۱۵)$$

عملگرهای یگانه: در این پروتکل پیشنهادی از عملگرهای کوانتومی I ، $i\sigma_y$ ، σ_x 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 :

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},i\sigma_y=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$$

$$\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},|0\rangle=\begin{pmatrix}1\\0\end{pmatrix},|1\rangle=\begin{pmatrix}0\\1\end{pmatrix} \quad (۱۶)$$

گفتیم که سرور شرایط لازم برای ارتباط آلیس و باب را فراهم می‌کند. سرور یکی از حالت های دوگانه بل را در نظر می-گیرد 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 می-شود.

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.

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

$$\sigma_{x_1}\chi^+ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{|0+\rangle + |1-\rangle}{\sqrt{2}}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$\frac{|1+\rangle + |0-\rangle}{\sqrt{2}} = \frac{|0-\rangle + |1+\rangle}{\sqrt{2}} = \omega^+$$

$$\sigma_{x_1}\chi^+ = \omega^+ \qquad (۱۷)$$

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.

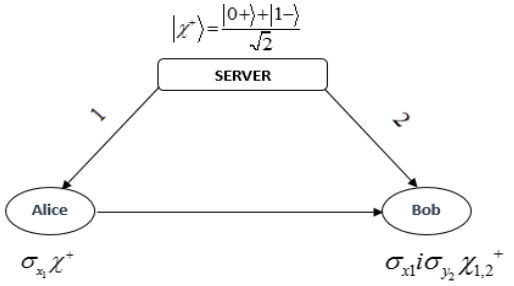
جدول۴: نتیجه عملگرهای یکانی که آلیس و باب به ترتیب بروی ذره اول و دوم اعمال می‌کنند.

	χ^+	χ^-	ω^+	ω^-
I_1I_2	χ^+	χ^-	ω^+	ω^-
$I_1\sigma_{x_2}$	χ^-	χ^+	ω^-	ω^+
$I_1i\sigma_{y_2}$	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 مطابقت 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 هممیتواند پاسخ آلیس را بدهد.



شکل۲: نحوه ارتباط آلیس و باب با استفاده از ذرات درهم‌تنیده دوگانه

۴- بررسی امنیت پروتکل

برای هرچه بیشتر امن کردن ارتباط در این پروتکل، از روش Decoy States Method استفاده شده است. فرض می‌کنیم، رشته ذراتی که آلیس قصد ارسال آن‌ها را دارد، به صورت زیر است:

$$Q=\{|q_1\rangle,|q_2\rangle,|q_3\rangle...|q_i\rangle...|q_n\rangle\} \quad (۱۸)$$

که Q رشته ذرات ارسالی آلیس و q_i ذره اول از یکی از حالات درهم‌تنیده دوگانه بل است که عملگرهای یکانی بروی آن‌ها اعمال شده است. حال رشته ذرات C را در نظر می‌گیریم:

$$C=\{|C_1\rangle,|C_2\rangle,|C_3\rangle...|C_i\rangle...|C_n\rangle\} \quad (۱۹)$$

که در C_i بر پایه X یا Z می باشد.

$$\{X=\{|0\rangle,|1\rangle\},Z=\{|+\rangle,|-\rangle\}\} \quad (۲۰)$$

آلیس هنگام ارسال رشته Q ، C را نیز به Q اضافه خواهد کرد و محل قرار گیری آن را از طریق کانال کلاسیک به سرور اطلاع می‌دهد. به طور مثال رشته ارسالی آلیس به صورت زیر خواهد شد:

$$Q+C=\{|q_1\rangle,|q_2\rangle,|C_1\rangle...|C_i\rangle...|q_n\rangle\} \quad (۲۱)$$

آلیس $Q + C$ را برای باب ارسال می‌کند. سرور محل قرار گیری ذرات C را به باب اطلاع داده است. بنابراین باب C_i ها را از رشته بیرون می‌کشد و آن‌ها را اندازه‌گیری می‌کند. و آن‌ها را با آلیس در کانال کلاسیک باهم مطابقت می‌دهد. در این بین اگر در هنگام ارسال ذرات در کانال کوانتومی شخص سومی ذرات را اندازه‌گیری و مجددا ارسال کرده باشد و باعث تغییر آن‌ها شده باشد، مشخص می‌شود و ارتباط قطع و مجددا از سر گرفته می‌شود[۴].

۵- نتیجه‌گیری

در این مقاله پروتکل امن تلفن کوانتومی بر پایه ذرات درهم‌تنیده دوگانه بل معرفی شد. در پروتکل، سرور، کانال ارتباطی لازم و شرایط امن بودن کانال بین فرستنده و گیرنده را فراهم می‌کند. در ابتدای مقاله چگونگی ایجاد ذرات درهم‌تنیده و همچنین ذرات درهم‌تنیده دوگانه بل توضیح داده شد و اینکه چطور می‌توان با استفاده از این ذرات یک راه ارتباطی امن ایجاد کرد. چون در پروتکل پیشنهادی راه ارتباطی بین فرستنده و گیرنده با سرور جداست، بنابراین شنود سرور هم،امکان‌پذیر نیست. کارهای آتی در این زمینه می‌توان به هرچه بیشتر امن کردن پروتکل اشاره کرد.

مراجع

[۱] 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.

[2] 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.

[3] Jia Mo, Zhaofeng Ma, Yixian Yang, Xinxin Niu: Journal Article(2013), A Quantum Watermarking Protocol Based on Bell Dual Basis, International Journal of Theoretical Physics

[4] Negin Fatahi·Mosayeb Naseri. "Quantum Watermarking Using Entanglement Swapping". Int J Theor Phys (2012).