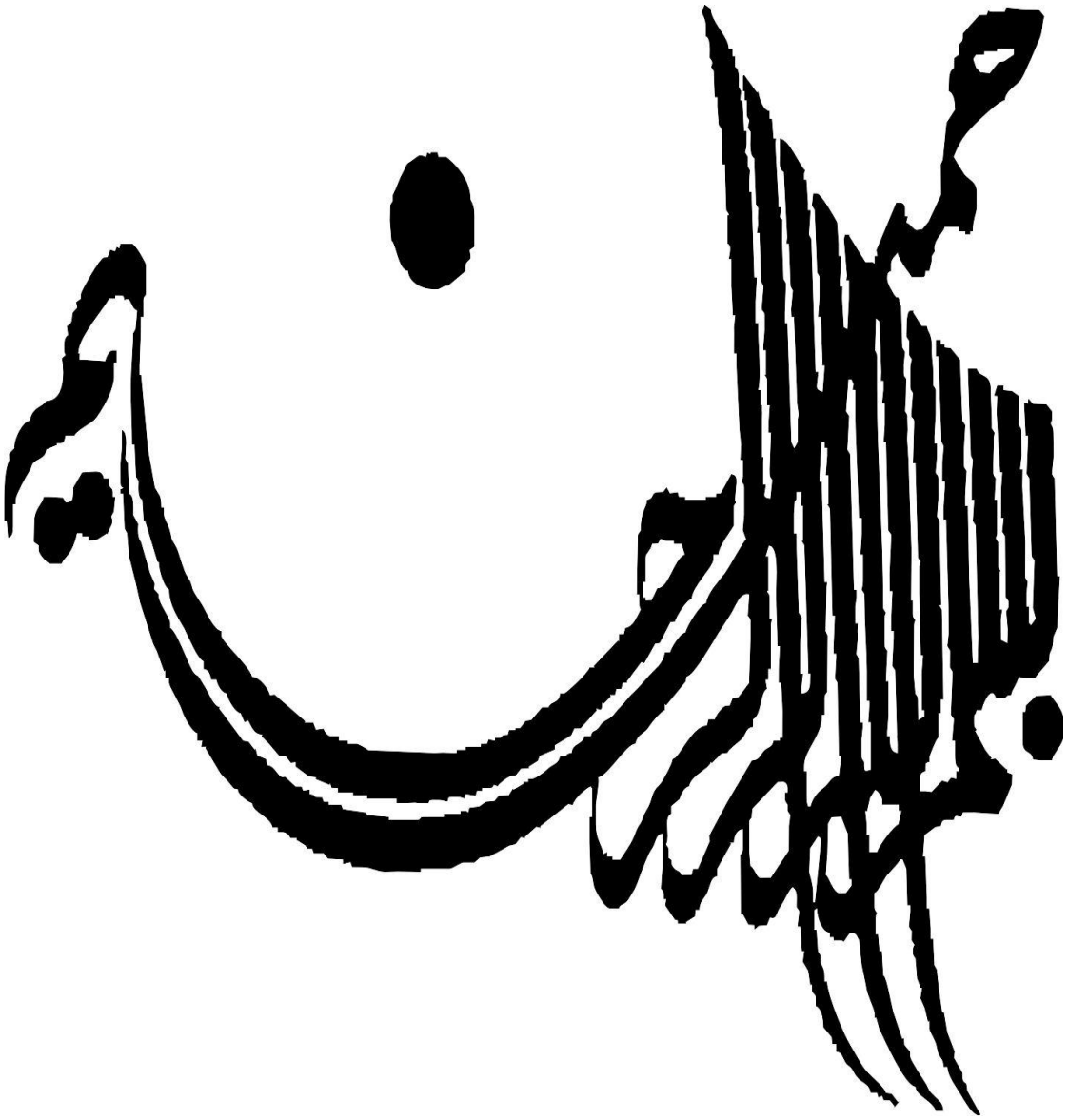


دانشکده فیزیک

پایان‌نامه کارشناسی ارشد

فیزیک ذرات بنیادی

عنوان:

انتقال بیت کوانتومی ایمن بدون شرط

ارائه‌دهنده:

الهام عابدینی‌نیا

استاد راهنما:

دکتر حسین موحدیان

پایان‌نامه کارشناسی ارشد جهت اخذ درجه کارشناسی ارشد

بهمن ۱۳۹۱

تقدیم به دو فرشته پاک و مهربان پدر و مادر عزیزم

از تو می پرسم ای اهورا:

چیست سرمایه ی رستگاری؟

(می رسد پاسخ از آسمان ها):

دل به مهر پدر آشنا کن

دین خود را به مادر ادا کن

من که امروز در باغ گیتی

چون درختی همه برگ و بارم

رنج های گران پدر را

با کدامین زبان پاس دارم

سر به پای پدر می گذارم

جان به راه پدر می سپارم

یاد جان سوختن های مادر

لحظه ای از وجودم جدا نیست

پیش پایش چه ریزم که جان را

قدر یک موی مادر بها نیست

او خدا نیست اما وفایش

کمتر از لطف و مهر خدا نیست...

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت های او ندانند و کوشندگان، حق او را گزاردن نتوانند. و سلام و درود بر محمّد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز...

بدون شک جایگاه و منزلت معلم، اجلّ از آن است که در مقام قدردانی از زحمات بی شائبه ی او، با زبان قاصر و دست ناتوان، چیزی بنگاریم. اما از آنجایی که تجلیل از معلم، سپاس از انسانی است که هدف و غایت آفرینش را تامین می کند و سلامت امانت هایی را که به دستش سپرده اند، تضمین؛ بر حسب وظیفه و از باب "من لم یشکر المنعم من المخلوقین لم یشکر الله عزّ و جلّ": از استاد عزیز و وارسته جناب آقای دکتر **حسین موحدیان** که در کمال سعه صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه بر من دریغ ننمودند و زحمت راهنمایی این رساله را بر عهده گرفتند تقدیر و تشکر ویژه می نمایم. باشد که این خردترین، بخشی از زحمات ایشان را سپاس گوید.

چکیده

رمزنگاری کوانتومی به بیان و توصیف کاربرد مکانیک کوانتومی برای انجام رمزنگاری و یا شکستن سیستم‌های رمزی و پنهانی می‌پردازد. مهمترین و شناخته شده‌ترین کاربرد رمزنگاری کوانتومی، توزیع کلید کوانتومی (QKD) است. هدف QKD استفاده از ارتباطات کوانتومی به منظور طراحی و به اشتراک‌گذاری یک کلید بین دو طرف است به طوریکه هیچ شخص سومی، حتی اگر تمام مخابرات و ارتباطات بین آلیس و باب را استراق سمع کند، نتواند هیچ گونه اطلاعاتی در مورد کلید به دست آورد. بدین منظور آلیس (فرستنده) بیت‌های کلید را به صورت داده‌های کوانتومی رمزگذاری کرده و آن‌ها را برای باب می‌فرستد. هر اقدام ایو مبنی بر کسب اطلاعات در مورد کلید، منجر به ایجاد اختلال در پیام شده و آلیس و باب مطلع می‌گردند. و در نهایت کلید برای مخابرات ایمن مورد استفاده قرار می‌گیرد. به دنبال کشف توزیع کلید کوانتومی و ایمنی بدون شرط، محققین تلاش نمودند که به کارها و اهداف رمزنگاری دیگر همراه با ایمنی بدون شرط دست یابند.

سوال اساسی و مهمی که در اینجا مطرح می‌شود اینست که با به کارگیری این طرح‌ها، آیا طرفین همواره کلید یکسان و مشابهی به دست می‌آورند؟ بر اساس پروتکل‌های QKD، چنانچه یکی از طرفین اقدام به تقلب نماید، کلیدی که طرفین در نهایت به دست می‌آورند مشابه و همانند نخواهد بود. به منظور غلبه بر این مشکل، ایده‌ی ارسال التزام آور بیت (BC) پیشنهاد و مطرح شد و پیش-بینی شد که اگر BC کوانتومی بر طرح‌های QKD اعمال شود، تقلب قابل شناسایی خواهد بود.

در یک طرح التزام‌آور بیت، آلیس یک بیت b را انتخاب، و سپس به واسطه‌ی سند التزامی که تهیه و در اختیار باب قرار می‌دهد، به آن بیت ملتزم می‌شود. به طوریکه باب به هیچ وجه نمی‌تواند بفهمد که b چیست و در ضمن آلیس بعداً می‌تواند با سند و مدرک این مقدار را برای وی افشا کند در حالیکه به هیچ وجه نمی‌تواند نظر خود را عوض نموده و مدعی شود که مقدار انتخابی اولیه‌اش چیز دیگری بوده است.

ادعای رمزنگاری کوانتومی همواره این بوده است که می‌تواند پروتکل‌هایی فراهم کند که ایمن بدون شرط هستند. یعنی بدون در نظر گرفتن هیچ گونه قید و شرطی بر روی مکان، زمان و تکنولوژی در دسترس متقلب همچنان ایمن باشد. در این پایان نامه، در ادامه‌ی بررسی QKD و بیان اصول موجود در BC، مختصراً به این موضوع می‌پردازیم که BC کوانتومی ایمن امکانپذیر نیست و در ادامه نیز دو پروتکل BC را مورد مطالعه قرار می‌دهیم: ۱) BC ایمن بدون شرط توسط انتقال خروجی‌های اندازه-گیری که متکی بر علیت مینکوفسکی و ویژگی‌های اطلاعات کوانتومی است و ۲) پروتکل BC حساس به تقلب ایمن بدون شرط بین دو شخص که نسبت به هم ظنین‌اند. این پروتکل تضمین می‌نماید که چنانچه یکی از طرفین تقلب نماید، طرف دیگر با احتمال غیر صفر آن را شناسایی خواهد کرد. این پروتکل غیر نسبیتی است و از اطلاعات کوانتومی به منظور اجرای اهدافی که از لحاظ کلاسیکی غیر ممکن است، استفاده می‌کند.

واژگان کلیدی: اطلاعات کوانتومی- اندازه گیری کوانتومی- درهم تنیدگی- انتقال بیت کوانتومی- ارسال التزام‌آور بیت.

فهرست مطالب **صفحه**

فصل اول: مروری بر رمزنگاری و مفاهیم مقدماتی

فصل دوم: درهم‌تنیدگی و فرآیندهای انتقال

فصل ۳: توزیع کلیدکوانتومی و ارسال التزام‌آور بیت

فهرست شکل‌ها

صفحه

فهرست جداول **صفحه**

فصل اول

مروری بر رمزنگاری و مفاهیم مقدماتی

۱-۱ مقدمه

رمزنگاری[۱]، علمی است که به وسیله‌ی آن می‌توان اطلاعات را به صورتی امن منتقل کرد حتی اگر مسیر انتقال اطلاعات (کانال‌های ارتباطی) ناامن باشد و یا پیام رمزشده افشا گردد. دریافت کننده‌ی اطلاعات پس از دریافت حالت رمزشده‌ی این اطلاعات، به کمک کلید می‌تواند آن‌ها را از حالت رمز خارج کرده و متوجه پیام اصلی شود. به این عمل در واقع رمزگشایی[۲] گفته می‌شود. رمزنگاری امروزه به طور خاص در علم مخابرات مورد استفاده قرار می‌گیرد. از رمزنگاری می‌توان برای تأمین امنیت و نیز اعتبار پیام به صورت جداگانه یا توأمان استفاده کرد. منظور از تأمین امنیت پیام این است که به غیر از گیرنده‌ی مجاز، شخص دیگری قادر به فهمیدن متن پیام نباشد. همچنین منظور از اعتبار پیام اینست که فرستنده‌ی واقعی پیام مشخص باشد. این امر به کمک یک کلید و یک الگوریتم رمزنگاری انجام می‌شود به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج متن اصلی از متن رمزشده باشد و شخصی که از یک و یا هر دوی آن‌ها اطلاعی ندارد، نتواند به محتوای پیام دسترسی داشته باشد. رمزنگاری از طریق پنهان نگاه داشتن الگوریتم رمزنگاری منسوخ است. در روش‌های جدید رمزنگاری فرض بر آن است که همگان الگوریتم رمزنگاری را می‌دانند و آنچه پنهان است فقط کلید است.

به خوبی روشن است که روش‌های معمول در رمزنگاری نمی‌توانند امنیت کامل اطلاعات ارسالی را تضمین و اثبات کنند و تمامی روش‌های رمزنگاری کلاسیکی فاقد توانائی کافی در جلوگیری از افشای داده‌های رمزشده‌ی ارسالی در طول مسیر ارسال هستند. در یک توصیف ساده، استراق‌سمع اطلاعات در دو مرحله انجام می‌شود. در ابتدا شخص استراق‌سمع‌کننده (عامل مزاحم) از نسخه‌ی اصلی اطلاعات کپی‌برداری می‌کند و سپس حامل‌های اطلاعات کد شده را بازگشایی کرده و نسخه‌ی اصلی را برای گیرنده‌ی حقیقی می‌فرستد و به این ترتیب گیرنده‌ی واقعی نمی‌تواند از استراق‌سمع اطلاعات

---

[۱] Cryptography
[۲] decrypting

توسط عامل مزاحم باخبر شود ولی در رمزنگاری کوانتومی که در آن از نظریه‌ی کوانتومی برای مخابره‌ی اطلاعات استفاده می‌گردد، انتقال اطلاعات از ایمنی بیشتری برخوردار است.

۱-۲ رمزنگاری کوانتومی

رمزنگاری کوانتومی اولین بار توسط وایزنر[۱] در اوایل دهه‌ی ۱۹۷۰ ارائه شد که مقاله‌ی وی در این زمینه در سال ۱۹۸۳ به چاپ رسید و در سال ۱۹۹۰ یک دانشجوی دوره‌ی دکتری دانشگاه آکسفورد به نام ایکرت[۲] روش دیگری برای رمزنگاری کوانتومی ارائه داد. رمزنگاری کوانتومی تنها برای تولید و توزیع کلید استفاده می‌شود و نه برای انتقال اطلاعات. این کلید در مراحل بعدی می‌تواند با یک الگوریتم رمزگذاری (یا رمزگشایی) برای تبدیل پیام اصلی به پیام رمز شده (یا بالعکس) استفاده شود. بر خلاف رمزنگاری کلاسیک که به دشواری انجام عملیات ریاضی مخصوصی وابسته است و نمی‌تواند شنودکننده را آشکارسازی و پنهان ماندن کلید را تضمین کند، رمزنگاری کوانتومی که بر پایه‌ی اصول مکانیک کوانتومی استوار است می‌تواند کلیدهایی با امنیت بالا طراحی نماید.

رمزنگاری کوانتومی بر پایه‌ی اصل عدم قطعیت هایزنبرگ[۳] استوار است که بیان می‌کند جفت‌های به خصوصی از خواص فیزیکی یک سیستم به شکلی به هم مربوطند که اندازه‌گیری همزمان آن‌ها غیرممکن است و اندازه‌گیری یکی از آن‌ها، از اندازه‌گیری کمیت دیگر به طور همزمان جلوگیری می‌کند. این اصل با توجه به این نکته است که در حالت کلی، اندازه‌گیری یک سیستم، حالت آن را تغییر می‌دهد. بنابراین وقتی در اندازه‌گیری قطبش فوتون، جهت اندازه‌گیری خاصی را انتخاب می‌کنیم این انتخاب، تمامی اندازه‌گیری‌های بعدی را تحت تأثیر قرار می‌دهد چون موجب تغییر قطبش می‌شود. برای مثال، اگر جهت عمودی را برای اندازه‌گیری قطبش یک فوتون انتخاب کنیم، فوتون عبوری (مستقل از اینکه دارای چه حالت اولیه‌ای بوده است) متأثر از این قطبش‌گر عمودی دارای قطبش عمودی خواهد بود (و نه افقی) حال اگر اندازه‌گیری دیگری در زاویه‌ی ۴۵ درجه از اندازه‌گیری اول

---

[۱] Stephen Wiesner
[۲] Artur Ekert
[۳] Heisenberg Uncertainty Principle

انجام دهیم، احتمال عبور فوتون از قطبش‌گر دوم دقیقاً $\frac{1}{2}$ است در اینصورت می‌گوییم که قطبش‌گر اول، اندازه‌گیری قطبش‌گر دوم را کاملاً تصادفی می‌کند. بنابراین اگر اتمی تحت تأثیر یک قطبش‌گر 0 یا ۹۰ درجه قرار گیرد، بعداً، در صورتی می‌توان جهت صحیح (اولیه) قطبش این اتم را تشخیص داد که یک قطبش‌گر 0 یا ۹۰ درجه انتخاب گردد. در غیر اینصورت چنانچه از قطبش‌گر ۴۵ یا ۱۳۵ درجه برای این منظور استفاده گردد، یک خروجی با همین قطبش‌ها (۴۵ یا ۱۳۵) خواهد داشت که این بدین معناست که قطبش اتم (با احتمال برابر) یا عمودی بوده است و یا افقی.

به طور کلی می‌توان رمزنگاری را به شیوه‌ی زیر تعریف کرد [۱] :

فرض کنید که رشته‌ای n بیتی حاوی پیام مشخصی است. این رشته را با M نشان می‌دهیم. در شیوه‌ای ساده که به رمزنگاری با کلید خصوصی[۱] معروف است، آلیس و باب یک کلید مثل K بین خود به اشتراک می‌گذارند. با توجه به این کلید، آلیس و باب دو نگاشت مشخص D_K و E_K را اختیار می‌کنند که دارای خاصیت زیر هستند:

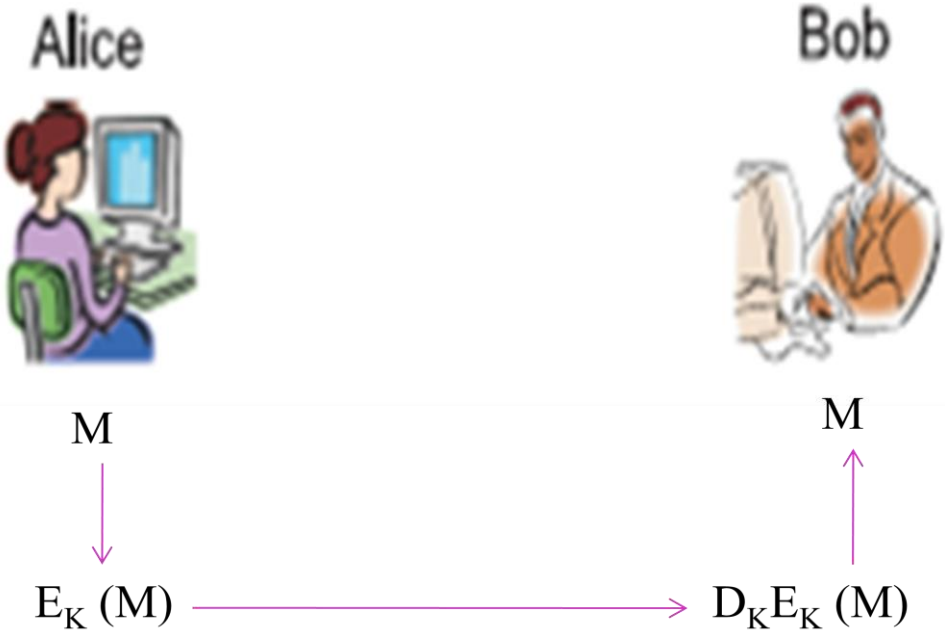
$$D_K \circ E_K = I \qquad (۱-۱)$$

(این رابطه بدان معناست که ترکیب این دو نگاشت همانی می‌باشد). بنابراین آلیس به جای پیام M (پیام اصلی[۲])، پیام رمزشده[۳] یعنی $E_K(M)$ را به باب ارسال می‌کند. در مقصد، باب با اعمال نگاشت D_K می‌تواند به پیام اصلی یعنی M دسترسی پیدا کند. زیرا $D_K(E_K(M)) = M$، شکل (۱-۱). سیستم رمزنگاری می‌بایست چنان باشد که در بین راه، شخص سوم (ایو) با داشتن پیام $E_K(M)$ نتواند به خود M دسترسی پیدا کند. حتی ایو نمی‌بایست با در دست داشتن تعدادی پیام مثل $\{M_1, M_2, ...M_n\}$ و رمزشده‌ی آن‌ها مثل $\{E_K(M_1), E_K(M_2), ...E_K(M_n)\}$ بتواند به کلید K دسترسی پیدا کند. البته در عمل ایو می‌تواند با در دست داشتن تعداد قابل توجهی از پیام‌های رمزشده و توجه به همبستگی‌هایی که بین آن‌ها وجود دارد و با ترکیبی از آنالیز دقیق و حدس و

---

[۱] Private Key
[۲] Plain Text
[۳] Cipher Text

گمان به کلید دست پیدا کرده و نهایتاً رمز را باز کند. به همین دلیل آلیس و باب می‌بایست کلید مورد استفاده‌ی خود را دائماً تغییر دهند. در رمزنگاری فرض بر آنست 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 فقط آلیس و باب باید از آن مطلع باشند. به عنوان مثال در ساده‌ترین نوع رمزنگاری، K یک رشته‌ی تصادفی مشترک بین آلیس و باب بوده و توابع E_K و D_K نیز عبارتند از جمع دو رشته بیت



شکل ۱-۱: نمونه‌ی کلی رمزنگاری با کلید خصوصی

به سنج دو:

$$E_K(M) = M \oplus K\ , \qquad D_K = E_K \tag{۲-۱}$$

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

$$E_K(m_1, m_2, m_3, \ldots m_n) = (m_1 \oplus k_1, m_2 \oplus k_2, m_3 \oplus k_3, \ldots m_n \oplus k_n) \tag{۳-۱}$$

از آنجا که $(a \oplus b) \oplus b = b$ واضح است که $D_K \circ E_K = I$ [۱]. البته این نوع رمز خیلی ساده است زیرا با داشتن تنها یک پیام M و رمزشده‌ی آن یعنی $E_K(M)$، بلافاصله کلید از رابطه‌ی

$K = E_K(M) \oplus M$ یافت می‌شود. در عمل، کلیدهای بسیار پیچیده‌تری برای مبادله‌ی ایمن اطلاعات مورد استفاده قرار می‌گیرد. باید تأکید کنیم که کلید K می‌بایست مرتباً عوض شده و کلیدهای جدیدی بین آلیس و باب به اشتراک گذارده شود. زیرا هر کلید ثابتی نهایتاً آنقدر همبستگی در پیام‌های ارسال شده ایجاد می‌کند که از رشته‌ی $\{E_K(M_1), E_K(M_2), ... E_K(M_n)\}$، به شرطی که n به اندازه‌ی کافی بزرگ باشد، بتوان کلید K را استخراج کرد.

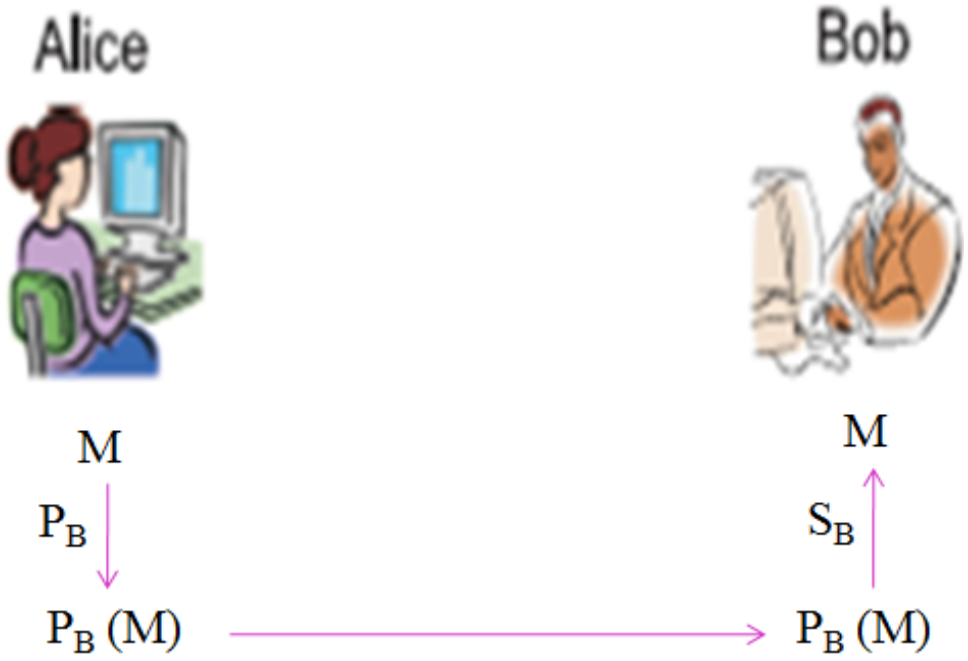
مشکلی که در این نوع رمزنگاری وجود دارد آنست که کلید K می‌بایست بین آلیس و باب به اشتراک گذاشته شود و واضح است که برای این کار، آلیس و باب نمی‌توانند یکدیگر را مرتباً ملاقات کنند. به نظر می‌رسد که در اینجا با یک دور بی‌پایان یعنی مسئله‌ی مبادله‌ی کلید به طریق ایمن روبرو هستیم که هرگز حل نخواهد شد. اما در سال ۱۹۷۴ راه حل جالبی برای این موضوع موسوم به کلیدهای عمومی[۱] ارائه شد. در این نوع رمزنگاری هر شخص از دو نوع کلید استفاده می‌کند. این دو کلید را برای آلیس به ترتیب P_A و S_A، و برای باب P_B و S_B می‌نامیم. به طور کلی، نگاشت‌های متناظر با رمزی کردن پیام یعنی E و بازگشایی رمز یعنی D (مربوط به شخص a) دارای این خاصیت هستند که :

$$\forall a \qquad D_{S_a} E_{P_a} = I \ . \tag{۴-۱}$$

کلید P یک کلید عمومی و کلید S یک کلید خصوصی است. کلید عمومی یک شخص برای همه‌ی افراد دیگر نیز معلوم است و آن‌ها می‌توانند با مراجعه به یک پایگاه داده معین، کلید عمومی هر شخص دلخواهی را به دست آورند. ولی کلید خصوصی هر شخص تنها برای خود او معلوم است. همچنین نکته‌ی اساسی در این نوع رمزنگاری آنست که به دست آوردن کلید خصوصی یک شخص از روی کلید عمومی او می‌بایست بسیار سخت باشد. در این نوع رمزنگاری نیازی به هیچ نوع مبادله‌ی کلیدی نیست. روشی که آلیس برای مبادله‌ی پیامی مثل M به باب در نظر می‌گیرد به این صورت

[۱] Public Keys

است: نخست کلید عمومی باب را پیدا می‌کند و نگاشت E_{P_B} را روی پیام M اعمال میکند. در مقصد، باب با اعمال نگاشت D_{S_B} روی پیام دریافت‌شده، پیام M را دریافت می‌کند، شکل (۱-۲).



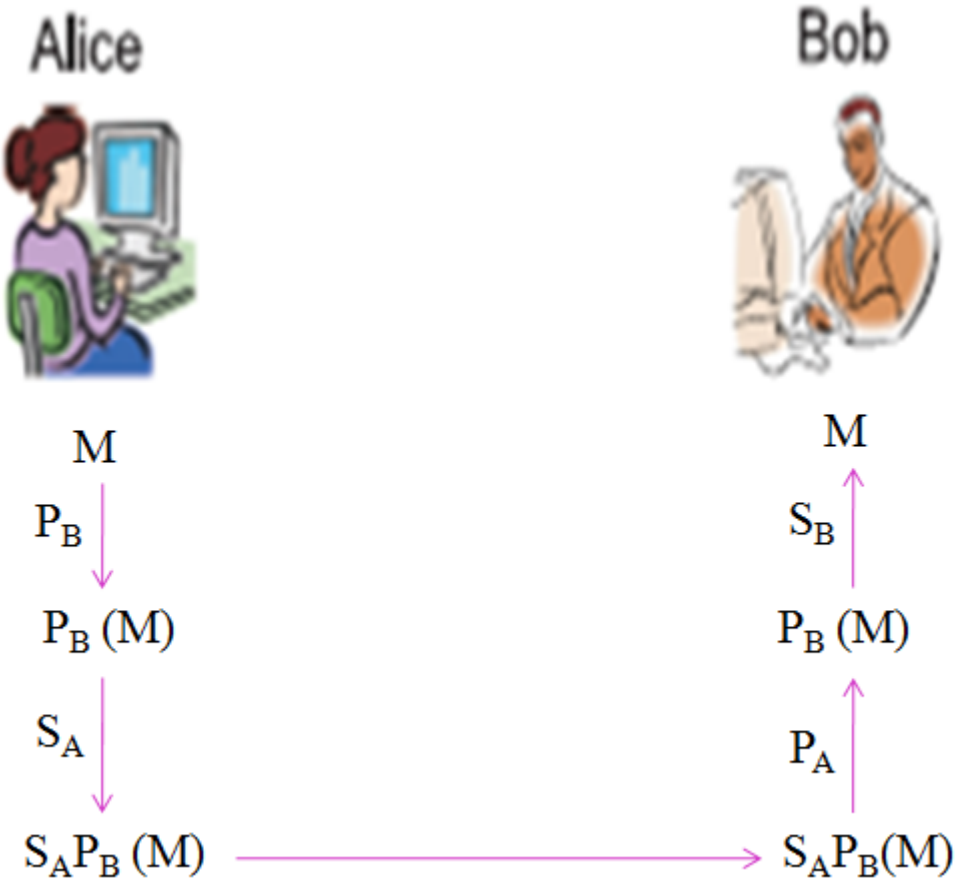
شکل۱-۲: نمونه‌ی کلی رمزنگاری با کلید عمومی. اشکال این روش این است که گیرنده نمی‌تواند از هویت فرستنده مطمئن شود.

دقت کنید که نگاشت‌های E و D وارون یکدیگر هستند به این معنا که رابطه‌ی زیر برقرار است:

$$D_{S_B} E_{P_B} = I \qquad (۵-۱)$$

(در ادامه و همچنین در شکل‌ها، برای ساده سازی به جای E_{P_B} و یا D_{S_B} از P_B و S_B استفاده می‌کنیم و در نتیجه رابطه‌ی فوق را به صورت $S_B P_B = I$ می‌نویسیم.) حال باب با یک مسئله‌ی مهم مواجه است و آن اینکه باب می‌بایست مطمئن شود که پیام M واقعاً توسط آلیس برای او فرستاده شده زیرا هر کس دیگری نیز می‌توانسته با نگاه کردن به کلید عمومی باب، پیام M را برای وی فرستاده باشد. به عبارتی، اگر پیام به وسیله‌ی کلید خصوصی رمزی شود دریافت کننده از هویت فرستنده مطمئن می‌شود و در مقابل، از آنجایی که همگان به کلید عمومی دسترسی دارند قادر به

رمزگشایی اطلاعات خواهند بود (عدم حفظ محرمانه بودن) و نیز چنانچه پیام توسط کلید عمومی رمزی شود، چون فقط دارنده‌ی کلید خصوصی قادر به رمزگشایی آن می‌باشد از این رو محرمانه بودن پیام حفظ می‌شود ولی باز هم به دلیل آنکه همگان از کلید عمومی مطلع هستند، گیرنده در تأیید هویت فرستنده با مشکل مواجه خواهد بود. راه غلبه بر این دشواری این است که آلیس پیام خود را دو بار رمزی کند. چگونگی این رمزنگاری در شکل (۱-۳) نشان داده شده است.



شکل ۱-۳: رمزنگاری با کلید عمومی. در این روش آلیس پیام را دو بار رمزی می‌کند، یک بار با کلید عمومی باب و بار دیگر با کلید خصوصی خودش.

آنچه که امروزه به عنوان کلیدهای عمومی و خصوصی مورد استفاده قرار می‌گیرد، متکی بر این است که یک عدد بسیار بزرگ را نمی‌توان به عوامل اول آن تجزیه کرد. به عبارت دیگر مسئله‌ی تجزیه‌ی

یک عدد به دو عامل اول آن مسئله‌ی بسیار سختی است به این معنا که زمان لازم برای حل این مسئله با افزایش تعداد رقم‌های آن عدد، به صورت نمایی افزایش می‌یابد. با کمی ساده سازی می-توانیم بگوییم که هر شخص دو عدد بسیار بزرگ p و q را اختیار کرده و آن‌ها را در هم ضرب می‌کند تا عددی مثل N = pq را به دست آورد. وی سپس عدد N را اعلان عمومی کرده و اعداد p و q را نزد خود نگه می‌دارد. کلید عمومی وی از روی عدد N و کلید خصوصی وی از روی اعداد p و q ساخته می‌شود [۱]. واضح است که کلید خصوصی را نمی‌توان از روی کلید عمومی به دست آورد.

رمزنگاری کوانتومی که در آن از نظریه‌ی کوانتومی برای بهبود امنیت مخابره‌ی اطلاعات استفاده می‌شود، نخستین بار توسط بنت، براسارد و وایزنر ارائه شد. در این روش، دستیابی به امنیت کامل و دقیق در مخابره‌ی اطلاعات با استفاده از چند مفهوم ساده‌ی حاکم بر مکانیک کوانتومی قابل اثبات است که عبارتند از:

۱) در حالت کلی، اندازه‌گیری بر روی یک سیستم کوانتومی، آن را مختل کرده و تغییر می‌دهد [۲].

۲) سیستم‌های کوانتومی اندازه‌گیری شده یا همبسته (درهم‌تنیده[۱]) نمی‌توانند به صورت ضرب مستقیم تانسوری تک تک حالت‌ها نوشته شوند: دو حالت کوانتومی می‌توانند در عمل به گونه‌ای همبسته گردند که انجام اندازه‌گیری بر روی یکی از حالت‌ها، نتیجه‌ی اندازه‌گیری حالت دیگر را به صورت آنی کاملاً تحت تأثیر قرار دهد (این موضوع در فصل ۲ شرح داده خواهد شد).

۳) مطابق اصول مکانیک کوانتومی، امکان کپی برداری از یک حالت فیزیکی نامعلوم وجود ندارد (قضیه‌ی عدم تکثیر[۲]). یعنی امکان ایجاد دستگاهی که بتواند از حالت سیستمی دلخواه کپی تهیه کند، وجود ندارد.

فرض کنید حالت کوانتومی نامعلومی در اختیار داریم که نمی‌دانیم $|\varphi\rangle$ است یا $|\psi\rangle$. برای اینکه بفهمیم حالت مورد نظر ما کدامیک از این دو می‌باشد می‌بایست یک اندازه‌گیری انجام دهیم. اگر $|\varphi\rangle$ و $|\psi\rangle$ متعامد نباشند، آنگاه هیچ اندازه‌گیری‌ای که بتواند آن‌ها را کاملاً از یکدیگر تمیز دهد

[۱] Entangled system
[۲] No Cloning

وجود ندارد و همواره دارای یک احتمال خطای ثابتی خواهیم بود. با این حال، یک عمل کوانتومی که بتواند از حالت‌ها کپی تهیه کند برای این منظور بسیار مفید خواهد بود. اگر بتوانیم از حالت نامعلوم کپی‌های بسیاری تهیه کنیم، می‌توان اندازه‌گیری مربوطه را چندین بار تکرار نموده و احتمال خطا را تا حد دلخواه کاهش داد. ولی قضیه‌ی عدم تکثیر بیان می‌دارد که این کار از نظر فیزیکی غیر ممکن می‌باشد و فقط مجموعه حالت‌هایی که دو به دو متعامد (معلوم) هستند می‌توانند توسط یک اپراتور یکانی U کپی سازی شوند.

عملگر خطی U را که مانند یک کپی ساز عمل می‌کند در نظر گرفته و اثبات می‌کنیم که چنین عملگری وجود ندارد [۳]: دو حالت خالص $|\psi\rangle$ و $|\varphi\rangle$ را در نظر بگیرید و فرض کنید که یک اپراتور یکانی U وجود دارد به طوریکه برای حالت هدف $|\chi\rangle$ داشته باشیم:

$$U(|\psi\rangle\otimes|\chi\rangle)=|\psi\rangle\otimes|\psi\rangle \qquad (۶-۱)$$

$$U(|\varphi\rangle\otimes|\chi\rangle)=|\varphi\rangle\otimes|\varphi\rangle \qquad (۷-۱)$$

با محاسبه‌ی ضرب داخلی سمت چپ روابط (۱-۶) و (۱-۷) و استفاده از این حقیقت که $U^{\dagger}U=I$، به دست می‌آید:

$$(\langle\psi|\otimes\langle\chi|U^{\dagger})(U|\varphi\rangle\otimes|\chi\rangle)=\langle\psi|\varphi\rangle\langle\chi|\chi\rangle=\langle\psi|\varphi\rangle \qquad (۸-۱)$$

و نیز چنانچه ضرب داخلی سمت راست روابط (۱-۶) و (۱-۷) را محاسبه کنیم خواهیم داشت:

$$(\langle\psi|\varphi\rangle)^2 \qquad (۹-۱)$$

از برابر قرار دادن این دو نتیجه به رابطه‌ی زیر می‌رسیم:

$$\langle\psi|\varphi\rangle=(\langle\psi|\varphi\rangle)^2 \qquad (۱۰-۱)$$

این رابطه فقط در دو حالت می‌تواند صحیح باشد: الف) اگر $\langle\psi|\varphi\rangle=0$، یعنی زمانی که حالت‌ها متعامدند و یا ب) زمانیکه $|\varphi\rangle=|\psi\rangle$. این نتیجه بدان معناست که در حالت کلی چنین اپراتور یکانی (U) که بتواند از حالت‌های کوانتومی دلخواه کپی تهیه کند وجود ندارد.

۱-۳ نظریه‌ی اندازه‌گیری کوانتومی

قبل از هر چیز بهتر است بدانیم که اندازه‌گیری کوانتومی، ابزاری برای توصیف نتایج اندازه‌گیری روی سیستم‌های کوانتومی فراهم می‌کند [۳].

اندازه‌گیری‌های کوانتومی توسط مجموعه عملگرهای اندازه‌گیری $\{M_m\}$ (در فضای هیلبرت سیستم در حال اندازه‌گیری)، توصیف می‌شوند. نتایج اندازه‌گیری که در آزمایش به دست می‌آیند را با m برچسب می‌زنیم. اگر حالت سیستم کوانتومی قبل از اندازه‌گیری $|\psi\rangle$ باشد آنگاه احتمال به دست آوردن نتیجه‌ی m عبارتست از [۳]:

$$P(m)=\langle\psi|M_m^\dagger M_m|\psi\rangle=Tr(M_m|\psi\rangle\langle\psi|M_m^\dagger) \qquad (۱۱-۱)$$

و نیز حالت سیستم بعد از اندازه‌گیری به صورت زیر خواهد بود:

$$|\psi'\rangle=\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \qquad (۱۲-۱)$$

عملگرهای اندازه‌گیری در رابطه‌ی تمامیت $\sum_m M_m^\dagger M_m=I$ صدق می‌کنند. این رابطه مبین این حقیقت است که می‌بایست جمع احتمالات برابر یک باشد:

$$\sum_m P(m)=\sum_m\langle\psi|M_m^\dagger M_m|\psi\rangle=1 \qquad (۱۳-۱)$$

یک مثال ساده اما مهم، اندازه‌گیری یک کیوبیت در پایه‌های محاسباتی $\{|0\rangle,|1\rangle\}$ است که به کمک عملگرهای اندازه‌گیری $M_0=|0\rangle\langle 0|$ و $M_1=|1\rangle\langle 1|$، شامل دو نتیجه خواهد بود. توجه داشته باشید که هر یک از عملگرها هرمیتی هستند و در روابط $M_0=M_0^2$ و $M_1=M_1^2$ صدق می‌کنند. بنابراین رابطه‌ی تمامیت برای دو عملگر به صورت زیر است:

$$I=M_0^\dagger M_0+M_1^\dagger M_1=M_0+M_1$$

در اینجا فرض می‌کنیم که حالت سیستمی که قرار است اندازه‌گیری شود به صورت زیر می‌باشد

$$|\psi\rangle=a|0\rangle+b|1\rangle$$

از این رو احتمال به دست آوردن نتیجه‌ی m=0 و m=1 به صورت

$$P(0)=\langle\psi|M_0^{\dagger}M_0|\psi\rangle=\langle\psi|M_0|\psi\rangle=|a|^2$$

$$P(1)=\langle\psi|M_1^{\dagger}M_1|\psi\rangle=\langle\psi|M_1|\psi\rangle=|b|^2 \qquad (۱۴-۱)$$

خواهد بود. بنابراین به علت داشتن دو نتیجه بعد از فرآیند اندازه‌گیری، دو حالت کوانتومی به دست آمده به صورت زیر خواهند بود:

$$|\psi'\rangle=\frac{M_0|\psi\rangle}{|a|}=\frac{a}{|a|}|0\rangle$$

$$|\psi'\rangle=\frac{M_1|\psi\rangle}{|b|}=\frac{b}{|b|}|1\rangle \qquad (۱۵-۱)$$

در این رابطه می‌توان (مثلاً) عبارات $\frac{a}{|a|}$ و $\frac{b}{|b|}$ را برابر با یک قرار داد و حالت‌های $|0\rangle$ و $|1\rangle$ را بعد از اندازه‌گیری به دست آورد [۴].

فصل دوم

درهم‌تنیدگی و فرآیندهای انتقال

۲-۱ درهم‌تنیدگی

۲-۱-۱ مقدمه

درهم تنیدگی کوانتومی[۱] یکی از مفاهیم مهم مکانیک کوانتومی می‌باشد که مشابه کلاسیکی ندارد. این پدیده موضوعی است که اخیراً به عنوان منبعی با ارزش، مورد توجه کسانی که به نظریه‌ی کوانتومی علاقمند هستند، قرار گرفته است. با به_کارگیری حالات درهم‌تنیده‌ی کوانتومی قادر به انجام اموری می‌شویم که در دنیای کلاسیکی، سخت و یا غیر ممکن هستند.

این مفهوم بیان می‌دارد که اگر دو ذره‌ی درهم‌تنیده را میلیونها کیلومتر از یکدیگر دور کنیم و روی یکی از آن دو ذره اندازه‌گیری انجام دهیم، در همان لحظه (و به طور آنی)، حالت ذره‌ی دوم نیز تحت تأثیر قرار می‌گیرد. به عبارت دیگر، آن دو ذره (ظاهراً) با سرعتی بالاتر از سرعت نور و به طور آنی، تحت تأثیر یکدیگر قرار می‌گیرند و در عین حال این رویداد با پذیرفتن قضیه‌ی عدم علامت‌دهی[۲]، اصل نسبیت خاص انیشتین را نقض نمی‌کند. به عبارت دیگر، در این بین هیچ اطلاعاتی مبادله نمی-شود و با اندازه‌گیری بر روی یکی از آن‌ها نمی‌توان هیچ گونه اطلاعاتی در مورد سیستم دیگر کسب نمود و تنها پیامد آن، تأثیر آنی بر روی حالت ذره‌ی دیگر است. انیشتین این موضوع را عملکرد شبح-وار[۳] (روح مانند) در فواصل زیاد نامید که شبیه به ارتباط دو تکه‌ی درهم‌تنیده توسط سیم‌های نامرئی است که ما هیچ اطلاعی از آن‌ها نداریم، اما برای محاسبات کوانتومی یک اصل کلی به شمار می‌آیند.

پدیده‌ی شگفت‌انگیز درهم‌تنیدگی در نظریه‌ی کوانتومی تحول عظیمی به وجود آورده و به تبع آن، نتایجی را نیز در رایانه‌های کوانتومی به دنبال داشته است. از نتایج بسیار مهم پدیده‌ی درهم‌تنیدگی کوانتومی این است که موضعیت[۴] را نقض کرده و ثابت می‌کند که ماهیت نظریه‌ی کوانتومی، ناموضعی[۵] می‌باشد [۱].

---

[۱] Quantum Entanglement

[۲] No-signaling

[۳] Spooky Action

[۴] Locality

[۵] Nonlocal

۲-۱-۲ تعریف: فرض کنید سیستم M از دو زیر سیستم A و B تشکیل شده است، $|\psi_{AB}\rangle$ حالت سیستم و $|i\rangle_A$ و $|\mu\rangle_B$ حالت‌های مربوط به هر یک از این زیر سیستم‌ها هستند. با فرض اینکه ρ_A و ρ_B ماتریس‌های چگالی مربوط به A و B باشند، ψ_{AB} را جداپذیر می‌گوییم اگر بتوان ماتریس چگالی آن را به صورت زیر نوشت:

$$\rho_{AB} = \sum a_{i\mu}\, \rho_A^i \otimes \rho_B^\mu \qquad (۱-۲)$$

که $a_{i\mu}$ بیانگر احتمال حضور سیستم در حالت i ام می‌باشد.

اگر ماتریس چگالی $|\psi_{AB}\rangle$ را نتوان به صورت حاصلضرب ماتریس چگالی زیر سیستم‌ها نوشت آن را درهم‌تنیده می‌نامند. ویژگی اصلی درهم‌تنیدگی اینست که چون ماتریس‌های چگالی ρ_A و ρ_B (در حالت کلی) خالص نیستند و نیز نمی‌توان حالت کلی سیستم را بصورت حاصلضرب حالت‌های مجزا نوشت، همچنین فضای هیلبرت یک حالت درهم‌تنیده بصورت $H_A \otimes H_B$ است که نمی‌توان آن را بصورت $|i\rangle_A |\mu\rangle_B$ نوشت، لذا در سیستم‌های درهم‌تنیده، اندازه‌گیری بر روی قسمتی از سیستم بر روی کل سیستم اثر (آنی) خواهد گذاشت. بر این اساس (و نیز به دلیل آنکه اندازه‌گیری باعث فروریزش سیستم مرکب می‌شود) هر اندازه‌گیری که عامل مزاحم به منظور کسب اطلاعات انجام دهد منجر به اختلال در سیستم شده و لذا می‌توان به وجود استراق‌سمع‌کننده پی برد.

۲-۱-۳ نامساوی بل

برای مخابره‌ی اطلاعات، از اطلاعات کوانتومی شامل درهم‌تنیدگی، عدم کپی سازی و نیز عملیات دیگری که انجام آنها از لحاظ کلاسیک امکانپذیر نیست، استفاده می‌شود.

حالت دو کیوبیتی زیر را در نظر بگیرید:

$$|s\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \qquad (۲-۲)$$

که در آن $|0\rangle$ معادل حالتی است که اسپین در جهت مثبت محور z قرار دارد و $|1\rangle$ معادل با جهت منفی آن می‌باشد. فرض کنید که کیوبیت اول در اختیار آلیس و کیوبیت دوم دست باب می‌باشد. اگر

آلیس اسپین کیوبیت خود را در راستای z اندازه بگیرد، احتمال بدست آوردن اسپین بالا یا پایین $\frac{1}{2}$ است ولی چنانچه وی طی اندازه‌گیری، اسپین ذره‌اش را در حالت بالا (پایین) بیابد، به این نتیجه میرسد که اسپین کیوبیت باب حتماً در حالت پایین (بالا) خواهد بود. این موضوع بیانگر نوعی همبستگی بین این دو کیوبیت است (این همبستگی کلاسیک نیست). برای روشن شدن این مطلب، ابتدا رابطه‌ی (۲-۲) را در پایه‌ی x ($|+\rangle$ و $|-\rangle$) می‌نویسیم. با توجه به اینکه :

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

$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \qquad (۳-۲)$$

داریم:

$$|s\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) \qquad (۴-۲)$$

حال اگر آلیس به طور دلخواه $\hat{s}_x$ یا $\hat{s}_z$ را اندازه‌گیری کند ولی باب فقط توانایی اندازه‌گیری $\hat{s}_x$ را داشته باشد، دو حالت ممکن است رخ بدهد:

الف) آلیس و باب هر دو $\hat{s}_x$ را اندازه‌گیری کنند: در اینصورت اگر نتیجه‌ی اندازه‌گیری آلیس + باشد، نتیجه‌ی اندازه‌گیری باب حتماً − خواهد بود. یعنی یک همبستگی کامل بین اندازه‌گیری‌های آلیس و باب وجود دارد.

ب) آلیس $\hat{s}_z$ و باب $\hat{s}_x$ را اندازه‌گیری کند: در اینصورت مستقل از نتیجه‌ی اندازه‌گیری آلیس، باب با احتمال $\frac{1}{2}$، نتیجه‌ی + یا − به دست می‌آورد و هیچ همبستگی بین نتیجه‌ی اندازه‌گیری‌های آلیس و باب دیده نمی‌شود. بنابراین وجود همبستگی بین نتایج، بستگی به این دارد که آلیس و باب چه اندازه‌گیری‌هایی انجام دهند. در مکانیک کوانتومی، اندازه‌گیری یک فرآیند گزینشی[۱] است یعنی وقتی

[۱] Selective Procedure

که آلیس حالت کیوبیت خود را $|+\rangle$ می‌بیند، کل سیستم حالت $|+-\rangle$ را گزینش کرده است و بنابراین اگر باب $\hat{s}_x$ کیوبیتش را اندازه بگیرد، حتماً – به‌دست خواهد آورد.

بسیاری از فیزیک‌دانان مانند انیشتین این تفسیر مکانیک کوانتومی از درهم‌تنیدگی را نپذیرفتند. انیشتین می‌خواست توصیف کاملی از طبیعت ارائه دهد. از نگاه وی نظریه‌ی کامل نظریه‌ای است که هر عنصر از واقعیت در آن قابل توصیف باشد و طبق تعریف وی، یک خاصیت فیزیکی در صورتی عنصری از واقعیت است که قبل از اندازه‌گیری بتوان مقدار آن را با قطعیت پیش‌بینی کرد (واقعیت-گرایی[۱]). اصل دیگری که انیشتین به آن معتقد بود اصل موضعیت است که به صورت ذیل بیان می-گردد [۳]:

– فرض کنید که دو سیستم A و B با یکدیگر همبسته و سپس جدا می‌شوند. هرگونه اندازه‌گیری بر روی سیستم A، به هیچ‌وجه حالت سیستم B را (که به صورت فضایی از A جدا شده) مختل نمی‌کند.

در سال ۱۹۳۵ انیشتین به همراه پودولسکی[۲] و روزن[۳]، نظریات خود را در مقاله‌ای منتشر کردند که به باطل نمای EPR معروف شد [۵]. چند سال بعد بل[۴] نشان داد که برقرار بودن اصل موضعیت انیشتین، سبب می‌شود که بین نتایج اندازه‌گیری‌های آزمایش‌های همبستگی، نامساوی آزمون‌پذیری وجود داشته باشد [۶]. این نامساوی به نامساوی بل معروف است و برای بدست آوردن آن دو فرض اساسی زیر لازم است:

۱) خواصی که اندازه‌گیری می‌شوند خصلت‌های واقعی هستند. یعنی مقدار کمیت‌های فیزیکی مستقل از انجام آزمایش‌اند.

۲) اصل موضعیت انیشتین

برای به دست آوردن نامساوی بل فرض کنید آلیس و باب به اندازه‌ی کافی از هم دور هستند. شخص سومی مانند ایو، دو ذره در حالت (۲-۲) تهیه می‌کند و این توانایی را نیز دارد که با تکرار

[۱] Realism
[۲] Podolsky
[۳] Rosen
[۴] J. S. Bell

عملیات، ذرات مشابه بسازد. ایو یکی از دو ذره را برای باب و دیگری را برای آلیس می‌فرستد و آلیس قادر است که دو خصلت واقعی ذره‌ی خودش مثل A و B را اندازه‌گیری کند. بنابراین به طور کاملاً تصادفی یکی از این مشخصه‌ها را انتخاب و اندازه‌گیری می‌نماید. فرض کنید نتیجه‌ی هر اندازه‌گیری $+1$ یا -1 باشد. یعنی $A=\pm1$ و $B=\pm1$. باب هم می‌تواند خصلت‌های واقعی C و D را برای ذره خویش اندازه بگیرد به طوریکه $C=\pm1$ و $D=\pm1$. و او نیز به طور کاملاً تصادفی خصلت C یا D را برای اندازه‌گیری کردن انتخاب می‌نماید. فرض کنید که آلیس و باب به طور همزمان بر روی ذرات خود اندازه‌گیری انجام دهند و چون آلیس و باب خیلی از هم دورند طبق اصل موضعیت، اندازه‌گیری آلیس نمی‌تواند تأثیری بر روی نتیجه‌ی اندازه‌گیری باب (و نیز بالعکس) داشته باشد. حال عبارت زیر را محاسبه می‌کنیم:

$$AC+BC+BD-AD=(A+B)C+(B-A)D$$

از آنجا که $A=\pm1$ و $B=\pm1$ ، پس یا $(A+B)=0$ است یا $(A-B)=0$ و با توجه به اینکه $C=\pm1$ و $D=\pm1$ خواهیم داشت:

$$AC+BC+BD-AD=\pm2 \qquad (۵-۲)$$

احتمال اینکه قبل از اندازه‌گیری، سیستم در حالت خاصی باشد عبارتست از $P(A,B,C,D)$. بنابراین داریم:

$$\begin{aligned}\text{avg}^{1}\ (AC+BC+BD-AD) &= \sum_{A,B,C,D} P(A,B,C,D)(AC+BC+BD-AD) \\ &\le \sum_{A,B,C,D} 2P(A,B,C,D)=2 \qquad (۶-۲)\end{aligned}$$

با توجه به اینکه تابع احتمال کاهیده[۲] به صورت زیر تعریف می‌شود

$$P(A,C)=\sum_{B,D}P(A,B,C,D) \qquad (۷-۲)$$

می‌توان نتیجه گرفت که:

[۱] Average
[۲] Reduced Probability

$$\sum_{A,B,C,D} P(A,B,C,D)\ \mathrm{AC} = \sum_{A,C} AC\ P(A,C) = \mathrm{avg\ (AC)} \qquad (۸-۲)$$

و در نهایت با توجه به روابط (۲-۶) و (۲-۸) خواهیم داشت:

$$\mathrm{avg\ (AC) + avg\ (BC) + avg\ (BD) - avg\ (AD)} \le 2 \qquad (۹-۲)$$

این رابطه، نامساوی بل می‌باشد که اغلب به نامساوی CHSH مشهور است (یک نامساوی آزمایش‌پذیر می‌باشد) و اولین آزمون (واقعی) است که کلازر[۱] و فریدمن[۲] در رابطه با نامساوی بل ارائه دادند [۷]. (این رابطه قسمتی از یک مجموعه بزرگتر از نامساوی‌های موسوم به نامساوی‌های بل می‌باشد.) اگر آلیس و باب چند بار آزمایش را تکرار کنند و سپس با هم تماس بگیرند و حالت‌هایی را که آلیس، A و باب، C اندازه گرفته است، با هم مرور کنند می‌توانند مقدار متوسط AC را محاسبه نمایند و به این ترتیب سمت چپ رابطه‌ی (۲-۹) محاسبه می‌گردد و می‌توان نامساوی بل را بررسی نمود.

حال این مسئله را از دیدگاه مکانیک کوانتومی بررسی می‌کنیم. فرض کنید ایو یک حالت تک تایی اسپینی که با رابطه‌ی زیر داده می‌شود را آماده کرده و اسپین اول را برای آلیس و اسپین دوم را برای باب ارسال می‌کند:

$$|s\rangle = \frac{1}{\sqrt{2}}\left(|10\rangle - |01\rangle\right) \qquad (۱۰-۲)$$

و نیز فرض کنید مشاهده‌پذیرهایی که آلیس و باب اندازه می‌گیرند به شکل زیر باشند:

$$A = \sigma_z^{(1)} \qquad ; B = \sigma_x^{(1)}$$

$$C = \frac{-1}{\sqrt{2}}(\sigma_z^{(2)} + \sigma_x^{(2)}) \qquad ; D = \frac{1}{\sqrt{2}}(\sigma_z^{(2)} - \sigma_x^{(2)}) \qquad (۱۱-۲)$$

با کمی محاسبه [۶] نتیجه می‌شود که:

$$\langle AC\rangle = \frac{1}{\sqrt{2}}; \quad \langle BC\rangle = \frac{1}{\sqrt{2}}; \quad \langle BD\rangle = \frac{1}{\sqrt{2}}; \quad \langle AD\rangle = \frac{1}{\sqrt{2}} \qquad (۱۲-۲)$$

و بنابراین

[۱] John Clauser
[۲] Stuart Freedman

$$\langle AC\rangle+\langle BC\rangle+\langle BD\rangle+\langle AD\rangle=2\sqrt{2} \qquad (۱۳-۲)$$

که با نامساوی بل متناقض است. بنابراین پیش‌بینی مکانیک کوانتومی و نامساوی بل با یکدیگر تناقض دارند. آزمایش‌های زیادی نشان داده‌اند که حالت‌های (۲-۱۰) نامساوی بل را نقض می‌کند. لذا پیش-بینی مکانیک کوانتومی با آزمایش سازگار است. و این بدین معناست که حداقل یکی از فرض‌هایی که منجر به نامساوی بل شده است، صحیح نمی‌باشد.

سوالی که مطرح می‌شود اینست که آیا علاوه بر حالت (۲-۱۰)، حالت‌های دیگری هم وجود دارند که نامساوی بل را نقض کنند؟ برای بررسی این مطلب، بردار حالت کلی یک سیستم دوتایی را در نظر می‌گیریم:

$$|\psi\rangle=a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle \qquad (۱۴-۲)$$

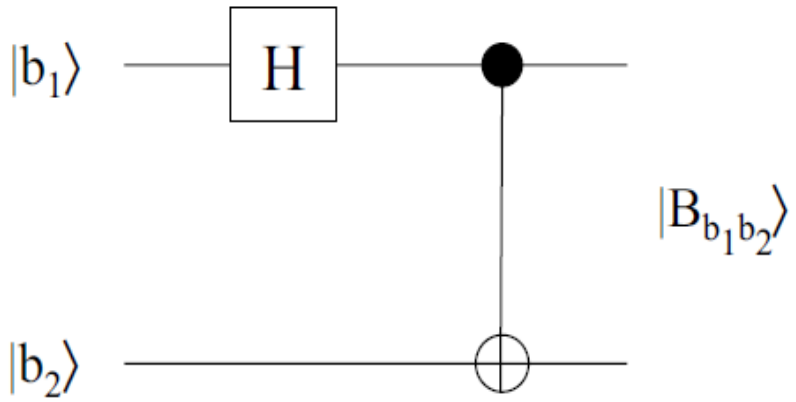
اگر بتوان این حالت را به صورت $|\psi\rangle=|\psi\rangle_1\otimes|\psi\rangle_2$ نوشت (در حالیکه $|\psi\rangle_1$ و $|\psi\rangle_2$ حالتهای مربوط به دو ذره‌اند)، این حالت تفکیک‌پذیر[۱] و در غیر اینصورت درهم‌تنیده است. و نیز چنانچه $|\varphi\rangle\in H_B$ ، $|\psi\rangle\in H_A$ و $|\chi\rangle=|\psi\rangle\otimes|\varphi\rangle\in H_A\otimes H_B$ آنگاه $|\chi\rangle$ یک حالت جدایی‌پذیر است. همچنین اگر در رابطه‌ی فوق $ad=bc$ باشد می‌توان این حالت را به صورت ضرب تانسوری حالت ذره‌ی اول در حالت ذره‌ی دوم نوشت (حالت تفکیک‌پذیر). از طرفی تمام حالت‌های درهم‌تنیده نامساوی بل را نقض می‌کنند [۸]. لذا نقض نامساوی بل در مکانیک کوانتومی واقعیتی دور از دسترس نیست. بعضی حالت‌های کوانتومی مثل حالت (۲-۱۰) دارای درهم‌تنیدگی بیشینه هستند. برای این حالت‌ها سمت چپ رابطه‌ی (۲-۹) برابر با $2\sqrt{2}$ است که بیشترین مقداری است که توسط مکانیک کوانتومی پیش‌بینی می‌شود [۸].

آنچه که واضح است اینست که اگر بخواهیم برای انتقال اطلاعات از ویژگی‌های مکانیک کوانتومی استفاده کنیم باید حالت‌های درهم‌تنیده را به کار گیریم و احتمالاً بیشترین تفاوتی که با حالت کلاسیکی حاصل می‌شود نتیجه‌ی استفاده از حالت‌هایی با بیشینه‌ی درهم‌تنیدگی خواهد بود.

[۱] Product or Separable States

۲-۱-۴ مدل ریاضی درهم تنیدگی کوانتومی

با استفاده از گیت‌های کوانتومی، می‌توان یک زوج فوتون درهم‌تنیده را به صورت ریاضی و طرح‌وار بیان کنیم [۹]. مدار مورد نظر متشکل از دو گیت هادامارد و C-NOT[۱] می‌باشد که به صورت سری قرار گرفته‌اند. اگر ورودی این مدار را یکی از حالات $|00\rangle$، $|01\rangle$، $|10\rangle$ و $|11\rangle$ در نظر بگیریم، چهار حالت درهم‌تنیده‌ی متفاوت به نام حالات بل به دست خواهد آمد.



شکل ۲-۱: مدار کوانتومی به وجود آورنده‌ی حالات بل

ورودی را در حالت اول، به صورت $|b_1\rangle\otimes|b_2\rangle=|b_1b_2\rangle=|00\rangle$ فرض کرده و خروجی مدار را محاسبه می‌کنیم. حالت $|0\rangle$ پس از عبور از گیت هادامارد به حالت زیر تبدیل می‌شود:

$$|0\rangle\rightarrow\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$

در نتیجه، قبل از تأثیر گیت C-NOT حالت کوانتومیِ ترکیبی عبارت است از:

---

[۱] گیت‌های هادامارد (Hadamard) و C-NOT دو نوع گیت کوانتومی‌اند: گیت هادامارد به منظور تهیه‌ی حالت‌های برهم‌نهی به کار می‌رود، ماتریس آن به صورت $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ و اثر آن بر روی حالت‌های پایه‌ی محاسباتی ($|0\rangle$ و $|1\rangle$) به صورت $H|0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ و $H|1\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ می‌باشد. در گیت C-NOT بسته به اینکه کیوبیت کنترلی (کیوبیت اول) در حالت مورد نظر چه باشد دو نتیجه در بر خواهد داشت: اگر کیوبیت کنترلی 0 باشد هیچ اتفاقی نمی‌افتد ولی چنانچه کیوبیت کنترلی 1 باشد، کیوبیت هدف (کیوبیت دوم) واورن می‌شود.

$$|00\rangle \xrightarrow{(H\otimes I)|00\rangle} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)$$

در اثر عبور این حالت کوانتومی از گیت C-NOT، حالت درهم‌تنیده‌ی زیر حاصل می‌شود:

$$\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle) \xrightarrow{\text{C-NOT}} \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) = |\varphi^+\rangle$$

چنانچه ورودی را سه حالت دیگر $|01\rangle$، $|10\rangle$و $|11\rangle$ در نظر بگیریم، سه حالت دیگر بل به دست می‌آیند و لذا به طور جمع‌بندی، نتیجه می‌شود که چهار حالت بل را که دربخش قبل معرفی کردیم حالتهایی با درهم‌تنیدگی بیشینه[۱] اصلی هستند [۳].

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

$$|10\rangle \to \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle) = |\varphi^-\rangle$$

$$|01\rangle \to \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) = |\psi^+\rangle$$

$$|11\rangle \to \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) = |\psi^-\rangle. \qquad (۱۶-۲)$$

۲-۱-۵ ناموضعیت و درهم‌تنیدگی حالات کوانتومی

حالت درهم‌تنیده‌ای مانند

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \qquad (۱۷-۲)$$

را در نظر می‌گیریم. فرض می‌کنیم که کیوبیت اول در اختیار آلیس و دومی در اختیار باب می‌باشد. حالت‌های $|0\rangle$ و $|1\rangle$ را برای نشان دادن ویژه حالت‌های اسپین در راستای Z به کار برده‌ایم. همانطور که قبلاً نیز اشاره شد، اگر آلیس بر روی ذره‌ی خود یک اندازه‌گیری در راستای Z انجام داده و مقدار ۰ را به دست آورد، می‌تواند به طور قطع نتیجه‌ی اندازه‌گیری باب را پیش‌بینی کند زیرا باب در صورت اندازه‌گیری در همین پایه به طور قطع مقدار ۱ را به دست خواهد آورد. بالعکس اگر آلیس مقدار ۱ را به دست آورد، به طور قطع می‌تواند بگوید که باب در اندازه‌گیری خود، نتیجه‌ی ۰ را به دست خواهد

[۱] Maximally Entangled States

آورد. این قدرت پیش‌بینی نتیجه‌ی باب توسط آلیس (و بالعکس)، حتی در وضعیتی که آلیس و باب فاصله‌ی فضاگونه با هم دارند نیز برقرار است. از آنجا که دو رویداد با فاصله‌ی فضاگونه هیچ گونه رابطه‌ی علی با یکدیگر ندارند، به نظر می‌رسد که یک اثر ناموضعی در مکانیک کوانتومی وجود دارد که هیچ نوع سابقه‌ای در فیزیک کلاسیک ندارد. هم‌چنین به نظر می‌رسد که این نوع پدیده‌ها به نوعی نسبیت خاص را نقض می‌کنند. اما می‌توان نشان داد که آلیس با اندازه‌گیری‌های خود تنها می‌تواند نتایج آزمایش‌های باب را پیش‌بینی کند و به هیچ‌وجه نمی‌تواند علامت یا سیگنالی را برای باب مخابره کند (عدم علامت‌دهی). برای فهم و اثبات این موضوع کافیست که ماتریس چگالی باب را قبل و بعد از اندازه‌گیری به دست آورده و با هم مقایسه کنیم.

بدین منظور فرض می‌کنیم حالتی که در اختیار آلیس و باب است، حالتی کلی به شکل زیر باشد:

$$|\psi\rangle = \sum_{i,\alpha} \psi_{i\alpha} |\, i, \alpha\rangle \qquad (۱۸-۲)$$

بنابراین ذره‌ای که در دست باب قرار دارد در حالت زیر خواهد بود:

$$\rho_B = Tr_A(|\psi\rangle\langle\psi|) \qquad (۱۹-۲)$$

حال فرض می‌کنیم که آلیس یک اندازه‌گیری تصویری با عملگرهای $\{P_m\}$ بر روی ذره‌ی خود انجام دهد. در این صورت حالت دو ذره به حالت زیر تبدیل می‌شود:

$$\rho' = \sum_m (P_m \otimes I)|\psi\rangle\langle\psi|(P_m^\dagger \otimes I) \qquad (۲۰-۲)$$

بعد از اندازه‌گیری، حالت ذره‌ای که در دست باب است برابر خواهد بود با:

$$\rho'_B = Tr_A(\rho') = Tr_A(\sum_m (P_m \otimes I)|\psi\rangle\langle\psi|(P_m^\dagger \otimes I)) \qquad (۲۱-۲)$$

از خاصیت دوره‌ای بودن تابع رد (که در آن مطابق رابطه‌ی زیر، عملگرهای X و Z روی فضای A عمل کرده و عملگر Y نیز روی هر دو فضای A و B عمل می‌کند) در رابطه‌ی بالا استفاده می‌کنیم:

$$Tr_A((X \otimes I)Y(Z \otimes I)) = Tr_A((Z \otimes I)(X \otimes I)Y) \qquad (۲۲-۲)$$

بنابراین (۲-۲۰) را می‌توان به شکل زیر بازنویسی کرد:

$$\rho'_B = Tr_A(\sum_m (P_m^\dagger \otimes I)(P_m \otimes I)|\psi\rangle\langle\psi|) = Tr_A(|\psi\rangle\langle\psi|) = \rho_B \qquad (۲۳-۲)$$

از این رو حالت ذره‌ای که در دست باب است با اندازه‌گیری‌های آلیس تغییر نمی‌کند و در نتیجه اندازه‌گیری‌های آلیس به هیچ‌وجه باعث تغییری در حالت ذره‌ی باب نخواهند شد و در نتیجه هیچ نوع علامت یا اطلاعی به باب مخابره نمی‌شود. این امر ادعای ما را اثبات می‌کند که ناموضعیت به معنای نقض نسبیت نیست. با این وجود، حالت‌های درهم‌تنیده یعنی حالت‌هایی مانند (۲-۱۷) که نشان-دهنده‌ی ناموضعیت در مکانیک کوانتومی هستند، خصلت‌های ناآشنایی دارند که آن‌ها را شایسته‌ی مطالعات جدی و وسیع می‌کند [۱].

۲-۱-۶ خالص سازی درهم‌تنیدگی[۱]

فرض کنید که سیستم A توسط ماتریس چگالی ρ توصیف می‌شود. آیا می‌توان سیستمی مثل B و حالتی از سیستم مرکب AB مثل $|\psi\rangle_{AB}$ را چنان یافت که:

$$\rho = Tr_B(|\psi\rangle_{AB}\langle\psi|) \qquad (۲۴-۲)$$

باشد. اگر چنین حالتی را پیدا کنیم، حالت $|\psi\rangle_{AB}$ را حالت خالص شده‌ی ماتریس چگالی ρ می-نامیم. برای اینکه حالت خالص شده‌ی یک ماتریس چگالی ρ_A با ویژه مقادیر p_i را پیدا کنیم می-بایست به ترتیب زیر عمل کنیم:

سیستم B را در نظر می‌گیریم که بعد فضای هیلبرت آن یعنی H_B حداقل با بعد H_A یکی باشد. هرگاه بردارهای $\{|i\rangle\}$ یک پایه‌ی متعامد برای سیستم A باشند، آنگاه برای $|\psi\rangle_{AB}$ خواهیم داشت:

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}\,|i,\hat{i}\rangle \qquad (۲۵-۲)$$

که در آن $\{|\hat{i}\rangle\}$ ، یک مجموعه بردار متعامد یکه برای فضای H_B هستند. در این صورت $|\psi\rangle_{AB}$ حالت خالص شده‌ی ρ_A است. در پایان متذکر می‌شویم که خالص‌سازی درهم‌تنیدگی، از مفاهیم

[۱] Entanglement Purification

اساسی نظریه‌ی اطلاعات کوانتومی به شمار می‌آید و در فصل آخر نیز از آن به عنوان یک موضوع مهم استفاده می‌گردد.

۲-۱-۷ تجزیه‌ی اشمیت[۱]

حالت یک سیستم کوانتومی را همواره نمی‌توان با یک بردار حالت خاص نشان داد. برخی از سیستم‌های کوانتومی آمیزه‌ای از حالت‌هایی هستند که با بردارهای حالت $|\psi\rangle$ توصیف می‌شوند. لذا برای توصیف این سیستم‌ها ناگزیر از ماتریسی به صورت زیر استفاده می‌کنیم

$$\rho = \sum_i \alpha_i |\psi_i\rangle\langle\psi_i| \qquad (۲۶-۲)$$

که در آن α_i احتمال حضور $|\psi_i\rangle$ در آنسامبل حالت‌هاست. ماتریس فوق، ماتریس چگالی سیستم خوانده می‌شود. بنابراین می‌توان گفت به طور کلی در مکانیک کوانتومی حالت یک سیستم با یک ماتریس چگالی توصیف می‌گردد.

دسته‌ای از ماتریس‌های چگالی وجود دارند که در آن‌ها $\rho^2 = \rho$ می‌باشد. این ماتریس‌ها مربوط به حالت‌های خالص[۲] هستند. در حقیقت می‌توان حالت این گونه سیستم‌ها را با یک بردار حالت مشخص نمود. دسته‌ی دیگر، سیستم‌هایی هستند که زیر سیستم‌های آن‌ها درهم‌تنیده‌اند در این حالت به کل سیستم می‌توان یک بردار خاص اختصاص داد ولی هر یک از زیر سیستم‌ها با یک بردار حالت مشخص، تعیین نمی‌شوند. مانند حالت زیر:

$$|s\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \qquad (۲۷-۲)$$

برای آنکه بتوان همبستگی بین زیرسیستم‌ها را بهتر درک نمود، تجزیه‌ی اشمیت را معرفی می‌نماییم:

---

[۱] Schmidt Decomposition
[۲] Pure states

فرض کنید که یک سیستم کوانتومی از دو بخش A و B تشکیل شده است. بردار حالت این سیستم متعلق به فضای $H_A \otimes H_B$ است. اگر H_A، N بعدی و H_B، M بعدی باشد، حالت کلی این سیستم به شکل زیر نوشته می‌شود:

$$|\psi\rangle = \sum_n \sum_m C_{nm} |a_n\rangle |b_m\rangle \qquad (۲۸-۲)$$

که $\{|a_n\rangle\}_{n=1}^{M}$ ($\{|b_n\rangle\}_{n=1}^{M}$) پایه‌های متعامد و یکه‌ی زیرفضای A (B) می‌باشد. همچنین فرض می‌کنیم که M > N و برای بدست آوردن تجزیه‌ی اشمیت مراحل زیر را طی می‌کنیم [۱]:

۱) ماتریس چگالی توصیف کننده‌ی سیستم کل را بدست می‌آوریم:

$$\rho = |\psi\rangle\langle\psi| = \sum_{n,m,p,q} \rho_{nmpq} |a_n\rangle\langle a_p| \otimes |b_m\rangle\langle b_q| \qquad (۲۹-۲)$$

که در آن $\rho_{nmpq} = C_{nm} C_{pq}^*$.

۲) ماتریس چگالی زیرسیستم A را با ردگیری روی زیر فضای H_B بدست می‌آوریم:

$$\rho_A = Tr_B(\rho) = \sum_{n,m} \sum_p \rho_{nmpq} |a_n\rangle\langle a_p| \qquad (۳۰-۲)$$

۳) حال ماتریس چگالی ρ_A را قطری می‌نماییم. اگر پایه‌ی $|a'_n\rangle$ از زیر فضای H_A، پایه‌ی قطری کننده‌ی ماتریس ρ_A باشد، داریم:

$$\rho_A = \sum_n |g_n|^2 |a'_n\rangle\langle a'_n| \qquad (۳۱-۲)$$

حال حالت $|\psi\rangle$ را بر حسب $|a'_n\rangle$ها می‌نویسیم:

$$|\psi\rangle = \sum_{n,m} C'_{nm} |a'_n\rangle |b_m\rangle \qquad (۳۲-۲)$$

که در آن

$$\sum_m C'_{nm} C'_{pm} = |g_n|^2 \delta_{np} \qquad (۳۳-۲)$$

۴) سپس ترکیبی از پایه‌های متعامد $|b_m\rangle$ می‌سازیم:

$$|b'_l\rangle = \sum_m \frac{C'_{lm}}{g_l} |b_m\rangle \qquad (۳۴-۲)$$

تبدیل $\{|b_m\rangle\}$ به $\{|b'_l\rangle\}$ یک تبدیل یکانی است. بنابراین $\{|b'_l\rangle\}$ ها یک پایه‌ی متعامد یکه برای زیرفضای H_B تشکیل می‌دهند.

۵) در مرحلی آخر، حالت $|\psi\rangle$ را بر حسب پایه‌های جدید $|b'_l\rangle$ می‌نویسیم و به تجزیه‌ی اشمیت حالت $|\psi\rangle$ می‌رسیم:

$$|\psi\rangle = \sum_n g_n |a'_n\rangle|b'_n\rangle \qquad (۳۵-۲)$$

در این رابطه g_nها ضرایب اشمیت نامیده می‌شوند که از ماتریس چگالی کاهیده‌ی $\rho_A = Tr_B(|\psi\rangle\langle\psi|)$ محاسبه می‌گردد. همچنین تعداد ویژه مقادیر غیر صفر g_n از ماتریس ρ_A را عدد اشمیت می‌نامند. عدد اشمیت نیز می‌تواند در تعیین درهم‌تنیدگی به کار رود به طوریکه:

۱- عدد اشمیت ۱ است اگر و تنها اگر حالت سیستم درهم‌ناتنیده (تفکیک پذیر) باشد.

۲- چنانچه حالت درهم‌تنیده باشد، آنگاه می‌بایست عدد اشمیت بزرگتر از ۱ شود.

تجزیه‌ی اشمیت دارای دو نتیجه‌ی بسیار مهم می‌باشد [۱۰]:

الف) اگر با استفاده از رابطه‌ی (۲-۳۵) حالت کاهش یافته‌ی زیر سیستم‌های A و B را بنویسیم، خواهیم داشت:

$$\rho_A = \sum_n |g_n|^2 |a'_n\rangle\langle a'_n|$$

$$\rho_B = \sum_m |g_m|^2 |b'_m\rangle\langle b'_m| \qquad (۳۶-۲)$$

یعنی هر دو زیر سیستم طیف مثبت یکسانی دارند.

ب) یک زیر سیستم N بعدی، نمی‌تواند با بیش از N حالت متعامد یکه از یک زیر سیستم دیگر درهم‌تنیده باشد.

در این بخش به مفهوم حالت‌های درهم‌تنیده اشاره کردیم. در بخش بعد نشان می‌دهیم که این حالت‌ها چگونه برای مبادله‌ی اطلاعات کوانتومی به کار می‌آیند.

۲-۲ فرآیندهایی برای انتقال اطلاعات کوانتومی

در این بخش می‌خواهیم ببینیم که چگونه مکانیک کوانتومی می‌تواند به شیوه‌ای مؤثر در انتقال اطلاعات کوانتومی به کار گرفته شود. در مخابره‌ی اطلاعات کوانتومی چه از حیث نظری و چه از جنبه‌ی تجربی، پیشرفت‌های به سزایی صورت گرفته است. آنچه که در انتقال اطلاعات کوانتومی نقش اساسی دارد خاصیت غیر موضعی بودن مکانیک کوانتومی و وجود حالت‌های درهم‌تنیده است. در این بخش نمونه‌هایی از فرآیندهایی را خواهیم دید که طی آنها از حالت‌های درهم تنیده برای انتقال اطلاعات استفاده می‌شود. البته هیچ یک از این فرآیندها ناقض نسبیت خاص نیستند. تقریباً تمام آزمایش‌هایی که تا کنون برای فرآیندهای انتقال اطلاعات کوانتومی انجام شده‌اند از حالت‌های درهم-تنیده‌ی قطبش فوتون‌ها استفاده می‌کنند. چنین حالتی معمولاً به شکل زیر است:

$$|\varphi\rangle = \frac{1}{2}(|H,V\rangle + |V,H\rangle) = \frac{1}{2}(|H\rangle_{Alice} \otimes |V\rangle_{Bob}) + (|V\rangle_{Alice} \otimes |H\rangle_{Bob}) \qquad (۳۷-۲)$$

که در آن H و V به ترتیب نشان‌دهنده‌ی قطبش افقی و عمودی فوتون‌ها در یک دستگاه مختصات معین بوده و شاخص‌های آلیس و باب نشان‌دهنده‌ی اینست که فوتون‌ها در دو نقطه‌ی متفاوت تحت کنترل آلیس و باب هستند (ممکن است این دو شخص کیلومترها از هم فاصله داشته باشند). امروزه می‌توان چنین فوتون‌هایی را در آزمایشگاه تولید کرده و سپس از طریق فیبرهای نوری یا هوای آزاد به فاصله‌های دوردست فرستاد. در عمل بسیاری از این زوج فوتون‌ها سالم به مقصد نمی‌رسند. بدین معنی که بسیاری از آن‌ها جذب محیط شده و یا درهم‌تنیدگی آن‌ها در اثر واکنش با محیط از بین می‌رود ولی همواره تعداد قابل توجهی از آن‌ها سالم و دست‌نخورده به مقصد می‌رسند به طوریکه بتوان با آن‌ها فرآیندهای انتقال اطلاعات را انجام داد. می‌توان فرض کرد که مرکزی وجود دارد که این زوج‌های درهم‌تنیده را تولید، و بین افرادی که می‌خواهند فرآیندهای اطلاعات کوانتومی را انجام دهند به اشتراک می‌گذارد.

قبل از بررسی این فرآیندها بهتر است چهار حالت بل را که همگی بیشینه‌ی درهم تنیدگی را داشته و در فرآیند انتقال اطلاعات نقش اساسی دارند، دوباره بیان کنیم. این حالت‌های بل برای کیوبیت‌ها عبارتند از:

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

$$|\varphi_{01}\rangle = |\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\varphi_{10}\rangle = |\varphi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\varphi_{11}\rangle = |\psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad (۳۸-۲)$$

این حالت‌ها یک پایه‌ی متعامد یکه برای فضای دو کیوبیتی تشکیل می‌دهند:

$$\langle \varphi_{mn} | \varphi_{kl} \rangle = \delta_{mk}\delta_{nl} \qquad (۳۹-۲)$$

$$\sum_{m,n} |\varphi_{mn}\rangle\langle\varphi_{mn}| = I \qquad (۴۰-۲)$$

از این پس منظور از اندازه‌گیری در پایه‌ی بل یعنی اندازه‌گیری‌ای که حالت کوانتومی را روی یکی از چهار حالت بل تصویر می‌کند. با این مقدمه‌ی کوتاه می‌توان به بیان فرآیندهای انتقال اطلاعات کوانتومی پرداخت.

۲-۲-۱ فرابرد کوانتومی[۱]

در فرابرد کوانتومی هدف آنست که به کمک پدیده‌ی درهم‌تنیدگی، با مخابره‌ی اطلاعات کلاسیکی- که طبیعتاً با سرعت نور صورت می‌گیرد- حالت کوانتومی یک کیوبیت را به نقطه‌ای دور دست منتقل کنیم. در این انتقال، جرم یا انرژی ذره منتقل نمی‌شود بلکه تنها حالت ذره انتقال می‌یابد. فرض کنید که آلیس فوتون یا الکترونی در اختیار دارد که در حالت $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ قرار دارد و باب که در فاصله‌ی دوری از آلیس قرار گرفته نیز الکترونی در اختیار دارد که در حالتی خاص می‌باشد و قصد

[۱] Quantum Teleportation

دارد با اطلاعاتی که از آلیس دریافت می‌کند کاری کند که الکترونش حالت $|\varphi\rangle$ را بپذیرد (یعنی در واقع حالت کوانتومی ناشناخته‌ی فوق که یک کیوبیت است را از آلیس دریافت کند). مستقیم‌ترین راه برای این کار آنست که آلیس مقدار دو عدد مختلط α و β را به باب مخابره کرده و وی با اعمال یک عملگر کوانتومی، حالت الکترون خود را به حالتی که در دست آلیس است ($|\varphi\rangle$) تبدیل نماید. اما این کار دو اشکال اساسی دارد. اول آنکه مخابره‌ی دو عدد مختلط فوق با دقت بی‌نهایت مستلزم مخابره‌ی بی‌نهایت اطلاعات می‌باشد و بنابراین می‌بایست به ساخت تقریبی حالت اکتفا نمود و دوم اینکه اصولاً معلوم نیست آلیس حالت الکترونی که در اختیار دارد را بداند (یعنی α و β نامعلوم است) و با این وجود بخواهد این حالت را برای باب بفرستد. فرابرد کوانتومی روشی است که با استفاده از درهم-تنیدگی این امکان را فراهم می‌آورد که بتوان حالت‌های ناشناخته و نامعلوم را به نقاط دور دست انتقال داد [11].

فرض کنید که حالت درهم‌تنیده‌ی:

$$|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ab} \qquad (۴۱-۲)$$

بین آلیس و باب به اشتراک گذاشته شده باشد. کیوبیت اول نزد آلیس بوده و با a مشخص می‌شود و کیوبیت دوم نزد باب بوده که با b مشخص می‌گردد. حالت (۲-۴۱) قرار است نقش یک خط ارتباط بین آلیس و باب را بازی کند. حال آلیس حالت $|\varphi\rangle$ (که می‌خواهد مخابره‌اش کند) را به کیوبیت خودش نزدیک می‌کند (برهم‌کنش این دو با هم را محاسبه می‌کند) و در نتیجه حالت زیر به دست می‌آید:

$$|\psi\rangle = |\varphi\rangle|\varphi^+\rangle = (\alpha|0\rangle + \beta|1\rangle)_a \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ab}$$

$$= \frac{1}{2}[|\varphi^+\rangle(\alpha|0\rangle + \beta|1\rangle)_b + |\varphi^-\rangle(\alpha|0\rangle - \beta|1\rangle)_b +$$

$$|\psi^+\rangle(\beta|0\rangle + \alpha|1\rangle)_b + |\psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle)_b] \qquad (۴۲-۲)$$

حال آلیس بر روی دو کیوبیتی که نزد خود دارد یک اندازه‌گیری در پایه‌ی بل انجام می‌دهد. نتیجه‌ی این اندازه‌گیری یکی از چهار حالت $\left|\varphi^{\pm}\right\rangle$ یا $\left|\psi^{\pm}\right\rangle$ است و طبق رابطه‌ی (۲-۴۲)، بسته به نتیجه‌ی اندازه‌گیری آلیس، حالت کیوبیتی‌ای که دست باب است به یکی از حالت‌هایی که در جدول (۲-۱) نشان داده شده کاهش می‌یابد. اگر آلیس نتیجه‌ی اندازه‌گیری خود را برای باب مخابره کند (به صورت کلاسیکی و تنها با انتقال دو بیت کلاسیکی)، باب می‌تواند بسته به اینکه نتیجه‌ی اندازه‌گیری آلیس چیست، با اعمال عملگر مناسب بر روی کیوبیت خویش مطابق جدول (۲-۱)، حالت کیوبیتش را به حالتی که دست آلیس بوده تبدیل نماید. نکته‌ای که در این روش حائز اهمیت است اینست که لازم نیست طرفین هیچ اطلاعاتی از حالت اولیه داشته باشند.

نتیجه‌ی اندازه گیری آلیس	حالت کیوبیت باب	عملگری که باب باید اعمال کند
$\left\|\varphi^{+}\right\rangle$	$\left\|\psi\right\rangle=\alpha\left\|0\right\rangle+\beta\left\|1\right\rangle$	I
$\left\|\varphi^{-}\right\rangle$	$\left\|\psi\right\rangle=\alpha\left\|0\right\rangle-\beta\left\|1\right\rangle$	σ_z
$\left\|\psi^{+}\right\rangle$	$\left\|\psi\right\rangle=\beta\left\|0\right\rangle+\alpha\left\|1\right\rangle$	σ_x
$\left\|\psi^{-}\right\rangle$	$\left\|\psi\right\rangle=-\beta\left\|0\right\rangle+\alpha\left\|1\right\rangle$	σ_y

جدول۲-۱: فرابرد کوانتومی

۲-۲-۲ کد گذاری چگال[۱]

در فرابرد کوانتومی دیدیم که اگر بین آلیس و باب یک زوج درهم‌تنیده به اشتراک گذاشته شده باشد، آنها می‌توانند با مبادله‌ی فقط دو بیت کلاسیکی، یک حالت کوانتومی یعنی یک کیوبیت را مخابره کنند. در این بخش به معرفی عکس این عمل می‌پردازیم: می‌توان با مبادله‌ی یک کیوبیت، اطلاعات مربوط به دو بیت کلاسیکی را انتقال داد [۱۲]. فرض کنید که حالت درهم‌تنیده‌ی:

$$\left|\varphi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right) \qquad (۴۳-۲)$$

[۱] Dense Coding

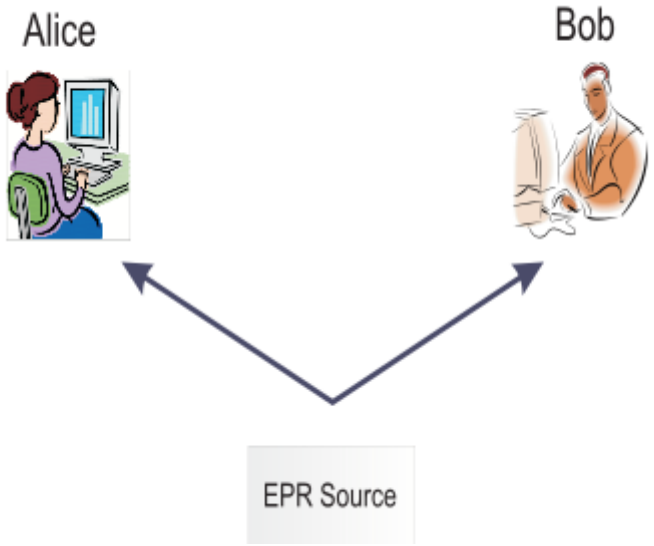
(یک زوج EPR) بین آلیس و باب به اشتراک گذاشته شده است. حال آلیس بسته به اینکه کدام یک از زوج بیت‌ها را بخواهد برای باب ارسال کند یکی از گیت‌های I، σ_x ، σ_y یا σ_z را بر روی کیوبیت خود اعمال می‌کند و تحت این اعمال، حالت به اشتراک گذارده شده به ترتیب زیر تغییر می‌کند:

زوج بیتی که قرار است مخابره شود	عملگری که آلیس اثر می‌دهد	حالت نهایی
00	I	$\|\phi^+\rangle$
01	σ_x	$\|\psi^+\rangle$
10	σ_y	$\|\phi^-\rangle$
11	σ_z	$\|\psi^-\rangle$

جدول۲-۲: کدگذاری چگال

حال آلیس کیوبیت خود را برای باب ارسال می‌کند و باب که اکنون هر دو کیوبیت را در دست دارد، یک اندازه‌گیری در پایه‌ی بل انجام می‌دهد و با توجه به نتیجه‌ی اندازه‌گیری و قراردادشان می‌تواند بفهمد که منظور آلیس ارسال کدام یک از زوج‌های ۰۰، ۰۱، ۱۰ یا ۱۱ بوده است. شاید به نظر برسد که این فرآیند آنچنان کارآمد هم نیست چرا که قبلاً از طریق به اشتراک گذاردن یک حالت بل، یک کیوبیت در دست باب بوده و یک کیوبیت هم آلیس برایش فرستاده است. پس به نظر می‌رسد که برای مبادله‌ی دو بیت کلاسیک از دو کیوبیت استفاده شده است. اما باید توجه داشت که حالت بل می‌تواند توسط یک منبع و یا شخص ثالث، بین آلیس و باب به اشتراک گذاشته شده باشد و نه خود آلیس (شکل ۲-۱). همچنین این حالت‌های درهم‌تنیده می‌توانست مدت‌ها پیش بین آلیس و باب به اشتراک گذارده شود و نه در موقعی که آن‌ها واقعاً می‌خواهند با هم مبادله‌ی اطلاعات انجام دهند. همچنین می‌بایست دقت کرد که اگر آلیس و باب فقط یک زوج کیوبیت به اشتراک گذاشته باشند آنگاه آلیس می‌تواند با ارسال تنها یک کیوبیت، یک حالت از چهار زوج‌ها را به وی اطلاع دهد. اما اگر

حالت به اشتراک گذاشته شده بین آلیس و باب، یک حالت بل در بعد d باشد (کیودیت)، آنگاه آلیس با ارسال یک کیودیت، یک حالت از d^2 را به باب اطلاع خواهد داد. یعنی این فرآیند کارآمدتر خواهد



شکل ۲-۲: منبع EPR: در تمام فرآیندهای مبادله‌ی اطلاعات کوانتومی می‌توان فرض کرد که منبع ثالثی، زوج‌های درهم‌تنیده را در اختیار متقاضیان قرار می‌دهد.

بود. و در نهایت، مهمترین موضوع اینست که وقتی آلیس کیوبیت را برای باب می‌فرستد این کیوبیت با کیوبیت قبلی درهم‌تنیده است و در نتیجه خودش در یک حالت کاملاً مخلوط است. این حالت مستقل از این است که آلیس چه عملی روی کیوبیت انجام داده است و بنابراین کیوبیتی که ارسال می‌شود حامل هیچ‌گونه اطلاعاتی که توسط شخص ثالث قابل حصول باشد نیست [۱].

فصل سوم

توزیع کلید کوانتومی و ارسال التزام‌آور بیت

۳-۱ توزیع کلید کوانتومی(QKD)[۱]

۳-۱-۱ مقدمه

مسلماً بهترین کاربرد شناخته شده از رمزنگاری کوانتومی، توزیع کلید کوانتومی (QKD) است. هدف از ارائه‌ی QKD، تولید و توزیع یک کلید بین طرفین ارتباط است به طوریکه اگر طرفین قصد داشته باشند پیام محرمانه‌ای را به یکدیگر بفرستند تنها راهی که می‌توانند مطمئن باشند هیچ استراق‌سمع کننده‌ای ارسال را کنترل نمی‌کند اینست که یک کلید محرمانه بین خود به اشتراک بگذارند. این کلید، یک رشته بیت تصادفی است که هر دو نفر از آن باخبرند ولی هیچ کس دیگری از آن مطلع نیست. برای ارسال یک پیام، فرستنده، آن را تبدیل به یک رشته بیت کرده، (مثلاً XOR بین هر یک از بیت‌های پیام و بیت‌های کلید را محاسبه کرده (پیام رمزی می‌شود) و سپس نتیجه را برای دریافت کننده می‌فرستد.

اساس رمزنگاری، توزیع کلید محرمانه بین دو کاربر قانونی است که به فاصله‌ی زیادی از هم قرار گرفته‌اند. این عمل در کلاسیک امکانپذیر نیست. علت آنست که ایمنی در رمزنگاری کلاسیکی بر اساس سختی مسائل ریاضی می‌باشد. مثلاً در رمزنگاری‌ای که مبتنی بر تجزیه‌ی اعداد به عوامل اول است، هر چه عدد مورد نظر بزرگ‌تر باشد، تجزیه‌ی آن به عوامل اول و در نتیجه رمزگشایی سخت‌تر خواهد بود. ولی با در اختیار داشتن یک کامپیوتر قوی می‌توان این کار را به راحتی و در مدت زمان کمتری انجام داد (مشکل‌ترین رمزهای کلاسیکی نهایتاً در شش ماه شکسته می‌شوند). ولی در رمزنگاری به روش کوانتومی، هنگامی که یک سیگنال رمزشده ارسال می‌گردد به جز دو کاربر قانونی، هیچ شخص دیگری نمی‌تواند رمز را بشکند. از طرفی اگر استراق‌سمع کننده (ایو) نیز دارای قدرت نامحدود (یعنی مسلط به کامپیوترهای کوانتومی) باشد به راحتی می‌تواند رمزهای کلاسیکی را بشکند. بنابراین توزیع کلید کوانتومی، ایمنی را در مقابل استراق‌سمع کننده‌ای با قدرت محاسباتی نامحدود ارائه می‌دهد. به عبارت دیگر، امنیت رمزنگاری کلاسیکی بر اساس خواص ریاضی کلید است

[۱] Quantum Key Distribution

در حالیکه در توزیع کلید کوانتومی این ایمنی به صورت خیلی حساس وابسته به خواص فیزیکی فرآیند خلق کلید است.

مبحث توزیع کلید کوانتومی از اصل عدم قطعیت مکانیک کوانتومی سود می‌جوید: در حالت کلی، اندازه‌گیری یک سیستم کوانتومی، آن را مختل می‌کند. بنابراین، استراق‌سمع یک کانال ارتباطی کوانتومی عموماً منجر به ایجاد اختلالی اجتناب‌ناپذیر در سیگنال مخابره شده می‌گردد که می‌تواند توسط کاربران (قانونی) شناسایی گردد. ذکر این نکته ضروریست که QKD فقط به منظور تهیه و توزیع کلید به کار می‌رود و نه برای انتقال پیام و یا داده. همچنین هدف QKD در اصل، محدود کردن توانایی محاسباتی و دسترسی شخص سومی که می‌خواهد به طور غیر قانونی به اطلاعات دسترسی یابد، می‌باشد.

۳-۱-۲ پروتکل BB84

یکی از پروتکل‌های شناخته شده در زمینه‌ی توزیع کلید کوانتومی، BB84 است که توسط بنت[۱] و براسارد[۲] در سال ۱۹۸۴ ارائه شد [۱۳]. این پروتکل مبتنی بر توابع پیچیده‌ی ریاضی نیست بلکه بر اساس خواص و ویژگی‌های مکانیک کوانتومی می‌باشد. این مدل، طرحی از توزیع کلید کوانتومی است که در آن، هر گونه استراق‌سمع قابل شناسایی خواهد بود. آلیس و باب توسط یک کانال کوانتومی و یک کانال کلاسیکی با یکدیگر ارتباط برقرار می‌کنند: آلیس، رشته بیت را از طریق کانال کوانتومی برای باب می‌فرستد و ایو می‌تواند از طریق این کانال کوانتومی به پیام دسترسی داشته باشد ولی نمی‌تواند (بعد از استراق‌سمع) مستقیماً پیام اصلی را برای باب بفرستد. سپس وقتی باب تمام کیوبیت‌ها را دریافت کرد، آلیس پایه‌های انتخابی خود را از طریق کانال کلاسیکی (عمومی) اعلام می‌کند. نکته‌ی قابل ذکر اینست که آلیس و باب فقط پایه‌های اندازه‌گیری را اعلام می‌کنند و هیچ یک از نتایج اندازه‌گیری آن‌ها منتشر نمی‌شود.

[۱] Charls Bennett
[۲] Cillen Brassard

در پروتکل BB84، آلیس یک رشته بیت کوانتومی (کیوبیت) کاتوره‌ای تهیه و برای باب می‌فرستد. هر یک از این بیت‌های کوانتومی ممکن است در یکی از ۴ حالت ممکن موجود درجدول (۳-۱) باشند (با احتمال یکسان). هنگامیکه باب رشته کیوبیت را دریافت کرد، به ازای هر کیوبیت، یکی از پایه‌های Z و یا X را به طور کاملاً رندوم انتخاب و کیوبیت را در آن پایه اندازه‌گیری و سپس نتایج را ثبت می-کند. حال باب یک رشته بیت رندوم در اختیار دارد. سپس آلیس پایه‌هایی که هر کیوبیت را در آن فراهم کرده (و نه حالت کیوبیت را) به باب اعلام می‌کند (یعنی ستون پایه در جدول (۳-۱) را) و باب نیز پایه‌هایی که در آنها اندازه‌گیری انجام داده را اعلام می‌کند. بر این اساس، چنانچه باب (در هر یک

مقدار	پایه	حالت
0	Z	$\|0\rangle$
1	Z	$\|1\rangle$
0	X	$\|0\rangle+\|1\rangle$
1	X	$\|0\rangle-\|1\rangle$

جدول ۳-۱: پروتکلBB84

از موقعیت‌ها) در همان پایه‌ای که آلیس برای آماده کردن کیوبیت‌ها از آن استفاده کرده، اندازه‌گیری کرده باشد، می‌بایست نتیجه را در ستون مقدار جدول یادداشت کند. آلیس و باب با مقایسه‌ی پایه-های انتخابی خود، بیت‌های متناظر با پایه‌های یکسان را نگه داشته و بقیه را (که در آن‌ها پایه‌ها متفاوت می‌باشد) دور می‌ریزند. اگر تعداد بیت‌های متفاوت زیاد بود، پروتکل قطع و دوباره از سر گرفته می‌شود. ولی اگر اینطور نبود، آلیس و باب رشته بیتی در اختیار خواهند داشت که ایو از آن بی‌اطلاع است و حال این دو شخص می‌توانند رشته بیت حاصله را به عنوان کلید (محرمانه) مورد استفاده قرار دهند (جدول۳-۲).

بیت انتخابی آلیس	0	1	1	0	1	0	0	1
پایه‌ی انتخابی‌آلیس	+	+	×	+	×	×	×	+
قطبشی که آلیس فرستاده	↑	→	↘	↑	↘	↗	↗	→
پایه‌ی‌اندازه-گیری باب	+	×	×	×	+	×	+	+
قطبشی که - باب اندازه گرفته	↑	↗	↘	↗	→	↗	→	→
بحث عمومی پایه‌ها	....	....	....	...	....	....	....	...
کلیدمحرمانه-ی توافق شده	0		1			0		1

جدول ۳-۲: بیت‌ها، پایه‌ها و قطبش انتخابی آلیس و باب و نیز کلید محرمانه‌ی توافق شده بین آن‌ها.

۳-۱-۳ ایمنی پروتکلBB84

فرض کنید ایو بر انجام این پروتکل توسط آلیس و باب نظارت دارد. او حتی می‌تواند به بعضی از کیوبیت‌هایی که از آلیس به باب فرستاده می‌شود دسترسی یابد. با این حال، هر اندازه‌گیری که ایو بر روی هر کیوبیت انجام می‌دهد تا بفهمد که چیست، ناچاراً آن حالت کوانتومی را مختل می‌کند. اگر ایو به طور اتفاقی پایه‌هایی مشابه با پایه‌های انتخابی باب انتخاب نماید، باب متوجه حضور وی نخواهد شد یعنی باب هم نتیجه‌ای مشابه با نتیجه‌ی ایو به دست خواهد آورد (این نتیجه همچنین مشابه نتیجه‌ای است که اگر ایو هیچ اندازه‌گیری بر روی کیوبیت انجام نمی‌داد باز هم باب آن را بدست می-آورد). ولی با این وجود ایو نمی‌داند که باب چه پایه‌ای را برای اندازه‌گیری انتخاب خواهد کرد. به عبارت دیگر، احتمال اینکه ایو پایه‌ی درست (مطابق با پایه‌ی انتخابی باب) انتخاب کند $\frac{1}{2}$ و نیز احتمال آن که باب پایه‌ای مخالف با آلیس انتخاب کند نیز $\frac{1}{2}$ است. بنابراین احتمال اینکه یک فوتون آشکار شده، جوابی غلط در کلید ایجاد کند $\frac{1}{4}$ است. یعنی با احتمال $\frac{3}{4}$ جواب درست خواهد بود. آلیس و باب با مقایسه‌ی عمومی n تا از بیت‌های کلید، از محرمانه بودن کل آن اطمینان حاصل می-

کنند (این n تا بیت فاش‌شده در نهایت از کلید حذف خواهند شد). پس احتمال اینکه هیچ خطایی در کلید ایجاد نشود $(\frac{3}{4})^n$ است و در نتیجه احتمال بروز خطا در کلید برابر است با:

$$P = 1 - (\frac{3}{4})^n$$

بر این اساس می‌توان با افزایش تعداد کیوبیت‌ها (n)، خطا را تا حد دلخواهی کاهش داد. این پروتکل آنقدر تکرار می‌شود تا از عدم حضور ایو اطمینان حاصل گردد.

در این پروتکل، ایو برای استراق‌سمع نمی‌تواند مستقیماً وارد عمل شده و بر روی کیوبیت‌ها اندازه-گیری انجام دهد چرا که پس از اندازه‌گیری، حالت آن فروریزش کرده و در اینصورت دیگر قابل بازیافت نیست. پس وی می‌بایست یک کپی از آن حالت تهیه کرده، بر روی یکی از آن دو (کپی و یا اصل آن) اندازه‌گیری کرده و دیگری را به باب بازگرداند تا وی متوجه حضورش نشود. ولی به دلیل خاصیت تکثیرناپذیری در مکانیک کوانتومی، ایو قادر به کپی‌برداری از حالت سیستم و ارسال دوباره‌ی آن‌ها به باب نمی‌باشد. بنابراین در این پروتکل حضور استراق‌سمع‌کننده قابل شناسایی خواهد بود و در حالت کلی این امر متکی بر دو موضوع اساسی در مکانیک کوانتومی می‌باشد: ۱) حالت مربوط به کیوبیت‌های کوانتومی قابل کپی شدن نیستند و ۲) هر حالت کوانتومی پس از اندازه‌گیری فروریزش کرده و دیگر قابل بازیابی نیست.

چند سال پس از ارائه‌ی طرح BB84 توسط بنت و براسارد، شخصی به نام ایکرت[۱] پروتکل توزیع کلید کوانتومی دیگری پیشنهاد داد [۱۴] که مبتنی بر همبستگی‌های میان ذرات درهم‌تنیده‌ای که با هم به اشتراک گذاشته‌اند، می‌باشد.

[۱] Ekert

۳-۲ ارسال التزام‌آور بیت[۱] (BC)

همانطور که در قسمت قبل اشاره شد، هدف QKD اینست که برای دو شخص که به فاصله‌ای از هم قرار گرفته‌اند، رشته بیت تصادفی یکسانی را (به عنوان کلید) تولید و به اشتراک گذارد. حال سؤال اساسی اینست که بر این اساس آیا در انتهای پروتکل، طرفین رشته بیت یکسانی (به عنوان کلید) در اختیار خواهند داشت؟ با توجه به پروتکل‌های توزیع کلید کوانتومی، چنانچه یکی از طرفین متقلب باشد کلیدی که در نهایت تولید و به اشتراک گذاشته می‌شود به هیچ وجه (برای دو طرف) یکسان و مشابه نخواهد بود.

برای روشن شدن موضوع، پروتکل توزیع کلید کوانتومی BB84 را در نظر بگیرید. مشابه تمام پروتکل‌های متداول دیگر، این پروتکل نیز یک فرآیند دو مرحله‌ای است. در مرحله‌ی اول، فرستنده یک رشته از فوتون‌های قطبیده‌ی 0، ۹۰، ۴۵ و ۱۳۵ را بطور رندوم انتخاب و ارسال می‌کند. تک فوتون‌های 0 و ۴۵ نمایشگر بیت 0 و تک فوتون‌های ۹۰ و ۱۳۵ نماینده‌ی بیت ۱ هستند. اگر ارسال کننده، اطلاعات مورد نیاز در خصوص مقادیر بیت (یعنی پایه‌های اندازه‌گیری) را به دریافت‌کننده بدهد، دریافت کننده قادر خواهد بود که از مقادیر واقعی بیت مطلع گردد. در مرحله‌ی دوم، ارسال کننده، اطلاعات مورد نیاز را در اختیار دریافت‌کننده قرار می‌دهد. حال مشکل اینست که: اگرچه ارسال کننده در مرحله‌ی اول مقادیر بیت خاصی را انتخاب نموده است ولی با این حال می‌تواند (با تغییر اطلاعاتی که برای دریافت کننده لازم و ضروریست و برایش می‌فرستد) مقدار بیت‌های موجود در رشته را تغییر داده و بیت‌هایی متفاوت از موارد انتخابی اولیه‌اش برای دریافت کننده افشا کرده و بدین ترتیب تقلب نماید.

به منظور غلبه بر این مشکل، ایده‌ی ارسال التزام‌آور بیت (BC) در اوایل دهه‌ی ۹۰ مطرح شد. بر اساس این ایده، پیش‌بینی شد که اگر BC کوانتومی بر طرح‌های QKD اعمال شود، تقلب قابل

[۱] Bit Commitment

شناسایی خواهد بود: در ارتباط‌های رمزی و مخفیانه، مکانیک کوانتومی می‌تواند مانع از آن شود که فرد ملزم شده تقلب نماید.

از ابتدا رمزنگاری علمی بوده است که به منظور حفاظت ارتباطات از استراق‌سمع و مداخلات به‌کار می‌رفته است و اخیراً نیز به شاخه‌های متعددی برای اهداف مختلف رمزنگاری تقسیم شده است. این اهداف، معمولاً دو یا چند نفر را شامل می‌شود که حتی بعضی از این افراد ممکنست متقلب و غیرقابل اعتماد نیز باشند. BC از زیربنایی‌ترین موضوعاتی است که به منظور طراحی و اجرای چنین کارهای رمزنگاری پیچیده‌ای مورد استفاده قرار می‌گیرد. رمزنگاری کوانتومی اغلب به یک کاربرد رمزنگاری که توزیع کلید [۱۳و۱۵] نامیده می‌شود وابسته است. با این حال، کاربردهای دیگری از مکانیک کوانتومی نیز برای رمزنگاری در نظر گرفته شده‌اند و می‌توان گفت که BC به عنوان اساس و مبنای اغلب این کاربردها بوده است. به عبارت دیگر، بعد از ابداع توزیع کلید کوانتومی و امنیت بدون قید و شرط، محققان تلاش کردند تا رمز نگاری با امنیت بی قید و شرط را توسعه دهند که یکی از این موارد، BC بود. هدف از این بحث، توصیف پروتکل‌های ویژه برای اهداف رمزنگاری است که ارسال التزام‌آور بیت نامیده می‌شود.

یک طرح BC، به آلیس (به عنوان فرد ملزم شونده) این اجازه را می‌دهد که چیزی را (به عنوان سند التزام و تعهد[۱]) برای باب بفرستد که بدان وسیله خود را به یک مقدار بیت انتخابی b ملزم می‌نماید بطوریکه به واسطه‌ی این سند، دیگر قادر به تغییر بیت انتخابی نبوده و در ضمن در نتیجه‌ی این طرح، باب نیز به هیچ وجه نمی‌تواند بفهمد که مقدار b چیست ولی آلیس بعداً می‌تواند (بنا به درخواست باب) اقدام به افشای سند التزام نموده و به وی نشان دهد که مقدار b انتخابی اولیه‌اش چه بوده است.

برای روشن شدن موضوع به بیان یک مثال ساده می‌پردازیم: فرض کنید آلیس و باب تصمیم می‌گیرند که بازی دو نفره‌ای انجام دهند و درصدد تعیین این موضوع برمی‌آیند که چه کسی شروع

[۱] commitment

کننده‌ی بازی باشد. بدین منظور تصمیم می‌گیرند که سکه‌ای پرتاب کنند اما خیلی زود متوجه می‌شوند که سکه‌ای در اختیار ندارند. آلیس یک راه‌حل پیشنهاد می‌دهد:"هر یک از ما یکی از اعداد ۰ یا ۱ را به صورت رندوم انتخاب کند. تو انتخاب خود را به من بگو و سپس من نیز مورد انتخابی‌ام را بازگو می‌کنم. اگر انتخاب هر دو یکسان بود، تو بازی را شروع کن و اگر متفاوت بود من شروع کننده‌ی بازی خواهم بود." ایرادی که باب به این پیشنهاد وارد می‌کند اینست که: "این امکان وجود دارد که تو بعد از دانستن انتخاب من، مورد انتخابی‌ات را (به نفع خود) عوض کنی. من چطور مطمئن باشم چیزی که به من اعلام می‌کنی واقعاً همان چیزی است که در ابتدا انتخاب کرده‌ای؟" آلیس نیز برای آنکه حسن نیت خود را نشان دهد پیشنهاد صادقانه‌ای مطرح می‌کند:"من عدد انتخابی خود را برروی یک کاغذ نوشته، آن را داخل یک گاوصندوق قرار داده و آن را به تو تحویل می‌دهم در حالی که کلید گاوصندوق را نزد خود نگه می‌دارم. بعد از آنکه تو گزینه‌ی انتخابی خود را برای من بازگو کردی، گاوصندوق را باز می‌کنیم. حال با مقایسه‌ی این دو مورد معلوم می‌شود که چه کسی شروع‌کننده‌ی بازی باشد". باب جوانب امر را بررسی کرده و چون مشکلی (تقلب) نمی‌یابد با این طرح موافقت می‌کند.

طرحی که آلیس پیشنهاد داد در واقع مورد ساده‌ای از BC است: آلیس یک بیت محرمانه (۰ یا ۱) انتخاب می‌کند و به واسطه‌ی گاوصندوقی که (به عنوان سند التزام) در اختیار باب قرار می‌دهد، لزوماً به آن مقدار بیت ملتزم می‌گردد. این بدان معناست که آلیس می‌تواند بعداً، هر موقع که اراده کرد، این بیت را برای باب (که در ابتدا برایش نامعلوم و مخفی است) افشا کند بطوریکه اولاً: باب کاملاً مطمئن می‌باشد که (طی این طرح) بیتی که آلیس برایش فاش می‌کند در واقع همانی خواهد بود که آلیس در ابتدا انتخاب می‌کند و دوماً: باب نمی‌تواند بیت آلیس را، قبل از اینکه خود آلیس آن را برایش فاش کند، متوجه شود. پس بطور کلی براساس این طرح، باب به هیچ وجه نمی‌تواند حدس بزند که مقدار بیت b چیست و با این حال آلیس بعداً (هر زمان که اراده کرد) طبق درخواست باب

می‌تواند با افشای سند مزبور، مقدار بیت انتخابی اولیه را برای وی آشکار نماید در حالیکه باب کاملاً مطمئن می‌باشد که آلیس تقلب نکرده و همان بیت اصلی را افشا نموده است.

به طور کلی، هدف QBC شناسایی تقلب (فرد متقلب) می‌باشد اما برای تولید و توزیع کلید می-بایست از QKD استفاده نمود. آلیس و باب در توزیع کلید کوانتومی با یکدیگر مشارکت و همکاری می‌کنند اما به دلیل عدم اعتماد طرفین نسبت به هم، QBC را اجرا می‌کنند.

در حالت کلی یک پروتکل BC شامل دو مرحله می‌باشد: ۱) مرحله‌ی التزام[۱]: در این مرحله، آلیس (به عنوان فرد ملزم‌شونده) مقدار بیتی را به صورت محرمانه انتخاب و به واسطه‌ی تهیه‌ی یک سند التزام و ارسال آن به باب، به آن بیت ملزم (متعهد) می‌گردد و ۲) مرحله‌ی افشا[۲]: آلیس با ارائه‌ی یکسری اطلاعات، بیت محرمانه‌ی خود را برای باب (به عنوان دریافت‌کننده) فاش می‌کند.

همانطور که قبلاً نیز بیان شد این پروتکل دارای دو جنبه‌ی اساسی است: ۱) هنگامی‌که آلیس بیت محرمانه‌ی خود را انتخاب نمود و (به واسطه‌ی سند التزامی که خود تهیه نموده و در اختیار باب قرار داده) به آن ملزم گردید، دیگر به هیچ وجه نمی‌تواند نظر خود را عوض کرده و هنگام فاش‌سازی مقدار بیت دیگری را افشا نماید (در مثالی که ذکر شد، هنگامی که آلیس مورد انتخابی خود را درون گاوصندوق قرار داده و به عنوان سند و مدرک تحویل باب می‌دهد دیگر قادر به تغییر مندرجات و محتویات داخل آن نیست). و ۲) تا زمانی که آلیس نخواهد، باب نمی‌تواند از بیت محرمانه‌ی آلیس آگاه شود (در مثال فوق، تا زمانی که آلیس کلید گاوصندوق را در اختیار باب قرار نداده باب نمی‌تواند از محتویات آن مطلع گردد).

آلیس می‌تواند طی مرحله‌ی التزام، توزیع احتمال b را انتخاب نماید. سند تعهدی که در مرحله‌ی التزام حاصل می‌شود مقید[۳] (الزام‌آور) نامیده می‌شود اگر آلیس به هیچ وجه نتواند این توزیع احتمالی انتخابی را تغییر دهد و نیز چنانچه باب نتواند بدون کمک آلیس هیچ‌گونه اطلاعاتی در مورد بیت

---

[۱] Committing phase
[۲] Unveiling phase
[۳] Binding

موردنظر به دست آورد، این سند مخفی[۱] نامیده می‌شود. سند التزام در صورتی ایمن خواهد بود که همزمان مخفی و مقید باشد. و نیز ایمن بدون شرط خواهد بود اگر در مقابل متقلبی (آلیس یا باب) با تکنولوژی و قدرت محاسباتی نامحدود همچنان ایمن باقی بماند.

در عمل، یک پروتکل BC ایمن در نظر گرفته می‌شود به شرطی که باب به هیچ وجه نتواند اطلاعاتی بیشتر از همان مقدار اطلاعاتی که خود سعی میکند تا به دست آورد و در ضمن بطور نمایی کوچک هستند در مورد بیت انتخابی آلیس به دست آورد. این بدان معناست که در یک پروتکل ایمن، مقدار اطلاعاتی که باب (بدون کمک آلیس) می‌تواند در مورد بیت انتخابی آلیس به دست آورد، با افزایش فوتون‌های مورد استفاده در پروتکل، به صورت نمایی سریعاً به صفر میل می‌کند.

از مسائل بسیار مهم در پروتکل‌های BC، طراحی آنها به صورت ایمن بدون شرط می‌باشد. بدین معنا که بدون در نظر گرفتن هیچ‌گونه قید و شرطی برای مکان، زمان، قدرت محاسباتی و تکنولوژی در دسترس شخص متقلب، پروتکل همواره ایمن باقی بماند. پس از طرح ایده‌ی BC، تلاش‌های بسیاری در جهت طراحی ایمن این پروتکل‌ها انجام شد ولی ایمنی تمام آن‌ها توسط مایرز رد شد. وی همچنین نشان داد که پروتکل ایمن بدون شرط امکانپذیر نیست مگر اینکه یک ابزار محاسباتی مانند باریکه‌ی شکاف، یک گیت کوانتومی و ...همزمان مورد اعتماد هر دو طرف باشد [۱۶].

دو نمونه از مواردی که BC در آن‌ها مفید واقع می‌شوند عبارتند از: ۱) پرتاب سکه[۲]: هنگامی به کار می‌رود که طرفین بخواهند رشته بیتی تهیه کنند که کاملاً رندوم باشد (در بسیاری از پروتکل‌ها لازمست که رشته بیتی تهیه شود که در نهایت بعنوان کلید مورد استفاده قرار گیرد). مثالی که در ابتدای بحث ذکر شد نمونه‌ای از این حالت است. راه‌حلی که آلیس و باب بر سر آن توافق می‌کنند فقط با فرض اینکه دو طرف، یک روش برای اجرای ارسال التزام‌آور بیت داشته باشند و حداقل یکی ازطرفین صادق باشد، کارآیی خواهد داشت. ۲) محاسبه (شمارش) چندطرفه[۳]: کاربرد این مورد

[۱] Concealing
[۲] Coin flipping
[۳] Multi-party Computation

هنگامی است که چندین نفر بخواهند برمبنای ورودی‌هایی که لازمست محرمانه حفظ شود نتیجه‌ای را محاسبه کنند. به عنوان مثال فرض کنید دو میلیونر قصد دارند بدانند که کدامیک ثروتمندتر است در حالیکه هیچ‌یک از طرفین (و نیز هیچ شخص سومی) از میزان دارایی طرف دیگر مطلع نگردد. این طرح همچنین می‌تواند مثلاً در یک رأی‌گیری الکترونیکی به‌کار رود: هر شهروند یک ورودی (رأی او) به صورت محرمانه دارد و نتیجه، تعداد کل رأی‌ها برای هر کاندید خواهد بود. مثال دیگر جمع‌آوری اطلاعات آماری است. به طوریکه آمارگیران یکسری اطلاعات آماری کلی که نیاز دارند را بدست می‌آورند در حالیکه نیازی به دانستن اطلاعات شخصی (و محرمانه‌ی) افراد ندارند.

از آنجائی که تنوع موضوعاتی که BC در آنها مفید واقع می‌شود بسیار زیاد است لذا لازمست تلاش‌های بیشتری به منظور یافتن روش‌های مناسب برای بکارگیری (تا حد امکان) ایمن آن انجام شود.

۳-۳ امنیت محاسباتی در مقابل ایمنی بدون شرط

مسئله‌ی بسیار مهم در هر پروتکل رمزی، امنیت آن می‌باشد. ایمنی می‌تواند به روش‌های متفاوتی تعیین و تعریف شود:

الف) امنیت محاسباتی[۱]

امنیت محاسباتی بر مبنای مقدار کاری که لازمست تا یک پروتکل رمزی توسط بهترین روش‌های موجود شکسته شود، سنجیده و تخمین زده می‌شود. اگر شکستن پروتکل نیازمند زمان بسیار زیادی باشد (مدت زمانی که عملاً غیر ممکن و غیر عملی باشد)، آن پروتکل از نظر محاسباتی ایمن تلقی می‌شود. از این‌رو اگر یک سیستم یا پروتکل، ایمن محاسباتی باشد تضمینی وجود ندارد که همینطور ایمن باقی بماند. به عنوان مثال در بسیاری از پروتکل‌هایی که بر مبنای تئوری اعداد شکل گرفته‌اند، اگر شخصی که قصد تقلب دارد بتواند اعداد صحیح بزرگی تعیین کند، پروتکل با شکست مواجه می‌شود. اگرچه، حتی روش‌های خیلی خوب در این زمینه نیز برای تعیین اعدادی صحیح (آن هم فقط تا مرتبه‌ی صدگان)، نیارمند زمانی حدود چند سال می‌باشند.

[۱] Computational Security

با تکامل تکنولوژی و ظهور الگوریتم‌های جدید، امنیت محاسباتی محدود شده است: کاری که انجامش توسط کامپیوترهای امروزی (کلاسیکی) هزاران سال به طول می‌انجامد، ممکنست با کامپیوترهایی که در آینده طراحی و ساخته می‌شوند (کوانتومی)، در مدتی کوتاه (و در حد فقط چند ساعت) به نتیجه برسد.

ب) ایمنی بدون شرط[۱]

ایمنی بدون شرط متکی بر تئوری اطلاعات بوده و ایمنی نظری- اطلاعاتی[۲] نامیده می‌شود. این موضوع اولین بار توسط شانون[۳] در دهه‌های ۱۹۴۰و۱۹۵۰ بسط و گسترش یافت. لازم به ذکر است که اثبات‌های مربوط به ایمنی بدون شرط، هیچ گونه فرضی در مورد قدرت محاسبه‌ی دشمن ایجاد نمی‌کنند.

در مورد ارسال التزام‌آور بیت (BC)، برقراری ایمنی بدون شرط مستلزم آنست که آلیس به هیچ طریقی نتواند بیت انتخابی خود را تغییر دهد و نیز تا زمانی که آن را برای باب افشا نکرده، باب هیچ چیز در مورد این بیت محرمانه نداند. با این حال، برقراری این نوع امنیت همواره امکانپذیر نیست و (همانطور که قبلاً نیز اشاره شد) فقط زمانیکه یک دستگاه اندازه‌گیری مورد اعتماد هر دو طرف باشد می‌توان به ایمنی بدون شرط دست یافت.

ج) ایمنی احتمالاتی

برای آنکه بتوان یک پروتکل ایمن بدون شرط را کاربردی و قابل اجرا نمود، می‌بایست تعریف خود از ایمنی را کمی متعادل‌تر و واقع‌گرایانه‌تر نمود. یعنی در واقع در طراحی آن‌ها احتمال وجود کمی خطا را نیز وارد بحث نموده و مورد فیزیکی (غیر ایده‌آلی) نیز بررسی گردد. در اینصورت اجرای پروتکل با احتمال خطا رابطه پیدا می‌کند: با کوچکتر شدن احتمال خطا، اجرای پروتکل سریعتر و ایمن‌تر انجام می‌شود. در حال حاضر، امنیت چنین پروتکل‌هایی فقط در حد تئوری-اطلاعاتی است و با انتخاب

---

۱ Unconditional security
۲ Information-Theoretic Security
۳ Shannon

مناسب پارامترهای مربوطه می‌توان احتمال خطا را تا حد دلخواهی کاهش داد ولی با این حال این نوع ایمنی نیز هیچ‌گونه فرضی در مورد قدرت محاسباتی شخص متقلب ایجاد نمی‌کند.

همانطور که اشاره شد در صورتی که ایده‌ی BC بر طرح‌های انتقال بیت اعمال شود، در صورتی که یکی از طرفین اقدام به تقلب نماید، تقلب قابل شناسایی خواهد بود. با این حال مایرز نشان داد که پروتکل‌های ایمن بدون شرط امکانپذیر نمی‌باشد [۱۸و۱۹]. در فصل بعد، مرور مختصری بر این موضوع نموده و در ادامه نیز به بررسی دو پروتکل BC می‌پردازیم.

فصل چهارم

بررسی عدم امکان BC ایمن و ارائه‌ی دو پروتکل

۴-۱ مقدمه

تقاضا و علاقه برای به‌دست آوردن یک پروتکلBC ایمن بدون شرط، اولین بار حدود۵۰ سال پیش ارائه شد. در تلاش برای کسب یک مجموعه‌ی متنوع از کاربردهایی با ایمنی بدون شرط در رمزنگاری کوانتومی، BC موضوعی است که به کار آمده و برای این منظور کفایت می‌کند. در سال۱۹۹۳ یک پروتکل BC کوانتومی (به نامBCJL) ارائه شد که مدعی بود (و نیز اثبات کرد که) ایمن است. یعنی سند التزام منتجه، ایمن بدون شرط می‌باشد. با این حال در سال ۱۹۹۵، مایرز و متعاقباً لو و چائو یک عیب اساسی در این پروتکل کشف کردند. بعدها مایرز این نتیجه را تعمیم داده و نشان داد که BC ایمن بدون شرط امکان‌پذیر نمی‌باشد [۱۶و۱۷].

در رمزنگاری کلاسیکی، یک محاسبه‌ی ایمن دو طرفه به وسیله‌ی یک واسطه‌ی مورد اعتماد و یا استفاده از یکسری فرض‌های محاسباتی مانند سختی تعیین اعداد صحیح بزرگ انجام می‌شود. بزرگترین انتظار و خواسته از رمزنگاری کوانتومی اینست که بتواند ما را از شر این الزامات و قیود رها کرده و تنها با استفاده از قوانین فیزیک، به همان هدف برسیم.

در این جا نشان می‌دهیم که تمام طرح‌های QBC غیر ایمن هستند: یک فرد متقلب می‌تواند از همبستگی‌های نوع EPR غیرموضعی در مکانیک کوانتومی بهره برده و با موفقیت تقلب نماید. بدین منظورلازمست که وی، همدوسی[۱] سیستم کوانتومی سهم خود را با استفاده از یک کامپیوتر کوانتومی حفظ نماید. در این قسمت نشان می‌دهیم که تمام طرح‌های QBC پیشنهاد شده، غیر ایمن هستند زیرا فرستنده (آلیس) تقریباً همواره می‌تواند با استفاده از یک نوع حمله‌ی EPR [۵] و نیز با به تأخیر انداختن اندازه‌گیری تا زمان بازگشایی و افشای سند التزام، با موفقیت تقلب نماید. منظور از تقلب در اینجا اینست که (به عنوان مثال) آلیس می‌تواند طی مرحله‌ی التزام، یک مقدار بیت خاص انتخاب نماید ولی در مرحله‌ی بازگشایی و افشا، مقدار دیگری را برای باب فاش کند. یک طرح BC در مقابل

[۱] coherence

چنین آلیس متقلبی ایمن خواهد بود فقط اگر چنین سند جعلی‌ای، توسط باب (دریافت‌کننده) قابل شناسایی باشد.

۲-۴ طرح ارسال التزام‌آور بیت BB84

در این‌جا بسیار آموزنده خواهد بود که ابتدا به بررسی یک پروتکل QBC ساده‌ای که بنت و براسارد طراحی کردند بپردازیم [۱۸]. طرز کار این پروتکل به صورت زیر است:

آلیس و باب، ابتدا بر روی یک پارامتر ایمنی[۱] (یک عدد صحیح مثبت S) توافق می‌کنند. فرستنده (آلیس) بیت b را انتخاب و به آن ملزم و مقید می‌گردد:

الف: اگر b=0 را انتخاب کند: وی یک رشته‌ی S فوتونی، که هر یک از آن‌ها به طور رندوم از فوتون-های قطبیده‌ی افقی یا عمودی (قطبش0 یا ۹۰ درجه) انتخاب می‌شوند، تهیه کرده و برای باب ارسال می‌کند. البته مقدار b، طی مرحله‌ی التزام محرمانه حفظ می‌شود و علاوه براین، قطبش واقعی (افقی یا عمودی) هر فوتون انتخابی توسط آلیس نیز به هیچ‌وجه برای باب اعلام نمی‌شود.

ب: اگر b=۱ را انتخاب نماید: آلیس یک رشته‌ی S فوتونی، به صورت رندوم از فوتون‌هایی با قطبش ۴۵ و یا ۱۳۵ درجه انتخاب و برای باب ارسال می‌کند (در اینجا نیز قطبش واقعی هر فوتون و مقدار واقعی b از جانب آلیس محرمانه حفظ می‌شود).

باب به صورت کاملاً رندوم، پایه‌های مستقیم[۲] (افقی و عمودی) و مورب[۳] (۴۵ یا ۱۳۵) را برای اندازه-گیری قطبش هر فوتون انتخاب می‌کند. در اینجا مرحله‌ی التزام کامل می‌شود.

با یک محاسبه‌ی ساده می‌توان نشان داد که دو ماتریس چگالی توصیف‌کننده‌ی S فوتون متناظر با b=0 و b=۱ دقیقاً مشابه و یکسان‌اند (و متناسب با ماتریس واحد) [۴]. در نتیجه باب به هیچ‌وجه نمی‌تواند چیزی در مورد مقدار b متوجه شود (برقراری شرط اخفا).

---

[۱] Security Parameter
[۲] Rectilinear Bases
[۳] Diagonal Bases

بعداً، آلیس می‌تواند با اعلام (و انتشار) مقدار b و قطبش واقعی هر یک از S فوتون، سند التزام خود را بازگشایی و افشا نماید. چون باب پایه‌ی (مستقیم یا مورب) اندازه‌گیری‌اش برای هر فوتون در مرحله‌ی التزام را به صورت رندوم انتخاب می‌کند از اینرو به طور متوسط، فقط نیمی از S فوتون، (توسط وی) در پایه‌ی صحیح (یعنی مطابق با پایه‌های انتخابی آلیس) اندازه‌گیری شده‌اند که برای این فوتون‌ها باب می‌تواند (در این مرحله) بررسی کرده و متوجه شود که قطبش‌های اعلام شده از سوی آلیس با نتایج اندازه‌گیری‌اش مطابقت دارد.

(به جز در مورد حملات EPR) آلیس متقلب می‌تواند (به عنوان مثال) در مرحله‌ی التزام، فوتون‌های مستقیم را ارسال نماید (و از این‌رو ظاهراً به b=0 ملزم گردد) اما در مرحله‌ی بازگشایی و افشا، به باب اعلام کند که فوتون‌های انتخابی مورب بوده‌اند (یعنی b=۱ را افشا کرده و وانمود کند که b انتخابی اولیه‌اش در واقع ۱ بوده است). این کار تقلب به شمار می‌آید. در اینصورت آلیس می‌بایست قطبش فوتون‌هایی که باب در امتداد پایه‌ی مورب اندازه‌گیری کرده را (به صورت کاملاً رندوم) حدس و تخمین بزند. از آنجایی که باب (به طور متوسط) $\frac{S}{2}$ فوتون‌ها را در امتداد پایه‌ی مورب اندازه‌گیری می‌کند، از اینرو آلیس با بکارگیری چنین استراتژی تقلبی دارای احتمال موفقیت (فقط) $(\frac{1}{2})^{\frac{S}{2}}$ می‌باشد [۱۹] (که می‌توان با افزایش S، این احتمال را تا حد دلخواهی کاهش داد).

یک ضعف اساسی در طرح BC بنت و براسارد اینست که آلیس با استفاده از جفت‌های EPR همواره می‌تواند تقلب موفقی داشته باشد: آلیس می‌تواند S جفت فوتون EPR تهیه کرده و طی مرحله‌ی التزام، قسمتی از هر جفت را برای باب بفرستد. وی از مرحله‌ی اندازه‌گیری جهش زده و در مورد مقدار b، فقط در شروع مرحله‌ی افشا تصمیم می‌گیرد: اگر وی تصمیم بگیرد که مقدار b صفر باشد (وانمود کند که b=0 بوده)، قطبش فوتون‌های سهم خود را در امتداد پایه‌ی مستقیم اندازه می‌گیرد. این یک ویژگی معمول و استاندارد یک جفت EPR (پارادوکس EPR) است که نتیجه‌ی اندازه‌گیری آلیس بر روی یک فوتون، همواره بر نتیجه‌ای که باب از فوتون دیگر آن جفت به دست می‌آورد عمود

است. از این رو آلیس می‌تواند (با خیال راحت) آن قطبش‌ها را منتشر کند. به همین نحو برای b=۱، آلیس به سادگی در امتداد پایه‌ی مورب اندازه‌گیری کرده و به روشی مشابه پیش می‌رود. در مقابل، برای باب هیچ راهی برای شناسایی این حمله وجود ندارد. با وجود این ضعف در پروتکل بنت و براسارد، طرح‌های QBC جدیدی پیشنهاد شد ولی تمام آن‌ها توسط یک نوع حمله‌ی EPR با شکست مواجه شدند. هدف ما در این قسمت اینست که نشان دهیم بر خلاف اعتقاد عموم، نوع مشابهی از حمله‌ی EPR، تمام طرح‌های QBCی که تا کنون پیشنهاد شده‌اند را با شکست مواجه می‌سازد. تمام طرح‌های پیشنهادی شامل ارتباطات و مخابرات (فقط) یک جانبه از آلیس به باب می‌باشند و نیز همه‌ی آن‌ها شامل ارسال دو سیستم کوانتومی از جانب آلیس به سمت باب هستند که یکی طی مرحله‌ی التزام (به عنوان سند التزام) و دیگری در جریان مرحله‌ی فاش‌سازی ارسال می‌شود. (بدون از دست‌دادن عمومیت مسئله و آنالیزها، می‌توان فقط ارتباطات کوانتومی را در نظر گرفت چرا که مخابرات کلاسیکی فقط مورد خاصی از ارتباطات کوانتومی به شمار می‌آیند.)

فرآیند کلی هر طرح QBC پیشنهادی می‌تواند به صورت زیر باشد:

۱) آلیس یک مقدار بیت b، که می‌خواهد (به واسطه‌ی تهیه‌ی سند التزام) به آن ملتزم گردد، را انتخاب می‌کند: اگر بیت انتخابی b=0 باشد، وی حالت زیر را تهیه می‌کند:

$$|0\rangle = \sum_i \alpha_i \left|e_i\right\rangle_A \otimes \left|\varphi_i\right\rangle_B \qquad (۱-۴)$$

در این رابطه $\left\langle e_i \middle| e_j \right\rangle_A = \delta_{ij}$. اما حالت‌های نرمالیزه‌ی $\left|\varphi_i\right\rangle_B$ الزاماً با یکدیگر متعامد نیستند. به طور مشابه، اگر b=۱، آلیس حالت زیر را فراهم می‌کند:

$$|1\rangle = \sum_j \beta_j \left|e'_j\right\rangle_A \otimes \left|\varphi'_j\right\rangle_B \qquad (۲-۴)$$

که $\left\langle e'_i \middle| e'_j \right\rangle_A = \delta_{ij}$. اما $\left|\varphi'_j\right\rangle_B$ها لزوماً با یکدیگر متعامد نیستند.

فرض می‌شود که هم آلیس و هم باب از حالت‌های $|0\rangle$ و $|1\rangle$ (روابط ۴-۱ و ۴-۲) مطلع هستند. این مطلب به طور ضمنی بر این موضوع دلالت دارد که هر دوی آن‌ها، از حالت‌های $\left|\varphi_i\right\rangle_B$ و $\left|\varphi'_j\right\rangle_B$

مطلع می‌باشند (در اینجا، حالت مزبور مستقل از پایه می‌باشد. درست مانند یک نقطه که مستقل از مختصاتی است که برای تعیین آن به کار می‌رود).

۲) حال فرض می‌شود آلیس (صادق) بر روی رجیستر اول اندازه‌گیری کرده و (اگر بخواهد b=0 باشد) مقدار i را تعیین می‌کند (اگر b=۱، مقدار j را تعیین می‌کند). لازم به ذکر است که اندازه‌گیری رجیستر اول در پایه‌ی استاندارد، (با احتمال $|\alpha_i|^2$) $|e_i|$ را نتیجه می‌دهد (و از اینرو i ها نیز مشابه $|e_i\rangle$ متعامد می‌باشند).

۳) آلیس، رجیستر دوم را به عنوان قطعه‌ای از سند التزامش به باب می‌فرستد. از آنجائی که باب به هیچ‌وجه به سهم آلیس از حالت فوق، دسترسی ندارد و نیز آلیس به هیچ‌وجه نتایج اندازه‌گیری خود را به وی اعلام نخواهد کرد (در واقع آلیس همچنین ممکنست بخواهد اندازه‌گیری‌ای انجام ندهد)، لذا چیزی که باب مشاهده می‌کند $Tr_A|0\rangle\langle 0|$ یا $Tr_B|0\rangle\langle 0|$ است که رد پاره‌ای[۱] بر روی سهم آلیس (یعنی رجیستر اول) گرفته می‌شود. مسلماً در اینجا، باب در حالت کلی یک حالت مخلوط[۲] مشاهده می‌کند.

۴) بعداً آلیس با اعلام مقدار b و i یا j، سند التزام خود را بازگشایی (افشا) می‌کند.

۵) باب اندازه‌گیری‌هایی بر روی رجیستر دوم انجام می‌دهد تا بدین طریق بررسی کند که آیا آلیس در واقع به همان مقدار بیتی (انتخابی اولیه) که اعلام کرده ملزم شده است یا نه. یعنی داده‌های دریافتی از آلیس (مقادیر b و نیز i یا j) صریحاً می‌بایست با نتایج (اندازه‌گیری) تجربی باب بر روی رجیستر دوم مطابقت داشته باشد. اگر چنین ارتباط‌ها و همبستگی‌های مورد انتظاری پدیدار گردند، آنگاه باب می‌پذیرد که آلیس پروتکل را به صورت صادقانه اجرا کرده است. در غیر اینصورت باب مشکوک می‌شود که آلیس تقلب نموده است.

دوباره تأکید می‌کنیم که تمام طرح‌های QBCی که تاکنون پیشنهاد شده‌اند از فرآیند ۵ مرحله‌ای که در بالا توصیف شد پیروی می‌کنند. به عنوان مثال در طرح بنت و براسارد که در ابتدای بحث بیان

---

[۱] Partial Trace
[۲] Mixed State

شد، اگر به باب این اختیار و اجازه داده شود که فوتون‌هایش را ذخیره نموده و آن‌ها را فقط بعد از بازگشایی سند التزام توسط آلیس (مرحله‌ی ۴) اندازه‌گیری کند، در اینصورت این طرح در این مقوله قرار خواهد گرفت. چنانچه آلیس بتواند در برابر چنین باب قدرتمندی تقلب نماید، بدیهی است که می‌تواند هنگامی که باب چنین توانائی برای ذخیره کردن ندارد نیز تقلب نماید.

۳-۴ عدم امکان QBC ایمن

در این قسمت درصدد اثبات عدم ایمنی QBC هستیم. ابتدا لازمست متذکر شویم که برای اینکه باب به هیچ‌وجه نتواند بفهمد که b چیست، رجیستر دوم (یعنی سیستم کوانتومی که باب طی مرحله‌ی التزام دریافت می‌کند) می‌بایست حاوی اطلاعات بسیار کمی در مورد اینکه آلیس چه بیتی را انتخاب کرده و به آن ملزم شده است، باشد. ابتدا مورد ایده‌آلی را که در آن، رجیستر دوم مطلقاً شامل هیچ‌گونه اطلاعاتی در مورد مقدار b نباشد را بررسی می‌کنیم [۲۰] (طرح BC بنت و براسارد از نوع ایده‌آلی می‌باشد) و در انتها نیز مورد غیرایده‌آلی را بررسی می‌کنیم.

در حالت ایده‌آلی، یکسان بودن ماتریس‌های چگالی وابسته به بیت‌های 0 و ۱ در رجیستر دوم یعنی

$$Tr_A|0\rangle\langle 0| \equiv \rho_0^B = \rho_1^B \equiv Tr_A|1\rangle\langle 1| \qquad (۳-۴)$$

می‌تواند ما را مطمئن و متقاعد سازد که باب هیچ‌گونه اطلاعاتی در مورد بیت b موردنظر به دست نمی‌آورد.

با توجه به تجزیه‌ی اشمیت [۲۱] داریم:

$$|0\rangle = \sum_K \sqrt{\lambda_K}\,|\hat{e}_K\rangle_A \otimes |\hat{\varphi}_K\rangle_B \quad , \qquad (۴-۴)$$

$$|1\rangle = \sum_K \sqrt{\lambda_K}\,|\hat{e}'_K\rangle_A \otimes |\hat{\varphi}_K\rangle_B \qquad (۵-۴)$$

که $\{|\hat{e}_K\rangle_A\}$، $\{|\hat{e}'_K\rangle_A\}$ و $\{|\hat{\varphi}_K\rangle_B\}$ پایه‌های اورتونرمال فضاهای هیلبرت مربوطه (متناظر) هستند و λ_Kها ویژه مقادیر عملگر چگالی کاهیده ($Tr_A|0\rangle\langle 0| = Tr_A|1\rangle\langle 1|$) هستند. توجه نمائید که λ_Kها و نیز $|\hat{\varphi}_K\rangle$ها برای دو حالت ($|0\rangle$ و $|1\rangle$)، یکسان بوده و تنها تفاوت موجود، در $|\hat{e}_K\rangle$ و $|\hat{e}'_K\rangle$ مربوط

به آلیس می‌باشد. حال تبدیل یکانی U_A که $|\hat{e}_K\rangle_A$ را به $|\hat{e}'_K\rangle_A$ تصویر می‌کند در نظر بگیرید. بدیهی است که این تبدیل $|0\rangle$ را به $|1\rangle$ تصویر می‌کند. به خاطر داشته باشید که تبدیل U_A فقط (صرفاً) بر روی سیستم آلیس اثر کرده و با این حال $|0\rangle$ را به $|1\rangle$ دوران می‌دهد. یعنی آلیس می‌تواند بدون کمک باب، U_A را به کار گرفته و اعمال نماید. بنابراین آلیس می‌تواند با تغییر b=0 به b=۱ در مرحله‌ی افشا، تقلب نماید (از آنجائیکه $|\hat{e}_k\rangle_A$ و $|\hat{e}'_k\rangle_A$ دو پایه‌ی اورتونرمال هستند، مسلماً یک تبدیل یکانی U_A وجود دارد که (فقط بر روی فضای هیلبرت آلیس اثر می‌کند و) برای هر k، $|\hat{e}_k\rangle_A$ را به $|\hat{e}'_k\rangle_A$ تبدیل می‌کند. در واقع این تبدیل، $\sum_k |\hat{e}'_k\rangle\langle\hat{e}_k|$ می‌باشد).

برای فهم و وضوح بیشتر، استراتژی تقلب ذیل را در نظر بگیرید: در مرحله‌ی اول آلیس همواره $|0\rangle$ (متناظر با b=0) را تهیه می‌کند. سپس وی از مرحله‌ی (اندازه‌گیری) دوم جهش زده (اندازه‌گیری را به تأخیر می‌اندازد) و رجیستر دوم را، همانطور که در توضیح مرحله‌ی ۳ ذکر شد، برای باب ارسال می‌کند. وی فقط در آغاز مرحله‌ی بازگشایی (مرحله‌ی۴)، در مورد اینکه چه بیتی را به عنوان مقدار b اعلام (آشکار) کند، تصمیم‌گیری می‌نماید: اگر وی بخواهد مقدار b را صفر اعلام کند، پروتکل را به صورت صادقانه اجرا می‌کند. به عبارت دیگر اگر وی اکنون تصمیم بگیرد که وانمود کند b انتخابی ۱ بوده است، تبدیل یکانی U_A را برای چرخاندن $|0\rangle$ به $|1\rangle$ اعمال کرده و در عوض، پروتکل را برای b=۱ اجرا می‌کند. در نتیجه، آلیس همواره می‌تواند با موفقیت تقلب نماید. توجه نمائید که اصولاً آلیس قادر است تقلب نماید زیرا وی می‌تواند اندازه‌گیری خود را تا مرحله‌ی ۴ به تأخیر بیندازد و بنابراین برای انجام این کار، وی عموماً به یک کامپیوتر کوانتومی نیاز دارد. (اگر چه ساخت یک کامپیوتر کوانتومی، یک شاهکار تکنولوژیکی چالش‌برانگیز به شمار می‌آید ولی با این حال، این کار توسط قوانین فیزیک کوانتومی ممنوع نشده است). در پروتکلی مانند طرح معروف BCJL [۲۲]، امکان جهش آلیس متقلب از مرحله‌ی دوم (یعنی به تأخیر انداختن اندازه‌گیری‌ها) در نظر گرفته نشده بود. به همین دلیل، پژوهشگران قبلی به اشتباه به این نتیجه رسیده بودند که طرح مزبور غیرقابل نفوذ (شکست ناپذیر) می‌باشند.

در بحث فوق یک موقعیت ایده‌آلی را در نظر گرفتیم. یعنی موقعیتی که در آن باب طی مرحله‌ی التزام، مطلقاً هیچ‌گونه اطلاعاتی در مورد مقدار b نداشته و از اینرو ماتریس‌های چگالی توصیف‌کننده‌ی رجیستر دوم برای دو مورد b=0 و b=۱ مشابه و همانند بودند (معادله‌ی ۴-۳ را ببینید). با این حال، طرح‌هایی نیز ارائه شده‌اند [۱۹ و ۲۲] که غیر ایده‌آلی هستند. بدین معنا که این طرح‌ها معادله‌ی (۴-۳) را اندکی نقض کرده و باب با یک احتمالی، می‌تواند بین ρ_0^B و ρ_1^B تمایز برقرار کند (یعنی ρ_0^B و ρ_1^B مشابه و یکسان نبوده و توسط باب قابل تشخیص می‌باشند). ولی به نظر می‌رسد که این موضوع، نتیجه را تغییر نمی‌دهد: اگر باب با احتمال زیادی هم بتواند بین دو حالت تمایز برقرار کند، باز هم طرح در برابر تقلب باب غیر ایمن خواهد بود. به عبارت دیگر، اگر احتمال تشخیص دو حالت توسط باب بسیار کوچک باشد، بدیهی است که دو ماتریس چگالی ρ_0^B و ρ_1^B می‌بایست بسیار نزدیک به هم (مشابه) بوده و نیز اساساً همان فیزیک بر آن اعمال شود.

حال، مورد غیرایده‌آلی یعنی زمانیکه $\rho_0^B \neq \rho_1^B$ است را در نظر می‌گیریم [۲۰]. نزدیکی و شباهت بین دو حالت باب (که به وسیله‌ی دو ماتریس چگالی ρ_0^B و ρ_1^B مشخص می‌گردد)، معمولاً توسط مفهومی به نام ضریب اطمینان[۱] [۴و۲۳] (که می‌تواند بر حسب مفهوم خالص‌سازی‌ها تعریف و معین گردد) توصیف می‌شود. سیستم A را در نظر بگیرید که به سیستم B مربوط به باب متصل است. حالت‌های خالص $|\psi_0\rangle$ و $|\psi_1\rangle$ بسیاری در سیستم مرکب حاصل وجود دارند به طوریکه

$$Tr_A(|\psi_0\rangle\langle\psi_0|) = \rho_0^B \quad \text{و} \quad Tr_A(|\psi_1\rangle\langle\psi_1|) = \rho_1^B \qquad (۶-۴)$$

حالت‌های خالص $|\psi_0\rangle$ و $|\psi_1\rangle$، خالص‌سازی‌های ماتریس‌های چگالی ρ_0^B و ρ_1^B نامیده می‌شوند. براین اساس، ضریب اطمینان می‌تواند بر حسب این خالص‌سازی‌ها به صورت زیر تعریف و تعیین گردد:

$$F(\rho_0^B, \rho_1^B) = Max\left|\langle\psi_0|\psi_1\rangle\right| \qquad (۷-۴)$$

[۱] Fidelity

که بیشینه‌سازی، بر روی تمام خالص‌سازی‌های ممکنه می‌باشد (همه‌ی خالص‌سازی‌های ممکنه را دربر می‌گیرد). مقدار ضریب اطمینان همواره بین 0 و ۱ می‌باشد ($0 \leq F \leq 1$). این مقدار برابر ۱ است اگر و فقط اگر $\rho_0^B = \rho_1^B$. لازم به ذکر است که برای هر خالص‌سازی ثابت ρ_1^B، مثلاً $|1\rangle$ در معادله‌ی (۴-۲)، یک خالص‌سازی موازی حداکثری[۱] ρ_0^B وجود دارد که در معادله‌ی (۴-۷) صدق می‌کند.

برای طرح‌های QBC غیر ایده‌آلی، این واقعیت که باب احتمال کمی برای تشخیص و ایجاد تمایز بین ρ_0^B و ρ_1^B دارد بدین معناست که [۲۴]

$$F(\rho_0^B, \rho_1^B) = 1-\delta \quad \text{(برای } \delta>0 \text{ کوچک)} \qquad (۴-۸)$$

سپس، از معادلات (۴-۷) و (۴-۸) چنین نتیجه می‌شود که (برای حالت $|1\rangle$ مفروض در معادله‌ی ۴-۲)، یک خالص‌سازی $|\psi_0\rangle$ از ρ_0^B وجود دارد به طوریکه:

$$\left|\langle\psi_0|1\rangle\right| = F(\rho_0^B, \rho_1^B) = 1-\delta. \qquad (۴-۹)$$

استراتژی‌ای که آلیس متقلب در مقابل یک طرح BC غیر ایده‌آل به کار می‌گیرد مشابه قبل است. وی در مرحله‌ی اول، حالت $|0\rangle$ که متناظر با b=0 می‌باشد را تهیه کرده، از مرحله‌ی (اندازه‌گیری) دوم جهش می‌زند و رجیستر دوم را - همانطور که در توضیح مرحله‌ی سوم بیان شد- برای باب می‌فرستد. وی فقط در شروع مرحله‌ی افشا (مرحله‌ی ۴) در مورد مقدار b تصمیم می‌گیرد. حال اگر وی تصمیم بگیرد که b=0 را افشا نماید، وی به سادگی، پروتکل را صادقانه دنبال می‌کند. ولی اگر b=۱ را انتخاب کند، یک تبدیل یکانی را بر روی سیستم کوانتومی سهم خود اعمال می‌کند تا حالت $|\psi_0\rangle$ای که در معادله‌ی (۴-۹) صدق می‌کند را به دست آورد. چنین تبدیل یکانی‌ای وجود دارد زیرا، همانطور که در تجزیه‌ی اشمیت می‌توان دید [۲۱]، تمام خالص‌سازی‌های $|\varphi\rangle_{AB}$ یک ماتریس چگالی ثابت ρ_B، توسط تبدیلات یکانی‌ای که فقط بر روی A اثر می‌کنند (فضای A در اختیار آلیس است)، به یکدیگر مربوط و وابسته‌اند. توجه نمائید که اگر آلیس صادق می‌بود، وی (در عوض) می‌بایست در مرحله‌ی اول، $|1\rangle$ را تهیه می‌کرد (معادله‌ی ۴-۲). با این حال، از آنجائی که $|\psi_0\rangle$ و $|1\rangle$ بسیار مشابه هم

[۱] Maximally Parallel Purification

هستند (معادله‌ی ۴-۹) باب، به سختی و با صرف زمان بسیار زیادی ممکنست موفق به شناسایی تقلب آلیس گردد. بنابراین آلیس با احتمال خیلی زیاد می‌تواند موفق به تقلب شود. (لازم به ذکر است که این استراتژی، تنها استراتژی تقلب ممکن نیست. به عبارت دیگر، با توجه به تقارن، می‌توان استراتژی تقلب دیگری به کار گرفت که در آن، کاربرد 0 و ۱ با یکدیگر جابه‌جا شده باشد. یعنی آلیس می‌تواند، مثلاً، در مرحله‌ی اول به جای تهیه‌ی حالت $|0\rangle$، حالت $|1\rangle$ را تهیه کرده و از اینرو به b=1 ملزم گردد و استراتژی را بر این اساس ادامه دهد.)

در همین راستا، مایرز نتیجه‌ی فوق را تعمیم داد [۱۶] و اثبات کرد که تمام طرح‌های BC کوانتومی، از جمله آنهایی که شامل ارتباطات (کوانتومی) دو طرفه بین آلیس و باب هستند، غیر ایمن می‌باشند. بعدها، لو نیز عدم امکان پروتکل‌های کوانتومی دیگر را اثبات کرد [۲۵]. این کشفیات غافلگیرکننده، یک پسرفت و مشکل در رمزنگاری کوانتومی به شمار می‌آید. از اینرو حد و مرز واقعی قدرت رمزنگاری کوانتومی به عنوان یک موضوع مهم برای تحقیقات آتی به شمار می‌آید.

حال، با این مقدمات، به بررسی دو پروتکل BC می‌پردازیم. ولی قبل از آن لازمست که توضیح مختصری در مورد مخروط نوری (که در پروتکل دوم مفهومی کلیدی می‌باشد) بیان کنیم:

۴-۴ مخروط نوری

در نظریه‌ی نسبیت خاص، مخروط نوری به توصیف ظاهری انتشار نور (که تجلی کننده‌ی یک تک رویداد است) در نمودار فضا-زمان مینکوفسکی اطلاق می‌شود. چنانچه شکل انتشار موج را بر روی محور افقی (طول و عرض) دو بعدی و محور عمودی (محور زمان) در نظر بگیریم این مخروط به شکل سه بعدی ترسیم خواهد شد.

براساس قانون ماکسول، سرعت نور همواره ثابت و مستقل از سرعت منبع نور است (این مسئله با اندازه‌گیری‌های دقیق اثبات شده است). بر این اساس، اگر پالسی از نور در لحظه و مکان به خصوصی منتشر شود، همچنان که زمان می‌گذرد مانند کره‌ای نورانی با سرعت نور گسترش پیدا می‌کند به طوریکه اندازه و وضعیت آن مستقل از سرعت جسم است. بعد از گذشت یک میلیونیم ثانیه، گسترش

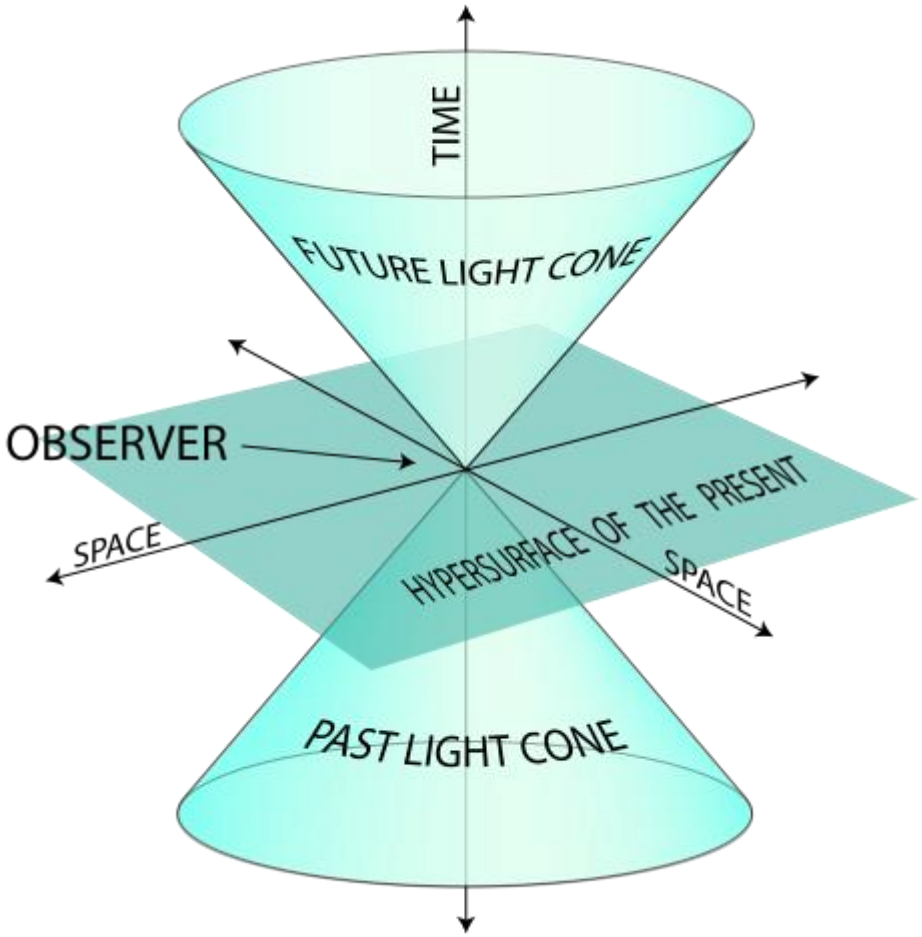
شعاع نور، کره‌ای به شعاع ۳۰۰ متر ایجاد خواهد کرد و به همین ترتیب بعد از گذشت دو میلیونیم ثانیه، شعاع این کره به دو مقدار قبل خواهید رسید و به همین ترتیب این مقدار افزایش پیدا می‌کند. این واقعه شبیه گسترش امواجی است که در اثر برخورد یک سنگ با سطح آب یک آبگیر به وجود می‌آید. این امواج به شکل دایره‌هایی ظاهر می‌شوند که با گذشت زمان بر شعاع آن‌ها افزوده می‌شود. اگر مجموعه‌ای از تصاویر امواج در حال گسترش را به ترتیب زمانی روی هم قرار دهیم، مخروطی سه بعدی تشکیل می‌شود که محور افقی آن را مختصات طولی و عرضی دایره‌ها تشکیل می‌دهند و محور عمودی آن، زمان می‌باشد. در نتیجه رأس این مخروط، لحظه‌ی برخورد سنگ با سطح آب می‌باشد. به همین نحو، گسترش شعاع‌های نور بر اثر یک رویداد، مخروطی سه بعدی در دستگاه چهار بعدی فضا-زمان تشکیل می‌دهد که به آن مخروط نوری آینده‌ی[۱] رویداد می‌گویند. به همین ترتیب، قادر به رسم مخروط دیگری خواهیم بود که معرف مجموعه رویدادهایی است که توسط آن‌ها، نور توانایی رسیدن به یک رویداد معین را دارد که این مخروط، مخروط نوری گذشته‌ی[۲] رویداد نام دارد.

مخروط‌های نوری گذشته و آینده‌ی رویداد p، فضا-زمان را به سه ناحیه تقسیم می‌کنند. آینده‌ی مطلق رویداد، درون مخروط نوری آینده‌ی p است و مجموعه‌ای از رویدادهایی است که می‌توانند از آنچه در p روی می‌دهد، متأثر گردند (نقاط زمان گونه[۳]). امواج منتشر شده از p، به رویدادهای خارج مخروط نوری آینده‌ی p (نقاط فضاگونه[۴]) دسترسی ندارند چرا که هیچ چیزی سریعتر از نور حرکت نمی‌کند (همچنین هیچ رابطه‌ی علی بین رویدادهای فضاگونه برقرار نیست). بنابراین، آنچه در p روی می‌دهد تأثیری بر این رویدادها ندارند و بالعکس. گذشته‌ی مطلق p، درون مخروط نوری گذشته قرار دارد و مجموعه‌ای از رویدادهاست که علائم آن‌ها با سرعت نور یا کمتر از آن حرکت می‌کنند و می‌توانند به p برسند (نقاط زمان گونه). از این رو این مجموعه، شامل همه‌ی رویدادهایی است که محتملاً بر آنچه در p می‌گذرد تأثیر داشته‌اند. اگر کسی خبر داشته باشد که در زمان معین، در همه‌ی

---

[۱] Future Light Cone
[۲] Past Light Cone
[۳] Time Like
[۴] Space Like

نقاط ناحیه‌ای از فضا-زمان که درون مخروط نوری گذشته‌ی p واقع شده، چه اتفاقاتی روی داده است، می‌تواند پیش‌بینی کند که در p چه چیز رخ خواهد داد. همه‌ی نقاط دیگر، ناحیه‌ای از فضا-زمان را تشکیل می‌دهند که در مخروط نوری آینده و گذشته‌ی p قرار ندارند (نقاط فضاگونه). آن‌ها نه بر رویدادهای p تأثیر می‌گذارند و نه از آن‌ها تأثیر می‌پذیرند.



شکل ۴-۱: مخروط نوری در فضای دو بعدی بعلاوه‌ی یک بعد زمان

۴-۵ پروتکل‌های QBC

۴-۵-۱ پروتکل BC کوانتومی غیرنسبیتی حساس به تقلب[۱]

یک پروتکل BC کوانتومی را حساس به تقلب می‌نامند، اگر در آن، با فرض اینکه سند التزام در نهایت فاش خواهد شد، آلیس به هیچ‌وجه نتواند (بدون وجود خطر ردیابی) احتمالات فاش‌سازی 0 یا ۱ را بعد از ملزم شدن، تغییر دهد (ویژگی تقید[۲]) و نیز باب به هیچ‌وجه نتواند قبل از فاش‌سازی، اطلاعات اضافی (و بیشتر) در مورد بیت انتخابی (و محرمانه‌ی) آلیس به دست آورده، تقلب نماید (ویژگی اخفا[۳]). یعنی آلیس و باب کاملاً متقاعد و مطمئن باشند که به محض انجام تقلب، با خطر شناسایی و ردیابی تقلب مواجه خواهند بود.

اگر یک BC توسط حالت‌های کوانتومی غیرمتعامد، رمزی شود، هر تلاش باب مبنی بر کسب اطلاعات بیشتر در مورد بیت انتخابی آلیس منجر به اختلال درحالت‌ها خواهد شد. این بدان معناست که اگر باب بعداً مجبور شود که حالت انتخابی آلیس را به وی بازگرداند با خطر ردیابی مواجه خواهد شد و نیز اگر آلیس حالتی را بفرستد و بعداً ادعا کند حالت دیگری را انتخاب کرده بود، تقلبش فاش می‌شود. این نکته یک استراتژی برای BC حساس به تقلب ارائه و پیشنهاد می‌دهد. مسئله‌ی اساسی و مهم اینست که این پروتکل‌ها به گونه‌ای طراحی شوند که طرفین به طور همزمان در معرض خطر شناسایی تقلب قرار گیرند. روش‌های BC کوانتومی استاندارد و معمول در اینجا مؤثر واقع نمی‌شوند. مثلاً چنانچه آلیس در زمان فاش‌سازی، حالتی که به آن ملزم شده است را به باب اعلام کند، در اینصورت پروتکل به هیچ‌وجه نمی‌تواند حساس به تقلب باشد زیرا باب حتی اگر حالت اولیه و اصلی را (به واسطه‌ی اندازه‌گیری) مختل کرده باشد باز هم می‌تواند یک کپی از حالت را به آلیس بازگرداند. همانطور که در ادامه نیز نشان داده خواهد شد، راه‌حل‌هایی پیرامون این مشکل وجود دارد.

حال درصدد توصیف یک پروتکل BC کوانتومی حساس به تقلب غیر نسبیتی برمی‌آئیم [۲۶]. برای

---

[۱] Cheat Sensitive
[۲] Binding property
[۳] Concealing Property

این منظور $|0\rangle$ و $|1\rangle$ را به عنوان حالت‌های کیوبیتیِ اورتونرمال (نرمالیزه و متعامد) درنظر گرفته و نیز داریم: $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. پروتکل در ۴ مرحله انجام می‌شود:

مرحله‌ی 0 : مرحله‌ی مقدماتی- در این مرحله، باب یک حالت یکتا[۱](تکتایه) به صورت زیر تهیه کرده و کیوبیت A را برای آلیس می‌فرستد:

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

حال هر دو شخص مزبور، یک نیمه از حالت یکتا (تکتایه) را در اختیار دارند. هر یک ازطرفین می‌تواند در هر مرحله از پروتکل، این حالت را به چالش [۲] بکشد (این شخص چالش‌گر[۳] نامیده می‌شود). بدین معنی که طرف دیگر می‌بایست یک کیوبیت را که فرض می‌شود نیمه‌ی دیگر تکتایه است را برای چالش‌گر بفرستد تا وی بتواند با استفاده از اندازه‌گیری تصویری مربوطه بررسی کند که آیا این دو حالت کیوبیتی، تشکیل یک حالت یکتا می‌دهند یا نه. و بدین طریق پی به تقلب ببرد. به طوریکه اگر در این تست، حالت، یکتا نبود، تقلب طرف مقابل شناسایی می‌گردد.

مرحله‌ی۱: تهیه‌ی سند التزام– چنانچه آلیس بخواهد به یک بیت کلاسیکی معین ملتزم شود، این پروتکل، فرآیند التزام ساده‌ای را پیش روی وی قرار می‌دهد: در صورت انتخاب 0، (برای ملتزم شدن به آن) وی یک کیوبیت C را به صورت رندوم از $|0\rangle$ یا $|-\rangle$ (هر یک با احتمال $\frac{1}{2}$) و برای ملزم شدن به ۱، C را از میان $|1\rangle$ یا $|+\rangle$ (با احتمال $\frac{1}{2}$) تهیه می‌کند. سپس کیوبیت C را (به عنوان سند التزام) برای باب می‌فرستد.

مرحله‌ی۲: افشا- قرارداد می‌شود که ابتدا آلیس در موقعیت (تست) چالش حالت قرار گیرد. اگر او این کار را انجام دهد و در نتیجه‌ی انجام چالش متوجه شود که حالت، یکتا نیست (تست با شکست مواجه شود)، توانسته تقلب (باب) را شناسایی کند. سپس، خواه آلیس چالش انجام دهد یا نه، وی

[۱] Singlet State
[۲] Challenge
[۳] Challenger

مؤظف است که مقدار بیت کلاسیکی انتخابی خود (و نه کیوبیت C استفاده شده به منظور رمزی کردن آن) را فاش کند. در نهایت (در صورتی که آلیس از موقعیت چالش خود استفاده نکند) باب در موقعیت انجام چالش قرار می‌گیرد. او نیز در صورت انجام این کار و شکستِ تست، پی به تقلب آلیس خواهد برد.

مرحله‌ی۳: بازی- چنانچه یکی از آن دو (و زودتر) تکتایه را به چالش بکشد، در این صورت خواه ناخواه بازی را از دست می‌دهند. ولی چنانچه هیچ‌یک از آن دو اقدام به چالش نکند، نوبت آن می‌رسد که هر یک، کیوبیت یکتایی که در اختیار دارند را در پایه‌ی $|1\rangle$ و $|0\rangle$ اندازه‌گیری کنند. سپس باب نتیجه‌ی اندازه‌گیری خود را برای آلیس فرستاده و آلیس آن را با نتیجه‌ی خود مقایسه می‌کند (که این دو باید عکس هم باشند). چنانچه این دو مقدار عکس هم نبودند، آلیس متوجه تقلب باب می‌شود. ولی چنانچه نتایج عکس هم باشند، بسته به اینکه نتیجه‌ی باب چیست، یکی از دو نفر بازی را می‌بازد: اگر نتیجه‌ی باب ۱ باشد، آلیس، و اگر 0 باشد باب بازنده خواهد بود (پس طبیعی است که باب بخواهد تقلب نماید). حال:

الف) اگر آلیس ببازد: وی می‌بایست حالتی را که برای رمزکردن بیت انتخابی‌اش، در کیوبیت C استفاده کرده فاش کند. سپس باب بر روی C اندازه‌گیری کرده تا بررسی کند که آیا این C در همان حالتی است که آلیس ادعا می‌کند یا خیر. که اگر اینطور نبود نشان می‌دهد آلیس تقلب نموده است.
ب) اگر باب ببازد: وی می‌بایست کیوبیت C را به آلیس برگرداند. سپس آلیس نیز یک اندازه‌گیری بر روی آن انجام می‌دهد تا ببیند آیا این کیوبیت هنوز در همان حالتی که در ابتدا آماده کرده و به باب تحویل داده بود، باقی مانده یا نه. که اگر اینطور نبود (نشان می‌دهد که باب به منظور کسب اطلاعات، بر روی آن اندازه‌گیری انجام داده و بدین طریق) تقلب را شناسایی نموده است.

در اینجا پروتکل به اتمام می‌رسد. توجه نمائید که تست‌های تقلب فقط به منظور شناسایی شخص متقلب صورت می‌پذیرد و همانطور که در رمزنگاری بدگمان[۱] مرسوم است این گونه پروتکل‌ها اساساً

[۱] Mistrustful Cryptography

به منظور محافظت از اشخاص صادق در برابر تقلب‌ها طراحی می‌شوند و نه لزوماً برای محافظت شخص متقلب در مقابل دیگری.

اثبات ایمنی این پروتکل [۲۶] مبتنی بر حقایق زیر است: ۱) باب به هیچ وجه نمی‌تواند در مقابل درخواست آلیس (به عنوان چالش‌گر) چیزی به غیر از نیم- تکتایه برای وی بفرستد چرا که در غیر اینصورت با خطر شکست تست چالش تکتایه مواجه خواهد شد. ۲) چنانچه آلیس یا باب، هرگونه اندازه‌گیری غیر بدیهی (با اهمیت) بر روی تکتایه انجام دهد، در معرض شکست تست چالش تکتایه قرار خواهد گرفت. اگر آلیس تست چالش خود را صرفاً به منظور اجتناب از اینکه مورد چالش واقع شود انجام دهد، مطمئن خواهد بود که بازی را از دست خواهد داد. این موضوع وی را ملزم به فاش-سازی و تهیه‌ی یک سند التزام صادقانه می‌سازد. ۳) هنگامی که آلیس و باب (دیگر) نتوانند به چالش کشیده شوند، آنها به هیچ وجه نمی‌توانند به طور مفید از کیوبیت تکتایه‌ی خود در هر پردازش اطلاعات کوانتومی استفاده کنند.

۴-۵-۲ ارسال التزام‌آور ایمن بدون شرط بیت بوسیله‌ی انتقال نتایج اندازه‌گیری

۴-۵-۲-۱ مقدمه

هدف از ارائه‌ی این بحث ایجاد یک ارتباط ایمن بین دو شخص (آلیس و باب)، از طریق مبادله‌ی نتایج اندازه‌گیری است. بدین منظور یک طرح جدید برای BC ایمن بدون شرط مبتنی بر علیت مینکوفسکی و خواص و ویژگی‌های اطلاعات کوانتومی پیشنهاد و ارائه می‌دهیم. در این پروتکل شخص دریافت‌کننده تعدادی از کیوبیت‌های BB84 را به صورت رندوم انتخاب کرده و به نقطه‌ای مفروض (و از قبل تعیین شده) از فضا-زمان برای شخصی که قرار است ملتزم شود[۱] می‌فرستد. (پس رویداد ارسال کیوبیت و دریافت آن، دو نقطه از فضا-زمان خواهند بود. این دو رویداد زمان‌گونه هستند بدان معنا که رویداد ارسال رشته کیوبیت می‌تواند در هر نقطه‌ای در دستگاه فضا-زمان باشد ولی رویداد دریافت آن می‌بایست نسبت به رویداد اول زمان گونه باشد). سپس فرد ملتزم بسته به

[۱] Committer

مقدار بیتی که قصد دارد انتخاب و به آن ملزم گردد در یکی از دو پایه‌ی BB84 [{۱و۰} و {- و +}] اندازه‌گیری انجام داده و نتایج اندازه‌گیری را به صورت ایمن، با سرعت نور (و یا نزدیک به سرعت نور) در جهت‌های مخالف به نمایندگانش که در مکانی دورتر از او قرار دارند می‌فرستد (این جهت‌ها توافقی بوده و در فضای مینکوفسکی به صورت دو جهت مخالف مکانی هستندکه معرف دو رویداد در مخروط نوری مربوطه‌اند). این نمایندگان برای افشا کردن بیت‌ها، خروجی‌های اندازه‌گیری را برای نمایندگان دریافت‌کننده (که در همان نزدیکی هستند) نمایان می‌کنند. در ادامه بررسی می‌شود که ایمنی این پروتکل [۲۷] (فقط) متکی بر ویژگی‌های ساده‌ی اطلاعات کوانتومی و عدم امکان علامت‌دهی با سرعت بیشتر از سرعت نور[۱] می‌باشد.

اکثر تحقیقاتی که برروی فیزیک و رمزنگاری انجام شده به منظور بررسی مسئله‌ی BC بوده است. موضوعی که یکی از اهداف بنیادین رمزنگاری به شمار می‌آید و کاربردهای بسیاری دارد (مثلاً [۲۸]). همانطور که قبلاً نیز بیان شد، در حالت کلی در یک پروتکل ارسال التزام‌آور بیت (BC)، فرد ملتزم (آلیس) یکسری عملیات انجام می‌دهد تا به یک مقدار بیت خاص (و یا درمورد کوانتومی یک برهم-نهی خاص از بیت‌ها) ملزم گردد. وی بعداً (یا در مورد نسبیتی، در یک یا چند نقطه در آینده‌ی علی commitment)، اگر بخواهد، می‌تواند یکسری اطلاعات کلاسیکی یا کوانتومی را به منظور افشای بیت انتخابی (و البته محرمانه)، به دریافت‌کننده یعنی باب بدهد.

به طور ایده‌آل و به عنوان یک اصل، (پروتکل‌های BC و در نتیجه) این پروتکل می‌بایست باب را کاملاً مطمئن سازد که آلیس به عملیات اولیه‌اش متعهد و پایبند می‌ماند و در مقابل به آلیس نیز این اطمینان (و تضمین) را بدهد که باب نمی‌تواند قبل از مرحله‌ی فاش‌سازی، هیچ‌گونه اطلاعاتی در مورد بیت انتخابی وی به‌دست آورد.

ارسال التزام‌آور بیت علاوه بر اینکه به خودی‌خود از نظر رمزنگاری بسیار مهم و کاربردی است، ارتباط عمیقی نیز با فیزیک بنیادی دارد. در ابتدا، کار در این محدوده فقط بر پروتکلهای BC مبتنی

[۱] No Signaling

بر مکانیک کوانتومی غیرنسبیتی متمرکز بود. بنت و براسارد اولین پروتکلBC کوانتومی را طراحی کردند و نشان دادند که این پروتکل در مقابل هر دو طرف تکنولوژی مزبور، ایمن است ولی چنانچه آلیس یک حافظه‌ی کوانتومی داشته باشد غیر ایمن خواهد بود [۱۸]. همین امر ایمنی این پروتکل را مشروط می‌نماید. در این میان مایرز[۱] [۱۶و ۱۷]، لو[۲] و چائو[۳] [۲۰و۲۹] نشان دادند که تلاش در زمینه‌ی پروتکل‌های غیرنسبیتی ایمن بدون شرط [مثلاً ۲۲] بی‌فایده است و تلاش‌های بعدی نیز نشان داد [۳۰و۳۱] که هیچ پروتکل BC کوانتومی غیرنسبیتی ایمن بدون شرطی نمی‌تواند وجود داشته باشد.

با این حال جهان نسبیتی است و با تقریب خوبی می‌توان گفت که فضا- زمان در اطراف و نزدیک زمین، مینکوفسکی است. ازاین رو، پروتکل‌های نسبیتی که در آنها به واسطه‌ی علیت مینکوفسکی قید علامت دهی[۴] به‌کار گرفته می‌شود، تصویر و دیدگاه قبلی را به طور اساسی تغییر می‌دهند.

در این‌جا یک پروتکل BC جدید نسبیتی کوانتومی پیشنهاد و مطرح می‌شود. این پروتکل از برخی فرض‌های مشابه با مرجع [۳۳] استفاده می‌کند: به موجب علیت مینکوفسکی، فرد ملزم شونده مجبور است که یک commitment خاص را از نقطه‌ای از فضا-زمان که پروتکل از آنجا شروع می‌شود انتخاب نماید (یعنی از همان نقطه‌ی فضا-زمانی که پروتکل BC شروع می‌شود علیت مینکوفسکی بر آن تحمیل و برقرار می‌شود. بدین معنی که سرعت نباید بیشتر از سرعت نور باشد و اگر رویدادی علت رویدادی دیگر است می‌بایست در قسمت زمان‌گونه‌ی مخروط نوری مربوطه باشد و بالعکس). با این حال، این پروتکل متکی بر اصل فیزیکی متفاوتی نیز هست و آن عبارتست از: عدم امکان انجام کامل یک اندازه‌گیری غیر موضعی بر روی حالتی که در خارج از مخروط نوری آینده‌ی مشترک اجزایش توزیع شده است. عملیاتی کردن و اجرای این پروتکل مستلزم (به‌کارگیری) کمترین تدابیر و منابع کوانتومی می‌باشد: لازمست که دریافت‌کننده، حالت‌های کوانتومی‌ای را (که می‌توانند کیوبیت‌های

---

[۱] Mayers
[۲] Lo
[۳] Chau
[۴] Signaling

غیر درهم‌تنیده باشند) برای فرد ملتزم بفرستد و نیز لازمست که این شخص به محض دریافت حالت-ها، برروی آنها اندازه‌گیری مجزا و منفرد[۱] انجام دهد. در این پروتکل نیاز به هیچ‌گونه مخابرات و ارتباطات کوانتومی بیشتری توسط طرفین، هیچ‌گونه درهم‌تنیدگی، اندازه‌گیری‌های جمعی[۲] و نیز ذخیره‌ی حالت‌های کوانتومی نیست.

همانگونه که در رمزنگاری کوانتومی مرسوم است، این پروتکل را نیز به‌صورت کاملاً ایده‌آلی مطرح می‌کنیم یعنی ارائه‌ی پروتکل با فرض کامل بودن اندازه‌گیری‌ها، انتقال‌ها و آماده‌سازی‌های حالت. این فرض‌های ایده‌آلی و غیر واقعی هیچ مشکل و مسئله‌ی قابل توجهی در اصول ایجاد نمی‌کنند: چرا که پروتکل‌ها در حضور خطا، تا یک حد آستانه‌ی معین، ایمن باقی می‌مانند که خطای انسانی ناشی از در نظر نگرفتن این فرض‌های ایده‌آلی نیز در همین حدود قرار می‌گیرند. در این پروتکل، یکسری ایده‌آل سازی‌ها در مورد هندسه‌ی نسبیت و سرعت علامت‌دهی انجام می‌دهیم، فرض می‌کنیم که آلیس و باب هر یک، نمایندگانی در آزمایشگاه‌های ایمن دارند که این آزمایشگاه‌ها به فاصله‌ی کمی از نقاط p، Q_1 و Q_0 قرار گرفته‌اند، آلیس قادر به مخابره‌ی سیگنال با سرعتی دقیقاً برابر با سرعت نور است و نیز تمام پردازش‌های اطلاعات به صورت آنی انجام می‌پذیرد. این فرض‌ها نیز در اصل هیچ مشکلی ایجاد نمی‌کنند. مشابه تمام پروتکل‌های این چنینی [۳۳و۳۴] این پروتکل نیز هنگامی که بصورت واقع-گرایانه به‌کار رود، یعنی فواصل (جدایی) محدود و ارتباطات با سرعتی نزدیک به سرعت نورانجام شوند، همچنان ایمن باقی خواهد ماند. اگر این تصحیحات کوچک باشند تنها تأثیر چشمگیری که می‌تواند در پی داشته باشد آنست که باب کاملاً مطمئن می‌شود سند التزام آلیس به جای آنکه از خود نقطه‌ی p مقید شود از یک نقطه‌ی p' در آینده‌ی علی نزدیک به p مقید می‌شود.

۴-۵-۲-۲ BC مبتنی بر انتقال نتایج اندازه‌گیری کوانتومی

در این‌جا نمونه‌ی ساده‌ای از طرح را با استفاده از حالت‌های کیوبیتی و نیز اندازه‌گیری‌هایی در پایه-ی BB84 استاندارد [۱۳] مطرح می‌کنیم [۳۵]. بدیهی است که این طرح می‌تواند به مجموعه‌ی

[۱] Individual Measurement
[۲] Collective Measurement

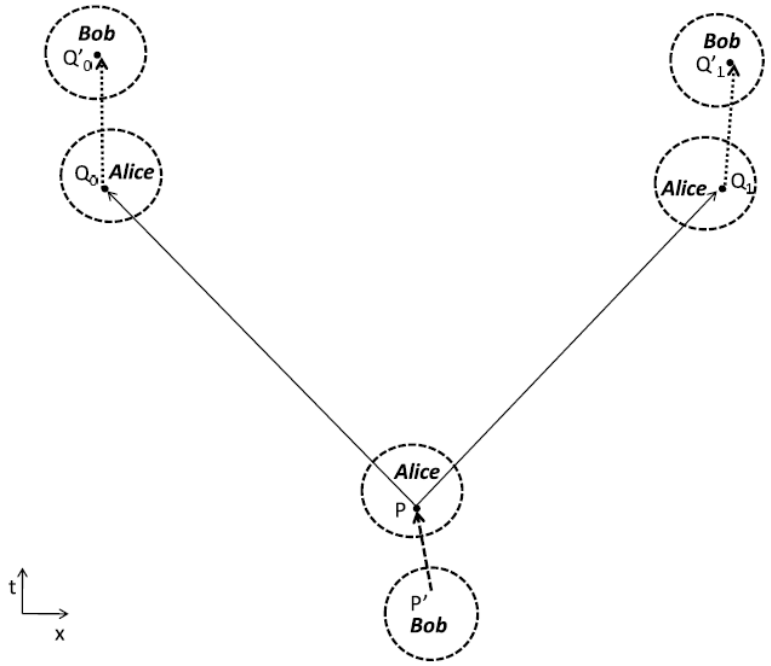
دیگری از اندازه‌گیری‌ها و حالت‌های کیوبیتی، به qudit ها و نیز به مواردی با نقاط فاش‌سازی بیشتر و متفاوت تعمیم داده شود.

آلیس و باب بر یک نقطه‌ی فضا-زمانی p به عنوان مبدأ، یک مجموعه مختصات (x, y, z, t) در فضای مینکوفسکی و (در ساده‌ترین مورد) دو نقطه‌ی $Q_0=(x,0,0,x)$ و $Q_1=(-x,0,0,x)$ که به صورت نور-گونه[1] از نقطه‌ی p قرار گرفته‌اند، با هم به توافق می‌رسند (در مخروط نوری مربوطه، نقطه‌ی p به عنوان زمان حال در مبدأ فرض می‌شود. بدین ترتیب Q_0 و Q_1 در دو جهت مخالف مکانی قرار گرفته و رویدادهای متناظر با این نقاط برروی مخروط قرار می‌گیرند. در نتیجه بر مبنای علیت مینکوفسکی، رویداد متناظر با نقطه‌ی p می‌تواند علت دو رویداد متناظر با Q_0 و Q_1 باشد چرا که برای رسیدن از p به Q_0 و Q_1 نیازمند سرعت نور هستند). آلیس و باب هر دو، در آزمایشگاه‌هایی ایمن نزدیک به هر یک از نقاط p، Q_0 و Q_1 نمایندگانی دارند که به منظور سهولت (و برای ساده‌سازی)، فاصله‌ی بین آزمایشگاه‌ها تا نقاط مربوطه را ناچیز فرض کرده و از این رو، نمایندگان (آزمایشگاه‌ها) در نقاط p، Q_0 و Q_1 (و نه نزدیک آن‌ها) فرض می‌شوند.

باب به طور کاملاً محرمانه، یک مجموعه کیوبیت $|\Psi i\rangle_{i=1}^{N}$ را به صورت مستقل و رندوم از حالت-های BB84 یعنی $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ (که $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$) انتخاب و تهیه کرده و سپس آن‌ها را برای آلیس فرستاده تا وی آن‌ها را در نقطه‌ی p دریافت کند (این کیوبیت‌ها به گونه‌ای ارسال می‌شوند که وقتی به p می‌رسند طبق قرارداد، آلیس در آنجا حضور داشته باشد یعنی یا آلیس در آن مکان حضور دارد و در غیراینصورت خود را در موعد مقرر به آنجا می‌رساند). سپس آلیس بر روی این حالت‌ها، یکسری اندازه‌گیری‌هایی انجام می‌دهد تا بدین طریق به یک مقدار بیت 0 یا ۱ متعهد گردد. به طوریکه: اگر وی بخواهد مقدار بیت 0 را انتخاب نموده و به آن ملزم گردد، هر حالت را در پایه‌ی z ($|0\rangle,|1\rangle$)، و برای انتخاب مقدار ۱، هر حالت را در پایه‌ی x ($|+\rangle,|-\rangle$) اندازه‌گیری می‌کند. حال

[1] Light-like

آلیس نتایج اندازه‌گیری خود را با کانال‌های کلاسیکی ایمن[۱] به نمایندگانش در Q_0 و Q_1 می‌فرستد (شکل۴-۲). این کانال‌های کلاسیکی ایمن آلیس می‌توانند (به عنوان مثال) توسط معابر تک زمانه‌ای[۲] (یک بار مصرف) که از قبل بین نماینده‌ی او در p و نیز نمایندگانش که در Q_0 و Q_1 حضور دارند، تعیین و به اشتراک گذاشته شده‌اند ایجاد شوند. در صورت لزوم و یا تمایل می‌توان این معابر را (توسط QKD و با استفاده از یکسری تغییرات جزئی در کیوبیت‌ها و انتقالات) به صورت متناوب، برای ایجاد ارتباط بین نمایندگان مربوطه استفاده نمود.



شکل ۴-۲: بکارگیری غیرایده‌آلی پروتکل در ابعاد۱+۱. آلیس و باب، نواحی فضا-زمانی گسسته‌ای که نمایش‌دهنده آزمایشگاه‌های ایمن مورد نظر هستند را تحت کنترل خود دارند. باب حالت‌های کوانتومی bb84 رندومی را در p' تولید کرده و آن‌ها را برای آلیس که در نقطه‌ی p حضور دارد می‌فرستد (پیکان خط تیره). سپس آلیس (در همان نقطه‌ی p)، در پایه‌های انتخابی‌اش، بر روی آنها اندازه‌گیری انجام داده و نتایج را با کانال‌های کلاسیکی ایمن و با سرعت (نزدیک به سرعت) نور به نمایندگانش واقع در نقاط Q_i می‌فرستد (پیکان‌های پیوسته و توپر). سپس نمایندگان آلیس این نتایج را به نمایندگان باب که در نزدیکی نقاط Q_i' قرار دارند مخابره می‌کنند (پیکان‌های نقطه‌چین).

[۱] کانال کلاسیکی ایمن کانالی است که در آنEve نتواند خود را به جای آلیس یا باب معرفی نماید.

[۲] One-time pads

برای افشای بیتی که آلیس به آن ملزم و مقید شده است، نمایندگان آلیس در (هر دو نقطه‌ی Q_0 و Q_1 نتایج اندازه‌گیری را برای نمایندگان باب (که در همان مکان حضور دارند) آشکار می‌کنند. سپس نمایندگان باب، داده‌های فاش‌شده را با یکدیگر مقایسه کرده تا مطمئن شوند که نتایج (خروجی اندازه‌گیری) اعلام شده (از سوی نمایندگان آلیس) در هر دو نقطه‌ی Q_0 و Q_1 یکسان باشد (در مکانی در فصل مشترک آینده‌ی مخروط‌های نوری مربوط به Q_0 و Q_1). و سپس بررسی می‌کنند که هر دوی این نتایج، با لیست حالت‌های ارسال شده (توسط باب) به p مطابقت داشته باشد. در اینصورت باب سند التزام و نیز فاش‌سازی را معتبر دانسته و آن را می‌پذیرد. ولی چنانچه نتایج بررسی در هر یک از مراحل فوق (نتایج اعلام شده) با یکدیگر مغایرت داشته باشند، باب متوجه تقلب آلیس شده و آن را شناسایی می‌کند. در این‌جا، این طرح و پروتکل BC تضمین می‌نماید که رشته بیتی که طرفین در نهایت بعنوان کلید در اختیار خواهند داشت کاملاً مشابه و یکسان است.

۴-۵-۲-۳ ایمنی پروتکل

بدیهی است که پروتکل در برابر باب ایمن خواهد بود چون (اگر و) تا زمانیکه آلیس نخواهد بیت انتخابی‌اش را برای باب فاش کند، باب به هیچ‌وجه نمی‌تواند چیزی در مورد کارها و عملیات آلیس متوجه شود (برقراری شرط اخفا).

در این پروتکل، آلیس مقید و ملزم شده است بدین معنا که می‌بایست بتواند در هر دو نقطه‌ی Q_0 و Q_1 داده‌ها و اطلاعات مرتبط با سند التزامش را افشا کند زیرا نمایندگان باب در این نقاط، زمان و مکان فاش‌سازی‌ها را بررسی می‌کنند و بعداً (همین نمایندگان) این داده‌ها را مقایسه کرده تا مطمئن شوند که با یکدیگر مطابقت دارند یا نه. به موجب علیت مینکوفسکی، توانائی آلیس برای آشکار کردن داده‌هایی مرتبط با سند التزام یک 0 یا ۱ در Q_0، فقط به عملیات و کارهایی که او بر روی خط pQ_0 انجام می‌دهد بستگی دارد. فرض کنید آلیس استراتژی‌ای دارد که طبق آن، یکسری عملیاتی را در p انجام می‌دهد. بدین معنا که استراتژی‌های بهینه‌ی S_i او که (با انجام عملیات مناسب در آینده‌ی علی p) برای افشای موفق مقادیر بیت i طراحی شده، دارای احتمال‌های موفقیت P_i می‌باشند به طوریکه

به ازای هر $\delta > 0$ داریم: $P_0+P_1>1+\delta$. به موجب علیت مینکوفسکی، هر عملیاتی که آلیس بر روی خط نیمه‌باز $[p,Q_0)$ انجام می‌دهد، به هیچ وجه نمی‌تواند بر روی احتمال تولید (و ارائه‌ی) داده‌های متناظر با افشای موفق هر یک از مقادیر بیت i در Q_1 اثر گذارد. به طور خاص، موردی را در نظر بگیرید که در آن آلیس، دستورالعمل‌های استراتژی S_0 را بر روی $[p,Q_0)$ و دستورالعمل‌های استراتژی S_1 را بر روی $[p,Q_1)$ اعمال می‌کند (یعنی بخواهد که در Q_0 مقدار بیت 0، و در Q_1 مقدار بیت ۱ را افشا کند). در اینصورت، احتمال‌های تولید داده‌های متناظر با یک افشای موفق مقدار بیت i در Q_i (برای آلیس)، P_i خواهد بود (یعنی P_0 احتمال افشای 0 در Q_0 و P_1 احتمال افشای ۱ در Q_1 می‌باشد) و از این رو با احتمال حداقل δ، وی می‌تواند داده‌ها و اطلاعاتی مرتبط با یک افشای موفق بیت 0 در Q_0 و مقدار بیت ۱ در Q_1 تولید کند. این بدان معناست که با احتمال حداقل δ، آلیس (با ترکیب داده‌هایش در Q_0 و Q_1 در نقاطی در آینده‌ی علی مشترکشان) می‌تواند داده‌هایی متناظر با هر دو مجموعه‌ی اندازه‌گیری در پایه‌های متمم تولید کند. بنابراین (به عنوان مثال)، برای هر حالت $|\psi_i\rangle$، وی می‌تواند زیر مجموعه‌ای دو حالته از $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ (یکی از هر پایه) تعیین کند که می‌بایست شامل $|\psi_i\rangle$ نیز باشند. چنانچه پارامتر ایمنی N به قدر کافی بزرگ انتخاب شود، باب می‌تواند مطمئن باشد (که برای هر $\delta > 0$ مفروض) احتمال موفقیت کلی آلیس (مبنی بر تعیین درست و دقیق چنین زیرمجموعه‌ای برای هر یک از N حالت) کوچکتر از δ خواهد بود. یعنی اینکه آلیس نمی‌تواند هیچ‌گونه استراتژی تقلب از نوعی که در بالا توصیف شد به کاربرد. از این رو پروتکل در برابر آلیس نیز ایمن است [۲۸].

۶-۴ مقایسه، بحث، پیشنهاد

تا اینجا مجموعه‌ی متنوعی از طرح‌های عملی و کاربردی برای BC در اختیار داریم که دو مورد از آنها در بالا و دو مورد دیگر نیز در مراجع [۳۲و ۳۳] ارائه و توصیف شده‌اند. همه‌ی این طرح‌ها، طرح-هایی کاربردی و کوانتومی مجزا از هم هستند که دارای ایمنی کامل (و قابل اثبات) می‌باشند و توانسته‌اند برای مشکلی که در گذشته فکر می‌شد غیرقابل حل است (یعنی انتقال ایمن اطلاعات) راهکارهای مناسبی ارائه دهند. حال به نظر می‌رسد که مسائل قابل بحث و پیش روی ما عبارتند از: فهم و درک تنوع و تفاوت موجود بین تکنیک‌ها و طرح‌های مختلف در زمینه‌ی BC، مقایسه‌ی امکانات و منابعی که هر یک از این طرح‌ها نیاز دارند و در نهایت شناسایی طرح‌هایی که در زمینه‌های موردنظر کاربردی‌تر هستند.

پروتکلی که در بخش اخیر توصیف شد دارای مزیت‌های کاربردی (عملی) چشمگیری می‌باشد. برخلاف پروتکل موجود در مرجع [۳۲]، در این پروتکل نیازی نیست که آلیس از قبل (و در ابتدا) مختصه‌ی زمانی commitment و نیز داده‌ها و اطلاعاتی را بین نمایندگانی که به صورت فضاگونه از هم قرار دارند به اشتراک بگذارد. در مقایسه با پروتکل [۳۳]، این پروتکل نیازمند تکنولوژی کوانتومی پیشرفته‌ای نیست: این پروتکل فقط مستلزم آماده‌سازی‌های نسبتاً معتبر و قابل اطمینان (توسط باب) و نیز اندازه‌گیری معتبر (توسط آلیس) بر روی تک‌کیوبیت‌ها (یی که به هیچ وجه نیاز نیست درهم-تنیده باشند) است و نیازی به اندازه‌گیری‌های جمعی[۱] و کانال‌های ارتباطی کوانتومی ایمن برای هیچ یک از طرفین نیست. و نیز باید به این نکته توجه نمود که حتی اگر آلیس توانائی و قابلیت کمی در شناسایی و ردیابی کیوبیت‌های منتقل شده (از طرف باب) داشته باشد، باز هم پروتکل ایمن باقی خواهد ماند. البته مشروط بر آنکه ۱) وی بتواند برروی کیوبیت‌هایی که شناسایی کرده (و بدست آورده)، اندازه‌گیری‌های موثق و معقول انجام دهد و۲) بتواند سریعاً به باب (یعنی در p و یا نزدیک آن) گزارش دهد که چه کیوبیت‌هایی را شناسایی (آشکار) و اندازه‌گیری کرده است.

[۱] Collective Measurement

البته لازمست که باب بتواند در آزمایشگاهش، حالت‌های کوانتومی انتخابی تصادفی را به صورت کاملاً ایمن و مخفیانه تهیه کند. درمقابل، آلیس نیز به کانال‌های ارتباطی کلاسیکی ایمن نیاز دارد: این کانال‌ها می‌توانند یا معابر تک‌زمانه (یکبار مصرف) باشند که به اندازه‌ی کافی طولانی‌اند و از قبل به اشتراک گذاشته شده‌اند و یا معابر کوتاهتری باشند که از ابتدا به اشتراک گذاشته شده‌اند و توسط QKD به طور نامحدود (برای یک مدت نامحدود) مورد استفاده قرار می‌گیرند.

در اجرا و بکارگیری واقع‌گرایانه‌ی پروتکل‌ها می‌بایستی در آماده‌سازی‌های باب، مخابره‌ی حالت‌ها به آلیس و همچنین اندازه‌گیری‌های آلیس، وجود خطا نیز در نظرگرفته شود (مورد غیر ایده‌آلی). چنانچه این خطاها کوچک باشند، پروتکل تفاوتی (اساسی) با مورد ایده‌آلی نخواهد داشت: چرا که باب برای انجام تست تقلب فقط لازمست نتایج اندازه‌گیری اعلام شده از جانب آلیس را تست و بررسی نموده تا این نتایج از لحاظ آماری، با اندازه‌گیری‌های مربوط به یک مقدار بیت انتخابی سازگار باشند و نیز از نظر آماری با بقیه موارد (ناسازگار و) متناقض باشد.

توجه نمائید که مشابه تمام پروتکل‌های BC کوانتومی‌ای که از نظر تکنولوژیکی بدون قید و الزام (محدودیت) هستند [۳۶و۳۷]، این پروتکل نیز به هیچ وجه مانع از آن نمی‌شود که آلیس یک برهم-نهی[۱] کوانتومی از بیت‌ها را انتخاب و به آن‌ها ملتزم شود. وی به راحتی می‌تواند یک برهم‌نهی $\alpha|0\rangle+\beta|1\rangle$ را به‌عنوان ورودی به یک کامپیوتر کوانتومی وارد کند. این کامپیوترها می‌توانند به گونه‌ای طراحی و برنامه‌ریزی شده باشند که برای ورودی‌های $|0\rangle,|1\rangle$، دو اندازه‌گیری کوانتومی مربوطه را به کار گرفته و دو کپی از داده‌های مربوط به نتایج کوانتومی را به Q_0 و Q_1 بفرستد و این در حالیست که این کامپیوترها تمام این داده‌ها را، تا زمانیکه آلیس اراده نکرده تا آنها را افشا کند، در سطح کوانتومی حفظ می‌کنند.

[۱] Superposition

مشابه پروتکل‌های [۳۲و۳۳]، پروتکل‌های حاضر نیز می‌توانند (به منظور برقراری ایمنی بیشتر و کارآمدتر) به صورت زنجیروار و متوالی مورد استفاده قرار گیرند. که در اینصورت BCی با جملات طولانی و بزرگتر (تولید و) حضور می‌یابند.

رمزنگاری کوانتومی نسبیتی، استراتژی‌هایی را مجاز دانسته و به‌کار می‌گیرد که هیچ‌گونه مفهومی در رمزنگاری کوانتومی یا کلاسیکی غیرنسبیتی ندارند. مثلاً (یک ویژگی مشترک جالبی که پروتکل اخیر با پروتکل [۳۳] دارد آنست که) آلیس بدون اینکه هیچ‌گونه اطلاعاتی (کلاسیکی یا کوانتومی) به باب بدهد خود را ملزم می‌سازد (سند التزام خود را تهیه می‌کند). این باعث می‌شود که از روش معمول (تفکر) در مورد BC تغییر رویه داده و به گونه‌ای دیگر عمل کنیم. یعنی: آلیس با در اختیار داشتن (و به کمک) داده‌ها و اطلاعاتی که به روشی خاص رمزی شده‌اند خود را ملزم می‌سازد و نیز با تحویل کلید رمزگشایی، فاش‌سازی را انجام می‌دهد. در عوض در این‌جا، علیت نسبیتی، آلیس را ملزم (و مجبور) می‌سازد که خود را به گونه‌ای ملتزم نماید که بعداً بتواند یک افشاسازی معتبر نیز انجام دهد.

مراجع

[1] كريمي‌پور وحيد، درسنامه‌ي محاسبات كوانتومي ۱۳۹۱.

http://sina.sharif.edu/vahid/teaching/Quantum Computation and Information.

[2] Sakurai., j. j Modern Quantum Mechanics, Addison Wesley Publication Company, Inc. 1985.

[3] D. Mc Mahon (2007), "Quantum Computing Explained, John Wiley and Sons, Inc, USA, ISBN 978-0-470-09699-4 (cloth).

[4] M. A. Nielson and Isaac L.Chuang Cambridge University Press (2000) , Quantum Computation and Quantum Information", Cambridge, United Kingdom.

[5] A. Einstein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777 (1935).

[6] J. S. Bell, *physics* 1, 195 (1964).

[7] S. J. Freedman and J. F. Clauser ،Experimental test of local hidden-variable theories ،Phys. Rev. Lett. 938 ,280 (1972).

[8] J. Preskill, (1998), Lecture Notes for Physics 229: Quantum information and computation (http://www.theory.caltech.edu/people/perskill).

[9] باغبان‌پور اميررضا، (۱۳۸۲) ، پايان نامه ارشد: **"مخابرات كوانتومی دو طرفه"**، دانشكده فيزيک، دانشگاه تبريز.

[10] Schmidt, E., Math. Ann. 63 (1906) 433.

[11] Ch. H. Bennett et al, Phys. Rev. Lett. **70**, 1895 - 1899 (1993).

[12] Ch H. Bennett, Phys. Rev. Lett. **69**, 2881 - 2884 (1992).

[13] C. H. Bennett and G. Brassard, Quantum Cryptography, public key distribution and coin tossing, proceeding of international conference on computer systems and signal processing, pp. 175-179, (1984).

[14] A. K. Ekert, Phys. Rev. Lett. 67, no. 6, 661-663(1991).

[15] Bennett, C.H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, “Experimental quantum cryptography”, Journal of Cryptology, Vol. 5, no. 1, 1992, pp. 3 – 28.

[16] Mayers, D., “Unconditionally secure quantum bit commitment is impossible”, Physical Review Letters, vol 78, pp. 3414 – 3417 (1997). Note that this paper has the same title as [17] even though it uses a different approach.

[17] D. Mayers, Unconditionally secure quantum bit commitment is impossible, Proceedings of the Fourth Workshop on Physics and Computation (New England Complex System Inst., Boston, 1996), p. 226.

[18] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, (IEEE, New York, 1984) p. 175.

[19] G. Brassard and C. Cr´epeau, in Advances in Cryptology: Proceedings of Crypto ’90, Lecture Notes in Computer Science, Vol. 537, (Springer-Verlag, 1991) p. 49.

[20] H.-K. Lo and H. Chau, Is quantum bit commitment really possible? , Phys. Rev. Lett. 78 3410-3413 (1997).

[21] See, for example, the Appendix of L. P. Hughston, R. Jozsa and W. K. Wootters, Phys. Lett. A183, 14 (1993).

[22] G. Brassard, C. Cr´epeau, R. Jozsa and D. Langlois, in Proceedings of the 34th annual IEEE Symposium on the Foundation of Computer Science, (IEEE Computer Society Press, Los Alamitos, CA, 1993) p. 362.

[23] R. Jozsa, Journal of Modern Optics 41, 2343 (1994).

[24] D. Mayers, “The trouble with quantum bit commitment,” Los Alamos preprint archive quant-ph/9603015, submitted to Journal of Cryptology.

[25] H.-K. Lo, “Insecurity of Quantum Secure Computations”, Los Alamos preprint archive quant-ph/9611031, submitted to Phys. Rev. A.

[26] Lucien Hardy, Adrian Kent, Cheat sensitive quantum bit commitment, Phys. Rev. Lett. 92,157 901 (2004).

[27] A. Kent, Sarah Croke, Security Details for Bit Commitment by Transmitting Measurement Outcomes, arXive: 1208. 1458 v1(2012).

[28] A. Broadbent and A. Tapp, Information-Theoretically Secure Voting Without an Honest Majority, arXiv:0806.1931.

[29] H.-K. Lo and H. Chau, Why quantum bit commitment and ideal quantum coin tossing are impossible, Proceedings of the Fourth Workshop on Physics and Computation (New England Complex System Inst., Boston, 1996), p. 76.

[30] D. Mayers, A. Kitaev and J. Preskill, Superselection rules and quantum protocols, Phys. Rev. A 69 052326 (2004).

[31] G. D'Ariano, D. Kretschmann, D. Schlingemann, R. Werner, Reexamination of Quantum Bit Commitment: the Possible and the Impossible, Phys. Rev. A 76, 032328 (2007).

[32] A. Kent, Secure Classical Bit Commitment using Fixed Capacity Communication Channels, J. Cryptology 18 (2005) 313-335.

[33] A. .Kent, Unconditionally Secure Bit Commtment with Flying Qudits, arXiv: 1101.4620 (2011).

[34] A. Kent, A No-summoning theorem in Relativistic Quantum Theory, arXiv:1101.4612 (2011).

[35] A. Kent, Unconditionally secure bit commitment by transmitting Measurement Outcomes, Phys. Rev. Lett. 109, 130501 (2012).

[36] A Kent, Impossibility of unconditionally secure commitment of a certified classical bit, Phys. Rev. A **61** 042301 (2000).

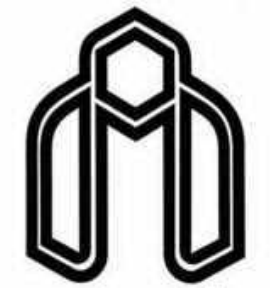
[37] A. Kent, Why Classical Certification is Impossible in a Quantum World, Quantum Information Processing DOI: 10.1007/s11128-011-0262-x.

Abstract

Quantum cryptography describes the use of quantum mechanical effects to perform cryptographic tasks or to break cryptographic systems. The most well known and developed application of quantum cryptography is quantum key distribution. QKD describes the process of using quantum communication to establish a shared key between two parties without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. This is achieved by Alice encoding the bits of the key as quantum data and sending them to Bob; if Eve tries to learn these bits, the messages will be disturbed and Alice and Bob will notice. The key is then typically used for encrypted communication (secure transmission). Following the discovery of quantum key distribution and its unconditional security, researchers tried to achieve other cryptographic tasks with unconditional security. Now, the main question is that do Parties always get the identical key? According to QKD protocols if one of the party attempt to cheat, they cannot get the identical key. In order to overcome this problem, the Bit Commitment (BC) idea was proposed and it was predicted that, if QBC apply to QKD schemes, the cheat will be detected.

A bit commitment scheme (between mistrustful parties) allows Alice to send something to Bob that commits her to a bit b of her choice in such a way that Bob cannot tell what b is, but such that Alice can later prove him what b originally was. The claim of quantum cryptography has always been that it can provide protocols that are unconditionally secure, that is, for which the security does not depend on any restriction on the time, space or technology available to the cheaters. We deal with a brief review on the impossibility of quantum bit commitment and Then express two BC protocols: 1."Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes" that based on Minkowski causality and the properties of quantum information, 2." unconditionally secure Cheat Sensitive Quantum Bit Commiment" protocol which guarantee that, if either cheats, the other has some nonzero probability of detecting the cheating. This protocol is cheat sensitive non-relativistic bit commitment protocol which uses quantum information to implement a task which is classically impossible.

Key words: quantum information, quantum measurement, entanglement, bit transmission, bit commitment.



Shahrood University of Technology

Faculty of Physics

Master of Science Thesis

Secure qubit transmission with no condition

By:
Elham Abedininia

Supervisor:
Dr.HosseinMovahhedian

Feb2013