چند فرایند ساده برای مبادله اطلاعات کوانتومی

وحیدکریمی پور_ دانشکده فیزیک ـ دانشگاه صنعتی شریف

۱۹ اردیبهشت ۱۳۹۸

protocol، ekert

۱ مقدمه

دراین درس هدف ما آن است که نشان دهیم مکانیک کوانتومی می تواند به طرق مختلف در انتقال اطلاعات آنهم به شیوه‌ای 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 آلگوریتم 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 فرایند ها ناقض نسبیت خاص نیستند. تقریباً تمام آزمایش هایی که تاکنون برای فرایندهای انتقال اطلاعات کوانتومی انجام شده‌اند از حالت های درهم تنیده قطبش فوتون ها استفاده می کنند. چنین حالتی معمولاً به شکل زیراست:

$$|\phi\rangle = \frac{1}{2}(|H,V\rangle + |V,H\rangle) = \frac{1}{2}(|H\rangle_{Alice} \otimes |V\rangle_{Bob} + |V\rangle_{Alice} \otimes |H\rangle_{Bob}), \qquad (۱)$$

[۱] Entangled States

که درآن H و V به ترتیب نشان دهنده قطبش افقی و عمودی فوتون ها در یک دستگاه مختصات معین است و شاخص های آلیس و باب نشان دهنده این است که فوتون ها در دو نقطه متفاوت تحت کنترل آلیس و باب هستند. ممکن است که این دو شخص کیلومترها از هم فاصله 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 فرایندهارا علاوه بر کیوبیت ها با کیودیت ها[۸] یعنی سیستم های dـحالته نیز می توان انجام داد ولی ما برای سادگی بررسی خود را محدود به سیستم های دوحالته می کنیم. در بعضی از تمرین ها تعمیم این فرایندها به بعد دلخواه خواسته شده است.

قبل از بررسی فرایند ها بهتراست به بعضی از خواص حالت های بل که در این فرایند ها نقش اساسی دارند، اشاره کنیم. این روابط هم چنین به خواننده نشان می دهند که چگونه می توان حالت های بل برای سیستم های d حالته را نوشت. حالت های بل برای کیوبیت ها عبارتند از:

$$|\phi^+\rangle := |\phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\psi^+\rangle := |\phi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

[۲] Parameteric Down Conversion
[۳] Teleportation
[۴] Dense Coding
[۵] Quantum Cryptography
[۶] Quantum Key Distribution
[۷] Quantum Secret Sharing
[۸] Qudit

$$|\phi^-\rangle := |\phi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\psi^-\rangle := |\phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \quad (۲)$$

دقت کنیم که برای حالت های بل دو نوع نماد بکار برده‌ایم. 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 فشرده‌ی زیر نیز نوشت:

$$|\phi_{mn}\rangle = Z^m \otimes X^n |\phi_{00}\rangle = \sum_{k=0}^{1} (-1)^{km} |k, k+n\rangle. \quad (۳)$$

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

$$\langle \phi_{mn} | \phi_{kl} \rangle = \delta_{mk} \delta_{nl}, \quad (۴)$$

و

$$\sum_{mn} |\phi_{mn}\rangle\langle\phi_{mn}| = I. \quad (۵)$$

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

$$(CNOT)(H \otimes I)|m, n\rangle = CNOT \sum_{k=0}^{1} (-1)^{km} |k, n\rangle = \sum_{k=0}^{1} (-1)^{km} |k, k+n\rangle = |\phi_{mn}\rangle. \quad (۶)$$

از آنجاهم CNO و هم H هردو مربع شان برابر با ماتریس واحد است، رابطه بالا نتیجه می دهد که

$$(CNOT)(H \otimes I)|\phi_{m,n}\rangle = |m, n\rangle. \quad (۷)$$

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.

---

۲ فرابردکوانتومی

درفرابرد کوانتومی هدف ما آن است که بامخابره اطلاعات کلاسیک که طبیعتاً با سرعت نورانجام می گیرد حالت کوانتومی یک شی را به نقطه ای دوردست انتقال دهیم. درساده ترین حالت فرض کنید که شخص A یا آلیس می خواهد حالت یک فوتون یاالکترون مثل $|\phi\rangle := \alpha|0\rangle + \beta|1\rangle$ را

به همکارخود B یا باب که درنقطه ای دوردست واقع است انتقال دهد. فرض مااین است که باب الکترونی دارد که دریک حالت معین قراردارد و می خواهد بااستفاده از اطلاعاتی که آلیس به او می دهد کاری کند که الکترون اش حالت $|\phi\rangle$ رااختیارکند. مستقیم ترین راه برای این کار آن است که آلیس مقادیر دو عدد مختلط α و β را به باب مخابره کند واو بااعمال یک عملگرکوانتومی حالت الکترون اش را به حالتی که دردست آلیس ست تبدیل کند. اما این کار دو اشکال اساسی دارد. اول آن که مخابره دوعدد مختلط فوق با دقت بی نهایت احتیاج به مخابره بی نهایت اطلاعات دارد. بنابراین باید به ساخت تقریبی حالت اکتفا کنیم. اگر بخواهیم این اعدادمختلط را تنها با دقت سه رقم اعشار مخابره کنیم احتیاج به مخابره $2 \times 2 \times 10 = 40$ بیت داریم. اشکال دوم آن است که اصولاً معلوم نیست آلیس حالت الکترونی را که دردست دارد بداند وبااین وجود بخواهد این حالت را به باب بفرستد. فرابرد کوانتومی روشی است که بااستفاده 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 زیرعمل می کنیم. نخست یک حالت درهم تنیده بل مثل

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)_{ab} \qquad (۸)$$

را بین A و B به اشتراک می گذاریم. کیوبیت اول که با a مشخص شده نزد آلیس و کیوبیت 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 باکیوبیتی که نزد خود دارد نزدیک کرده تاحالت زیربدست آید:

$$\begin{aligned} |\Psi\rangle = |\phi\rangle|\phi^+\rangle &= (\alpha|0\rangle + \beta|1\rangle)_a \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)_{ab} \\ &= \frac{1}{\sqrt{2}}\left(\alpha|0,0,0\rangle + \beta|1,0,0\rangle + \alpha|0,1,1\rangle + \beta|1,1,1\rangle\right). \end{aligned} \qquad (۹)$$

سپس آلیس روی دوکیوبیت که نزد خود نگاه داشته است یک اندازه گیری درپایه بل انجام می دهد. برای اینکه حاصل اندازه گیری رابفهمیم حالت $|\Psi\rangle$ را به صورت زیربازنویسی می کنیم:

$$\begin{aligned} |\Psi\rangle &= \frac{1}{2}(|\phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + |\phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) \\ &+ |\psi^+\rangle(\beta|0\rangle + \alpha|1\rangle) + |\psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle)). \end{aligned} \qquad (۱۰)$$

بنابراین بعدازاندازه گیری یکی از نتایج زیربرای آلیس بدست می آید و حالتی که دردست باب است به یکی از حالت های نشان داده شده درجدول زیر کاهش پیدا می کند. آلیس می تواند بامخابره تنها دوبیت 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 کنیدکه دراین 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	$-\beta\|0\rangle + \alpha\|1\rangle$	$\|\phi^+\rangle$

(۱۱)

به این ترتیب باب می تواند با اطلاعاتی که از آلیس دریافت می کند، براحتی حالت اولیه را بازسازی کند.

---

۳ کذگذاری چگال

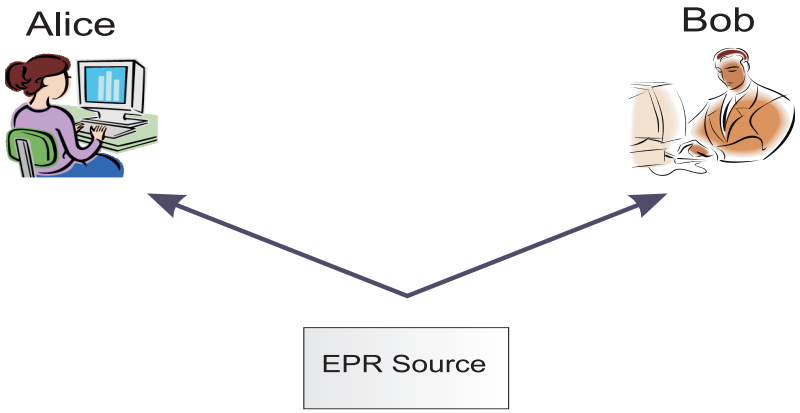
در فرابرد کوانتومی نشان دادیم که می توان به شرط آنکه بین فرستنده و گیرنده یک زوجِ درهم تنیده به اشتراک نهاده شده باشد، آن دو می توانند با مبادله فقط دو بیت کلاسیک یک حالتِ کوانتومی یعنی یک کیوبیت را مبادله کنند. یک سوال طبیعی این است که آیا می توان وارون این کار را نیز انجام داد، یعنی با مبادله یک کیوبیت 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 صورتِ

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

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:

$$\begin{aligned} 00 &\longrightarrow I \longrightarrow |\phi^+\rangle, \\ 01 &\longrightarrow X \longrightarrow |\psi^+\rangle, \\ 10 &\longrightarrow Z \longrightarrow |\phi^-\rangle, \\ 11 &\longrightarrow Y \longrightarrow |\psi^-\rangle. \end{aligned} \qquad (۱۲)$$

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 $00,\ 01,\ 10,\ 11$



شکل ۱ : درتمام فرایندهای مبادله اطلاعات کوانتومی می توان فرض کرد که منبع ثالثی زوج های درهم تنیده را در اختیار متقاضیان می گذارد.

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 (شکل۱).

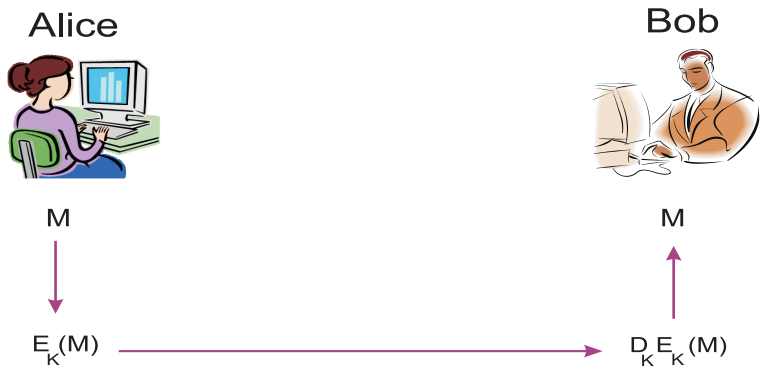
هم چنین این حالت های درهم تنیده می توانسته مدتها پیش بین آلیس و باب به اشتراک گذراده شود و نه در موقعی که آنها واقعا می خواهند باهم مبادله اطلاعات انجام دهند. بالاخره باید دقت کرد که اگر آلیس و باب فقط یک زوج کیوبیت به اشتراک گذاشته باشند، آنگاه آلیس می تواند با ارسال تنها یک کیوبیت یک حالت از چهار حالت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

---

۴ رمزنگاری کوانتومی

رمزنگاری[۹] شاخه‌ای از مهندسی مخابرات است که هدف آن تدوین پروتکل هایی برای مبادله ایمن اطلاعات از یک نقطه به یک نقطه دیگراست. 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 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

[۹] Cryptography



شکل ۲: نمونه کلی رمز نگاری با کلید خصوصی

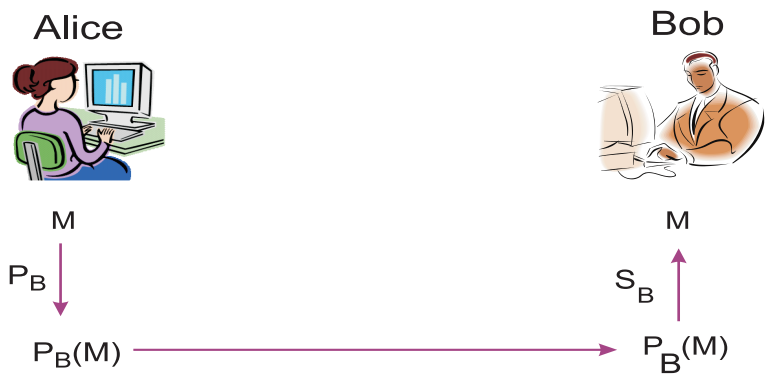
و باب دو نگاشت مشخصِ E_K و D_K اختیار می کنند که دارای خاصیت زیر هستند:

$$D_K \circ E_K = I, \tag{۱۳}$$

بنابراین آلیس بجای پیامِ M یا $PlainText$ پیام رمزشده یا $CipherText$ یعنی $E_K(M)$ را به باب ارسال می کند. در مقصد، باب با اعمال نگاشتِ D_K می تواند به پیام اصلی یعنی M دسترسی پیدا کند، زیرا $D_K(E_K(M)) = M$، شکل (۲). سیستم رمز نگاری می بایست چنان باشد که اگر در بین راه شخص سومی که معمولاً به آن ایو[۱۰] گفته می شود، نتواند با داشتن یک پیامِ $E_K(M)$ به خودِ M دسترسی پیدا کند. حتی ایو نمی بایست با در دست داشتن تعداد معدودی پیام مثل $\{M_1, M_2, \cdots M_n\}$ و رمز شده آنها مثلِ $\{E_K(M_1), E_K(M_2), \cdots E_K(M_n)\}$ بتواند به کلیدِ 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 نهایتا رمز را بازکند. به همین دلیل آلیس و باب می بایست کلید مورد استفاده خود را دائماً تغییر دهند. در رمز نگاری فرض برآن است که توابعِ E_K و D_K یعنی نوع رمزِ 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 می تواند 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 جمعِ بیت به بیت):

$$E_K(M) = M \oplus K, \qquad D_K = E_K. \tag{۱۴}$$

[۱۰] Eve



شکل ۳: 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 $K = (k_1, k_2, k_3, \cdots, k_n)$ آنگاه

$$E_K(m_1, m_2, m_3, \cdots, m_n) = (m_1 \oplus k_1, m_2 \oplus k_2, m_3 \oplus k_3, \cdots m_n \oplus k_n). \qquad (۱۵)$$

از آنجا که $(a \oplus b) \oplus b = b$ واضح است که $D_K \circ E_K = I$. البته این نوع رمز خیلی ساده است زیرا با داشتن تنها یک پیامِ M و رمز شده‌ی آن یعنی $E_K(M)$، بلافاصله کلید از رابطه‌ی $K = E_K(M) \oplus M$ یافته می شود. در عمل کلیدهای بسیار پیچیده‌تری 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 گذارده شود، زیرا هر کلید ثابتی نهایتاً انقدر هم بستگی در پیام های ارسال شده ایجاد می کند که از رشته‌ی $\{E_K(M_1), E_K(M_2), \cdots E_K(M_n)\}$ به شرطی که n به اندازه کافی بزرگ باشد، بتوان کلیدِ K را استخراج کرد.

مشکلی که در این نوع رمز نگاری وجود دارد، آن است که کلیدِ 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 دراینجا با یک دورِ بی پایان یعنی مسئله مبادله کلید[۱۱] به طریق ایمن روبرو هستیم که هرگز حل نخواهد شد. اما در سال ۱۹۷۴ راه حل جالبی برای این موضوع موسوم به کلیدهای عمومی [۱۲] یافته شد. دراین 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

$$D_{S_a} E_{P_a} = I_a, \qquad \forall a. \qquad (۱۶)$$

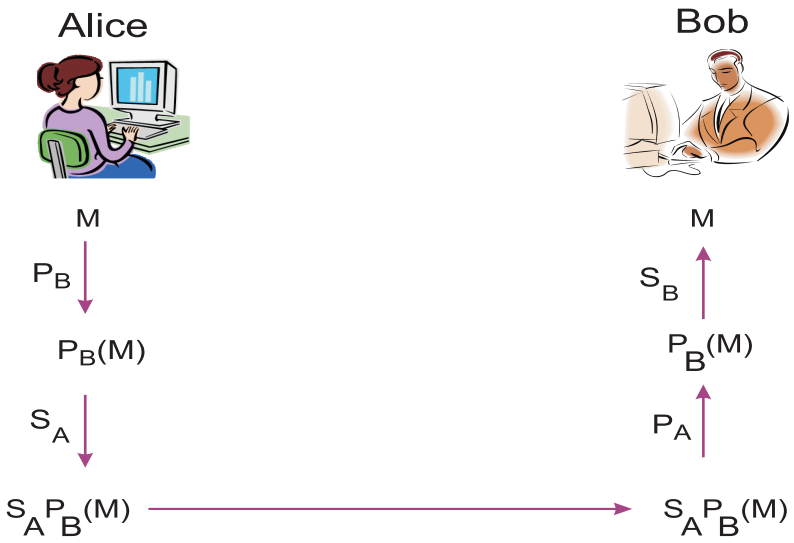
[۱۱] Key Distribution Problem
[۱۲] Public Key System

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 دراین نوع رمز نگاری آن است که بدست آوردن کلید خصوصی یک شخص از روی کلید عمومی او می بایست یک مسئله بسیار بسیار سخت باشد. دراین 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 زیراست. نخست کلید عمومی باب را پیدا می کند و نگاشتِ E_{P_B} را روی پیامِ M اعمال می کند. در مقصد باب با اعمال نگاشتِ D_{S_B} روی پیام دریافت شده پیامِ M را دریافت می کند، شکل ۳. دقت کنید که نگاشت های E و D وارون یکدگیر هستند به این معنا که برقراراست

$$D_{S_B}E_{P_B} = I, \qquad (۱۷)$$

در ادامه این بحث و هم چنین در شکل های ۳ و شکل ۴ 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 $S_BP_B = I_B$ می نویسیم. حال باب با یک مسئله مهم مواجه‌است و آن اینکه می بایست مطمئن شود که پیامِ M واقعاً توسط آلیس برای او فرستاده شده است، زیرا هر کس دیگری نیز می توانسته‌است با نگاه کردن به کلید عمومیِ باب پیامِ M را برای او فرستاده باشد. راه غلبه براین دشواری این است که آلیس پیام خود را دو بار رمز کند. چگونگی این رمزنگاری و رمز گشایی در شکل ۴ نشان داده شده‌است 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 باافزایش تعداد رقم های آن عدد به صورت نمایی افزایش می یابد. با کمی ساده سازی می توانیم بگوییم که هر شخص دو عدد بسیار بزرگِ p و q را اختیار کرده و آنها را درهم ضرب می کند تا عددی مثل $N = pq$ را بدست آورد. وی سپس عددِ N را اعلان عمومی کرده و اعداد p و q را نزد خود نگاه می دارد. کلید عمومی وی از روی عددِ N و کلید خصوصی وی از روی اعدادِ p و q ساخته می شود. واضح است که کلید خصوصی را نمی توان از روی کلید عمومی بدست آورد. امروزه روشی که مبتنی براین نوع مبادله کلیه است موسوم به روشِ RSA [۱۳] است و کاربرد بسیار وسیع یافته است.

[۱۳] .....



شکل ۴: رمز نگاری با کلید عمومی. دراین روش آلیس دو بار پیام را رمز می کند ، یک بار با کلید عمومی باب و بار دیگر با کلید خصوصی خودش.

۵ روش رمزنگاری با استفاده از کلید عمومی

روش RSA که از نام های مخترعان این نوع رمزنگاری گرفته شده است[۱۴] ، 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.

۱.۵ روش ساختن کلیدهای عمومی و خصوصی

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

$$n = pq. \qquad (۱۸)$$

حال تعداد اعدادی که از n کوچکتر بوده و نسبت به آن اول هستند برابراست با $(p-1)(q-1)$. این عدد را با $\phi(n)$ نشان می دهیم. بنابراین

$$\phi(n) = (p-1)(q-1). \qquad (۱۹)$$

[۱۴] Rivest, Shamir, Adelman

■ تمرین: ثابت کنید که $(p-1)(q-1)$ وافعاً تعداد اعدادی است که از n کوچکتر بوده و نسبت به آن اول هستند.

حال عددی مثل $1 < e < n$ را اختیار کنید طوریکه نسبت به $\phi(n)$ اول باشد. این به این معناست که

$$gcd(\phi(n), e) = 1, \qquad (۲۰)$$

که درآن gcd به معنای بزرگترین مقسوم علیه مشترک است. سپس آلیس معکوس عدد e را به سنج $\phi(n)$ حساب می کند. بنابراین عدد d در رابطه زیر صدق می کند:

$$de = k\phi(n) + 1, \qquad (۲۱)$$

که درآن k یک عدد صحیح است. دقت کنید که تمام مراحل فوق براحتی یعنی در زمانی که نسبت به عدد n از مرتبه چند جمله‌ای است انجام پذیرهستند. حال آلیس جفت عددهای (n, e) را به طور عمومی اعلام می کند و جفت عددهای (d, n) را نزد خود نگاه می دارد. بنابراین کلیدهای خصوصی و عمومی آلیس به شرح زیرهستند:

$$S_A = (n_A, d_A) \ , \ P_A = (n_A, e_A). \qquad (۲۲)$$

دقت کنید که با دردست داشتن (e, n) نمی توان (d, n) را بدست آورد زیرا این امر مستلزم دانستن $\phi(n)$ است که بدون دانستن p و q امکان پذیر نیست. به این ترتیب مرحله ساختن کلیدهای خصوصی و عمومی تمام می شود.

■ **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 دوعدد اول باشند. سپس یک کلید عمومی و خصوصی برای خود بسازید.

۲.۵ نحوه رمزکردن یک پیام

پس از ساختن کلیدهای خصوصی و عمومی می رسیم به نحوه رمز کردن پیام ها. نخست آلیس پیام خود را به صورت رشته‌ای عددی مثل M در می آورد. فرض این است که عددِ M از n کوچکتراست. چنانچه پیام بزرگتر باشد آلیس می بایست آن را به قطعات کوچکتر تقسیم کند و هرقسمت را جداگانه رمزگذاری و ارسال کند. برای آنکه آلیس عدد M را به باب بفرستد، نخست کلید عمومی باب یعنی (n_B, e_B) مربوط به باب را می گیرد و عدد یا پیامِ M را به صورت زیر تبدیل به عدد یا پیام رمزیده‌ی C می کند:

$$C := M^{e_B} \ mod \, n_B. \qquad (۲۳)$$

در مقصد باب پیام C را به صورت زیر تبدیل به پیام اصلی می کند:

$$C^{d_B} \ mod \, n_B = (M^{e_B})^{d_B} \ mod \, n_B = M^{d_B e_B} \ mod \, n_B = M^{k\phi(n_B)+1} \ mod \, n_B. \qquad (۲۴)$$

آنچه که باعث می شود عبارت طرف راست با M برابر شود اتحاد زیر است که قضیه اویلر نام دارد.

قضیه اویلر: به ازای هر عدد صحیح n و هر عدد صحیح $M \leq n$ داریم:

$$M^{k\phi(n)+1} \ mod \, n = M. \qquad (۲۵)$$

به این ترتیب باب می تواند پیام رمز شده توسط آلیس را دریافت کند.

- **تمرین:** صحت قضیه اویلر را برای جفت اعداد زیر بیازمایید:

$$(M, n) \in \{(3, 6), (4, 7), (6, 9), (7, 12), (8, 15), (9, 20), (6, 30)\}. \qquad (۲۶)$$

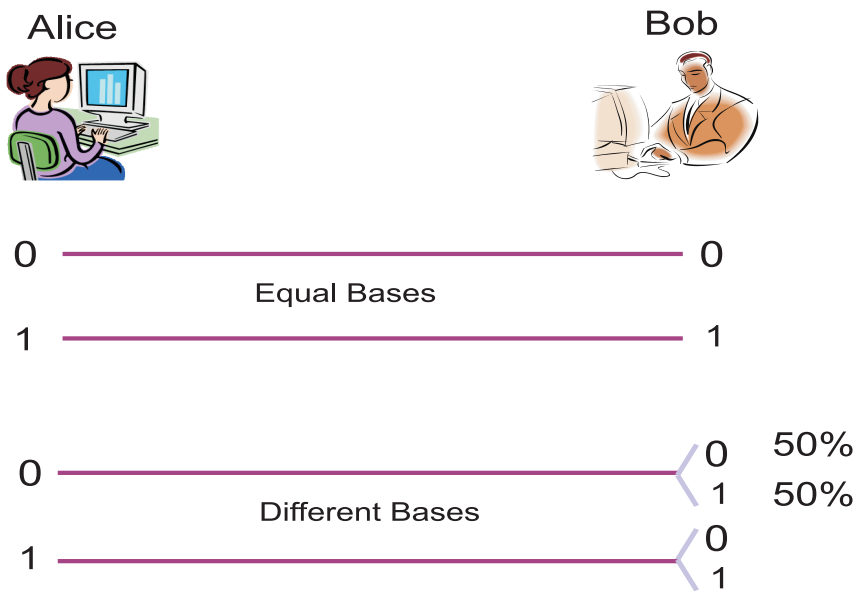
- **تمرین:** در بخش قبل دیدیم که برای آنکه هویت ارسال کننده نیز تایید شود پیام دو بار رمزیده شود. مراحل این کار را در روش RSA توضیح دهید.

۶ 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 [۱۵] یک فرایند کوانتومی برای توزیع کلید ارایه کردند. از آن به بعد این فرایند به طرق گوناگون تعمیم یافته‌است. ما در این جا همان فرایند اولیه بنت و براسار را که به فرایندِ $BB84$ موسوم است بررسی می کنیم. دراین 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 Z و X هستند. ویژه حالت های با ویژه مقدار مثبت به معنای بیت 0 و ویژه حالت های با ویژه مقدار منفی به معنای بیت 1 هستند. حال آلیس رشته‌ای کاملاً تصادفی از این حالت ها را به باب می فرستد و باب نیز به طور تصادفی حالت های دریافتی را در پایه های Z و X اندازه گیری می کند. بعد از مبادله تمام حالت ها، آن دو پایه‌هایی را که برای ارسال و اندازه گیری حالت ها به کار برده‌اند 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 ۲/۱ 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 ۵ . باید به این نکته توجه کنیم که کلید تنها بعد از اعلان عمومی پایه ها توسط الیس 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 توانند با هیچ فرایند کوانتومی کیوبیت های ارسال شده توسط آلیس را تکثیر کرده و یکی را برای خود نگاه داشته ودیگری را برای باب ارسال کند و بعد از اعلان پایه ها به کلید دسترسی پیدا کند، زیرا قبلا دیده ایم که هیچ فرایند کوانتومی نمی تواند حالت های نامتعامد 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 ان 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 پایه‌ای مثل آنهاانتخاب کرده است و بعد از اعلان عمومی وی می تواند به نیمی از رشته کلید دست

[۱۵] Charles Bennett and Gilles Brasard



شکل ۵: 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.

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 درنتیجه 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 پایه‌ی X را برای اندازه گیری اختیار کند. دراین 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 پایه‌ی Z خواهد بود. دراین پایه وی با احتمال $1/2$ حالت $|z,+\rangle$ و با احتمال $1/2$ حالت $|z,-\rangle$ را بدست خواهد آورد. هرکدام از این حالت ها را که برای باب بفرستد تنها با احتمال $1/2$ 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 ار رشته طولانی بیت هایی که مربوط به پایه های یکسان هستند و هیچ کس بجز خود آلیس و باب از انها 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. دراین 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 مجموعه‌ای از زوج های درهم تنیده در حالت

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|x+, x-\rangle - |x-, x+\rangle) \qquad (۲۷)$$

بین خود به اشتراک بگذارند. (درعمل آنها می بایست چنین زوج هایی را از یک منبع خریداری 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 پایه‌ی Z نیز به شکل $|\psi\rangle = \frac{1}{\sqrt{2}}(|z+, z-\rangle - |z-, z+\rangle)$ نوشته می شوند. بنابراین هرگاه آلیس و باب هردو یک پایه برای اندازه گیری خود انتخاب کنند، نتایج آنها کاملاً وارون هم خواهد بود(به عبارت بهتر همبستگی کامل ولی معکوس دارند[۱۶] 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.

۱.۶ اشتراک رمز

علاوه بر توزیع کلید می توان مکانیک کوانتومی را برای حل بدیع مسائل دیگری از رمز نگاری بکاربرد. منظور از مسئله اشتراک رمز 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 نفرِ باب و چارلی قابل اعتماد نیستند و نمی بایست به تنهایی اطلاعات مهمی مثل رمز حساب بانکی را دراختیار داشته باشند. یک راه حل کلاسیک و بسیار ساده برای این کار آن است که آلیس پیام M با یک رشته تصادفی 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 رشته های K و N دارای معنای مشخصی نیستند. حال آلیس رشته های K و N را به طور جداگانه به باب و چارلی می فرستد. این پیام ها برای آنها هیچ استفاده‌ای در برندارد. تنها وقتی می توانند از رشته های دریافت شده‌ی خود استفاده کنند که آنها رابا هم جمع کنند. دراین صورت با توجه به رابطه‌ی

$$N \oplus K = (M \oplus K) \oplus K = M, \qquad (۲۸)$$

[۱۶] Anit-correlation

آنها می توانند محتوی اصلی پیام را دریافت کنند. البته آلیس می بایست از یک فرایند رمزنگاری جداگانه استفاده کند تا بتواند رشته های K و N را به طور ایمن برای باب و چارلی ارسال کند. وی می بایست 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 رشته ها به باب و چارلی استفاده کند، زیرا فرض این است که آنها به کانال های یک دیگر دسترسی دارند یا به عبارت دیگر تلاش خود را برای استراق سمع و آگاهی یافتن از رشته‌های یک دیگر به کار می برند. بنابراین آلیس می بایست 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 تعمیم های دیگری نیز دارد به این معنا که آلیس پیام می خواهد پیامِ M را به n نفر ارسال کند، و هر زیرمجموعه‌ی k نفری از این n نفر می بایست با مشارکت یکدیگر بتوانند، به رمز ارسال شده توسط آلیس دست یابند و هیچ زیرمجموعه‌ای با تعداد عضو کمتراز k نتوانند این کار را انجام دهند. مثال های زیر راه‌های ساده‌ای را برای این کار نشان می دهند.

مثال ۱: دراین مثال آلیس می خواهد 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 بتوانند پیامِ 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 می فرستد که از ترکیب پیام اصلی با پیام های تصادفی دیگر درست شده‌اند.

$$\begin{aligned} &\longrightarrow \quad B_1 \qquad (K_1, K_2 \oplus M), \\ &\longrightarrow \quad B_2 \qquad (K_2, K_3 \oplus M), \\ &\longrightarrow \quad B_3 \qquad (K_3, K_1 \oplus M). \end{aligned} \tag{۲۹}$$

خواننده با نگاهی به رشته ها می تواند تایید کند که واقعاً هر دو نفر می توانند با هم کاری هم پیام M را بفهمند.

مثال ۲: دراین مثال آلیس می خواهد 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 پیامِ 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 می فرستد که از ترکیب پیام اصلی با پیام های تصادفی دیگر درست شده‌اند.

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

$$\longrightarrow \quad B_4 \qquad (K_2, K_3 \oplus M). \tag{۳۰}$$

خواننده با نگاهی به رشته ها می تواند تایید کند که واقعاً هر دو نفر می توانند با هم کاری هم پیام M را بفهمند.

- یک تمرین خوب و سرگرم کننده برای خواننده آن است که سعی کند طرحی را پیاده کند که طی آن هر زیر مجموعه‌ی سه نفری و نه کمتر از یک مجموعه چهارنفری بتوانند یک پیام M را باز کنند.

همانطور که از مثال های بالا پیداست، در فرایند اشتراک رمز، دو مرحله‌اساسی وجود دارد، یکی اینکه پیام اصلی به دو یا چند قسمت شکسته شود، [۱۷] و دوم اینکه هر قسمت از پیام به طریق ایمن به گیرنده ها ارسال شود، به نحوی که هیچ کدام از آنها یا اشخاص دیگر نتوانند با استراق سمع به قسمت های مختلف پیام دسترسی پیدا کرده و خودِ پیام را بازگشایی کنند. آیا می توان هردوی این مراحل را در یک فرایند کوانتومی با هم تلفیق کرد؟ پاسخ این سوال مثبت است و راه حل آن استفاده از حالت های درهم تنیده‌ی GHZ است [۱۸]، [۱۹].

---

۷ تمرین ها:

- اگر در فرابرد کوانتومی حالت درهم تنیده‌ی بین آلیس و باب بجای $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ حالتِ $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ باشد تغییری که در مراحل فرابرد 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 نوفه ای به ترتیب زیرباشد:

$$0 \longrightarrow 1 \qquad p$$

[۱۷] Message Splitting

[۱۸] V. Buzek, M. Hillery and A. Berthiaume, Physical Review A, 1998

[۱۹] S. Bagherinezhad, V. Karimipour, Physical Review A (2001)

$$1 \longrightarrow 0 \qquad p. \tag{۳۱}$$

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 چقدرخواهد بود.

- فرض کنید که در فرابرد کوانتومی حالت درهم تنیده خالص نبوده بلکه به صورت زیرباشد:

$$\rho = (1-p)|\phi\rangle\langle\phi| + p|00\rangle\langle 00|, \tag{۳۲}$$

که درآن $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. 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 چقدرخواهد بود.

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

$$|\phi\rangle = a|0\rangle + b|1\rangle + c|2\rangle, \tag{۳۳}$$

و حالت درهم تنیده بین آلیس و باب به صورت زیراست:

$$|\psi\rangle := \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle). \tag{۳۴}$$

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

$$X := |1\rangle\langle 0| + |2\rangle\langle 1| + |0\rangle\langle 2|, \qquad Z := |0\rangle\langle 0| + \omega|1\rangle\langle 1| + \omega^2|2\rangle\langle 2|, \tag{۳۵}$$

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

- فرابرد کوانتومی را برای حالت های پیوسته صورت بندی کنید. یک حالت پیوسته به صورت زیراست:

$$|\phi\rangle = \int dx \phi(x)|x\rangle, \tag{۳۶}$$

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