

چند استفاده ساده از درهم تنیدگی در اطلاعات کوانتومی

وحیدکریمی پور- دانشکده فیزیک - دانشگاه صنعتی شریف

۱۱ بهمن ۱۴۰۴

۱ مقدمه

در این درس هدف ما آن است که نشان دهیم مکانیک کوانتومی می تواند به طرق مختلف در انتقال اطلاعات آنهم به شیوه ای بسیار موثر مورد استفاده واقع شود. ممکن است سالها و بلکه دهه ها طول بکشد تا یک کامپیوتر کوانتومی ساخته شود تا بتوان روی آن یک الگوریتم کوانتومی برای تجزیه یک عدد بزرگ را پیاده سازی کرد. در عوض دانش و فناوری مربوط به مخابره اطلاعات کوانتومی سرشتی کاملاً متفاوت دارند و تا به امروز پیشرفت های بزرگی در این حوزه چه به صورت نظری و چه به صورت تجربی صورت گرفته است. آنچه که در انتقال اطلاعات کوانتومی نقش اساسی دارد، خاصیت غیرموضعی بودن مکانیک کوانتومی و وجود حالت های درهم تنیده^۱ است. در زیر نمونه های متعددی از فرایندهایی را خواهیم دید که طی آن از حالت های درهم تنیده برای انتقال اطلاعات استفاده می شود. البته هیچ کدام از این فرایندها ناقض نسبیت خاص نیستند. تقریباً تمام آزمایش هایی که تاکنون برای فرایندهای انتقال اطلاعات کوانتومی انجام شده اند از حالت های درهم تنیده قطبش فوتون ها استفاده می کنند. چنین حالتی معمولاً به شکل زیر است:

$$|\phi\rangle = \frac{1}{2}(|H, V\rangle + |V, H\rangle) = \frac{1}{2}(|H\rangle_{Alice} \otimes |V\rangle_{Bob} + |V\rangle_{Alice} \otimes |H\rangle_{Bob}), \quad (1)$$

که در آن H و V به ترتیب نشان دهنده قطبش افقی و عمودی فوتون ها در یک دستگاه مختصات معین است و شاخص های آلایس و باب نشان دهنده این است که فوتون ها در دو نقطه متفاوت تحت کنترل آلایس و باب هستند. ممکن است که این دو شخص کیلومترها از هم فاصله

^۱Entangled States

داشته باشند. امروزه در آزمایشگاه می توان از طریق فرایندی که به آن تبدیل پارامتری معکوس^۲ می گویند، می توان چنین فوتون هایی را تولید کرده و سپس از طریق فیبرهای نوری یا هوای آزاد به فاصله های دوردست فرستاد. درعمل بسیاری از این زوج فوتون ها سالم به مقصد نمی رسند، به این معنی که بسیاری از آنها جذب محیط شده و یا درهم تنیدگی آنها در اثر واکنش با محیط از بین می رود ولی همواره تعداد قابل توجهی از آنها سالم و دست نخورده به مقصد می رسند به طوریکه بتوان با آنها فرایندهای انتقال اطلاعات را انجام داد. می توان فرض کرد که مرکزی وجود دارد که این زوج های درهم تنیده را تولید کرده و آن را بین مشتریانی که بخواهند فرایندهای اطلاعات کوانتومی را انجام می دهند، به اشتراک می گذارد. امروزه تهیه و توزیع چنین حالت هایی دشوار و گران است ولی مثل هرنوع فناوری دیگر، می توان روزی را تصور کرد که این کار با بازدهی فوق العاده بالا و با بهای کم انجام بپذیرد.

دراین درس هدف ما تنها معرفی چند فرایند ساده برای مبادله اطلاعات است. مطالعه نظریه اطلاعات کوانتومی موضوعی است که در انتهای درسنامه به آن خواهیم پرداخت. فرایندهایی که دراین درس مورد مطالعه قرار می گیرند، عبارتند از فرابرد کوانتومی^۳، کدگذاری چگال^۴، رمزنگاری کوانتومی^۵، مبادله کوانتومی کلید^۶ و اشتراک کوانتومی رمز^۷. تمامی این فرایندها علاوه بر کیوبیت ها با کیودیت ها^۸ یعنی سیستم های d -حالت نیز می توان انجام داد ولی ما برای سادگی بررسی خود را محدود به سیستم های دوحالت می کنیم. در بعضی از تمرین ها تعمیم این فرایندها به بعد دلخواه خواسته شده است.

۲ حالت های بل

قبل از بررسی فرایند ها بهتر است به بعضی از خواص حالت های بل که در این فرایند ها نقش اساسی دارند، اشاره کنیم. این حالت ها حالت هایی هستند با ماکزیمم درهم تنیدگی و یک پایه کامل و متعامد یکه برای فضای دو کیوبیت تشکیل می دهند. در درس های آینده یاد خواهیم گرفت که چرا این حالت ها بیشترین مقدار درهم تنیدگی را دارند. فعلا به این بسنده می کنیم که بگوییم، فرایندهای خارق العاده مبادله اطلاعات کوانتومی (مثل فرابرد کوانتومی، کدگذاری چگال و نظایر آن) به کمک این حالت هاست که امکان پذیر است.

^۲Parametric Down Conversion

^۳Teleportation

^۴Dense Coding

^۵Quantum Cryptography

^۶Quantum Key Distribution

^۷Quantum Secret Sharing

^۸Qudit

این روابط هم چنین به خواننده نشان می دهند که چگونه می توان حالت های بل برای سیستم های d حالت را نوشت. حالت های بل برای کیوبیت ها عبارتند از:

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

دقت کنیم که برای حالت های بل دو نوع نماد بکار برده ایم. نمادهای اول متدوال ترند ولی نمادهای دوم برای نوشتن سیستماتیک این حالت ها بخصوص برای بعدهای دلخواه مناسب ترند. این حالت ها را می توان به شکل فشرده ی زیر نیز نوشت:

$$|\phi_{mn}\rangle = Z^m \otimes X^n |\phi_{00}\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^1 (-1)^{km} |k, k+n\rangle. \quad (3)$$

این حالت ها یک پایه متعامد برای فضای دو کیوبیت تشکیل می دهند. یعنی اینکه

$$\langle \phi_{mn} | \phi_{kl} \rangle = \delta_{mk} \delta_{nl}, \quad (4)$$

و

$$\sum_{mn} |\phi_{mn}\rangle \langle \phi_{mn}| = I. \quad (5)$$

با استفاده از یک گیت هادامارد و یک گیت $CNOT$ می توان حالت های چهارگانه فوق را تولید کرد:

$$(CNOT)(H \otimes I)|m, n\rangle = CNOT \frac{1}{\sqrt{2}} \sum_{k=0}^1 (-1)^{km} |k, n\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^1 (-1)^{km} |k, k+n\rangle = |\phi_{mn}\rangle. \quad (6)$$

از آنجا هم $CNOT$ و هم H هردو مربع شان برابر با ماتریس واحد است، رابطه بالا نتیجه می دهد که

$$(CNOT)(H \otimes I)|\phi_{m,n}\rangle = |m, n\rangle. \quad (7)$$

به یک نکته مهم دیگر هم باید اشاره کنیم و آن اینکه اگر چه این حالت ها بر هم عمودند، اما با اعمال یک عملگر موضعی توسط آلیس یا باب به هم تبدیل می شوند. در واقع براحتی می توان دید که:

$$(X \otimes I)|\phi^+\rangle = |\psi^+\rangle \quad (Z \otimes I)|\phi^+\rangle = |\phi^-\rangle \quad (XZ \otimes I)|\phi^+\rangle = |\psi^-\rangle. \quad (8)$$

منظور از اندازه گیری در پایه بل، یعنی اندازه گیری با عملگرهای تصویری $\{P_{mn} = |\phi_{mn}\rangle\langle\phi_{mn}|\}$. با توجه به روابط بالا این نوع اندازه گیری را می توان نخست با اعمال گیت های $(H \otimes I)$ و سپس $CNOT$ و بعد از آن اندازه گیری در پایه محاسباتی انجام داد. به این نکته هم می توانیم توجه کنیم که رابطه ساده ای بین حالت های بل و عملگرهای پاوولی وجود دارد. در واقع با تعویض کت های دوم در حالت های بل به عملگرهای پاوولی می رسم:

$$|\phi_{mn}\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^1 (-1)^{km} |k, k+n\rangle \leftrightarrow \frac{1}{\sqrt{2}} \sum_{k=0}^1 (-1)^{km} |k\rangle \langle k+n| = \frac{1}{\sqrt{2}} \sigma_{mn}. \quad (9)$$

خواننده براحتمی می تواند تصدیق کند که عملگرهای σ_{mn} با احتساب I (مجموعه عملگرهای پاوولی هستند. تمامی این روابط را می توان به ابعاد دلخواه یعنی برای کیودیت ها هم تعمیم داد. کافی است که بنویسیم:

$$|\phi_{mn}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} (\omega)^{km} |k, k+n\rangle \quad (10)$$

که در آن $\omega^d = 1$ و همه جمع ها هم به هنگ d انجام می شود. عملگرهای هادامارد و $CNOT$ هم نیز به شکل زیر تعمیم خواهند یافت:

$$H = \sum_{m,n=0}^{d-1} \omega^{mn} |m\rangle\langle n|, \quad CNOT|m, n\rangle = |m, m+n \pmod{d}\rangle. \quad (11)$$

تناظر بین حالت های بل و عملگرهای تعمیم یافته پاوولی نیز همچنان برقرار خواهند بود.

۳ فرابرد کوانتومی

درفربرد کوانتومی هدف ما آن است که بامخبره اطلاعات کلاسیک که طبیعتاً با سرعت نور انجام می گیرد حالت کوانتومی یک شی را به نقطه ای دوردست انتقال دهیم. در ساده ترین حالت فرض کنید که شخص A یا آلیس می خواهد حالت یک فوتون یا الکترون مثل $|\phi\rangle := \alpha|0\rangle + \beta|1\rangle$ را به همکار خود B یا باب که در نقطه ای دوردست واقع است انتقال دهد. فرض ما این است که باب الکترونی دارد که در یک حالت معین قرار دارد و می خواهد با استفاده از اطلاعاتی که آلیس به او می دهد کاری کند که الکترون اش حالت $|\phi\rangle$ را اختیار کند. مستقیم ترین راه برای این کار آن است که آلیس مقادیر دو عدد مختلط α و β را به باب مخبره کند و او با اعمال یک عملگر کوانتومی حالت الکترون اش را به حالتی که در دست آلیس است تبدیل کند. اما این کار دو اشکال اساسی دارد. اول آن که مخبره دو عدد مختلط فوق با دقت بی نهایت احتیاج به مخبره بی نهایت

اطلاعات دارد. بنابراین باید به ساخت تقریبی حالت اکتفا کنیم. اگر بخواهیم این اعداد مختلط را تنها با دقت سه رقم اعشار مخابره کنیم احتیاج به مخابره $40 = 2 \times 2 \times 10$ بیت داریم. اشکال دوم آن است که اصولاً معلوم نیست آلیس حالت الکترونی را که دردست دارد بداند و باین وجود بخواهد این حالت را به باب بفرستد. فرابرد کوانتومی روشی است که با استفاده از درهم تنیدگی این امکان را بوجود می آورد که بتوانیم حتی حالت های ناشناخته را آنهم با مخابره حداقل تعداد بیت های کلاسیک به نقاط دوردست انتقال دهیم. برای این کار به ترتیب زیر عمل می کنیم. نخست یک حالت درهم تنیده بل مثل

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)_{ab} \quad (12)$$

را بین A و B به اشتراک می گذاریم. کیویت اول که با a مشخص شده نزد آلیس و کیویت دوم که با b مشخص شده نزد باب خواهد بود. این حالت نقش یک خط ارتباطی کوانتومی بین آلیس و باب را ایفا می کند. حال آلیس حالت $|\phi\rangle$ را با کیویتی که نزد خود دارد نزدیک کرده تا حالت زیر بدست آید:

$$\begin{aligned} |\Psi\rangle = |\phi\rangle|\phi^+\rangle &= (\alpha|0\rangle + \beta|1\rangle)_a \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)_{ab} \\ &= \frac{1}{\sqrt{2}}(\alpha|0,0,0\rangle + \beta|1,0,0\rangle + \alpha|0,1,1\rangle + \beta|1,1,1\rangle). \end{aligned} \quad (13)$$

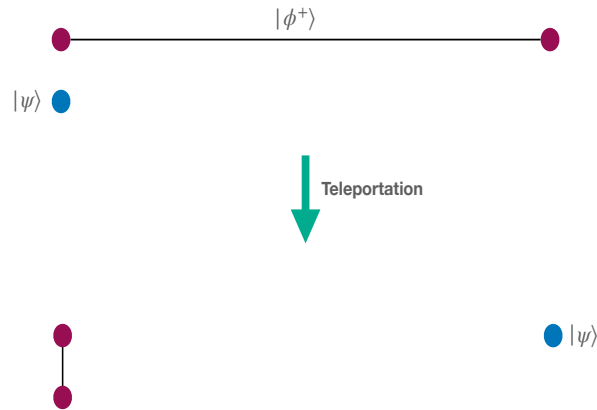
سپس آلیس روی دو کیویتی که نزد خود نگاه داشته است یک اندازه گیری در پایه بل انجام می دهد. برای اینکه حاصل اندازه گیری را بفهمیم حالت $|\Psi\rangle$ را به صورت زیر بازنویسی می کنیم:

$$\begin{aligned} |\Psi\rangle &= \frac{1}{2}(|\phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + |\phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) \\ &+ |\psi^+\rangle(\beta|0\rangle + \alpha|1\rangle) + |\psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle)). \end{aligned} \quad (14)$$

بنابراین بعد از اندازه گیری یکی از نتایج زیر برای آلیس بدست می آید و حالتی که دردست باب است به یکی از حالت های نشان داده شده در جدول زیر کاهش پیدا می کند. آلیس می تواند با مخابره تنها دو بیت کلاسیک نتیجه بدست آمده توسط اندازه گیری اش را به باب اطلاع دهد که به نوبه خود عملگر مناسب را روی حالت کاهش یافته اعمال می کند تا حالت اولیه ای که دردست آلیس بوده است نزد باب احیاشود. توجه کنید که در این روش لازم نیست که طرفین هیچ نوع اطلاعی از حالت اولیه داشته باشند.

I	$\alpha 0\rangle + \beta 1\rangle$	$ \phi^+\rangle$
Z	$\alpha 0\rangle - \beta 1\rangle$	$ \phi^-\rangle$
X	$\beta 0\rangle + \alpha 1\rangle$	$ \psi^+\rangle$
Y	$-\beta 0\rangle + \alpha 1\rangle$	$ \psi^-\rangle$

(15)



شکل ۱: فرابرد کوانتومی برای یک حالت خالص. حالتی که نزد آلیس است از بین رفته و نزد باب پدیدار می شود.

دقت کنید که در این فرایند هیچ حالتی تکثیر و کپی نشده است، چرا که حالت اولیه ای که نزد آلیس بود از بین رفته و نزد باب پدیدار شده است. شکل (۳) به صورت شماتیک فرابرد کوانتومی را برای یک حالت خالص نشان می دهد.

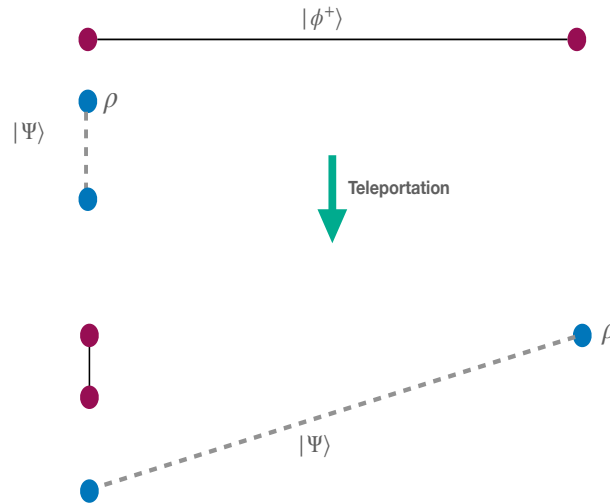
به این ترتیب باب می تواند با اطلاعاتی که از آلیس دریافت می کند، براحتی حالت اولیه را بازسازی کند. معمولاً در نظریه اطلاعات کوانتومی مفهومی به نام هزینه^۹ معرفی می شود که نشان دهنده میزان منابعی^{۱۰} است که برای انجام یک عمل خاص مصرف کرده ایم. تعیین این منابع از آن جهت اهمیت دارد که از نظر آزمایشگاهی و طبیعتاً از نظر مالی تهیه بعضی از منابع رایگان و تهیه دیگر منابع نیازمند هزینه است. این هزینه بستگی به محدودیت های آزمایشگاهی ما دارد. یک قسمت مهم از نظریه اطلاعات کوانتومی نظریه منابع^{۱۱} به مطالعه این موضوع می پردازد. به عنوان مثال تهیه یک زوج درهم تنیده دور از هم از نظر آزمایشگاهی کاری است سخت. اگر دو آزمایشگاه دور از هم زوج درهم تنیده ای را از یک آزمایشگاه سوم دریافت کنند می توانند با آن اعمالی انجام دهند که در غیر این صورت نمی توانستند به انجام رسانند. اگر هزینه یک زوج درهم تنیده را یک ای بیت^{۱۲} بنامیم، کاری که در فرابرد کوانتومی انجام داده ایم این است که یک ای بیت و دو بیت کلاسیک را مصرف کرده

^۹Cost

^{۱۰}Resources

^{۱۱}Resource Theory

^{۱۲}ebit



شکل ۲: فرابرد کوانتومی برای یک حالت درهم تنیده.

ایم تا بتوانیم یک کیوبیت را از نقطه ای به نقطه دیگر منتقل کنیم. بنابراین می توانیم بنویسیم:

$$1 \text{ ebit} + 2 \text{ bit} \longrightarrow 1 \text{ qubit}. \quad (۱۶)$$

■ **توضیح اول:** هرگاه حالتی که در دست باب باشد، یک حالت آمیخته مثل ρ باشد، بازهم فرابرد کوانتومی، حالت ρ را برای باب ایجاد کرده و حالت دست آلیس نابود می شود. دلیل اش هم خیلی ساده است: حالت ρ یک تجزیه به صورت $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ دارد و در اثر فرابرد هر کدام از حالت ها صحیح و سالم به دست باب می رسند. در نتیجه حالت دست باب نیز همان ترکیب محدب از حالت های $|\psi_i\rangle$ خواهد بود و نهایتاً حالت ρ برای باب بازسازی می شود. نگاه بهتری به این مسئله این است که حالت ρ بخشی از یک حالت خالص ولی درهم تنیده باشد که نیمه دیگرش در نقطه ای دیگر و خارج از کنترل آلیس است. در این صورت در اثر فرابرد کوانتومی درهم تنیدگی بین باب و آن نقطه ایجاد می شود. شکل (۳) این نکته را نشان می دهد:

3:

■ **توضیح دوم:** به همین ترتیب که در مورد کیوبیت ها عمل کردیم، با به اشتراک گذاشتن حالت های درهم تنیده تعمیم یافته و اعمال تصحیحات با عملگرهای پاوولی تعمیم یافته می توان حالت های دلخواه کیودیت را نیز فرابرد کوانتومی کرد.

۴ کدگذاری چگال

در فرابرد کوانتومی نشان دادیم که می توان به شرط آنکه بین فرستنده و گیرنده یک زوج درهم تنیده به اشتراک نهاده شده باشد، آن دو می توانند با مبادله فقط دو بیت کلاسیک یک حالت کوانتومی یعنی یک کیوبیت را مبادله کنند. یک سوال طبیعی این است که آیا می توان وارون این کار را نیز انجام داد، یعنی با مبادله یک کیوبیت اطلاعات مربوط به دو بیت کلاسیک را انتقال داد؟ پاسخ این سوال نیز مثبت است و به فرایندی که طی آن این کار انجام می شود، کدگذاری چگال می گویند. برای این کار آلیس و باب یک زوج EPR به صورت

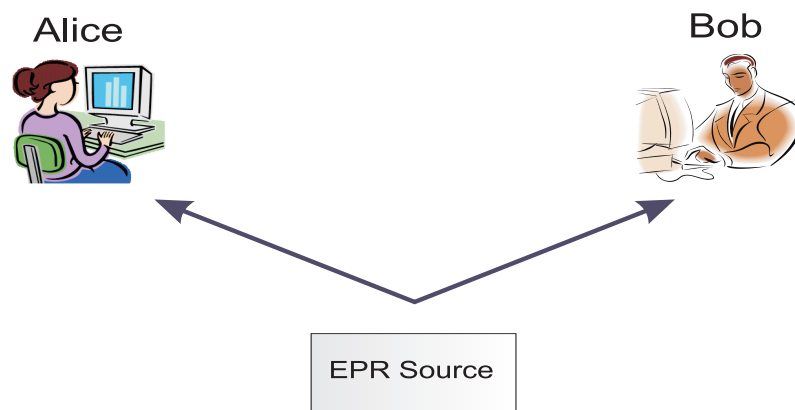
$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

به اشتراک می گذارند. سپس آلیس بسته به این که کدام یک از زوج بیت ها را بخواهد برای باب ارسال کند یکی از گیت های Z, Y, X, I را روی کیوبیت خودش اعمال می کند. تحت این اعمال حالت به اشتراک گذارده شده به ترتیب نشان داده شده در روابط زیر تغییر می کند:

$$\begin{aligned} 00 &\longrightarrow I \longrightarrow |\phi^+\rangle, \\ 01 &\longrightarrow X \longrightarrow |\psi^+\rangle, \\ 10 &\longrightarrow Z \longrightarrow |\phi^-\rangle, \\ 11 &\longrightarrow Y \longrightarrow |\psi^-\rangle. \end{aligned} \quad (۱۷)$$

سپس وی کیوبیت خودش را برای باب ارسال می کند. حالا هر دو کیوبیت در دست باب هستند و وی می تواند با اندازه گیری در پایه بل نوع حالت ارسال شده را بفهمد و با توجه به قرارداد فی مابین خودش و آلیس بفهمد که منظور آلیس ارسال کدام یک از جفت زوج های $00, 01, 10, 11$ بوده است. به شکل فعلی به نظر می رسد که این فرایند، آنچنان مهم و جالب نیست، زیرا بالاخره یک کیوبیت قبلاً در دست باب بوده است (از طریق به اشتراک گذاردن یک حالت بل). اما باید توجه داشت که حالت های بل را افراد یا شرکت های ثالث و نه آلیس می توانسته اند بین افراد متقاضی به اشتراک گذارده باشند (شکل ۳).

هم چنین این حالت های درهم تنیده می توانسته مدتها پیش بین آلیس و باب به اشتراک گذارده شود و نه در موقعی که آنها واقعا می خواهند باهم مبادله اطلاعات انجام دهند. بالاخره باید دقت کرد که اگر آلیس و باب فقط یک زوج کیوبیت به اشتراک گذاشته باشند، آنگاه آلیس می تواند با ارسال تنها یک کیوبیت یک حالت از چهار حالت زوج ها را به وی اطلاع دهد، اما اگر حالت به اشتراک گذارده شده یک حالت بل در



شکل ۳: در تمام فرایندهای مبادله اطلاعات کوانتومی می توان فرض کرد که منبع ثالثی زوج های درهم تنیده را در اختیار متقاضیان می گذارد.

بعد d باشد، آنگاه آلیس با ارسال یک کیودیت، یک حالت از d^2 را به باب اطلاع خواهد داد که مقدار فشرده سازی را بالا می برد.

نکته مهم این است که آلیس می تواند کیوبیت اول را در یک زمان و کیوبیت دوم را مدت زمانی بعد برای باب بفرستد (بعد از اینکه عمل مربوطه را روی آن انجام داد). به این ترتیب نه کیوبیت اول و نه کیوبیت دوم هیچکدام حاوی اطلاع مشخصی نیستند، چرا که ماتریس چگالی هر دو کیوبیت یک حالت کاملاً آمیخته است و اطلاع (دو بیت) تنها در همبستگی کوانتومی بین این دو کیوبیت است. به این ترتیب می توان کدگذاری چگال را به صورت زیر خلاصه کرد:

$$1 \text{ ebit} + 1 \text{ qubit} \longrightarrow 2 \text{ bits.} \quad (۱۸)$$

۵ رمزنگاری کلاسیک

رمزنگاری^{۱۳} شاخه‌ای از مهندسی مخابرات است که هدف آن تدوین پروتکل‌هایی برای مبادله ایمن اطلاعات از یک نقطه به یک نقطه دیگر است. این رشته تاریخ طولانی دارد و خواننده علاقمند می بایست به کتب عمومی یا تخصصی مربوطه نگاه کند تا با تحولات جالب این رشته که از متدهای بسیار ابتدایی آغاز شده و به متدهای متکی به ریاضیات پیشرفته منتهی می شود، نیز آشنایی پیدا کند. می توان به طور کلی و انتزاعی رمز نگاری را به شیوه زیر تعریف کرد. فرض کنید که رشته‌ای به طول n از بیت ها حاوی پیام مشخصی است. این رشته را با M نشان می دهیم. در

^{۱۳}Cryptography



شکل ۴: نمونه کلی رمز نگاری با کلید خصوصی

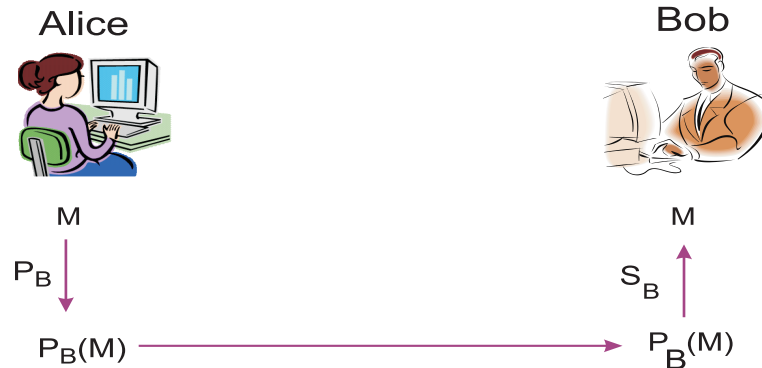
یک شیوه ساده که به رمزنگاری خصوصی معروف است، آلیس و باب یک کلید مثل K بین خود به اشتراک می گذارند. وابسته به این کلید آلیس و باب دو نگاشت مشخص E_K و D_K اختیار می کنند که دارای خاصیت زیر هستند:

$$D_K \circ E_K = I, \quad (19)$$

بنابراین آلیس بجای پیام M یا $PlainText$ پیام رمز شده یا $CipherText$ یعنی $E_K(M)$ را به باب ارسال می کند. در مقصد، باب با اعمال نگاشت D_K می تواند به پیام اصلی یعنی M دسترسی پیدا کند، زیرا $D_K(E_K(M)) = M$ (شکل ۴). سیستم رمز نگاری می بایست چنان باشد که اگر در بین راه شخص سومی که معمولاً به آن ایو^{۱۴} گفته می شود، نتواند با داشتن یک پیام $E_K(M)$ به خود M دسترسی پیدا کند. حتی ایو نمی بایست با در دست داشتن تعداد محدودی پیام مثل $\{M_1, M_2, \dots, M_n\}$ و رمز شده آنها مثل $\{E_K(M_1), E_K(M_2), \dots, E_K(M_n)\}$ بتواند به کلید K دسترسی پیدا کند. البته در عمل ایو می تواند با در دست داشتن تعداد قابل توجهی از پیام های رمز شده و توجه به همبستگی هایی که بین آنها وجود دارد و با ترکیبی از آنالیز دقیق و حدس و گمان به نوع کلید دست پیدا کند و نهایتاً رمز را باز کند. به همین دلیل آلیس و باب می بایست کلید مورد استفاده خود را دائماً تغییر دهند. در رمز نگاری فرض بر آن است که توابع E_K و D_K یعنی نوع رمز استفاده شده، برای همگان معلوم است. آنچه که نامعلوم است نوع کلید استفاده شده یعنی K است که تنها می بایست آلیس و باب از آن مطلع باشند و نه هیچ کس دیگر. به عنوان مثال در ساده ترین نوع رمز نگاری K یک رشته تصادفی مشترک بین آلیس و باب است و توابع E_K و D_K نیز عبارتند از جمع دو رشته به سنج دو (البته جمعیت به بیت):

$$E_K(M) = M \oplus K, \quad D_K = E_K. \quad (20)$$

Eve^{۱۴}



شکل ۵: نمونه کلی رمز نگاری با کلید عمومی. اشکال این روش این است که گیرنده نمی تواند از هویت فرستنده مطمئن شود.

به عبارت دیگر اگر $K = (k_1, k_2, k_3, \dots, k_n)$ آنگاه

$$E_K(m_1, m_2, m_3, \dots, m_n) = (m_1 \oplus k_1, m_2 \oplus k_2, m_3 \oplus k_3, \dots, m_n \oplus k_n). \quad (21)$$

از آنجا که $(a \oplus b) \oplus b = a$ واضح است که $D_K \circ E_K = I$. البته این نوع رمز خیلی ساده است زیرا با داشتن تنها یک پیام M و رمز شده ی آن یعنی $E_K(M)$ ، بلافاصله کلید از رابطه ی $K = E_K(M) \oplus M$ یافته می شود. در عمل کلیدهای بسیار پیچیده تری امروزه برای مبادله ایمن اطلاعات مورد استفاده قرار می گیرد. باید تاکید کنیم که کلید K می بایست مرتباً عوض شده و کلیدهای جدیدی بین آلیس و باب به اشتراک گذاشته شود، زیرا هر کلید ثابتی نهایتاً انقدر هم بستگی در پیام های ارسال شده ایجاد می کند که از رشته ی $\{E_K(M_1), E_K(M_2), \dots, E_K(M_n)\}$ به شرطی که n به اندازه کافی بزرگ باشد، بتوان کلید K را استخراج کرد.

مشکلی که در این نوع رمز نگاری وجود دارد، آن است که کلید K می بایست بین آلیس و باب به اشتراک گذاشته شود و واضح است که برای این کار آلیس و باب نمی توانند یکدیگر را مرتباً ملاقات کنند. به نظر می رسد که در اینجا با یک دور بی پایان یعنی مسئله مبادله کلید^{۱۵} به طریق ایمن روبرو هستیم که هرگز حل نخواهد شد. اما در سال ۱۹۷۴ راه حل جالبی برای این موضوع موسوم به کلیدهای عمومی^{۱۶} یافته شد. در این نوع رمز نگاری هر شخص مثلاً آلیس از دو نوع کلید استفاده می کند. این دو کلید را به ترتیب P_A و S_A می نامیم. هم چنین باب هم دو نوع کلید در اختیار دارد که آن ها را P_B و S_B می نامیم. نگاشت های رمزنگارنده یعنی E و رمزگشاینده یعنی D دارای این خاصیت هستند که

$$D_{S_a} E_{P_a} = I_a, \quad \forall a. \quad (22)$$

^{۱۵}Key Distribution Problem

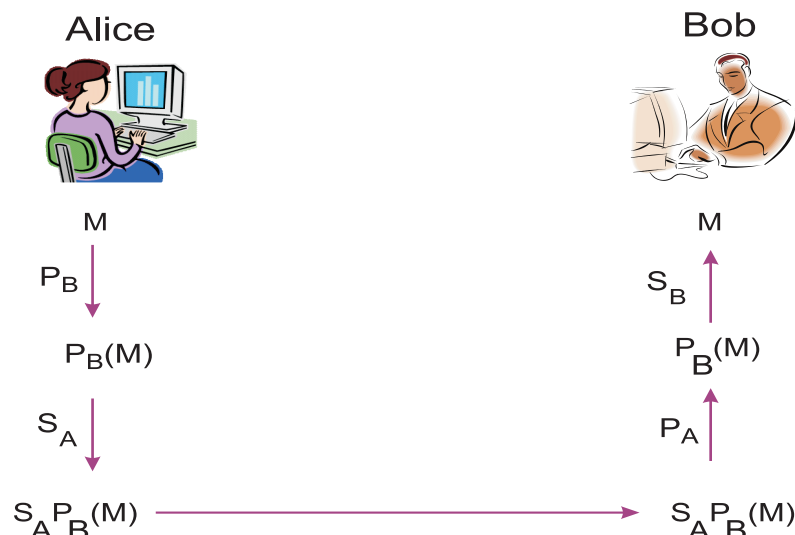
^{۱۶}Public Key System

کلید P یک کلید عمومی و کلید S یک کلید خصوصی است. کلید عمومی یک شخص برای همه افراد دیگر نیز معلوم است و آن ها می توانند با مراجعه به یک پایگاه داده معین کلید عمومی هر شخص دلخواهی را بدست آورند. ولی کلید خصوصی هر شخص تنها برای خود او معلوم است. هم چنین نکته اساسی در این نوع رمز نگاری آن است که بدست آوردن کلید خصوصی یک شخص از روی کلید عمومی او می بایست یک مسئله بسیار سخت باشد. در این نوع رمزنگاری احتیاج به هیچ نوع مبادله کلیدی نیست. روشی که آلیس برای مبادله پیامی مثل M به باب در نظر می گیرد به شرح زیر است. نخست کلید عمومی باب را پیدا می کند و نگاشت E_{P_B} را روی پیام M اعمال می کند. در مقصد باب با اعمال نگاشت D_{S_B} روی پیام دریافت شده پیام M را دریافت می کند، شکل ۵. دقت کنید که نگاشت های E و D وارون یکدیگر هستند به این معنا که برقرار است

$$D_{S_B} E_{P_B} = I, \quad (23)$$

در ادامه این بحث و هم چنین در شکل های ۵ و شکل ۶ از یک نمادگذاری ساده تر استفاده می کنیم به این معنا که مثلاً بجای E_{P_B} و یا D_{S_B} بسادگی از P_B و از S_B استفاده می کنیم و در نتیجه رابطه بالا را به شکل $S_B P_B = I_B$ می نویسیم. حال باب با یک مسئله مهم مواجه است و آن اینکه می بایست مطمئن شود که پیام M واقعاً توسط آلیس برای او فرستاده شده است، زیرا هر کس دیگری نیز می توانسته است با نگاه کردن به کلید عمومی باب پیام M را برای او فرستاده باشد. راه غلبه بر این دشواری این است که آلیس پیام خود را دو بار رمز کند. چگونگی این رمزنگاری و رمز گشایی در شکل ۶ نشان داده شده است و نیازی به توضیح ندارد. آنچه که امروزه به عنوان کلیدهای عمومی و خصوصی مورد استفاده واقع می شود، متکی بر این است که یک عدد بسیار بزرگ را نمی توان به عامل های اول آن تجزیه کرد. به عبارت دیگر مسئله تجزیه یک عدد به دو عامل اول آن مسئله بسیار سختی است به این معنا که زمان لازم برای حل این مسئله با افزایش تعداد رقم های آن عدد به صورت نمایی افزایش می یابد. با کمی ساده سازی می توانیم بگوییم که هر شخص دو عدد بسیار بزرگ p و q را اختیار کرده و آنها را درهم ضرب می کند تا عددی مثل $N = pq$ را بدست آورد. وی سپس عدد N را اعلان عمومی کرده و اعداد p و q را نزد خود نگاه می دارد. کلید عمومی وی از روی عدد N و کلید خصوصی وی از روی اعداد p و q ساخته می شود. واضح است که کلید خصوصی را نمی توان از روی کلید عمومی بدست آورد. امروزه روشی که مبتنی بر این نوع مبادله کلید است موسوم به روش SAR^{۱۷} است و کاربرد بسیار وسیع یافته است. این روش را در بخش بعدی توضیح می دهیم.

Rivest, Shamir, Adelman^{۱۷}



شکل ۶: رمز نگاری با کلید عمومی. در این روش آلیس دو بار پیام را رمز می کند ، یک بار با کلید عمومی باب و بار دیگر با کلید خصوصی خودش.

۶ روش RSA

روش RSA که از نام های مخترعان این نوع رمزنگاری گرفته شده است ^{۱۸} ، یک روش رمزنگاری با کلید عمومی است که اینک به توضیح آن می پردازیم. برای این کار نخست باید بگوییم که آلیس و باب چگونه کلید های خصوصی و عمومی خود را می سازند. سپس باید روشن کنیم که چگونه با استفاده از این کلیدها به مبادله ایمن پیام های خود می پردازند.

شخص آلیس را در نظر بگیرید. آلیس دو عدد بسیار بزرگ اول مثل p و q را انتخاب می کند. حاصل ضرب این دو عدد را با N نشان می دهیم. بنابراین داریم

$$N = pq. \quad (۲۴)$$

حال آلیس عددی مثل $e < N$ را چنان انتخاب می کند که نسبت به $(p-1)(q-1)$ اول باشد. پیدا کردن چنین عددی همواره آسان است. سپس وارون این عدد را به سنج $(p-1)(q-1)$ حساب کرده و آن را با d نشان می دهد. بنابراین

$$de = 1 \mod (p-1)(q-1). \quad (۲۵)$$

کلید عمومی هرکسی از جمله آلیس عبارت است از:

$$P = (N, e)$$

^{۱۸}Rivest, Shamir, Adelman

و کلید خصوصی او عبارت است از:

$$S = (N, d)$$

واضح است که از هیچکدام از این کلید ها نمی توان دیگری را به دست آورد، چرا که این امر نیازمند دانستن تجزیه N به pq است که کار فوق العاده سختی است. حال نحوه رمز کردن یک پیام مثل M را که قبلا به صورت یک عدد بزرگ در آمده است (مثلا از طریق یک کدگذاری عمومی و رایج) توضیح می دهیم. پیام رمز شده توسط آلیس را با M' نشان می دهیم. داریم:

$$M \longrightarrow M' = M^{e_B} \text{ Mod } N. \quad (26)$$

این پیام به شکل زیر باز می شود که در آن از یک قضیه در نظریه اعداد به نام قضیه اویلر استفاده شده است. بر مبنای این قضیه داریم:

$$M^{1+(p-1)(q-1)} \text{ Mod } pq = M. \quad (27)$$

یک نکته: قضیه اویلر بیان می کند که اگر دو عدد M و N نسبت به هم اول باشند، آنگاه

$$M^{\phi(N)+1} \text{ mod}(N) = M. \quad (28)$$

در مسئله حاضر M و N نسبت به هم اول نیستند. ولی در واقع از این موضوع استفاده می کنیم که با توجه به این که p و q اول هستند، می توانیم بنویسیم

$$M^{p-1} \text{ mod}(p) = 1,$$

و

$$M^{q-1} \text{ mod}(q) = 1.$$

خواننده از ترکیب این دو رابطه می تواند نشان دهد که رابطه (28) برای وقتی که $N = pq$ برقرار است بدون اینکه نیازی به اول بودن N نسبت به M وجود داشته باشد.

به این ترتیب وقتی که باب پیام رمز شده را دریافت می کند می تواند این پیام را به شکل زیر بازایی کند:

$$M' \longrightarrow M'^{d_B} = M^{e_B d_B} \text{ Mod } N = M. \quad (29)$$

■ **تمرین:** صحت قضیه اوایلر را برای جفت اعداد زیر بیازمایید:

$$(M, n) \in \{(3, 6), (4, 7), (6, 9), (7, 12), (8, 15), (9, 20), (6, 30)\}. \quad (۳۰)$$

■ **تمرین:** در بخش قبل دیدیم که برای آنکه هویت ارسال کننده نیز تایید شود پیام دو بار رمزیده شود. مراحل این کار را در روش *RSA* توضیح دهید.

■ **تمرین:** قرار دهید $p = 7$ و $q = 11$ و برای خود یک کلید عمومی و یک کلید خصوصی بسازید.

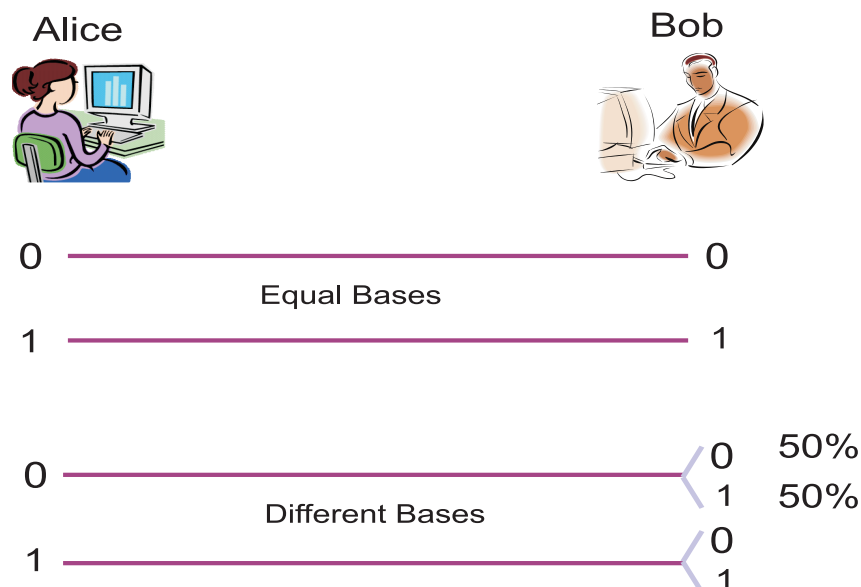
■ **تمرین:** قرار دهید $p = 13$ و $q = 17$ و برای خود یک کلید عمومی و یک کلید خصوصی بسازید.

■ **تمرین:** برای p و q دو عدد ۴ رقمی اختیار کنید به نحوی که این دو عدد اول باشند. سپس یک کلید عمومی و خصوصی برای خود بسازید.

۷ روش *BB84* برای مبادله کوانتومی کلید

آیا با استفاده از خصوصیات غیرموضعی مکانیک کوانتومی می توان راه حل متفاوتی برای مسئله توزیع کلید ابداع کرد، راه حلی که مبتنی بر خصلت های ذاتی و طبیعی اشیاء باشد و نه مبتنی بر مسائل حل ناپذیر ریاضیات. امروزه می دانیم که پاسخ این سوال مثبت است. نخستین بار چارلز بنت و ژیل براسار^{۱۹} یک فرایند کوانتومی برای توزیع کلید ارایه کردند. از آن به بعد این فرایند به طرق گوناگون تعمیم یافته است. ما در این جا همان فرایند اولیه بنت و براسار را که به فرایند *BB84* موسوم است بررسی می کنیم. در این فرایند آلیس و باب حالت هایی را به صورت $|z, \pm\rangle$ یا $|x, \pm\rangle$ در نظر می گیرند. این حالت ها ویژه بردارهای عملگرهای X و Z هستند. ویژه حالت های با ویژه مقدار مثبت به معنای بیت

^{۱۹}Charles Bennett and Gilles Brassard



شکل ۷: رمز نگاری کوانتومی. هرگاه پایه های آلیس و باب مثل هم باشد، بین بیت های آنها همبستگی صد در صد وجود دارد. بنابراین آنها می توانند در این حالت ها رشته بیت ها را به عنوان کلید انتخاب کنند.

0 و ویژه حالت های با ویژه مقدار منفی به معنای بیت 1 هستند. حال آلیس رشته ای کاملاً تصادفی از این حالت ها را به باب می فرستد و باب نیز به طور تصادفی حالت های دریافتی را در پایه های X و Z اندازه گیری می کند. بعد از مبادله تمام حالت ها، آن دو پایه هایی را که برای ارسال و اندازه گیری حالت ها به کار برده اند به طور علنی اعلام می کنند. واضح است که خود حالت های ارسالی و یا نتیجه اندازه گیری ها اعلام عمومی نمی شود. مسلم است که برای آن بیت هایی که پایه های آلیس و باب با هم برابر باشند، نتیجه اندازه گیری باب درست همانی است که آلیس فرستاده است و برای آن بیت هایی که این پایه ها برهم منطبق نباشند، نتیجه اندازه گیری باب با احتمال $\frac{1}{2}$ با آنچه که آلیس فرستاده است منطبق نخواهد بود. بنابراین بعد از اعلان عمومی پایه ها، آلیس و باب تنها بیت هایی را که پایه های آن ها برای هردو یکی است نگاه داشته (زیرا در این حالت ها نتایج آلیس و باب همبستگی کامل دارند) و بقیه بیت ها را رها می کنند (زیرا در این حالت ها نتایج آلیس و باب هیچ نوع همبستگی با هم ندارند) و به این ترتیب بدون اینکه یک دیگر را ملاقات کنند، موفق به توافق بر روی یک رشته بیت های صفر و یک به عنوان کلید می شوند، شکل ۷. باید به این نکته توجه کنیم که کلید تنها بعد از اعلان عمومی پایه ها توسط آلیس و باب مشخص می شود و از قبل این کلید نه برای آلیس و نه برای باب شناخته شده نیست. هم چنین خاصیت اصلی مبادله کوانتومی کلید آن است که آلیس و باب می توانند از وجود ایو در صورتی که مشغول استراق سمع باشد پی ببرند. دقت کنید که ایو نمی تواند با هیچ فرایند کوانتومی کیوبیت های ارسال شده توسط آلیس را تکثیر کرده و یکی را برای خود نگاه داشته و دیگری را برای باب ارسال کند و بعد از اعلان پایه ها به کلید دسترسی پیدا کند، زیرا قبلاً دیده ایم که هیچ فرایند کوانتومی نمی تواند حالت های نامتعامل را تکثیر کند. بنابراین تنها کاری که می تواند انجام دهد آن است

که او نیز کیوبیت های ارسال شده توسط آلیس را به طور تصادفی در پایه های X و Z اندازه گیری کرده و پس از مشخص شدن حالت، نمونه ای از آن حالت را برای باب ارسال کند. اما به دلیل اینکه ایو از قبل نمی داند که پایه های آلیس و باب در کدام موارد با هم توافق دارد، وی می بایست پایه ای به صورت تصادفی برای خود انتخاب کند. در نتیجه در نیمی از حالت هایی که آلیس و باب پایه شان باهم یکی است ایو نیز پایه ای مثل آنها انتخاب کرده است و بعد از اعلان عمومی وی می تواند به نیمی از رشته کلید دست پیدا کند. اما وی به این ترتیب حضور خود را نیز بر باب و آلیس آشکار می سازد، زیرا در نیمی از مواردی که آلیس و باب پایه شان یکی است پایه ایو با آنها متفاوت بوده و در نتیجه حالتی را که اندازه گیری کرده و برای باب دوباره ارسال کرده توسط اندازه گیری او مختل شده است. به عنوان مثال فرض کنید که آلیس حالت $|x, +\rangle$ را برای باب ارسال کند و باب نیز پایه ای X را برای اندازه گیری اختیار کند. در این صورت وی نیز حالت ذره را $|x, +\rangle$ تشخیص داده و در نتیجه آلیس و باب روی بیت 0 باهم توافق می کنند. اما اگر ایو دخالت کند به احتمال ۵۰ درصد پایه ای که برای اندازه گیری اش انتخاب می کند پایه ای Z خواهد بود. در این پایه وی با احتمال ۱/۲ حالت $|z, +\rangle$ و با احتمال ۱/۲ حالت $|z, -\rangle$ را بدست خواهد آورد. هرکدام از این حالت ها را که برای باب بفروشد تنها با احتمال ۱/۲ منجر به نتیجه $|x, +\rangle$ برای باب خواهد شد. در نتیجه باب با احتمال $\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}$ نتیجه $|x, -\rangle$ بدست خواهد آورد که با حالتی که آلیس برای او فرستاده است نمی خواند. این اتفاق در نیمی از مواردی که پایه های آلیس و باب یکی هستند رخ می دهد یعنی در کل این موارد، با احتمال $\frac{1}{4}$ بیت های آلیس و باب بجای آنکه با هم توافق داشته باشند، با هم اختلاف دارند. آلیس و باب برای پی بردن به حضور ایو کافی است که از رشته طولانی بیت هایی که مربوط به پایه های یکسان هستند و هیچ کس بجز خود آلیس و باب از آنها خبر ندارد، شمار اندکی را به طور علنی با هم مقایسه کنند. (می توانند این شمار اندک را به طور تصادفی از رشته طولانی بیت ها انتخاب کنند.) اگر ایو دخالتی نکرده باشد، این شمار از بیت ها کاملاً باهم یکسان هستند. در این حالت، این شمار از بیت ها را از رمز خود کسر کرده و بقیه بیت ها را برای کلید ایمن خود به کار می برند. اما اگر ایو دخالت کرده باشد، حدود یک چهارم از این بیت ها مورد توافق آنها نخواهد بود و به این ترتیب آنها از وجود ایو خبردار می شوند و می بایست از یک کانال دیگر برای ارسال کیوبیت ها استفاده کنند.

باید اضافه کنیم که این فرایند را می شد به این ترتیب نیز انجام داد که آلیس و باب مجموعه ای از زوج های درهم تنیده در حالت

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|x+, x-\rangle - |x-, x+\rangle) \quad (31)$$

بین خود به اشتراک بگذارند. (به احتمال زیاد این نوع اشتراک کلید آن چیزی است که در آینده عملی خواهد شد زیرا از نظر تجربی ممکن است همه آزمایشگاه ها امکان مبادله حالت های کوانتومی بین یک دیگر را نداشته باشند ولی می توانند از یک ایستگاه مرکزی مثل یک ماهواره ذره کوانتومی دریافت کنند.) چنین زوج هایی در حالت اسپین کل صفر قرار دارند و در هرپایه ای به همین شکل خواهند بود، یعنی جهت اسپین ذرات با هم همواره مخالف خواهد بود. به عبارت دیگر این حالت ها در پایه ای Z نیز به شکل $|\psi\rangle = \frac{1}{\sqrt{2}}(|z+, z-\rangle - |z-, z+\rangle)$ نوشته

می شوند. بنابراین هرگاه آلیس و باب هر دو یک پایه برای اندازه گیری خود انتخاب کنند، نتایج آنها کاملاً وارون هم خواهد بود (به عبارت بهتر همبستگی کامل ولی معکوس دارند)^{۲۰} و هرگاه پایه های آنها مخالف هم باشند، هم بستگی بین اندازه گیری های آنها وجود ندارد. بقیه این فرایند درست مثل قبل است و تفاوتی با آن ندارد.

■ تمرین: روش توزیع کلید با استفاده از حالت های درهم تنیده را نخستین بار آرتور اکرت^{۲۱} ابداع کرد. البته او از سه نوع اندازه گیری به جای دو نوع اندازه گیری برای هر شرکت کننده استفاده کرد. در روش او آلیس و باب همه اندازه گیری های خود را در صفحه $x - y$ انجام می دهند. راستاهای اندازه گیری آلیس با محور x به ترتیب زاویه های $0, 45, 90$ و راستاهای اندازه گیری باب با این محور به ترتیب زاویه های $45, 90, 135$ است. همه زاویه ها بر حسب درجه هستند. حساب کنید که در چند درصد موارد آلیس و باب نتایج وابسته به هم بدست می آورند که از آن می توانند برای اشتراک کلید استفاده کنند؟

۸ روش شش حالت

این روش نخستین بار توسط داگمار بروس^{۲۲} ابداع شد و نسبت به روش BB84 یک مزیت و یک نقصان دارد که در زیر آن را توضیح می دهیم. اساس این روش مبتنی بر ایده پایه های متوازن است. عملگرهای پاولی X, Y, Z را در نظر بگیرید. بردارهای ویژه این عملگرها سه پایه مختلف برای فضای یک کیوبیت به شکل زیر می سازند:

$$\begin{aligned} Z : \quad & \{|0\rangle, |1\rangle\} = \{|z_+\rangle, |z_-\rangle\} \\ X : \quad & \{|+\rangle, |-\rangle\} = \{|x_+\rangle, |x_-\rangle\} \\ Y : \quad & \{|y_+\rangle, |y_-\rangle\}, \end{aligned} \quad (32)$$

که در آن

$$|y_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad |y_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).$$

^{۲۰}Anit-correlation

^{۲۱}Arthur Ekert

^{۲۲}Bruss Dagmar

براحتی معلوم می شود که هر سه این پایه ها نسبت به هم متوازن^{۲۳} هستند، به این معنا که

$$|\langle a_i | b_j \rangle| = \frac{1}{\sqrt{2}} \quad (۳۳)$$

که در آن $|a_i\rangle$ از یک پایه و $|b_j\rangle$ از یک پایه دیگر انتخاب شده اند. این متوازن بودن به این معناست که هرگاه برداری مثل $|a_i\rangle$ را در پایه ناهماهنگی مثل B اندازه بگیریم، آن گاه نتیجه اندازه گیری کاملاً تصادفی است و هیچ ترجیحی نسبت به یک طرف ندارد. با این مقدمه می توانیم بفهمیم که اساس پروتکل شش حالت چیست. تمامی مراحل یعنی ارسال حالت ها توسط آلیس، اندازه گیری تصادفی توسط باب، اعلام پایه های اندازه گیری و چک کردن یک زیررشته از کلید به صورت علنی و سپس دور ریختن آن درست مثل پروتکل BB84 است، با این تفاوت که به جای دو پایه X و Z از سه پایه X , Y , Z استفاده می کنیم. در این روش آلیس و باب تنها در یک سوم موارد از پایه یکسان استفاده می کنند. بنابراین می بایست دو سوم بیت ها را دور بریزند. این یک نقصان نسبت به روش BB84 است. اما در همین موارد، یعنی مواردی که پایه آنها یکسان است، اگر ایو مداخله کند، با احتمال $\frac{2}{3}$ پایه او با پایه های آلیس و باب تفاوت دارد و درست به دلیل همین متوازن بودن، احتمال این که خطایی در بیت های ارسالی و دریافتی توسط آلیس و باب ایجاد کند برابر است با

$$P_{error} = \frac{2}{3} \times \frac{1}{2} = \frac{1}{3},$$

که نسبت به خطای ایجاد شده در روش BB84 یعنی $\frac{1}{4}$ بیشتر است. بنابراین در این روش احتمال کشف مداخله ایو بیشتر است و این یک مزیت برای روش شش حالت است.

۱۰.۸ اشتراک کوانتومی رمز

علاوه بر توزیع کلید می توان مکانیک کوانتومی را برای حل بدیع مسائل دیگری از رمز نگاری بکاربرد. منظور از مسئله اشتراک رمز^{۲۴} آن است که یک فرستنده مثل آلیس می خواهد پیام مهمی مثلاً رمز یک حساب بانکی را به دو شخص متفاوت به نام های باب و چارلی ارسال کند ولی بنابه دلایلی می خواهد که هیچ کدام از آن دو مستقلاً نتوانند به این رمز دسترسی پیدا کنند، بلکه تنها با همکاری یکدیگر بتوانند محتوی این پیام را بفهمند. در مسئله اشتراک رمز فرض می شود که هیچ کدام از دو نفر باب و چارلی قابل اعتماد نیستند و نمی بایست به تنهایی اطلاعات مهمی مثل رمز حساب بانکی را در اختیار داشته باشند. یک راه حل کلاسیک و بسیار ساده برای این کار آن است که آلیس پیام M با یک رشته تصادفی

^{۲۳}Mutually Unbiased
^{۲۴}Secret Sharing

مثل K جمع کند و پیام $N = M \oplus K$ را درست کند. از آنجا که رشته‌ی K کاملاً تصادفی است، رشته‌ی N نیز کاملاً تصادفی خواهد بود. بنابراین هیچ کدام از رشته‌های K و N دارای معنای مشخصی نیستند. حال آلیس رشته‌های K و N را به طور جداگانه به باب و چارلی می‌فرستد. این پیام‌ها برای آنها هیچ استفاده‌ای در بر ندارد. تنها وقتی می‌توانند از رشته‌های دریافت شده‌ی خود استفاده کنند که آنها را با هم جمع کنند. در این صورت با توجه به رابطه‌ی

$$N \oplus K = (M \oplus K) \oplus K = M, \quad (۳۴)$$

آنها می‌توانند محتوی اصلی پیام را دریافت کنند. البته آلیس می‌بایست از یک فرایند رمزنگاری جداگانه استفاده کند تا بتواند رشته‌های K و N را به طور ایمن برای باب و چارلی ارسال کند. وی می‌بایست این کار را با دوکلید جداگانه که بین خودش و باب و هم چنین بین خودش و چارلی به اشتراک گذاشته است انجام دهد. دقت کنید که کافی نیست که آلیس از دو کانال جداگانه برای ارسال رشته‌ها به باب و چارلی استفاده کند، زیرا فرض این است که آنها به کانال‌های یک دیگر دسترسی دارند یا به عبارت دیگر تلاش خود را برای استراق سمع و آگاهی یافتن از رشته‌های یک دیگر به کار می‌برند. بنابراین آلیس می‌بایست با علم به این موضوع فرایند اشتراک رمز را انجام دهد. به عنوان آخرین نکته در باره صورت مسئله اشتراک رمز باید اضافه کنیم که این مسئله تعمیم‌های دیگری نیز دارد به این معنا که آلیس پیام می‌خواهد پیام M را به n نفر ارسال کند، و هر زیرمجموعه‌ی k نفری از این n نفر می‌بایست با مشارکت یکدیگر بتوانند، به رمز ارسال شده توسط آلیس دست یابند و هیچ زیرمجموعه‌ای با تعداد عضو کمتر از k نتوانند این کار را انجام دهند. مثال‌های زیر راه‌های ساده‌ای را برای این کار نشان می‌دهند.

مثال ۱: در این مثال آلیس می‌خواهد پیام M را به یک مجموعه‌ی سه نفری موسوم به B_1, B_2 و B_3 بفرستد، به طوری که هر زیرمجموعه‌ی دو نفری از آنها بتواند پیام M را باز کنند، ولی هیچ کس به تنهایی نتواند پیام M را بفهمد. برای این کار وی به هر کدام از این دو نفر دو رشته‌ی تصادفی می‌فرستد که از ترکیب پیام اصلی با پیام‌های تصادفی دیگر درست شده‌اند.

$$\begin{aligned} \longrightarrow B_1 & \quad (K_1, K_2 \oplus M), \\ \longrightarrow B_2 & \quad (K_2, K_3 \oplus M), \\ \longrightarrow B_3 & \quad (K_3, K_1 \oplus M). \end{aligned} \quad (۳۵)$$

خواننده با نگاهی به رشته‌ها می‌تواند تایید کند که واقعاً هر دو نفر می‌توانند با هم کاری هم پیام M را بفهمند.

مثال ۲: در این مثال آلیس می‌خواهد پیام M را به یک مجموعه‌ی چهار نفری موسوم به B_1, B_2, B_3 و B_4 بفرستد، به طوری که هر

زیرمجموعه‌ی دو نفری از آنها بتوانند پیام M را باز کنند، ولی هیچ کس به تنهایی نتواند پیام M را بفهمد. برای این کار وی به هرکدام از این دو نفر دو رشته‌ی تصادفی می‌فرستد که از ترکیب پیام اصلی با پیام‌های تصادفی دیگر درست شده‌اند.

$$\begin{aligned} &\longrightarrow B_1 && (K_1, K_2 \oplus M), \\ &\longrightarrow B_2 && (K_2, K_3), \\ &\longrightarrow B_3 && (K_1 \oplus M, K_2 \oplus M) \\ &\longrightarrow B_4 && (K_2, K_3 \oplus M). \end{aligned} \quad (۳۶)$$

خواننده با نگاهی به رشته‌ها می‌تواند تایید کند که واقعاً هر دو نفر می‌توانند با هم کاری هم پیام M را بفهمند.

■ یک تمرین خوب و سرگرم‌کننده برای خواننده آن است که سعی کند طرحی را پیاده کند که طی آن هر زیرمجموعه‌ی سه نفری و نه کمتر از یک مجموعه چهارنفری بتواند یک پیام M را باز کنند.

در فرایند اشتراک رمز نیز با همان مسئله دیرین مواجه هستیم به این معنا که خود این کلیدها را چگونه باید به اشتراک بگذاریم بدون اینکه در یک دور بی‌پایان گرفتار شویم. سوال این است که آیا بازهم می‌توانیم از مکانیک کوانتومی استفاده کنیم و فرایند اشتراک رمز را به شکلی مشابه انجام دهیم. پاسخ این سوال مثبت است. فرایند مورد نظر اشتراک کوانتومی رمز^{۲۵} خوانده می‌شود. در ساده‌ترین حالت هدف از این فرایند این است که کلیدی بین سه نفر به اشتراک گذاشته شود که در رابطه

$$K_1 + K_2 + K_3 = 0 \quad (۳۷)$$

صدق کند بدون اینکه این افراد نیازی به ملاقات با یکدیگر داشته باشند. این کار مشابه با فرایند اشتراک رمز اکرت انجام می‌شود و متکی بر خاصیت حالت در هم تنیده‌ای است که در بخش بعد آن را معرفی می‌کنیم.

^{۲۵}Quantum Secret Sharing

۹ حالت های GHZ

حالت سه تایی زیر

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|z+, z+, z+\rangle + |z-, z-, z-\rangle). \quad (38)$$

به حالت GHZ معروف است و دلیل اش هم نام اول کسانی است که نخستین بار آن را مطالعه کرده اند ^{۲۶}. فرض کنید که ذره اول در دست آلیس، ذره دوم در دست باب و ذره سوم در دست چارلی است. برای این سه نفر به ترتیب حروف A، B و C را به کار می بریم. هرگاه این سه نفر اندازه گیری های خود را در پایه Z انجام دهند به طور تصادفی به یکی از نتایج زیر دست می یابند:

$$Z_a Z_b Z_c = (1, 1, 1) \quad \text{یا} \quad Z_a Z_b Z_c = (-1, -1, -1) \quad (39)$$

این امر نشان دهنده یک نوع همبستگی غیرموضعی بین سه کمیت فوق است. فرض کنید که دو نفر اول اندازه گیری خود را در راستای Y و نفر سوم در راستای X انجام دهند. برای تعیین نتایج اندازه گیری ها می بایست حالت $|GHZ\rangle$ در پایه مناسبی بسط دهیم. برای این کار از روابط آشنای زیر استفاده می کنیم:

$$\begin{aligned} |z+\rangle &= \frac{1}{\sqrt{2}}(|x+\rangle + |x-\rangle) & |z-\rangle &= \frac{1}{\sqrt{2}}(|x+\rangle - |x-\rangle) \\ |y+\rangle &= \frac{1}{\sqrt{2}}(|y+\rangle + |y-\rangle) & |y-\rangle &= \frac{-i}{\sqrt{2}}(|y+\rangle - |y-\rangle). \end{aligned} \quad (40)$$

با استفاده از روابط بالا می توان براحتی نشان داد که حالت $|GHZ\rangle$ بسط زیر را دارد:

$$|GHZ\rangle = \frac{1}{2}(|y+, y+, x-\rangle + |y+, y-, x+\rangle + |y-, y+, x+\rangle + |y-, y-, x-\rangle) \quad (41)$$

دقت کنید که حاصل اندازه گیری این سه نفر در مورد مولفه های اسپین دارای یک خصلت ویژه است و آن اینکه حاصل ضرب مولفه های سه ذره در راستای مربوطه برابر است با -1. به عبارت دیگر داریم

$$Y_a Y_b X_c = -1. \quad (42)$$

یعنی مقادیر این کمیت های واقعی فیزیکی آنچنان است که حاصل ضرب $Y_a Y_b X_c$ همواره برابر با -1 است. اگر این سه نفر اندازه گیری های خود را در راستاهای YXY یا XYY انجام دهند نتایج مشابه بدست می آید، به این معنا که:

$$X_a Y_b Y_c = -1$$

^{۲۶}Greenberger, Horne, Zeilinger

$$\begin{aligned} Y_a X_b Y_c &= -1 \\ Y_a Y_b X_c &= -1. \end{aligned} \quad (43)$$

هم چنین اگر این حالت را در پایه ی XXX بسط دهیم می بینیم که نتیجه اندازه گیری های این سه نفر بازهم کاملاً همبسته است: در واقع بسط حالت $|GHZ\rangle$ در این پایه چنین است:

$$|GHZ\rangle = \frac{1}{2} (|x+, x+, x+\rangle + |x+, x-, x-\rangle + |x-, x+, x-\rangle + |x-, x-, x+\rangle). \quad (44)$$

این بسط به این معناست که هرگاه روی سه ذره اندازه گیری های در پایه های فوق انجام دهیم همواره مقادیری که بدست می آوریم در رابطه $X_a X_b X_c = 1$ صدق می کند.

۱۰ اشتراک حالت های کوانتومی

آنچه که در بخش قبلی گفتیم اشتراک یک کلید کوانتومی بین چند نفر یا چند آزمایشگاه یا ایستگاه است. در این فرایند یک رشته تصادفی از صفرها و یک ها بین این افراد به اشتراک گذاشته می شود و خود این افراد نیز تا پایان فرایند از این رشته آگاه نیستند چرا که کاملاً تصادفی است. حال می خواهیم به فرایند جدیدی توجه کنیم که در آن یک حالت کوانتومی به چند نفر فرستاده می شود و این افراد می بایست با همکاری یک دیگر حالت کوانتومی را بازبازی کنند. چنین فرایندی را اشتراک سری حالت کوانتومی می نامند^{۲۷}. در ساده ترین حالت دو نفر قرار است یک حالت کوانتومی را که به آنها فرستاده شده با کمک یک دیگر بازبازی کنند. حالت را به صورت زیر در نظر می گیریم:

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (45)$$

کافی است که حالت های پایه را به صورت زیر تبدیل کنیم.

$$|0\rangle \longrightarrow |\bar{0}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

^{۲۷}Quantum State Sharing

$$|1\rangle \longrightarrow |\bar{1}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \quad (46)$$

در نتیجه حالت اولیه یک کیوبیتی به صورت زیر درمی آید و به گیرندگان که آنها را آلیس و باب می نامیم ارسال می شود.

$$|\bar{\psi}\rangle = a|\bar{0}\rangle + b|\bar{1}\rangle \quad (47)$$

حال به راحتی می توانید نشان دهید که آلیس و باب می توانند با انجام یک عمل $CNOT$ حالت را بازیابی کنند.

$$(CNOT)_{AB}|\bar{\psi}\rangle_{AB} = |+\rangle_A |\psi\rangle_B. \quad (48)$$

به این ترتیب همکاری آلیس لازم است تا باب بتواند حالت را بازیابی کند. بدیهی است که به خاطر قضیه عدم تکثیر هر دو نفر نمی توانند یک نسخه از حالت را بازیابی کنند. آنچه که تا کنون توضیح دادیم طرح اشتراک رمز $(2, 2)$ خوانده می شود که بیان می کند یک حالت کوانتومی بین دو نفر به اشتراک گذاشته می شود و دو نفر نیز با همکاری هم می توانند حالت را احیا کنند. در حالت کلی می توان پرسید که آیا می توان طرح های آستانه 28 از نوع (k, n) را نیز پیاده کرد یا خیر؟ از همان آغاز می دانیم که چنین طرح هایی تنها وقتی امکان پذیرند که $k > \frac{n}{2}$ باشد، چرا که در این صورت قضیه عدم تکثیر نقض خواهد شد. علاوه بر این باید گفت که اجرای این طرح ها حتی به صورت نظری کاری دشوار است. در ادامه یک طرح ساده که در واقع اولین طرح از این نوع نیز بوده است یعنی طرح $(2, 3)$ را معرفی می کنیم: 29 نشان داده است که اجرای چنین طرحی با یک کیوبیت امکان پذیر نیست. ولی می توان یک حالت کوانتومی سه بعدی یعنی یک کیوتریت را بین سه نفر به اشتراک گذاشت به قسمی که هر دو نفری از آنها قادر به بازیابی این حالت باشند. طرح چنین است:

$$\begin{aligned} |0\rangle \longrightarrow |\bar{0}\rangle &= \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle) \\ |1\rangle \longrightarrow |\bar{1}\rangle &= \frac{1}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle) \\ |2\rangle \longrightarrow |\bar{2}\rangle &= \frac{1}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle). \end{aligned} \quad (49)$$

به این ترتیب یک حالت دلخواه به صورت زیر رمز می شود:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \longrightarrow |\bar{\psi}\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle + \gamma|\bar{2}\rangle. \quad (50)$$

■ تمرین: نشان دهید که رابطه زیر برقرار است:

²⁸Threshold Scheme

²⁹R. Cleve, D. Gottesman, H. K. Lo, How to share a quantum secret, Phys.Rev.Lett. 83 (1999) 648-651

$$Tr_{BC}|\bar{i}\rangle\langle\bar{j}| = \frac{1}{3}\delta_{ij}I_A \quad (51)$$

اگر تمرین بالا را حل کرده باشید براحتهی خواهید دید که

$$\rho_A = \frac{1}{3}I_A, \quad \rho_B = \frac{1}{3}I_B, \quad \rho_C = \frac{1}{3}I_C. \quad (52)$$

در نتیجه هیچ کدام از سه نفر مطلقاً هیچ اطلاعی در باره حالت به اشتراک گذاشته شده ندارند. اما یک محاسبه ساده نشان می دهد که اگر عملگر C_{AB} را به معنای یک عملگر کنترلی $CNOT$ به کار ببریم که توسط A کنترل می شود و روی B به شکل

$$C_{AB}|i, j\rangle = |i, i+j\rangle \quad (53)$$

آنگاه داریم:

$$C_{BA}C_{AB}|\bar{i}\rangle = |i\rangle_A|\phi\rangle_{BC} \quad (54)$$

که در آن

$$|\phi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |12\rangle + |21\rangle). \quad (55)$$

به این ترتیب خواهیم داشت:

$$C_{BA}C_{AB}|\bar{\psi}\rangle \longrightarrow |\psi\rangle_A|\phi\rangle_{BC}. \quad (56)$$

یعنی اینکه آلیس و باب بدون اینکه چارلی هیچ مشارکتی داشته باشد می توانند حالت کوانتومی به اشتراک گذاشته شده را بازیابی کنند. طبیعی است که به دلیل تقارن حالت اولیه این کار برای هر دو نفری از آنها نیز امکان پذیر است.

۱۱ تمرین ها:

■ اگر در فرایرد کوانتومی حالت درهم تنیده ی بین آلیس و باب بجای $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ حالت $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ باشد تغییری که در مراحل فرایرد ایجاد می شود چیست؟

■ فرض کنید که در فرابرد کوانتومی کانال کلاسیکی که آلیس با استفاده از آن دو بیت کلاسیک را به باب اطلاع می دهد دارای نوبه ای به ترتیب زیر باشد:

$$\begin{aligned} 0 &\longrightarrow 1 & p \\ 1 &\longrightarrow 0 & p. \end{aligned} \quad (57)$$

آلیس و باب بدون اینکه از این خرابی اطلاع داشته باشند پروتکل فرابرد کوانتومی را به همان صورت همیشگی اجرا می کنند. تشابه حالت ارسالی و خروجی وقتی که روی تمام حالت های ورودی متوسط بگیریم چقدر خواهد بود.

■ فرض کنید که در فرابرد کوانتومی حالت درهم تنیده خالص نبوده بلکه به صورت زیر باشد:

$$\rho = (1-p)|\phi\rangle\langle\phi| + p|00\rangle\langle 00|, \quad (58)$$

که در آن $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. آلیس و باب بدون اینکه از این خرابی اطلاع داشته باشند پروتکل فرابرد کوانتومی را به همان صورت همیشگی اجرا می کنند. تشابه حالت ارسالی و خروجی وقتی که روی تمام حالت های ورودی متوسط بگیریم چقدر خواهد بود.

■ فرض کنید که در فرابرد کوانتومی حالت درهم تنیده دچار نوبه شده و به حالت زیر تبدیل شده باشد:

$$\rho = (1-p)|\phi^+\rangle\langle\phi^+| + p|\phi^-\rangle\langle\phi^-|, \quad (59)$$

که در آن $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$. آلیس و باب بدون اینکه از این خرابی اطلاع داشته باشند پروتکل فرابرد کوانتومی را به همان صورت همیشگی اجرا می کنند. تشابه حالت ارسالی و خروجی وقتی که روی تمام حالت های ورودی متوسط بگیریم چقدر خواهد بود.

■ فرابرد کوانتومی را برای حالت های 3 بعدی صورت بندی کنید. هر حالت سه بعدی به صورت زیر نوشته می شود:

$$|\phi\rangle = a|0\rangle + b|1\rangle + c|2\rangle, \quad (60)$$

و حالت درهم تنیده بین آلیس و باب به صورت زیر است:

$$|\psi\rangle := \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle). \quad (61)$$

راهنمایی: از عملگرهای X و Z و توان های آنها استفاده کنید. این عملگرها که تعمیمی از عملگرهای پاولی هستند به صورت زیر تعریف می شوند:

$$X := |1\rangle\langle 0| + |2\rangle\langle 1| + |0\rangle\langle 2|, \quad Z := |0\rangle\langle 0| + \omega|1\rangle\langle 1| + \omega^2|2\rangle\langle 2|, \quad (62)$$

که در آن $\omega = e^{\frac{2\pi i}{3}}$.

■ فرابرد کوانتومی را برای حالت های پیوسته صورت بندی کنید. یک حالت پیوسته به صورت زیر است:

$$|\phi\rangle = \int dx \phi(x)|x\rangle, \quad (63)$$

■ یک سیستم اشتراک رمز کلاسیک طراحی کنید که در آن تعداد گیرنده ها ۵ نفر است و هر مجموعه سه نفری یا بیشتر می توانند به پیام دسترسی پیدا کنند ولی هیچ مجموعه کوچکتر از ۳ نفر نمی تواند پیام را دریافت کند.

۱۲. قدردانی

این درسنامه را حسین محمدی دانشجوی دانشکده فیزیک در آبان ماه ۱۴۰۱ به دقت خوانده و اشکالات متعدد آن را به من یادآوری کردند. برای این لطف بزرگ از ایشان تشکر می کنم. هم چنین از امید ادیب نیا دانشجوی این درس در پاییز ۱۴۰۴ که چندین اشکال تایپی را یادآوری کردند سپاسگزارم.