دانشگاه صنعتی شاهرود

دانشکده فیزیک

پایان نامه کارشناسی ارشد

فیزیک ذرات بنیادی

عنوان:

پروتکل توزیع کلید کوانتومی محرمانه در چارچوب نظریهٔ فرا کوانتومی

ارائه دهنده:

یداله فرهمند

استاد راهنما:

دکتر حسین موحدیان

زمستان ۱۳۸۵

تقدیم به:

همسر مهربانم

و فرزند دوست داشتنی ام

تقدیر و تشکر:

حمد و سپاس پروردگار یکتا را که لطف و کرم بی کرانش اینجانب را نیز در بر گرفت تا به وسع اندیشه و توان خود گامی کوچک در گستره پهناور علم و معرفت بردارم.

اکنون که با یاری خداوند متعال، این دوره از تحصیلم را به پایان رسانده ام؛ هرچند واژه ها یارای آن نیست که لطف، محبت و بزرگواری کسانی را که در تمام دوران زندگیم جرعه نوش دریای بیکران مهر و محبتشان بوده ام را به تصویر بکشم، اما به رسم ادب و احترام بوسه بر دستانشان زده و برخود واجب می دانم زحمات تمامی اعضای خانواده ام، مخصوصاً مادر و همسر دلسوزم، که با ایجاد جوی صمیمی راه گشای مشکلاتم در تمام مراحل زندگی بوده اند و کلیه معلمان، اساتید و دوستان دوران تحصیلم را ارج نهاده و مراتب تشکر قلبی و باطنی خویش را از الطاف و مهربانی های آنها ابراز دارم. در ابتدا لازم می دانم که از زحمات فراوان و کارگشای استاد فرزانه و بزرگوارم جناب آقای **دکتر حسین موحدیان** که با راهنمایی ها و نظرات ارزنده و گهربارشان و صبر و حوصله فراوان، نقش مهمی در به ثمر رسیدن این تحقیق داشته اند و روحیه تحقیق و پژوهش را در بین دانشجویان خود زنده کردند، صمیمانه تقدیر و تشکر نمایم؛ بی تردید انجام این پایان نامه بدون همکاری ایشان هرگز ممکن نبود.

همچنین بر خود لازم می دانم از تمامی اساتید محترم دانشگاه صنعتی شاهرود و هیأت محترم داوران به خاطر قبولی داوری و نقد و بررسی پایان نامه کمال تشکر را داشته باشم. و در نهایت از تمام دوستان خود در دانشکده فیزیک دانشگاه صنعتی شاهرود تشکر می کنم.

خلاصهٔ کلام آنکه, در کار انجام یافته حاضر اگر چه نهایت دقت و علاقه مرعی گردیده با این همه خالی از نقص و عیب نمی تواند باشد لذا بزرگترین امیدم آنست که اساتید دانشمند و صاحب نظران فاضل با لطف و توجه خاصّه خود نقایص کار را بدیدهٔ عنایت بنگرند از راهنمائیم دریغ نفرمایند.

چکیده:

اطلاعات محرمانه و انتقال آن به طور ایمن همواره یکی از دغدغه های بشر در طول تاریخ بوده است با پیشرفت علم و تکنولوژی و ساخت رایانه های کلاسیکی اطلاعات محرمانه با امنیت نسبتاً قابل قبولی انتقال می یابد ولی هرگز انتقال این اطلاعات با ایمنی صد در صد تضمین نمی شود. فیزیکدانان نظریه پرداز اخیراً توانسته اند بر پایه تئوری یا اصول فیزیکی معتبر پروتکل های رمزنگاری به همراه توزیع کلید کوانتومی محرمانه با ایمنی قابل اثبات به دنیای اطلاعات عرضه کنند، آنها امنیت پروتکل توزیع کلید کوانتومی را بر اساس اعتبار تئوری کوانتومی،نسبیت و دیگر اصول فیزیکی معتبر با قطعیت تضمین نموده اند. در اینجا ما نیز اطلاعات محرمانه را به صورت بیت های کوانتومی در رایانه های کوانتومی کد بندی نموده و با استفاده از تئوری کوانتومی ابتدا ساختار یک رایانه کوانتومی را بررسی کرده ایم و توسط گیت دو کیوبیتی آن، کیوبیتی در هم تنیده حامل اطلاعات محرمانه مشترک بین دو کاربر مجاز را بدست آورده و سپس به کاربرد های کیوبیت دو طرفه که همان حالت های کوانتومی در هم تنیده هستند را در رایانه های کوانتومی پرداخته ایم در ادامه با استفاده از سازگاری تئوری کوانتومی و نسبیت که در آنها سرعت انتقال اطلاعات در کیوبیت های در هم تنیده حداکثر با سرعت نور می باشد بررسی نموده و با بیان قضیه EPR به شناخت بهتر پدیده شگفت انگیز حالت های کوانتومی در هم تنیده پرداخته و علاوه برآن بطور موشکافانه در تئوری کوانتومی موجبیت، موضعیت و متغیرهای پنهانی بررسی نموده ایم، سپس با فرض متغیر های موجبتی موضعیتی نامساوی بِل را در تئوری کوانتومی بدست آورده و مثال هایی را به عنوان نمونه برای نقض نامساوی بِل و تعمیم های آن به کار برده ایم. با استفاده از حالت های کوانتومی درهم تنیده پروتکل های رمزنگاری کوانتومی را به همراه توزیع کلید کوانتومی محرمانه معرفی نموده و ایده های اساسی اینگونه پروتکل ها را به همراه امنیت آن که با استفاده از اصل عدم قطعیت و نقض نامساوی بِل حاصل از نویز ایجاد شده توسط استراق سمع کننده در حالت کوانتومی که عامل اصلی امنیت توزیع کلید کوانتومی است را به طور مفصل به آن پرداخته ایم. سرانجام به پروتکل توزیع کلید کوانتومی محرمانه در نظریه فرا کوانتومی پرداخته که این پروتکل امنیت توزیع کلید محرمانه را فقط بر پایه اعتبار تئوری نسبیت تضمین می نماید یعنی حداکثر سرعت علامت دهی برابر سرعت نور فرض می شود و به استراق سمع کننده اجازه می دهیم که با استفاده از تئوری فراکوانتومی به استراق سمع بپردازد در این پروتکل نسبت به تئوری کوانتومی شکاک می باشیم و اعتبار تئوری کوانتومی هرگز برای امنیت آن استفاده نمی شود و به استراق سمع کننده اجازه آن را می دهیم که بتواند تئوری مکانیک کوانتومی را نقض نماید. امنیت این پروتکل با نقض نامساوی بِل در محدوده ناموضعیت به طور قابل اثبات تضمین می کنیم.

فهرست مطالب

عنوان **صفحه**

فهرست اشکال

فهرست جداول

فصل ۱:

مقدمه ای بر رایانه های کوانتومی

- مقدمه
- رایانه های کلاسیکی وکوانتومی
- طرح کد دهی اسکی کاراکترها
- نمایش کره بلاخ برای کیو بیت های کوانتومی
- فروپاشی(تقلیل) حالت کوانتومی
- بررسی گیت های کلاسیکی و کوانتومی
- تئوری نو کِلونینگ
- نتیجه گیری

۱- ۱- مقدمه

روشی که بتوان از آن برای انتقال اطلاعات کوانتومی از حالت های کوانتومی مانند قطبش خطی ومدور فوتون، اسپین الکترون یا نوترون وغیره استفاده کرد، می‌تواند برای ایجاد شبکه‌های اطلاعاتی جهانی رسوخ‌ناپذیر و رایانه‌هایی که با سرعت مبهوت‌کننده کار می‌کنند، به کار رود. ایجاد ارتباط بین حافظه‌های کوانتومی (حالت های کوانتومی)، برای ساخت شبکه‌های پیچیده‌ای که از پدیده‌های کوانتومی (همانند در هم تنیدگی[1] و بر هم نهی[2]) بهره می‌برند، ضروری است. شبکه‌های کوانتومی با وجودی که برای ایجاد ارتباطات امن و محاسبات فوق سریع بسیار مناسب می‌باشند اما حالت های کوانتومی حامل اطلاعات، نسبت به تداخل بسیار حساسند بنابراین می توان از آنها برای ایجاد کانال‌های ارتباطی راه دور نوری[3]-کوانتومی استفاده کرد. این کانال‌ها قابلیت ایجاد یک ارتباط کاملاً نفوذناپذیر را دارا می‌باشند، چرا که هرگونه تلاش برای کسب اطلاعات توسط استراق سمع[4]، منجر به برهم خوردن طبیعت کوانتومی داده‌های ارسالی می‌شود. قبل از آن که بتوان برای اهداف کاربردی از این روش استفاده کرد، نیازمند توسعه نظری بیشتری در این زمینه هستیم. در این فصل به بررسی حالت های کوانتومی می پردازیم که قابلیت آن را دارند برای ساخت شبکه های پیچیده کوانتومی مورد استفاده قرار گیرند،سپس با استفاده از یک حالت کوانتومی نمونه مانند حالت کوانتومی اسپین ذرّات (الکترون) به ساختار اولیه و اصلی یک رایانه کوانتومی می پردازیم؛ با استفاده از تئوری کوانتومی هر یک از حالت های کوانتومی را توسط بیت های کوانتومی معرفی کرده و تحوّل دینامیکی آنها را مورد بررسی قرار می دهیم و گیت های کوانتومی را معرفی خواهیم نمود و عملکرد آنها را در رایانه های کوانتومی بررسی می کنیم.

---

[1] Entanglement
[2] Superposition
[3] Teleportation
[4] Eavesdropping

۱-۲- رایانه های کلاسیکی

رایانه ها با چیزهای مختلفی از جمله اعداد، علامتها، کلمات، تصاویر، صداها و برنامه ها و غیره سر و کار دارند. رایانه ها می تواند چنین چیزهایی را دریافت، ایجاد، تغییر یا ارائه دهند. همچنین به صورتهای مختلفی با دنیای اطرافشان در ارتباطند و انجام کارهای بسیار متنوعی به آنها واگذار شده است. جالب است که بر خلاف این همه گوناگونی در نهایت همه چیز در داخل آن به صورت یکسان نمایش داده می شود که به صورت مجموعه ای از صفر و یک هاست. حافظه رایانه های کلاسیکی رشته ای از بیتهای صفر و یک است که در علم اطلاعات هر بیت کوچکترین جزئی است که می تواند حامل اطلاعات کلاسیکی باشد. واحد تجزیه ناپذیر و اصلی اطلاعات کلاسیکی بیت و داده های ورودی[۱] و خروجی[۲] بر حسب این واحدهای اصلی بیان می شوند. هر بیت دارای دو مقدار صفر و یک در رشتهای از مقادیر بر مبنای دودویی[۳] نمایش داده می شوند.استفاده از مبنای دودویی در رایانه داشتن ساختار نسبتاً آسان برای نمایش بیت است.

کاراکترها

یک حرف، عدد، علامت دستوری یا نشانه دیگر یا کد کنترلی که توسط یک واحد (بایت متشکل از هشت بیت) به رایانه معرفی می شود. قابل دید بودن یک کاراکتر روی صفحه الزامی نیست؛ این نوع کاراکترها ممکن است سیگنال (علامت) برای صدا ، و پیکسلی از یک تصویر روی صفحه نمایش و ... باشد.

طرح کد دهی اسکی[۴]

برای آنکه هر یک از کاراکترهای مشخصی را که می خواهیم به رایانه بدهیم، برای آن قابل فهم باشد نیاز به طرح کدگذاری آن کاراکتر داریم. طرح های کدگذاری معروف از جمله، اسکی و ای بی سی دیک[۵] می باشند. رایانه های شخصی، از کد اسکی استفاده می کنند؛ و طرح

---

[1] Output
[2] Input
[3] Binary Representation
[4] ASCII
[5] EBCDIC

کدگذاری کاراکترهای اسکی در هر رایانه شخصی جاسازی شده است. این طرح کد دهی با استفاده از هشت بیت که مقادیر عددی را به ۲۵۶ کاراکتر شامل حروف، اعداد، علامت گذاری ها و کاراکترهای کنترلی و سایر نشانه ها نسبت می دهد. در سال ۱۹۶۸ طرح کد دهی اسکی توسعه یافت، تا انتقال داده ها بین سیستمهای نرم افزاری و سخت افزاری جداگانه را استاندارد نماید.

نمونه کددهی کامپیوتر

اگر بخواهیم چند کاراکتر را به عنوان داده ورودی، به کامپیوتر بدهیم، مثلاً کلمه Door، نیاز به ۴ کاراکتر داریم که هر کاراکتر ۸ بیت می باشد. با فشردن کلید D بر روی صفحه کلید رایانه، به عنوان کاراکتر ورودی، و با توجه به طرح کد دهی اسکی که در رایانه های شخصی جاسازی شده است، آن را سریعاً به بیتهای زیر کد دهی می کند.

تبدیل کاراکترها در طرح کد دهی اسکی:

$$D \xrightarrow{ASCII} 01000100$$
$$o \xrightarrow{ASCII} 01101111$$
$$o \xrightarrow{ASCII} 01101111$$
$$r \xrightarrow{ASCII} 01110010$$

بنابراین هر یک ازکاراکترها دراین طرح کد دهی به صورت بیت های صفر و یک، برای رایانه ها قابل فهم می باشد.

کاراکترها	r	o	o	D
کد دهی اسکی کاراکترها	01110010	01101111	01101111	01000100

و بدین ترتیب، رایانه شخصی، با در نظر گرفتن کاراکترهای کد دهی شده، به صورت بایت بایت، می تواند به انجام عملیات نرم افزاری آن بپردازد؛ به طور مثال آن کاراکتر را در نرم افزار تایپی (ورد)، روی صفحه نمایشگر رایانه تایپ نماید. طرح کد دهی اسکی به صورت جدولی در تمام مراجع مربوط به علم رایانه (کتاب های رایانه) وجود دارد.

۱-۳- رایانه های کوانتومی

رایانه های کوانتومی در صورت تحقق عملی می توانند گـوی سـبقت را از بهتـرین رایانـه های امروزی بربایند دردنیای کوانتومی، پدیده ها به گونه ای متفاوت و شگفت انگیز وجـود دارنـد که استفاده از آن ها در ساخت رایانه های کوانتومی برای پردازش اطلاعات مناسب است.

مهندسینی که رایانه های کوانتومی را طراحی می کنند و متخصیصن مکانیک کوانتومی امیدوارند از یکی از بنیادی ترین اصول نظریه های کوانتومی بـرای طراحـی سیـستم هـایی(ماشـین هـایی) استفاده کنند که قادرند به طور هم زمان محاسبات موازی را انجام دهند. این محاسبات امکان حل آسان ومنطقی برخی از مسائل غیر قابل حل در رایانه های کلاسیکی و نیز مشکل موجود در زمینه رمز نگاری را فراهم می سازند.

حافظه یک رایانه کوانتومی حالت های کوانتومی است. رایانه های کوانتومی از کیو بیت ها[1] تشکیل شده است. کیو بیت به طور هم زمان می تواندبیت صفر و یک را داشته باشند؛ یعنی با بر هم نهـی بیت های کلاسیکی هم ارز می باشند. بنابراین حالت های کوانتومی می توانند به عنوان بیت های رایانه های کوانتومی در نظرگرفته شوند. با توجه بـه آنکـه حالـت هـای کوانتـومی از پدیـده هـای مکانیک کوانتومی حاصل می شوند بنابراین، محاسبات رایانه های کوانتومی بـر اسـاس فراینـدهای فیزیکی و اصول کوانتومی پایه ریزی شده است.

۱-۳-۱- بیت کوانتومی (کیو بیت)

کیو بیت کوچکترین جزء یک سیستم (واحد حافظه) در رایانه هـای کوانتـومی اسـت کـه مانسته بیت در رایانه های کلاسیکی می باشد. هر حالت کوانتومی که بر هم نهی حالت های $|0\rangle$ و $|1\rangle$ باشد را می توان به عنوان کیوبیت در نظر گرفت به زبان ریاضی داریم:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad , \quad |\alpha|^2 + |\beta|^2 = 1 \qquad (۱-۱)$$

$\{|0\rangle, |1\rangle\}$ پایه های کوچکترین فضای هیلبرت (دوبعدی) هستند.

---

[1] qubit

با توجه به شرط به هنجارش تعداد بی نهایت مقادیر برای α, β و بینهایت حالت همزمان برای کیوبیت $|\psi\rangle$ وجود دارد. اساس کار رایانه های کوانتومی طوری است که می توانند کیوبیت هـایی را که شامل بینهایت حالت هستند به طور همزمان پردازش کنند. بر اساس اصـول بنیـادی نظریـه مکانیک کوانتومی یک کیوبیت که می تواند به طور همزمـان حالـت صـفر و یـک را داشـته باشـد بنابراین این امکان وجود دارد که یک کیوبیت در آن واحد در بیش از یک محاسبه شرکت داشـته باشد، به همین دلیل است که رایانه های کوانتومی قادر به اجرای موازی محاسبات فراوانی هستند. نکته اصلی در این جا این است که ساخت یک رایانه کوانتومی در عمل بسیار دشوار است، بـا ایـن وجود گام جدیدی به سوی آن برداشته شده است. در یک رایانـه کوانتـومی بـه جـای اسـتفاده از ترانزیستورها و مدارهای رایانه ای معمولی از اتـم هـا و سـایر ذرات ریـز بـرای پـردازش اطلاعـات استفاده می شود. یک اتم می تواند به عنوان یـک بیـت حافظـه در رایانـه عمـل کنـد و جابجـایی اطلاعات از یک محل به محل دیگر نیز توسط نور امکان می پذیرد.

بخش اصلی نمونه اولیه رایانه های کوانتومی ساخته شده بر اساس لایه های (حالت هـای)انـرژی[1] اتم کلسیم می باشد و برنامه ای توسط این رایانه اجرا شده است. نمونهٔ دیگر اتم کادمیوم می باشد که در یک لحظه می تواند در هر دو حالت کوانتومی داخلی[2] یک و صفر قرار داشته باشد.

طرح های زیادی برای چگونگی ساختن رایانه های کوانتومی وجود دارد و نیـز طـرح هـای بـسیار دیگری در پیش است؛ $|0\rangle$ و $|1\rangle$ مـی توانـد یـک کیوبیـت حالـت پایـه و برانگیختـهٔ یـک اتـم ، پلاریزآسیون (دوقطبی شدن) فوتون ها و یا یک حالت اسپینی ذره باشد و غیره [۱،۴،۱۰،۱۶].

[1] Energy levels
[2] Internal state

۱-۳-۲- معرفی کیوبیت ها در حالت های کوانتومی مختلف:

حالت های کوانتومی مختلفی در نظریه کوانتومی وجوددارد که می تواند به عنوان کیوبیت ها در رایانه های کوانتومی بکار رود؛ یعنی با شبیه سازی رفتار حالت های کوانتـومی از هـر سیـستم فیزیکی درتئوری مکانیک کوانتومی می توان رشته هایی از کیوبیـت هـا را تـشکیل دادکـه بـه آن اشاره می کنیم:

فوتون:

الف- می توان قطبش خطی فوتون را مثلاً در راستای z $(\updownarrow)$ یا x $(\leftrightarrow)$ که حالـت هـای کوانتـومی قطبش خطی فوتون ها هستند در نظر گرفت و به ترتیب کیو بیت $|0\rangle$ و $|1\rangle$ را به آنها نسبت داد. بنابراین هر فوتون می تواند در هر جهتی در صفحه xz به صورت بر هم نهـی قطـبش خطـی زیـر باشد.

$$|\psi\rangle = \alpha(\updownarrow) + \beta(\leftrightarrow) \quad , \quad |\alpha|^2 + |\beta|^2 = 1 \qquad (۲-۱)$$
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

ب- قطبش مدور فوتون به طریق مشابه می توان در ساختار اصلی رایانه های کوانتومی با در نظـر گرفتن حالت کوانتومی قطبش فوتون پاد ساعتگرد وساعتگرد را به ترتیب بـا کیوبیـت $|0\rangle$ و $|1\rangle$ بکار بر د.

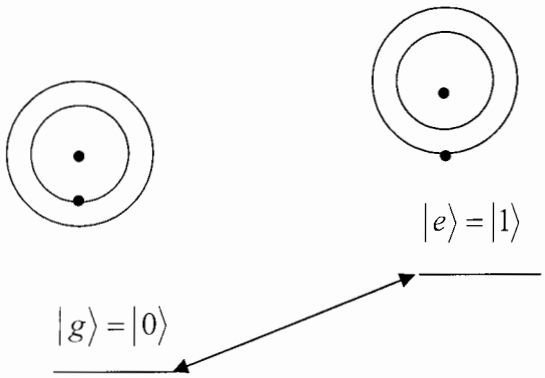
الکترون (نوترون):

اسپین الکترون در راستای بالا را با حالت کوانتومی $|\uparrow\rangle$ و اسپین الکترون در راستای پـایین را بـا حالت کوانتومی $|\downarrow\rangle$ نشان می دهند که به ترتیب کیوبیت $|0\rangle$ و $|1\rangle$ را می توان به آن نسبت داد. با توجه به اصول تئوری مکانیک کوانتومی اسپین هر الکتـرون مـی توانـد بـر هـم نهـی از حالـت کوانتومی اسپینی زیر را داشته باشد.

$$|\psi\rangle = \alpha(\uparrow) + \beta(\downarrow) \quad , \quad |\alpha|^2 + |\beta|^2 = 1 \qquad (۳-۱)$$
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

اتم:

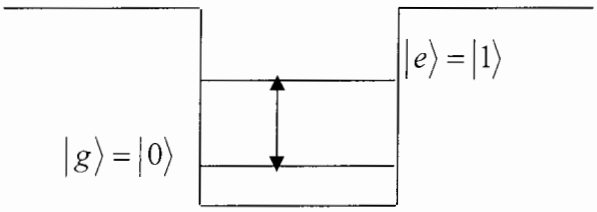
در ساختار اصلی رایانه های کوانتومی می توان از حالت های داخلی یک اتم یعنی حالت پایـه $|g\rangle$ و حالت بر انگیخته $|e\rangle$ برای نمایش کیوبیت های $|0\rangle$ و $|1\rangle$ استفاده نمود.



شکل(۱-۱) : کیوبیت پایه در ساختار کوانتومی حالت های داخلی اتم

کوانتوم دات:

سطوح انرژی (لایه های انرژی) در اتم ها نیز همانند مورد های قبلی می توانند دارای کیو بیتهایی مطابق شکل زیر باشند و در ساختار اصلی رایانه های کوانتومی بکار روند.



شکل(۱-۲) : کیوبیت پایه در ساختار کوانتومی سطوح انرژی اتم

بنابراین تا زمانی که راهی برای قرار دادن سیستم در یک حالت بر هم نهی کوانتومی وجود دارد و همچنین راهی برای تداخل متقابل کیوبیت ها وجود دارد این سیستم به صورت بالقوه، مـی توانـد به عنوان یک رایانه کوانتومی استفاده شود[۹،۲،۱].

برای ذخیره اطلاعات با استفاده از حالت مغناطیسی اتم،می توان از یک اتم کادمیوم به دام افتاده در میدان الکتریکی استفاده کردند. در این روش انرژی توسط یک لیزر به درون اتم پمپاژ شده و اتم را وادار به گسیل فوتونی می کند که فوتون گسیل شده رونوشتی از اطلاعات اتم (حالت های کوانتومی اتم) را در بر دارد و توسط آشکارساز قابل تشخیص است.

در حال حاضر، فوتون‌هایی که داده‌های کوانتومی را حمل می‌کنند، تنها می‌توانند چند ده کیلومتر از طریق کابل نوری منتقل شوند و سپس از بین می‌روند. اما استفاده از یک «تکرارکننده کوانتومی» که می‌تواند اطلاعات کوانتومی فوتون را ذخیره نموده و سپس آن را دوباره انتقال دهد، این امکان را به وجود می‌آورد که بتوان داده‌های کوانتومی را در فاصله‌های زیادی منتقل نمود. با تحت کنترل درآوردن این روش و انتقال داده‌ها از یک قسمت حافظه دستگاه به قسمت دیگر، می‌توان رایانه‌های کوانتومی تولید نمود. ذرات کوانتومی می‌توانند همزمان در بیش از یک حالت کوانتومی وجود داشته باشند و این از نظر تئوری به معنی آن است که می‌توان میلیاردها محاسبه را به طور همزمان انجام داد.

بیت های متحرک حامل اطلاعات کوانتومی، قابلیت کیلومترها پیمایش را دارند. در نتیجه امکان برقراری ارتباطات کوانتومی از فواصل بسیار دور وجود خواهد داشت.

با این وجود تنها مشکل در رایانه های کوانتومی نحوه کار با کیوبیت ها می باشد. تنظیم مقادیر اولیه برای آنها دشوار است و بنابراین خواندن نتایج نیز کار ساده‌ای نمی‌باشد. هنگامیکه محاسبات در حال انجام می‌باشند، لازم است کیوبیتهای متفاوتی به روش مناسب و کنترل شده بر یکدیگر اثر گذارند و این در حالیست که سیستم باید نسبت به محیط خارج کاملا ایزوله شده باشد.

رایانه کوانتومی دکتر گالد که بر اساس ایده حالت های کوانتومی یون کلسیم پایه ریزی کرده است و آزمایشی که بر روی رایانه خود انجام داد الگوریتم جوزا- دیوچ[1] [۴] نام داشت. این الگوریتم که به افتخار دو تن از پیشگامان محاسبات کوانتومی دیوید داچ و ریچارد یوتزا به این نام خوانده می‌شود، روشی برای تشخیص برابری یک سکه است. یک سکه زمانی دارای برابری (صادق) است که در یک رو دارای علامت شیر و در روی دیگر دارای علامت خط باشد. اگر سکه‌ای در هر دو روی خود علامت شیر و یا خط داشته باشد دارای برابری نمی‌باشد. در دنیای غیر کوانتومی،

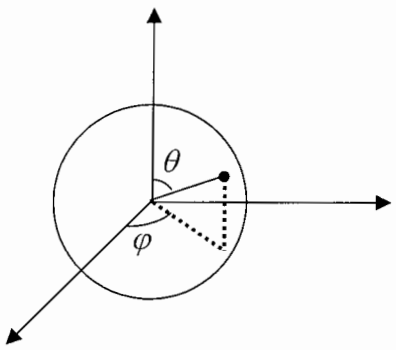
[1] Deutsch-Jozsa

بررسی یک سکه دارای دو مرحله می‌باشد: نگریستن به یک روی سکه و سپس نگریستن به روی دیگر آن. دکتر داچ و دکتر یوتزا، بر روی روشی برای استفاده از یک رایانه کوانتومی‌جهت بررسی یک سکه فرضی در یک مرحله کار کردند. این روش شامل اندازه‌گیری کیوبیتی است که نسبت یکسانی از دو حالت شیر و خط را دارد. نتیجه حاصله نشان داد که علامتهای حسابی منفی و مثبت در این کیوبیت به برابری و نابرابری سکه وابسته می‌باشد؛ علامت منفی حالت برابری و مثبت حالت نابرابری را نشان می‌داد. اندازه‌گیری یک کیوبیت که مانند نتیجهٔ نگریستن به دو روی سکه در یک لحظه می‌باشد فرایندی یک مرحله‌ای است.

مشهورترین مثال از قدرت رایانه های کوانتومی الگوریتم پیتر شُر[1][۱۶] برای تجزیه اعداد بزرگ است. یک مشکل مهم در رمز نویسی، تجزیه عدد به عوامل اول است، به عنوان مثال امنیت به رمزآوری کلید عمومی، RSA که به تجزیه به عامل های اول بستگی دارد، با وجود تحقیقات فراوان الگوریتم محاسبات کلاسیکی کارآمدی برای آن شناخته نشده است. در واقع شُر این مشکل را حل نمود و خوشبختانه الگوریتم مؤثر کوانتومی برای این تبدیلات وجود دارد[۹].

۱-۴- نمایش کره بلاخ[2]

بلاخ از کره ای به شعاع واحدکه زاویه θ,φ نقاط روی کره را نشان می دهند، برای نمایش کیوبیت ها استفاده نمود. شکل مقابل و روابط زیر معروف به نمایش کره بلاخ می باشد.



شکل(۱-۳) :نمایش کره بلاخ برای کیوبیت ها

[1] P. Shor
[2] Bolch Sphere Representation

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad , \quad \alpha^2 + \beta^2 = 1$$

$$\alpha = Cos\frac{\theta}{2} \quad , \quad \beta = e^{i\varphi}Sin\frac{\theta}{2} \quad ; \quad 0 \le \theta \le \pi, 0 \le \varphi \le 2\pi \qquad (۴-۱)$$

نمایش کیوبیت در قطب شمال و جنوب کره بلاخ:

$$\{\theta = 0 \quad , \phi = 0\} \to \alpha = Cos0 = 1, \quad \beta = e^{i0}Sin0 \to |\psi\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad (۵-۱)$$

$$\{\theta = \pi \quad , \phi = 0\} \to \alpha = Cos\frac{\pi}{2} = 0, \quad \beta = e^{i0}Sin\frac{\pi}{2} = 1 \to |\psi\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (۶-۱)$$

$\left\{|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\}$ کوچکترین فضای هیلبرت (دوبعدی) هستند؛ کیوبیت حالتی در فضای هیلبرت دوبعدی است که می تواند هر حالتی به صورت $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ با شرط بهنجارش $\alpha^2 + \beta^2 = 1$ باشد.

با توجه به حالت بالا می توان حالت پایه اسپینی ذره (الکترون، ...) در راستای محور z را به عنوان حالت های پایه یک کیوبیت در نظر گرفت.

حالت پایه S_z:

$$|0\rangle \leftrightarrow |\uparrow_z\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad (۷-۱)$$

$$|1\rangle \leftrightarrow |\downarrow_z\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (۸-۱)$$

نمایش کیوبیت در راستای محورx:

$$\left\{\theta = \frac{\pi}{2} \quad , \phi = 0\right\} \to \alpha = Cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}, \quad \beta = e^{i0}Sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} \to$$

$$|\psi\rangle = |0\rangle_x = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\left\{\theta = \frac{\pi}{2} \quad , \phi = \pi\right\} \to \alpha = Cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}, \quad \beta = e^{i\pi}Sin\frac{\pi}{4} = -\frac{\sqrt{2}}{2} \qquad (۹-۱)$$

$$|\psi\rangle = |1\rangle_x = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \qquad (۱۰-۱)$$

حالت پایه S_x خود نیز بر هم نهی از حالت پایه S_z است و به عنوان کیو بیت مطابق شکل زیر بیان می شود.

$$\left|\uparrow_X\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_Z\right\rangle + \left|\downarrow_Z\right\rangle\right) \rightarrow \left|0\right\rangle_X = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_Z + \left|1\right\rangle_Z\right) \qquad (۱۱-۱)$$

$$\left|\downarrow_X\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_Z\right\rangle - \left|\downarrow_Z\right\rangle\right) \rightarrow \left|1\right\rangle_X = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_Z - \left|1\right\rangle_Z\right) \qquad (۱۲-۱)$$

نمایش کیوبیت در راستای محور y:

$$\left\{\theta = \frac{\pi}{2} \quad , \phi = \frac{\pi}{2}\right\} \rightarrow \alpha = Cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}, \quad \beta = e^{i\frac{\pi}{2}} Sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} i \rightarrow$$

$$\left|\psi\right\rangle = \left|0\right\rangle_Y = \frac{\sqrt{2}}{2}\begin{pmatrix}1\\ i\end{pmatrix} \qquad (۱۳-۱)$$

$$\left\{\theta = \frac{\pi}{2} \quad , \phi = \frac{3\pi}{2}\right\} \rightarrow \alpha = Cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}, \quad \beta = e^{i\frac{3\pi}{2}} Sin\frac{\pi}{4} = -\frac{\sqrt{2}}{2} i \rightarrow$$

$$\left|\psi\right\rangle = \left|1\right\rangle_Y = \frac{\sqrt{2}}{2}\begin{pmatrix}1\\ -i\end{pmatrix} \qquad (۱۴-۱)$$

حالت پایه S_Y :

$$\left|\uparrow_Y\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_Z\right\rangle + i\left|\downarrow_Z\right\rangle\right) \rightarrow \left|0\right\rangle_Y = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_Z + i\left|1\right\rangle_Z\right) \qquad (۱۵-۱)$$

$$\left|\downarrow_Y\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_Z\right\rangle - i\left|\downarrow_Z\right\rangle\right) \rightarrow \left|1\right\rangle_Y = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_Z - i\left|1\right\rangle_Z\right) \qquad (۱۶-۱)$$

بنابراین می تواند نمایش هر کیوبیتی را مانند S_i را در کره بلاخ مشاهده کرد[۴،۲].

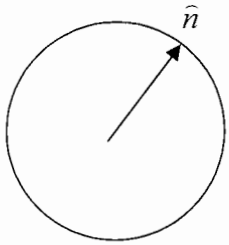
ماتریس چگالی کیوبیت با توجه به نمایش کره بلاخ:

ماتریس چگالی برای هر حالت کوانتومی مطابق رابطه زیر است[۱۴،۶]:

$$|\psi(\theta,\varphi)\rangle_{r=1} = \begin{pmatrix} \cos(\frac{\theta}{2}) \\ e^{i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix} \qquad (۱۷-۱)$$

$$\rho = |\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)| = \begin{pmatrix} \cos(\frac{\theta}{2}) \\ e^{i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix}\begin{pmatrix} \cos(\frac{\theta}{2}) & e^{-i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix} \qquad (۱۸-۱)$$

برای هر بردار یکه در جهت دلخواه روی کره بلاخ $\hat{n}$



شکل(۱-۴) : نمایش بردار یکه در جهت دلخواه

بنابراین داریم:

$$(\hat{n}\cdot\delta) = (\sin(\theta)\cos(\varphi),\sin(\theta)\sin(\varphi),\cos(\theta))\cdot(\delta_x,\delta_y,\delta_z) =$$

$$\sin(\theta)\cos(\varphi)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \sin(\theta)\sin(\varphi)\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + \cos(\theta)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} =$$

$$\begin{pmatrix} \cos(\theta) & \sin(\theta)(\cos(\varphi) - i\sin(\varphi)) \\ \sin(\theta)(\cos(\varphi) + i\sin(\varphi)) & -\cos(\theta) \end{pmatrix} = \begin{pmatrix} \cos(\theta) & \sin(\theta)e^{-i\varphi} \\ \sin(\theta)e^{i\varphi} & -\cos(\theta) \end{pmatrix}$$

$$(\hat{n}\cdot\delta) = \begin{pmatrix} \cos(\theta) & \sin(\theta)e^{-i\varphi} \\ \sin(\theta)e^{i\varphi} & -\cos(\theta) \end{pmatrix} \qquad (۱۹-۱)$$

$$\begin{pmatrix} \cos(\frac{\theta}{2}) \\ e^{i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix}\begin{pmatrix} \cos(\frac{\theta}{2}) & e^{-i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix} = \begin{pmatrix} \cos^2(\frac{\theta}{2}) & \cos(\frac{\theta}{2})e^{-i\varphi}\sin(\frac{\theta}{2}) \\ \cos(\frac{\theta}{2})e^{i\varphi}\sin(\frac{\theta}{2}) & e^{i\varphi}\sin(\frac{\theta}{2})e^{-i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix} =$$

$$\begin{pmatrix} \frac{1}{2}(\cos(\theta)+1) & \frac{1}{2}\sin(\theta)e^{-i\varphi} \\ \frac{1}{2}\sin(\theta)e^{i\varphi} & \frac{1}{2}(1-\cos(\theta)) \end{pmatrix} = \frac{1}{2}\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} \cos(\theta) & \sin(\theta)e^{-i\varphi} \\ \sin(\theta)e^{i\varphi} & -\cos(\theta) \end{pmatrix}\right] =$$

$$\rho = \frac{1}{2}(I + \vec{n}\cdot\delta) \qquad (۲۰-۱)$$

مقدار انتظاری کیوبیت ها در راستای محورZ [۹،۲]:

$$\langle\psi(\theta,\varphi)|\delta_Z|\psi(\theta,\varphi)\rangle = \begin{pmatrix} \cos(\frac{\theta}{2}) & e^{-i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos(\frac{\theta}{2}) \\ e^{i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix} =$$

$$\begin{pmatrix} \cos(\frac{\theta}{2}) & -e^{-i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix}\begin{pmatrix} \cos(\frac{\theta}{2}) \\ e^{i\varphi}\sin(\frac{\theta}{2}) \end{pmatrix} = \cos^2(\frac{\theta}{2}) - \sin^2(\frac{\theta}{2}) = \cos(\theta)$$

$${}_\psi\langle\delta_Z\rangle_\psi = \cos(\theta) \qquad (۲۱-۱)$$

۱-۵- نمایش کیوبیت ها به شکل ماتریسی

کیوبیت ها را نیز همچنین می توان به شکل ماتریس بیان نمود[۴،۱].

کیوبیت های منفرد

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad (۲۲-۱)$$

$$|0\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad (۲۳-۱)$$

$$|0\rangle_Y = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + i\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \qquad (۲۴-۱)$$

کیوبیت های دوتایی

در صورتی که، دو کیوبیت در کنار هم قرار گیرند،یعنی همبستگی[1] بین کیوبیت اول و دوم به وجود می آید با اعمال ضرب تانسوری بین آن دو، نمایش ماتریسی آن حاصل می شود.

$$|0\rangle|0\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}1\\0\end{pmatrix}\\0\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad (۲۵-۱)$$

$$|0\rangle|0\rangle_X = |0\rangle \otimes |0\rangle_X = \begin{pmatrix}1\\0\end{pmatrix} \otimes \left[\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}1\begin{pmatrix}1\\1\end{pmatrix}\\0\begin{pmatrix}1\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\1\\0\\0\end{pmatrix} \qquad (۲۶-۱)$$

کیوبیت های سه تایی و چند تایی

$$|0\rangle|1\rangle|0\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}0\\0\\1\\0\end{pmatrix}\\0\begin{pmatrix}0\\0\\1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix} \qquad (۲۷-۱)$$

$$|0\rangle|1\rangle_X|0\rangle|1\rangle\ldots\ldots\ldots\ldots = ?$$

ضرب تانسوری ماتریس های دودردو در هم[۳،۱]

$$\begin{pmatrix}x_1 & x_2\\x_3 & x_4\end{pmatrix} \otimes \begin{pmatrix}y_1 & y_2\\y_3 & y_4\end{pmatrix} = \begin{pmatrix}x_1\begin{pmatrix}y_1 & y_2\\y_3 & y_4\end{pmatrix} & x_2\begin{pmatrix}y_1 & y_2\\y_3 & y_4\end{pmatrix}\\x_3\begin{pmatrix}y_1 & y_2\\y_3 & y_4\end{pmatrix} & x_4\begin{pmatrix}y_1 & y_2\\y_3 & y_4\end{pmatrix}\end{pmatrix} \qquad (۲۸-۱)$$

[1] Correlation

۱-۶- اندازه گیری کیوبیت[1]

اگر حالت $|\psi\rangle$ را مورد اندازه گیری قرار دهیم داریم:

$$|\psi\rangle = \sum a_x |x\rangle \xrightarrow{M_x} |x\rangle \qquad ; P = |a_x^2|; \quad \sum a_x^2 = 1 \qquad (۲۹-۱)$$

برای مثال:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle \xrightarrow{M_{0,1}} \begin{cases} |0\rangle; & \text{احتمال} \quad |a_0^2| \\ |1\rangle; & \text{احتمال} \quad |a_1^2| \end{cases} \quad ; \quad |a_0^2| + |a_1^2| = 1$$

بنابراین خروجی آن حالت ها $|0\rangle$ یا $|1\rangle$ خواهد شد[۱].

۱-۶-۱- فروپاشی (تقلیل) حالت کوانتومی[2]

اندازه گیری S_Z یک کیوبیت باعث فروپاشی به یکی از حالت های پایه S_Z یعنی $|0\rangle$ و $|1\rangle$ می شود. در اینجا فرایند اندازه گیری در سیستمهای تک کیوبیتی ودو کیوبیتی مورد بررسی قرارمی دهیم.

الف- اگر یک سیستم تک ذره ای با اسپین $\frac{1}{2}$ در حالت $|\psi\rangle$ داشته باشیم آنگاه:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \xrightarrow{M_{S_Z}} \quad |0\rangle \quad \text{یا} \quad |1\rangle \qquad (۳۰-۱)$$

پس از اندازه گیری کیوبیت به یکی از حالتهای اصلی با احتمال مساوی $\frac{1}{2}$ فروپاشی می شود.

---

[1] Measurement of qubit
[2] Collapses

ب- اگر یک سیستم دوکیوبیتی که هر کدام اسپین $\frac{1}{2}$ در حالت $|\psi\rangle$ داشته باشند:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2\right) \xrightarrow{M_{Sz}} \quad |0\rangle_1|1\rangle_2 \quad \text{یا} \quad |1\rangle_1|0\rangle_2 \qquad (۳۱-۱)$$

پس ازاندازه گیری،کیوبیت به یکی ازحالت های اصلی دیگر با احتمال مساوی $\frac{1}{2}$فروپاشی می شود. عمل اندازه گیری در آفریدن حالت خروجی جدید نقش دارد، و اندازه گیری هنگامی صورت می پذیرد که دستگاه اندازه گیری با سیستم بر هم کنش انجام دهد[۴،۲،۱].

در واقع، اکثر واکنش هایی که در محیط وجود دارد، مانند یک عمل اندازه گیری، باعث فروپاشی حالت های کوانتومی می شود. دنیا در یک مقیاس انسانی پیوسته در حال فروپاشی حالت های بر هم نهشی به حالت های کلاسیکی تر هستند، این جریان را برگشت به حالت کلاسیکی[1]می گویند. اگر ما بخواهیم یک حالت کوانتومی را برای مدت زمانی بدون انجام هر گونه محاسبه ای حفظ کنیم، و یا بخواهیم آن را از طریق یک کانال معمولی دارای پارازیت[2] بفرستیم، محاسبات حالت های کوانتومی باید بی نقص باشد؛ و برای یک کامپیوتر کوانتومی این مشکل بزرگی است، اگر ما نتوانیم آن را از واکنش (فعل و انفعال) با محیط متوقف کنیم، بهتر از یک کامپیوتر کلاسیکی نخواهیم داشت. واضح است که مسئله توقف مسئله ای مانند جلوگیری از پارامترهای عمومی است. راه حل این مسئله استفاده از کد تصحیح خطای کوانتومی است.

ساده ترین کد تصحیح خطای کلاسیکی کد تکرار است، ما صفر را به رمز 000 و یک را به رمز 111 در می آوریم سپس حتی اگر یک ذره بر هم کنش با محیط انجام دهد ممکن است ما به حالت 011 برسیم؛ و می توانیم آن را با استفاده از کد تصحیح خطاکه حالت اصلی 111 برگردانیم[۹،۴،۲،۱] .

---

[1] Decoherence
[2] Noise

۱-۷- گیت[1] (GATE)

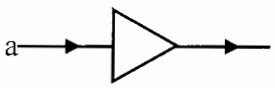
فرایند یا انتقال بیت یا کیوبیت را توسط گیت نمایش می دهند.

۱-۷-۱- گیت های کلاسیکی

اولین بحث رایانه های کلاسیکی (محاسبات کلاسیکی) فرایند یا تبدیل بیت کلاسیکی است. تنها عنصر اصلی این فرایند کلاسیکی بیت ها، گیت ها می باشند. یک پردازنده رایانه الکترونیکی جدید شامل صدها و میلیون ها گیت است، و هر کدام از گیت ها فرایند مخصوص به خود را انجام می دهند.

گیت های کلاسیکی بر طبق داده های ورودی به شکل زیر بیان می شوند:

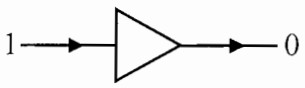
گیت تک ورودی کلاسیکی

(A) NOT gate: 

این گیت ساده مقدار ورودی بیت را از 0 به 1 و برعکس تغییر می دهد.

عملیات ریاضی آن به شکل زیر است.

($\oplus$ اشاره به باقیمانده حاصل جمع برمبنای دو دارد)



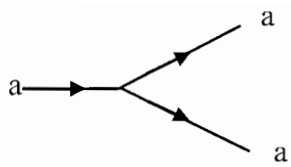
(۱-۳۲)

$$NOT(a) = 1 \oplus a \qquad ; \quad (\oplus = addition \bmod (2))$$

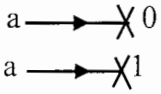
مثال:

$$NOT(1) = 1 \oplus 1 = \bmod(\frac{1+1}{2}) = 0$$

[1] Gate

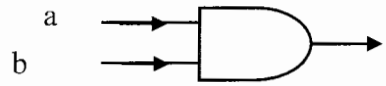
(B) FANOUT (Copy) gate 

FANOUT gate شاخه بیت ورودی به دو شاخه بیت خروجی حامل دو بیت مشابه با بیت ورودی می باشد. در رایانه های کوانتومی این گیت برقرار نیست، یعنی فرایندی وجود ندارد که یک بیت به دو بیت مشابه با خود تبدیل شود.

(B) ERASE gate: 

بیت ورودی را به صفر یا یک تبدیل می کند.

گیت های دو ورودی کلاسیکی

(A) AND gate: 

a AND b = ab

یک خروجی از دو ورودی بدست می آید و عملیات ریاضی آن مانند حاصل ضرب می باشد.

خروجی هنگامی یک است که هر دو ورودی یک باشند، در غیر این صورت خروجی برابر صفر خواهد شد.

(B) ORgate: 

a OR b

خروجی هنگامی صفر است که هر دو ورودی صفر باشند، در غیر این صورت خروجی برابر یک خواهد شد.

(C) XOR gate: 

a XOR b

خروجی این نوع گیت برابر یک است اگر فقط یکی از رودی ها مخالف هم باشند، در بقیه حالت ها خروجی برابر صفر است.

عملیات ریاضی آن به شکل زیر است:

$$aXORb = a \oplus b \qquad (۳۳-۱)$$

گیت های دو ورودی را به راحتی می توان توسط جدول زیر نمایش داد.

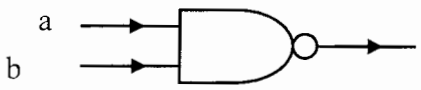
جدول(۱-۱):حاصل گیت های AND,OR,XOR برای بیت های مختلف

a	b	AND	OR	XOR
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

گیت OR می تواند از ترکیبی از AND و XOR ساخته شود

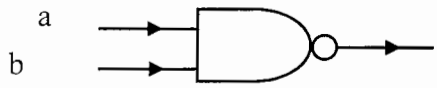
a OR b = (a AND b) XOR (a XOR b) (۳۴-۱)

(D) NAND gate:



a NAND b = NOT (a AND b)

(E) NOR gate:



a NOR b = NOT (a OR b)

با استفاده از ترکیب این گونه گیت ها می توان تمام ساختار مداری رایانه ها را تشکیل داد[۴].

۱-۸- گیت های کوانتومی

گیت های کوانتومی تبدیل کننده بیت های کوانتومی هستند، مشابه گیت های کلاسیکی که بیت های کلاسیکی را تغییر می دهند با این تفاوت که گیت های کوانتومی همیشه برگشت پذیر هستند[۹،۸].

۱-۸-۱- دینامیک

تحول زمانی و مکانی (انتقال، چرخش) در سیستم کوانتومی برطبق قوانین مکانیک کوانتومی توسط عملگرهای یکانی توصیف می شوند.

۱-۸-۱-۱-عملگر یکانی چرخش حول محور Z

بسط تیلور توابع چند متغیره را می توان به شکل زیر بیان کرد:

$$f(\vec{r}+\vec{a})=\sum_{n=0}^{\infty}\frac{1}{n}\left(\vec{a}\cdot\vec{\nabla}\right)f(\vec{r})\Big|_{r=a} \qquad (۳۵-۱)$$

با تقریب مرتبهٔ اول تابع حالت سیستم در بسط تیلور به شکل زیر است:

$$\psi(x+\varepsilon,y+\varepsilon,z)=\psi(r)+\varepsilon y\frac{d\psi}{dx}-\varepsilon x\frac{d\psi}{dy}$$

$$\frac{d\psi}{dx}=\frac{i}{\hbar}\left(\frac{\hbar}{i}\vec{\nabla}\Big|_x\right)\psi \quad , \quad \vec{P}_X=\frac{\hbar}{i}\vec{\nabla}\Big|_x$$

$$\psi(x+\varepsilon,y+\varepsilon,z)=\left[1+i\varepsilon\left(y\vec{P}_x-x\vec{P}_y\right)\right]\psi \quad ; \quad \vec{r}\times\vec{P}_z=(x\vec{P}-y\vec{P})=J_z$$

$$\psi(x+\varepsilon,y+\varepsilon,z)=\left[1-i\varepsilon J_z\right]\psi(x,y,z) \qquad (۳۶-۱)$$

از طرفی با تقریب مرتبه اول بسط تیلور این عملگر یکانی به شکل زیر است:

$$U_{(\varepsilon)}=(1-i\varepsilon J_z) \qquad (۳۷-۱)$$

در تصویر هایزنبرگ می توان گفت:

$$UU' = (1 - i\varepsilon J_z)(1 + i\varepsilon J_z') = 1 + i\varepsilon(J_z - J_z') + \mathrm{O}(\varepsilon^2).....$$

$$(J_z = J_z') \rightarrow UU' = 1 \qquad (۳۸-۱)$$

(تصویر هایزنبرگ)

$$U'HU = H'; H = H' \rightarrow U'HU = H$$
$$U'HU = (1 - i\varepsilon J_z)H(1 + i\varepsilon J_z') = H + i\varepsilon J_z'H - i\varepsilon HJ_z + \mathrm{O}(\varepsilon^2).....$$
$$= H + i\varepsilon(J_zH - HJ_z) = H + i\varepsilon\left[J_z, H\right] = H$$

$$\left[J_z, H\right] = 0 \rightarrow J_z \qquad (۳۹-۱)$$

بنابراین J_z ثابت حرکت می باشد.

چرخش به اندازه $U(\theta)$وθمتناهی را می توان از n چرخش بینهایت کوچک پی در پی $U(\varepsilon)$ ساخت.که در اینجا

$$U(\theta) = U(\varepsilon)^n = \mathrm{Limt}_{n\to\infty}\ (1 - \frac{\theta}{n}J_z) \qquad (۴۰-۱)$$

$$\mathrm{Limt}_{n\to\infty}\ (1 + \frac{x}{n}J_z)^n = e^x \qquad (۴۱-۱)$$

$$U(\theta) = e^{-i\theta J_z} \qquad (۴۲-۱)$$

درحالت کلی :

$$U(\theta_i) = e^{-i\theta_i J_i} \qquad (۴۳-۱)$$

مولدهای گروه چرخش در پایین ترین بعد $J_z = \frac{1}{2}$ به صورت زیر است:

$$U(\theta_i) = e^{-i\theta_z \frac{\sigma_z}{2}} \qquad (۴۴-۱)$$

و در حالت کلی داریم:

$$U(\theta_i) = e^{-i\theta_i \frac{\sigma_i}{2}} \qquad (۴۵-۱)$$

(σ_i ماتریس پائولی می باشد.)[۹،۲،۱]

۱-۸-۱-۲- عملگر یکانی تحول زمانی

تحول زمانی حالت کوانتومی، یکانی است که با عملگر خود الحاقی H که هامیلتونی سیستم نامیده می شود ایجاد می گردد. بسط تیلور تابع $\psi(r,t+dt)$ با تقریب مرتبه اول برای زمان بینهایت کوچک dt داریم:

$$\psi(r,t+dt)=\psi(r,t)+idt\frac{d\psi(r,t)}{dt} \qquad (۴۶-۱)$$

با توجه به معادله شرودینگر

$$\frac{d\psi(r,t)}{dt}=-iH\psi(r,t) \qquad (۴۷-۱)$$

$$\psi(r,t+dt)=(1-iHdt)\psi(r,t) \qquad (۴۹-۱)$$

$$U(dt)=(1-iHdt) \qquad (۴۸-۱)$$

چون عملگر H یک عملگر هرمیتی است. $(H=H^{\dagger})$

$$UU^{\dagger}=1 \qquad (۵۰-۱)$$

در حالتی که H به طور صریح وابسته به زمان نباشد و تحول زمانی U در زمانهای متناهی t داریم:

$$U(t)=e^{-itH} \qquad (۵۱-۱)$$

بنابراین هر گیت کوانتومی دارای یک اُپراتور (عملگر) یکانی است، از آنجایی که تحول یکانی، تحولی برگشت پذیر است، گیت های کوانتومی همیشه برگشت پذیرند.

$$|\psi_{in}\rangle\rightarrow|\psi_{out}\rangle=U|\psi_{in}\rangle \quad , \quad |\psi_{in}\rangle=U^{\dagger}|\psi_{out}\rangle \qquad (۵۲-۱)$$

U عملگر یکانی است، یعنی بزرگی و طول حالت را تغییر نمی دهد؛ بنابراین عملگر خطی و یکانی U به صورت یک گیت کوانتومی توصیف می شود که می تواند بر پایه های اصلی کیوبیت های منفرد $|0\rangle$ و $|1\rangle$ اعمال شود.

بر خلاف تحول یکانی فرایند اندازه گیری باعث فروپاشی از یک حالت به حالت دیگر (حالت های پایه اصلی) می شود یعنی سیستم کوانتومی با دستگاه اندازه گیری بر هم کنش می کند، می توان گفت فرایند اندازه گیری، فرایند برگشت پذیر نیست.

در زیر گیت های کوانتومی منفرد و گیت های کوانتومی دو تایی را نشان می دهیم[۴].

۱-۸-۲- گیت های کوانتومی منفرد

(A) The Quantum NOT (X) gate:

$$|0\rangle \rightarrow |1\rangle \quad , \quad |1\rangle \rightarrow |0\rangle$$

عملگر X یعنی ماتریس یکانی زیر را برای آن تعریف می کنیم. گیت کوانتومی NOT مشابه گیت کلاسیکی NOT عمل می کند.

$$NOT(X)gate \rightarrow \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

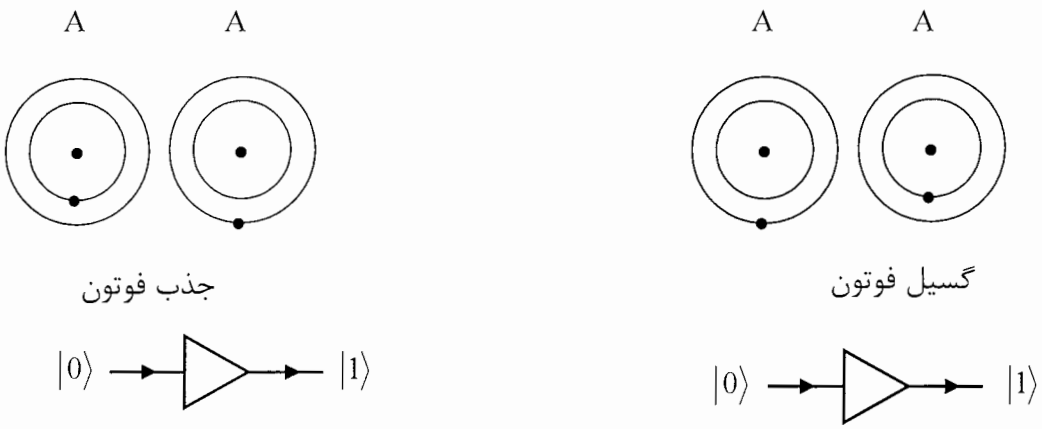
مثال:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad (۵۳-۱)$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad (۵۴-۱)$$

۱-۸-۲-۱- نمونه فیزیکی گیت NOT(X):

بر اساس ایده حالت های داخلی اتم کیو بیت ها، نمونه فیزیکی گیت NOT(X) به صورت جذب یا گسیل فوتون با انرژیی برابر اختلاف حالت پایه و برانگیخته اتم A به شکل زیر نمایش داده می شود[۲۴] .



شکل(۱- ۵): نمایش گیت NOT(X) (فوتون) و کیوبیت های حاصل ازحالت های داخلی اتم

گیت مشابه با NOT(X) گیت Y می باشد با ماتریس زیر نشان می دهند:

$$Y=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$

(B) Z gate: $|1\rangle \to -|1\rangle$, $|0\rangle \to |0\rangle$

ماتریس مطابق با آن به شکل زیر است:

$$Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

(C) Hadamard (H) gate:

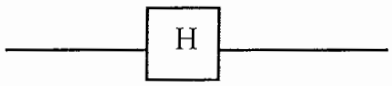
پایه های محاسباتی توسط عملگر هادامارد گیت به صورت زیر است:

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad ; \quad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

ماتریس متناظر با آن:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

معمولاً نماد هادامارد گیت به شکل زیر است:



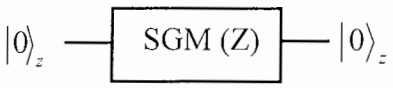
گیت Z و H هیچگونه مشابه کلاسیکی ندارند.

۱-۸-۲-۲- نمونه فیزیکی گیت های Z و H :

می توان نمونه فیزیکی گیت های Z و H را بر روی حالت های کوانتومی اسپینی درآزمایشات اشترن گرلاخ[1] به صورت زیر مشاهده کرد.

می توان دید[۱۲،۹].

گیت Z :



با ویژه مقدار $\left(\frac{\hbar}{2}\right)$

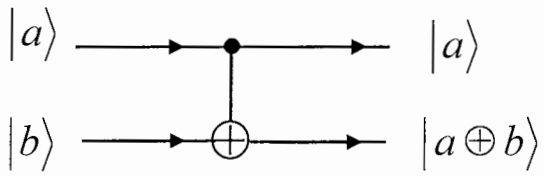
گیت X :

شکل(۱- ۶) : آزمایش اشترن گرلاخ نمونه فیزیکی گیت های Z,H

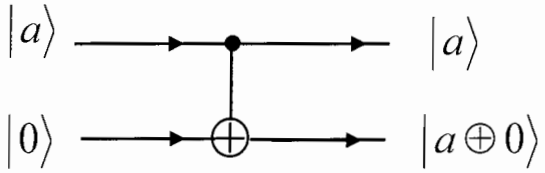
[1] Stern-gerlach experiments

۱-۸-۳- گیت کوانتومی دوتایی

The Controlled NOT (C-NOT) gate:



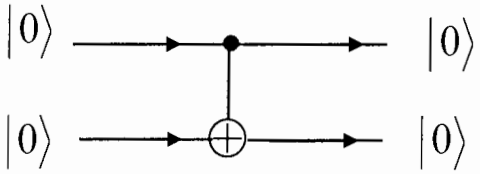
اگر b = 0 باشد، گیت بالا مانند کپی عمل می کند.



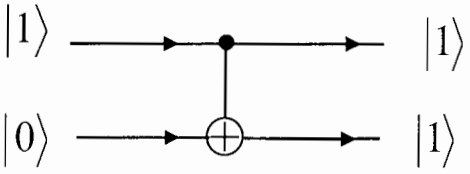
$$,0\rangle = |a\rangle|0\rangle = |a\rangle \otimes |0\rangle = \xrightarrow{(C\text{-}NOT)Gate} |a\rangle|a\rangle$$

۱-۸-۳-۱- نمونه های اعمال گیت C-NOT بر روی حالت های راست هنجار:

عمل کپی توسط گیت C-NOT بر روی حالت های راست هنجارزیر مشاهده می شود.



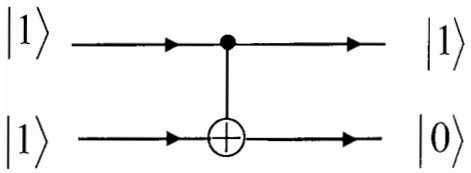
یعنی $|0\rangle|0\rangle \xrightarrow{(C\text{-}NOT)Gate} |0\rangle|0\rangle$



یعنی $|1\rangle|0\rangle \xrightarrow{(C\text{-}NOT)Gate} |1\rangle|1\rangle$

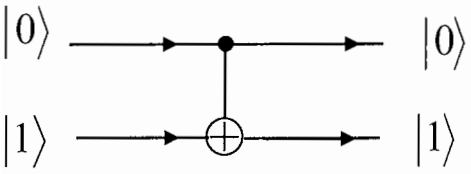
۱-۸-۳-۲- اعمال گیت C-NOT در نمونه های دیگر:

همچنین عمل گیت C-NOT بر روی کیو بیت های زیر را نیز داریم:



یعنی

$$|1\rangle|1\rangle \xrightarrow{(C\text{-}NOT)Gate} |1\rangle|0\rangle$$



یعنی $|0\rangle|1\rangle \xrightarrow{(C\text{-}NOT)Gate} |0\rangle|1\rangle$

(C – NOT) gate یکی از مهمترین گیت های کوانتومی است.

اگر چه این طرح و نقشه های اولیه بر اساس اصول فیزیکی نشان داده شده است، اما نحوه به انجام رساندن آن کاری بسیار مشکل می باشد. در سال ۱۹۹۴ افرادی چون زولر[1] و کریک[2] از دانشگاه اینسبراخ[3] به همراه یک مدل پیشنهادی پا به عرصه گذاشتند. آنها دامی را در نظر گرفتند که تعدادی یون را به طور مستقیم نگه می دارد؛ این یون ها با لیزر سرد می شوند، و سپس هر یک به طور انتخابی توسط نور ضعیف لیزر به طور خاص تحریک می شوند، در نتیجه این دام به عنوان یک سرد کننده کوانتومی با حالت کوانتومی هر یک از یون ها که نقش کیوبیت را بازی می کند، عمل خواهد کرد. این تابش های نوری می تواند موجب ارتعاش یون ها گردد. این ارتعاشات توسط تمامی یون های موجود در تله (دام) مورد نظر به اشتراک گذاشته می شوند، و قادر به انتقال اطلاعات کوانتومی بین فواصل یون ها هستند. و همچنین ابزاری برای گیت های منطقی کوانتومی

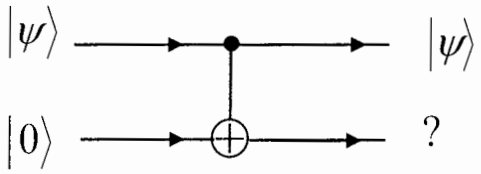
---

[1] Zoller
[2] Cirac
[3] Innsbruck

می باشد. در اواسط سال ۱۹۹۵ دانشمندان مؤسسه ملی استانداردها و تکنولوژی[1] از ایده زولر و کریک و نظر به منظور ساختن اولین گیت کوانتومی که بر روی دو کیوبیت راه اندازی می شد استفاده کردند[۲،۳،۴،۱۶].

۱-۸-۴- تئوری نوکِلونینگ[2]

در گیت (C – NOT) کپی برای حالت های پایه محاسباتی عمل می شود، اگر کنترل کیوبیت حالت عمومی $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ که $\alpha^2 + \beta^2 = 1$ باشد آیا عمل کپی برای این کیوبیت وجود دارد؟ وچگونه گیت (C – NOT) بر حالت بالا عمل می کند؟



$$|\psi\rangle|0\rangle = |\psi\rangle \otimes |0\rangle = \alpha|0,0\rangle + \beta|1,0\rangle \xrightarrow{(C\text{-}NOT)Gate} \alpha|0,0\rangle + \beta|1,1\rangle \qquad (۵۵\text{-}۱)$$

به عبارت دیگر اگر کنترل کیوبیت به درستی کپی شود حالت نهایی می باید

$$|\psi\rangle|\psi\rangle = |\psi\rangle \otimes |\psi\rangle = \alpha^2|0,0\rangle + \beta^2|1,1\rangle + \alpha\beta|0,1\rangle + \beta\alpha|1,0\rangle \qquad (۵۶\text{-}۱)$$

فقط به ازاء $\alpha = 0$ یا $\beta = 0$ این دو رابطه مشابه هم می شود، طوری که کیوبیت ورودی حالت های پایه محاسباتی باشد.

آیا امکان دارد گیت ها و مدارهای پیچیده تری استفاده شود که هر حالت کوانتومی دلخواه را کپی کند؟ پیرو گیت های کوانتومی و خطی، جواب، نه می باشد، که این نتیجه از تئوری نوکِلونینگ می باشد.

---

[1] NIST
[2] NO cloning theorem

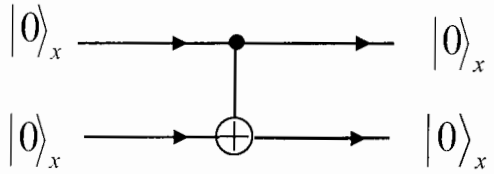
تئوری نوکِلونینگ [۴،۲]

"" کپی شدن برای حالت های پایه راست هنجار امکان پذیر است نه برای هر حالت کوانتومی دلخواه""

تئوری کِلونینگ به این معنی نیست که هرگز نمی توان کیوبیت هایی مانند $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ را کپی نمود بلکه اگرحالت راست هنجار برای آن وجود داشته باشد می توان با استفاده با تئوری کِلونینگ آن حالت را کپی نمود.

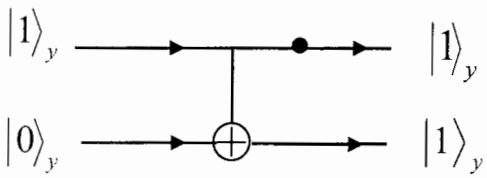
مثال(۱):

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



مثال(۲):

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



۱-۹- نتیجه گیری

امروزه دستیابی های جالب بسیاری در زمینه محاسبه کوانتومی و تکنولوژی های مربوط به آن وجود دارد. شرایط و پیش نیازهای مربوط به سخت افزار کوانتومی به سادگی بیان می شود، بطوریکه در عمل بسیار ضروری می باشند. اولاً یک ثبت کننده چندگانه مربوط به کیوبیت ها ی کوانتوم می بایست در یک شکل قابل نوشتن تهیه گردد، و از تأثیرات محیطی که سبب آسیب و غیر منسجم شدن حالات کوانتوم می شوند، به دور باشند. ثانیاً، با وجود پیوستن ضعیف به دنیای خارج، کیوبیت ها می بایست با یکدیگر ازطریق یک مکانیسم کنترلی خارجی به منظور اجرای عملکردهایی در گیت منطقی متصل گردند. ثالثاً، می بایست یک روش خواندن جهت تعیین حالت هر کیوبیت در پایان محاسبه وجود داشته باشد.

تعداد بسیاری از آزمایشات وجود دارند که نشان می دهد این شرایط و پیش نیازها حد اقل در اصل کار می بایست تأمین و برآورده شوند.

این آزمایشات شامل تکنولوژی هایی از قبیل نورهای خطی، طنین مغناطیسی هسته ای (NMR)، الکترودینامیک های حفره کوانتومی (QED)، اتم های خنثی در شبکه های وابسته اپتیکی، ذره های تعاملی کوانتومی، ابزارها و وسایل ابر رسانا یا فوق هادی و بسیاری از تکنولوژی های دیگر می باشند[۴،۲].

فصل ۲:

حالت های درهم تنیدگی و کاربردهای آن

- مقدمه
- حالت های در هم تنیده
- ماتریس چگالی
- سیستم های کوانتومی دو طرفه
- معادله تفکیک اشمیت
- درهم تنیدگی وکاربرد آن
- نتیجه گیری

۲-۱- مقدمه

درتئوری مکانیک کوانتومی پدیده در هم تنیدگی مشاهده می شود که شامل دو ذره (فوتون یا الکترون) در فضای جدا از هم ولی خواص آن ها به نوعی به هم وابسته هستند، دستگاه (سیستم) از این نوع در ابتدا به وسیله انیشتین- پودولسکی و روزن[1] [۱۳،۹،۲] مطرح شد،مانند یک جفت ذره هر یک با اسپین $\frac{1}{2}$ و اسپین کل صفر که دارای تکانه زاویه ای کل صفر هستند. جفت ذراتی با این خواص را می توان با پراکندگی باریکه ای از پروتون کم انرژی از گاز هیدروژن تولید نمود.

اطلاعات (کیوبیت ها) با استفاده از پدیده در هم تنیدگی حالت های کوانتومی دو شئ انتقال می یابند. به بیانی دیگر در صورت در هم تنیدگی حالت های کوانتومی دو شئ می توانند از نظر فیزیکی در مکان های جدا از هم باشند، ولی اطلاعات (کیوبیت ها) مشترکی در یک زمان داشته باشند.

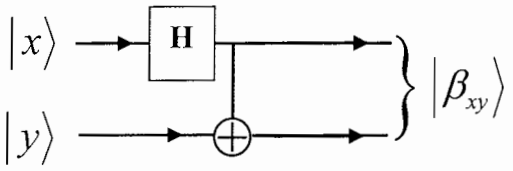
محققان قبلاً موفق به در هم تنیدن جفت هایی از حالت کوانتومی قطبش فوتون ها و جفت هایی ازحالت کوانتومی اسپین الکترون ها شده بودند، به هر حال پدیده ای غیر قابل انتظار و دور از تصور در تئوری مکانیک کوانتومی است.

در این فصل به حالت های در هم تنیده می پردازیم و ماتریس چگالی و مقدار انتظاری حالت های در هم تنیده را به صورت ریاضی فرمول بندی می کنیم ،موضعیت را در پدیده های در هم تنیده بررسی خواهیم کرد. و کاربرد های حالت های در هم تنیده در انتقال کیوبیت ها را بیان می کنیم.

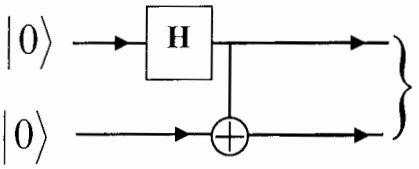
[1] A.Einstein , B.Podolski , N.Rosen (EPR)

۲-۲- حالت های در هم تنیده

اگر به دو کیوبیت گیت زیر اعمال شود کیوبیت خروجی حاصل کیوبیت در هم تنیده است.



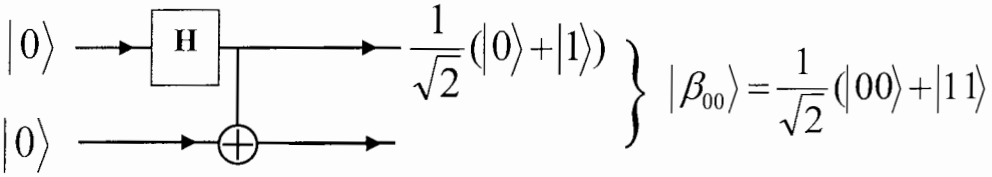
خروجی در مدار بالا برای x = y =0 حالت کیوبیت است.



و $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$

محاسبه:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\right] = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$$|0\rangle \oplus |0\rangle = |0\rangle \quad , \quad |1\rangle \oplus |0\rangle = |1\rangle$$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \xrightarrow{(C\text{-}NOT)\,gate} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (۱-۲)$$

این حالت را نمی توان توسط دو کیوبیت منفرد نمایش داد؛ و همبستگی بین دو کیو بیت وجود دارد به این کیوبیت ها در هم تنیده گفته می شود. این همبستگی دو کیوبیت حتی در فاصله های بسیار زیاد از همدیگر جدا نمی شوند.

این نوع همسبتگی معروف به همبستگی ناموضع ای بل[1] است. و آن پاسخی برای پارادوکس (باطلنما) EPR است[۵۰]. حالت های مشابه در هم تنیده و همبستگی حالت های دو کیوبیتی که به حالت های EPR یا بل معروفند[۴،۵،۶،۹،۱۳] عبارتند از:

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

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad (۳-۲)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad (۴-۲)$$

۲-۲-۱- نمونه ساده کوانتومی حالت در هم تنیده

برای ذکر نمونه ساده حالت در هم تنیده کوانتومی می توان به یک سیستم دو الکترونی که فقط دارای اسپین هستند بپردازیم. اگر اسپین الکترون اول را با S_1 و اسپین دوم را با S_2 نمایش دهیم می توانیم به این سیستم یک اسپین کل S نسبت دهیم:

$$S = S_1 + S_2$$

$$[S_{ix}, S_{iy}] = i\varepsilon_{xyz}\hbar S_{iz} \qquad (۴-۲)$$

اندازه S کل از رابطه زیر بدست می آید[۱۲] و روابط (۲-۵) و (۲-۶) حالت های درهم تنیده اسپینی هستند:

$$|S_1 - S_2| \le S \le (S_1 + S_2)$$

$$Example: S_1 = \frac{1}{2}; S_2 = \frac{1}{2}$$

$$\begin{cases} |\uparrow\uparrow\rangle \\ \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \quad * \quad Triplet \\ |\downarrow\downarrow\rangle \end{cases} \qquad (۵-۲)$$

$$\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \quad * \quad Singlet \qquad (۶-۲)$$

[1] John.s. Bell non local correlation

۲-۳- ماتریس چگالی

۲-۳-۱- در سیستم کوانتومی تک کیوبیتی

عملگر چگالی توسط فون نیومن در سال ۱۹۲۷ ابداع شد، که مسائل فیزیکی در چارچوب آنسامبل های آمیخته و محض (خالص) به صورت کمی تشریح می کند[۱۲].

بحث کلی که ارائه می شود به سیستمهای اسپین $\frac{1}{2}$ محدود نمی شود، اما برای روشن شدن به سیستمهای $\frac{1}{2}$ می پردازیم:

۲-۳-۱-۱- آنسامبل محض[1]

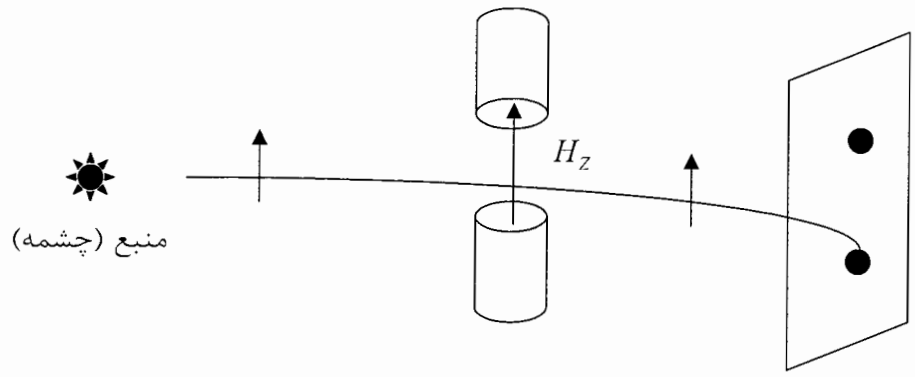
اجتماعی از سیستمهای فیزیکی به گونه ای است که همهٔ اعضا با کت یکسان $|\alpha\rangle$ مشخص می شوند.

$$|\alpha\rangle = a_0|0\rangle + a_1|1\rangle \qquad (۵-۲)$$

و چگالی ماتریس آن به صورت زیر بیان می گردد[۱۲،۹].

$$\rho = |\alpha\rangle\langle\alpha| \qquad (۶-۲)$$

مثال(۱)



شکل(۲-۱): آزمایش اشترن گرلاخ

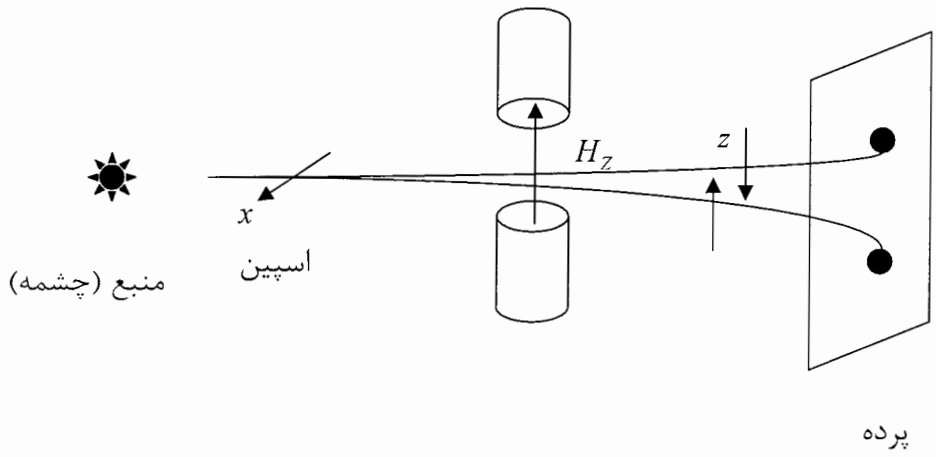
[1] Ensemble pure

$$|\alpha\rangle = |0\rangle$$

$$\rho = |\alpha\rangle\langle\alpha|$$

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

مثال(۲)



شکل(۲-۲): آزمایش اشترن گرلاخ

$$\rho = |\alpha\rangle\langle\alpha|$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\rho = |\psi\rangle\langle\psi| = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]\left[\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\right] = \frac{1}{2}\left[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\right] =$$

$$\frac{1}{2}\left[\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix}\right] =$$

$$\frac{1}{2}\left[\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} + \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\1 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}\right] = \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$$

۲-۳-۱-۲- آنسامبل های آمیخته[1]

به صورت غیر دقیق می توان آنسامبل های آمیخته را به صورت آمیزه ای از آنسامبل های محض تصور نمود.

آنسامبل های آمیخته کسری از اعضا با جمعیت ω_i با $|\alpha^i\rangle$ مشخص می شوند.

$w_1 \quad |\alpha^1\rangle$

$w_2 \quad |\alpha^2\rangle$

$\vdots$

$\vdots$

$w_i \quad |\alpha^i\rangle$

$$|\alpha\rangle = w_1|\alpha^1\rangle + w_2|\alpha^2\rangle + \ldots\ldots\ldots\ldots$$

$$\rho = \sum_i w_i |\alpha^i\rangle\langle\alpha^i|$$

$$\rho = \sum_i w_i \rho_i \qquad (۷-۲)$$

مقدار انتظاری هر عملگر A در رابطه زیر همواره برقرار است:

$$\langle A\rangle = tr(\rho A) \qquad (۸-۲)$$

اثبات:

$$\langle A\rangle = \sum_i w_i \langle\alpha^i|A|\alpha^i\rangle = \sum_i w_i \sum_b \sum_{b'} \langle\alpha^i|b\rangle\langle b|A|b'\rangle\langle b'|\alpha^i\rangle =$$

$$\sum_b \sum_{b'} \sum_i w_i \langle b'|\alpha^i\rangle\langle\alpha^i|b\rangle\langle b|A|b'\rangle = \sum_b \sum_{b'} \langle b'|\sum_i w_i |\alpha^i\rangle\langle\alpha^i|\,|b\rangle\langle b|A|b'\rangle =$$

$$\sum_b \sum_{b'} \langle b'|\rho|b\rangle\langle b|A|b'\rangle = \sum_b \sum_{b'} \langle b'|\rho A|b'\rangle = tr(\rho A) \quad ; \quad \sum_b |b\rangle\langle b| = 1$$

[1] Ensemble mixed

۲-۴- سیستم کوانتومی دو طرفه[1] (دو کیو بیتی)[۲]

شگفتیهای مکانیک کوانتومی را می توان در بررسی خواص حالت های کوانتـومی دو کیـوبیتی یافت. $\{|0\rangle_A,|1\rangle_A\},\{|0\rangle_B,|1\rangle_B\}$ به ترتیب نمایش پایه های ارتونرمال A وB می باشـند، فـرض مـی کنیم حالت کوانتومی دو کیو بیتی به شکل زیر باشد.

$$|\psi\rangle_{AB}=a|0\rangle_A\otimes|0\rangle_B+b|1\rangle_A\otimes|1\rangle_B \qquad (۹-۲)$$

در این حالت کیو بیت A وB نسبت به یکدیگر همبسته هستند.

اندازه گیری کیوبیت A به وسیله تصویر روی پایه های $\{|0\rangle_A,|1\rangle_B\}$ با احتمـال $|a|^2$ نتیجـه $|0\rangle_A$ را مـی دهـد و انـدازگیری حالـت $\{|0\rangle_B,|1\rangle_B\}$ را نمایـان مـی کنـد و بـا احتمـال $|b|^2$ نتیجـه $|1\rangle_A$ و حالت $|1\rangle_A\otimes|1\rangle_B$ را ظاهر می سازد؛ بنابر این اگر ما نتایج $|1\rangle_A,|0\rangle_A$ را بدست بیاوریم می توانیم با تضمین (با احتمال یک) نتایج $|1\rangle_B,|0\rangle_B$ را بیابیم.

بطور مشابه با اندازه گیـری کیـو بیـت B نتـایج مـشابهی بدسـت مـی آیـد. یعنـی خروجـی هـای $\{|0\rangle_A,|1\rangle_A\},\{|0\rangle_B,|1\rangle_B\}$ حاصل از اندازه گیرها در حالت $|\psi\rangle_{AB}$ کاملاً همبسته هستند.

بحث حالت دو کیوبیتی $|\psi\rangle_{AB}$ به عنوان سیستم کوانتومی دو طرفه (غیر قابل تقسیم به دو قسمت) مطرح می شود.

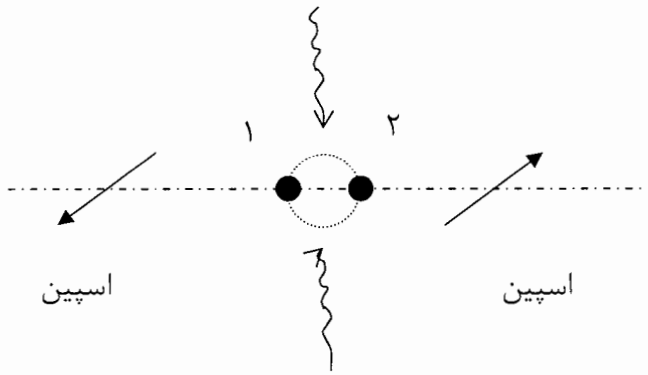
فضای هیلبرت سیستم دو طرفه $H_A\otimes H_B$ شامل دو بخش است یعنی $\{|i\rangle_A\}$ پایه هـای اُرتونرمـال برای H_A و$\{|\mu\rangle_B\}$ پایه های اُرتونرمال برای H_B سپس $\{|i\rangle_A\otimes|\mu\rangle_B\}$ پایـه هـای اُرتونرمـال بـرای $H_A\otimes H_B$ هستند.

در حالت کلی حالت محض دو طرفه را می توان به شکل زیر بیان نمود:

$$|\psi\rangle_{AB}=\sum_{i\mu}a_{i\mu}|i\rangle_A\otimes|\mu\rangle_B \qquad (۱۰-۲)$$
$$\sum_{i\mu}a_{i\mu}=1$$

[1] The bipartite quantum system

نمونه فیزیکی کیو بیت در هم تنیده در تولید ونابودی زوج:



شکل (۲-۳): حالت در هم تنیده در تولید ونابودی زوج

۲-۴-۱- محاسبه مقدار انتظاری مشاهده پذیر M_A روی حالت محض دو طرفه $|\psi\rangle_{AB}$

با در نظر گرفتن مشاهده پذیر به صورت $M_A \otimes I_B$ که M_A عملگر خود الحاقی است که روی A اعمال می شود و I_B عملگر واحد است،که روی B اعمال می شود.

$$\langle M_A\rangle = {}_{AB}\langle\psi|M_A\otimes I_B|\psi\rangle_{AB} = \sum_{j,\nu} a^*_{j\nu}\,{}_A\langle j|\otimes_B\langle\nu|(M_A\otimes I_B)\sum_{i,\mu} a_{i\mu}|i\rangle_A\otimes|\mu\rangle_B =$$
$$\sum_{i,j,\mu} a^*_{i\mu}a_{i\mu}\,{}_A\langle j|M_A|i\rangle_A = \ldots\ldots\ldots = tr(M_A\rho_A) \qquad (۱۱-۲)$$

با توجه به محاسبات قبل برای تک کیوبیت و با در نظر داشتن رابطه زیر برای چگالی ماتریس داریم[۲]:

$$\rho_A = tr_B(|\psi\rangle_{AB\,AB}\langle\psi|) = \sum_{i,j,\mu} a^*_{j\mu}a_{i\mu}|i\rangle_{A\,A}\langle j| \qquad (۱۲-۲)$$

مثال:

$$|\psi\rangle_{AB} = a|0\rangle_A\otimes|0\rangle_B + b|1\rangle_A\otimes|1\rangle_B$$
$$\langle M_A\rangle = {}_{AB}\langle\psi|M_A\otimes I_B|\psi\rangle_{AB} =$$
$$(a^*{}_A\langle 0|\otimes_B\langle 0| + b^*{}_A\langle 1|\otimes_B\langle 1|)(M_A\otimes I_B)(a|0\rangle_A\otimes|0\rangle_B + b|1\rangle_A\otimes|1\rangle_B) =$$
$$\ldots\ldots\ldots\ldots = |a|^2{}_A\langle 0|M_A|0\rangle_A + |b|^2{}_A\langle 1|M_A|1\rangle_A = tr(M_A\rho_A)$$
$$\rho_A = (|a|^2|0\rangle_{A\,A}\langle 0| + |b|^2|1\rangle_{A\,A}\langle 1|)$$

حالت های در هم تنیده را می توان به صورت معادله تفکیک اشمیت[1] بیان نمود.

۲-۵- معادله تفکیک اشمیت

یک حالت محض دو طرفه $|\psi\rangle_{AB}$را میتوان به شکل استاندارد تفکیک اشمیت که بسیار مورد استفاده قرار می گیرد بیان نمود.

$$|\psi\rangle_{AB} = \sum_{i\mu} a_{i\mu}|i\rangle_A \otimes |\mu\rangle_B$$

$$\sum_{i\mu} a_{i\mu} = 1$$

که در آن $\{|i\rangle_A, |\mu\rangle_B\}$ پایه های اُرتو نرمال فضا های هیلبرت $H_A \otimes H_B$ می باشند.

با توجه به اینکه بردار دلخواه $|\psi\rangle_{AB}$ در فضای $H_A \otimes H_B$ بسط داده شده است.می توان پایه های $\{|i\rangle_A\}$ را به گونه ای انتخاب کنیم که ماتریس چگالی ρ_A به صورت زیر باشد.

$$\rho_A = \sum_i p_i |i\rangle_{A\,A}\langle i| \qquad (۱۳-۲)$$

از طرفی برای یک سیستم مرکب می توان ρ_A را به صورت زیر نوشت:

$$\rho_A = tr_B(|\psi\rangle_{AB\,AB}\langle\psi|) = \sum_i p_i |i\rangle_{A\,A}\langle i| \qquad (۱۴-۲)$$

$$|\psi\rangle_{AB} = \sum_{i\mu} a_{i\mu}|i\rangle_A|\mu\rangle_B = \sum_i \sum_\mu a_{i\mu}|i\rangle_A|\mu\rangle_B = \sum_i |i\rangle_A \sum_\mu a_{i\mu}|\mu\rangle_B \qquad (۱۵-۲)$$

که در آن $|\tilde{i}\rangle_B = \sum_\mu a_{i\mu}|\mu\rangle_B$ است ودر نتیجه خواهیم داشت:

$$|\psi\rangle_{AB} = \sum_i |i\rangle_A |\tilde{i}\rangle_B \qquad (۱۶-۲)$$

که در آن پایه های $|\tilde{i}\rangle_B$ لزوماً اُرتونرمال نیستند، بنابراین نیاز به تعریف پایه های اُرتونرمال داریم، که به صورت زیر بدست می آید:

$${}_B\langle\tilde{i}|\tilde{j}\rangle_B = p_i\delta_{ij} \xrightarrow{p_i\neq 0} |i'\rangle = p^{-\frac{1}{2}}|\tilde{i}\rangle \qquad (۱۷-۲)$$

[1] Schmidt decomposition

راه حل:

$$\rho_A = tr_B(|\psi\rangle_{AB\,AB}\langle\psi|) = tr_B(\sum_i |i\rangle_A |\tilde{i}\rangle_B \sum_j {}_A\langle j|_B\langle\tilde{j}|) \qquad (۱۸-۲)$$

به شکل تانسوری می نویسم:

$$\rho_A = tr_B(\sum_{ij} |i\rangle_{A\,A}\langle j| \otimes |\tilde{i}\rangle_{B\,B}\langle\tilde{j}|) \qquad (۱۹-۲)$$

در فضای هیلبرت H_B اثر می کند بنابراین با استفاده از تعریف ماتریس tr_B داریم:

$$tr_B(|\tilde{i}\rangle_{B\,B}\langle\tilde{j}|) = \sum_K {}_B\langle k|\tilde{i}\rangle_{B\,B}\langle\tilde{j}|k\rangle_B = \sum_K {}_B\langle\tilde{j}|k\rangle_{B\,B}\langle k|\tilde{i}\rangle_B = {}_B\langle\tilde{j}|\tilde{i}\rangle_B \qquad (۲۰-۲)$$

که $\sum_k |k\rangle_{B\,B}\langle k| = 1$

$|k\rangle_B$ پایه های اُرتونرمال فضای H_B می باشد.

سپس پایه های اُرتونرمال را به شکل زیر جایگزین می کنیم:

$$|i'\rangle_B = p_i^{-\frac{1}{2}} |\tilde{i}\rangle_B \qquad (۲۱-۲)$$

خواهیم داشت:

$$|\psi\rangle_{AB} = \sum_i \sqrt{p}|i\rangle_A |i'\rangle_B \qquad (۲۲-۲)$$

که $|i'\rangle_B$, $|i\rangle_A$ پایه های اُرتو نرمال ویژه از فضای هیلبرت H_B , H_A هستند.

معادله بالا تفکیک اشمیت حالت محض دو طرفه $|\psi\rangle_{AB}$ می باشد. هر حالت محض دو طرفه را می توان به این شکل بیان نمود؛ البته پایه های بکار رفته به حالت محض در حال بسط بستگی دارد. در کل ما نمی توانیم $|\varphi\rangle_{AB} \in H_A \otimes H_B$, $|\psi\rangle_{AB}$ را به طور همزمان، به شکلی که پایه های اُرتونرمال یکسانی برای H_B , H_A داشته باشند،بسط دهیم.

با گرفتن trace روی کل فضای H_A می توان چگالی ماتریس ρ_B را به شکل زیر نمایش داد:

$$\rho_B = tr_A(|\psi\rangle_{AB\,AB}\langle\psi|) = \sum_i p_i |i'\rangle_{B\,B}\langle i'| \qquad (۲۳-۲)$$

ρ_B , ρ_A ویژه مقادیر غیر صفر یکسان دارند؛ البته لزومی ندارد H_B , H_A دارای بعد یکسانی باشند، بنابراین تعداد ویژه مقادیر غیر صفر ρ_B , ρ_A می تواند با هم فرق کند[۱۳،۲] .

مثال (حالت محض دو طرفه دو ذره ای) :

$$i=\{0,1\}\rightarrow\left\{|\psi\rangle_{AB}=\sum_{i=0}^{1}\sqrt{p_i}|i\rangle_A|i'\rangle_B\right.$$

$$|\psi\rangle_{AB}=\sqrt{p_0}|0\rangle_A|0'\rangle_B+\sqrt{p_1}|1\rangle_A|1'\rangle_B$$

$$\rho_A=\sum_{i=0}^{1}p_i|i\rangle_{A\,A}\langle i|=p_0|0\rangle_{A\,A}\langle 0|+p_1|1\rangle_{A\,A}\langle 1|=p_0\left[\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right]+p_1\left[\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right]=$$

$$\left[\begin{pmatrix}p_0&0\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\0&p_1\end{pmatrix}\right]=\begin{pmatrix}p_0&0\\0&p_1\end{pmatrix}$$

مثال:

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

$$\rho_A=\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

با توجه به معادله تفکیک اشمیت هر حالت محض کامل دو طرفه $|\psi\rangle_{AB}$ را می توانیم با یک عدد صحیح مثبت به هم مربوط سازیم؛ عدد اشمیت که تعداد مقادیر عددی غیر صفر در ρ_A یا ρ_B است،در نتیجه آن تعداد روابط موجود در تفکیک اشمیت $|\psi\rangle_{AB}$ را به هم وابسته می کند. در روابط این کمّیت می توانیم آنچه را که به معنی جداناپذیر و نا منفک بودن حالت محض دو طرفه است به صورت زیر تعریف کرد:

$|\psi\rangle_{AB}$در هم تنیده (جفت شده ،جداناپذیر) است ، مشروط بر اینکه عدد اشمیت بزرگتر از یک باشد؛ در غیر این صورت غیر در هم تنیده (جفت نشده، جدا پذیر) می باشد.

در نتیجه حالت محض دو طرفه غیر در هم تنیده یک نتیجه مستقیم از حالات محض در فضای هیلبرت H_A,H_B است؛ می توان به صورت زیر نمایش داد:

$$|\psi\rangle_{AB}=|\varphi_A\rangle\otimes|\chi_B\rangle \qquad (۲۴-۲)$$

بنابراین ماتریس های چگالی کاهش یافته $\rho_A=|\varphi\rangle_{A\,A}\langle\varphi|$ و $\rho_A=|\varphi\rangle_{B\,B}\langle\varphi|$ محض (خالص) می باشند. هرحالتی که نمی تواند همانند چنین نتیجهٔ مستقیمی بیان شود؛حالت در هم تنیده خواهد بود، در نتیجه ρ_A,ρ_B حالت های آمیخته (مرکب) می باشند.

یکی از اهداف اصلی ما در این روابط درک بهتر و اهمیت در هم تنیدگی خواهد بود. اگر بگوئیم $|\psi\rangle_{AB}$ غیر درهم تنیده (مجزا و تفکیک پذیر) باشد، و نیز صحیح نیست بگوئیم زیر ساختارهای A و B غیر همبسته[1] خواهند بود. به عنوان مثال حالت مجزای $|\uparrow\rangle_A|\uparrow\rangle_B$ مطمئناً همبسته هستند، هر دو آنها در یک راستا نشان داده شده اند.

امّا همبستگی بین A وB در حالت در هم تنیده نسبت به همبستگی A وB در یک حالت غیر در هم تنیده، دارای خواص متفاوت هستند. شاید تفاوت منتقدانه این باشد،که حالت در هم تنیده در موضعیت[2] نمی تواند آفریده شود، به عبارت دیگر در هم تنیدگی موضعیت را نقض می کند که در فصل چهارم مفصل به آن اشاره می شود. تنها راه برای درهم تنیدگی مربوط به دو زیر ساختار A و B می باشد که به طور مستقیم با یکدیگر برهم کنش می کنند. می توانیم حالت $|\uparrow\rangle_A|\uparrow\rangle_B$ را به منظور اسپین های A وB که همواره در تماس هستند و با اسپین یکدیگر می آیند تهیه نمائیم،که تنها یک پیغام کلاسیکی را به هر دو کاربر آلیس[3] و باب[4] ارسال نمائیم و به هر دوی آنها اعلام کنیم که یک نقطه اسپینی در امتداد محور z تهیه نمایند.

اما تنها راه، برای دگرگون کردن(اندازه گیری) حالت $|\uparrow\rangle_A|\uparrow\rangle_B$ در درون یک حالت درهم تنیده مانند $\frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A|\uparrow\rangle_B+|\downarrow\rangle_A|\downarrow\rangle_B\right)$ بکار بردن تبدیلات یکانی مشترک به این حالت می باشد. تبدیلات یکانی موضعی $U_A\otimes U_B$ و اندازه گیری های موضعی که توسط آلیس و باب انجام می شود نمی تواند عدد اشمیت حالت دو کیو بیتی را افزایش دهد. هیچ مسئله ای مبنی بر اینکه چه اندازه آلیس و باب بر سر آن چیزی که انجام می دهند بحث و گفتگو می کنند وجود ندارد.

برای در هم تنیدگی دو کیو بیت می بایست آنها را با یکدیگر بیاوریم و اجازه دهیم که با یکدیگر بر هم کنش کنند. این نکته قابل بحث وجوددارد که احتمال دارد تمایزی بین حالات آمیخته دو طرفه تفکیک پذیر و درهم تنیده وجود داشته باشد[۹،۵،۴،۲].

---

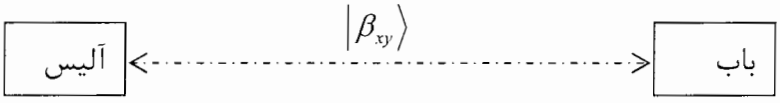
[1] Uncorrelated
[2] Locality
[3] Alice
[4] Bob

۲-۶- کاربردهای حالت درهم تنیده

در بعضی از روش ها که فرآیند در هم تنیدگی می تواند در آن به منظور استفاده کاربردی قرار گیرد، به دو مورد از آن می پردازیم[۲،۴،۹،۱۰] :

۲-۶-۱- رمز گذار ابر چگال[1]

فرض کنیم آلیس در آمستردام تمایل دارد دو بیت از اطلاعات را به دوستش باب در بوستون ارسال نماید؛ به طور کلاسیکی بهترین روش فرستاده شدن دو بیت مجزا می باشد. سؤال این است که آیا طبق نظریه مکانیک کوانتومی برای ارسال آن می توان توسط تنها تک کیوبیت منفرد به مرحله اجرا در آید؟ پاسخ آری است، در این زمینه مطالعات زیادی انجام گرفته است که پیام کلاسیکی دو بیتی را در یک جفت ذره در هم تنیده کد گذاری می کنند بنابراین مشروط بر آنکه آلیس و باب کیوبیت را در حالت بِل با یکدیگر سهیم شده باشند، مثلاً $|\beta_{00}\rangle$.



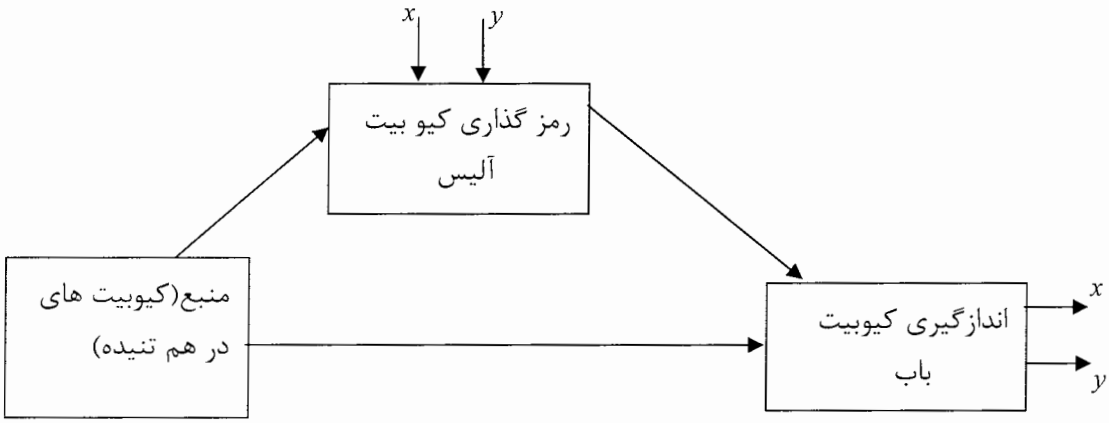
شکل(۲-۴) : یک جفت در هم تنیده از کیو بیت ها متعلق به آلیس و باب که با یکدیگر سهیم هستندبرای مقدمات رمز نگاری ابر چگال ضروری است

اگر این کیوبیتی که می بایست فرستاده شوند 00 باشند، درنتیجه آلیس به سادگی کیوبیت خود رابه باب که حالا کیوبیت درحالت $|\beta_{00}\rangle$ دارد، ارسال می کند. اگرکیوبیتی که می بایست ارسال گردد 01 باشند، درنتیجه آلیس یک گیت کوانتومی NOT X برای کیوبیت خود بکار می برد (فرض بر اینکه اولین عضو این جفت متعلق به آلیس باشد) و آنرا به باب که حالا جفت مورد نظر را در حالت بِل $|\beta_{01}\rangle$ دارد ارسال می کند. آلیس متشابهاً تغییر شکل های مناسبی را برای کیوبیت خود بکار می برد. کیوبیت های مورد نظری که باید ارسال شوند، می توانند به صورت ترکیب های دیگری از 10 و11 باشندکه به باب ارسال می شود.

---

[1] Super-dense coding

نتیجه کلی این است که دو بیت کلاسیکیxy بوسیله یک حالت بِل منفرد $|\beta_{xy}\rangle$ رمز گذاری(کد بندی) می شود. این نوع رمزگذاری بوجود آمده از یک تعداد بیت های کلاسیکی توسط یک حالت کوانتومی در هم تنیده منفرد، به عنوان رمز گذاری بسیار انبوه شناخته می شود.از آنجائیکه چهار حالت بِل راست هنجار هستند، در نتیجه آنها یقیناً بوسیله یک اندازه گیری مناسب، قابل تشخیص می گردند. بنابراین باب می تواند حالت در هم تنیده کیوبیتی را که در اختیار دارد "رمز گشایی" کند و اطلاعات دو بیت کلاسیکی را بدست آورد.



شکل(۲- ۵):در طرح رمز گذاری ابر چگال دو بیت درکیو
بیت در هم تنییده رمز گذاری و سپس رمز گشایی می شوند.

اگر کیو بیت در هم تنیده به صورت $|\beta_{00}\rangle$باشد، آلیس برای ارسال آن هیچ اقدامی بر روی آن انجام نخواهد داد؛ اما اگر دو کیو بیت در هم تنیده به صورت دیگر مثلاً $|\beta_{11}\rangle,|\beta_{10}\rangle,|\beta_{01}\rangle$ باشد و آلیس بخواهد آنرا به باب ارسال کند او باید اقدامات زیر را برای هر کدام انجام دهد.

$$|\beta_{00}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\xrightarrow{NOT(X)gate}\frac{1}{\sqrt{2}}(|10\rangle+|01\rangle) \qquad (۲۵-۲)$$

$$|\beta_{00}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\xrightarrow{(Z)gate}\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle) \qquad (۲۶-۲)$$

$$|\beta_{00}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\xrightarrow{(iY)gate}\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \qquad (۲۷-۲)$$

در این صورت آلیس مطابق شکل(۲- ۵) دو بیت کلاسیکی را در کیو بیت در هم تنیده رمز گذاری می کند. سپس باب با اندازه گیری بر روی کیو بیت دو بیت کلاسکی رارمز گشایی خواهد نمود.

فرض کینم آلیس وباب در کیو بیت در هم تنیده $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$ با یکدیگر سهیم هستند که کیو بیت اول برای آلیس و کیو بیت دوم برای باب باشد. با اندازه گیری باب بر روی حالت درهم تنیده او اگر کیوبیت $|0\rangle$را بدست آورد یعنی بیت کلاسیکی $y = 0$را رمز گشایی نموده است. و دانستن کیو بیت در هم تنیده می تواند نتیجه بگیرد که $x = 1$ است، بنابراین با یک اندازه گیری توسط باب بیت های کلاسیکی در کیو بیت در هم تنیده رمز گشایی می شود[۹،۴] .

۲-۶-۲- ارسال اطلاعات (کیوبیت) از راه دور[1]

آلیس در آمستردام می خواهد، یک حالت تک کیوبیتی دلخواه $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ را به باب در بوستون ارسال نماید. او نمی تواند این حالت را تعیین کند و اطلاعات مورد نظر را به باب ارسال نماید. مگر آنکه دوباره فرض شود که آلیس و باب یک جفت از کیوبیت های در هم تنیده را در یکی از حالت های بِل سهیم شده باشند، مانند:

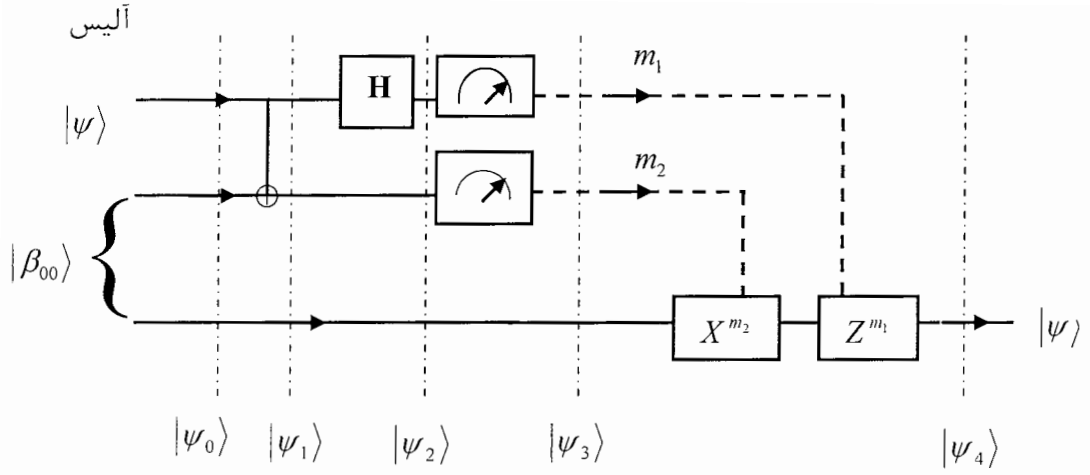
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (۲۸-۲)$$

کیوبیتی که باید بهمراه حالت در هم تنیده (جفت) از راه دور ارسال گردد از حالت سه کیوبیتی آغاز می گردد.

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right) \qquad (۲۹-۲)$$

در اینجا، به طور معمول، دو کیوبیت اول به همراه آلیس و سومین کیوبیت به همراه باب می باشد.

[1] Quantum Teleportation



باب

شکل(۲- ۶): مدار کوانتومی برای ارسال نور ترابی یک کیوبیت

حالا آلیس دو کیوبیت خود را در سرتاسر یک گیت C – NOT قرار می دهد. این روند کیوبیتی را که باید به همراه بخشی از حالت در هم تنیده متعلق به آلیس ، از راه دور ارسال گردد را گیر می اندازد و آنها را جفت می کند. این حالت درهم تنیده البته برای بوجود آمدن و آغاز کردن کار گیر انداخته می شد. در نتیجه این سه کیوبیت در حالت گیرافتاده (در هم تنیده) منتهی می شوند به:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|10\rangle + |01\rangle\right)\right] \qquad (۳۰-۲)$$

با توجه به نمونه های اشاره شده در (۱-۸-۳-۱) و (۱-۸-۳-۲) رابطه بالا بدست می آید.

بعد از آن آلیس اولین کیوبیت را در سرتاسر یک گیت هادامارد ارسال می کند و دو کیوبیت خود را در مبنای محاسبه ای اندازه گیری می نماید. حالت این سه کیوبیت بعد از گیت هادامارد به این صورت می باشد.

با اعمال گیت هاداماراد بر روی کیو بیت $|\psi\rangle$داریم:

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

$$= \frac{1}{\sqrt{2}}\left[\alpha(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle)\right] \qquad (۳۱-۲)$$

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right] \quad (۳۲-۲)$$

با یک عملیات حاصل ضرب تانسوری ساده ومنتقل کردن ضرایب α, β به کیو بیت سوم داریم:

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{2}[|00\rangle(\alpha|0\rangle) + |01\rangle(\alpha|1\rangle) + |10\rangle(\alpha|0\rangle) + |11\rangle(\alpha|1\rangle)) \\ &\quad + |01\rangle(\beta|0\rangle) + |00\rangle(\beta|1\rangle - |11\rangle(\beta|0\rangle - |10\rangle(\beta|1\rangle)] \\ &= \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ &\quad + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)] \end{aligned} \quad (۳۳-۲)$$

بنابراین، نتیجهٔ اندازه گیری آلیس با احتمال $\frac{1}{4}$ یکی از جفت های $00,01,10,11$ خواهد بود و حالات مطابق با آن در هر کدام از کیوبیت های باب که در سمت چپ خواهند بود به این صورت می باشند.

$$00 \rightarrow |\psi_{00}\rangle = \alpha|0\rangle + \beta|1\rangle \quad (۳۴-۲)$$

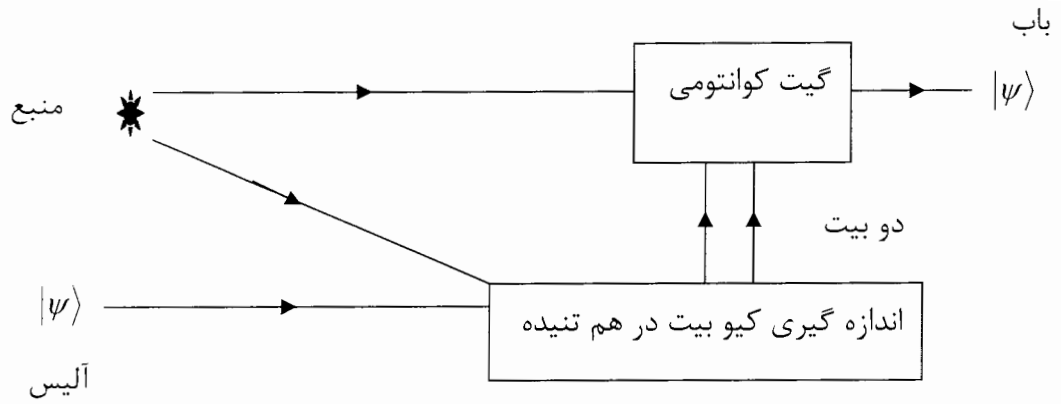
$$01 \rightarrow |\psi_{01}\rangle = \alpha|1\rangle + \beta|0\rangle \quad (۳۵-۲)$$

$$10 \rightarrow |\psi_{10}\rangle = \alpha|0\rangle - \beta|1\rangle \quad (۳۶-۲)$$

$$11 \rightarrow |\psi_{11}\rangle = \alpha|1\rangle - \beta|0\rangle \quad (۳۷-۲)$$

اگر حالا آلیس نتیجه خود را با باب در ارتباط بگذارد (بر روی یک کانال کلاسیکی مثل تلفن یا ایمیل یا یک کانال کوانتومی مانند کد گذاری بسیار انبوه) باب از چگونگی تغییر شکل و تبدیل حالت کیوبیت خود به $|\psi\rangle$ مطلع خواهد شد. اگر نتیجه مورد نظر 00 باشد باب هیچ کاری را انجام نخواهد داد، زیرا کیوبیت وی هم اکنون در حالت $|\psi\rangle$ به سر می برد. برای نتایج احتمالی دیگر باب می بایست یک ترکیب مناسب از گیت های Z , X به کار ببرد. اگر نتیجه اندازه گیری $m_1 m_2$ باشد، بنابراین نتیجه کلی به این صورت خواهد بود[۴،۹،۱۰]:

$$Z^{m_1} X^{m_2} |\psi_{m_1 m_2}\rangle = |\psi\rangle \quad (۳۸-۲)$$



شکل(۲- ۷): پس از اعلام دو بیت کلاسیکی توسط آلیس باب با انتخاب گیت مناسب کیو بیت $|\psi\rangle$ را دریافت خواهد نمود.

مثلاً: اگر آلیس کیو بیت $|\psi_{01}\rangle$در اندازه گیری اش بدست آورد با فرستادن پیغام به باب (دو بیت کلاسیکی) باب را مطلع خواهد نمود که کیو بیتی که به سوی او فرستاده شده است $|\psi_{01}\rangle = \alpha|1\rangle + \beta|0\rangle$می باشد، باب با بکار بردن گیت مناسب یعنی گیتNOT(X) کیو بیت مورد نظر را دریافت خواهد نمود.

$$X|\psi_{01}\rangle = X\alpha|1\rangle + X\beta|0\rangle = \alpha X|1\rangle + \beta X|0\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (۳۹-۲)$$

این همانند جادویی در مکانیک کوانتوم به نظر می رسد. به هر حال این مسئله عملاً در آزمایشگاه به وسیله ارسال یک اشعه یا نور فوتون از یک اتاق به اتاق دیگر به دست آورده شده است.

نکته ای که دراینجاست:

- فرآیند ارسال از راه دور از تئوری نوکلونیگ را نقض نمی کند. یعنی کپی یک حالت ناشناخته دلخواه صورت نمی گیرد، بلکه حالت اصلی $|\psi\rangle$ در روند جریان تغییر شکل جزئی پیدا می کند.
- فرآیند ارسال از راه دور تئوری نسبیت خاص را نقض نمی کند، براین اساس اطلاعات عملی از نظر فیزیکی ناگذیر با سرعت کمتر از نور، ارتباط برقرار می کنند.

۲-۷- نتیجه گیری

درهم تنیدگی یکی از منابع ایجاد ارتباطات کوانتومی محرمانه است. این پدیده می گوید که اگر دو ذره با هم در هم تنیده شوند، اگر این دو ذره حتی میلیون ها کیلومتر از هم دور شوند و روی یکی از آن دو عمل اندازه گیری انجام شود در همان لحظه اطلاعات ذره دوم را می توان بدست آورد. روی هم تحت تأثیر قرار می گیرند، یعنی بالاتر از سرعت نور و به طور آنی! در هم تنیدگی از جهتی شبیه به شکستن یک سکه به دو تکه است که با مشاهده یک نصفه از آن می توان به شکل و مشخصات تکه دیگر پی برد، زیرا دو تکه به صورت مشترک اطلاعات سکه کامل را در اختیار دارند؛ به عبارت دیگر مشاهده یک تکه، مشخصات تکه دوم را کاملاً روشن می سازد حتی اگر کیلومترها از هم دور باشند. انیشتین این موضوع را عملکرد شبح وار در فواصل زیاد نامید که شبیه به ارتباط دو تکه در هم تنیده توسط سیم های نامرئی است که ما اطلاعی از آنها نداریم، اما برای محاسبات کوانتومی یک اصل کلی بشمار می آید. دانشمندانی همچون انیشتین، پودلوسکی و روزن که نظریه EPR را مطرح نمودند.

پدیده شگفت انگیز در هم تنیدگی در تئوری مکانیک کوانتومی تحولی عظیم در تئوری کوانتومی و به طبع آن در رایانه های کوانتومی ایجاد نمود؛علاوه بر کاربرد های اشاره شده در این فصل پدیده در هم تنیدگی کاربرد بسیار جالبی در رایانه های کوانتومی یعنی توزیع کلید کوانتومی محرمانه دارد که اهمیت آن بر هیچ کس پوشیده نیست.از نتایج بسیار مهم پدیده در هم تنیدگی آن است که موضعیت را نقض می کند و ثابت نمود که طبیعت تئوری مکانیک کوانتومی نا موضعی است.

فصل ۳:

بررسی تئوری نسبیت در نظریه مکانیک کوانتومی

- مقدمه
- علامت دهی و ناعلامت دهی
- ماشین حالت خوان
- سرعت بیشتر از نور
- نتیجه گیری

۳-۱- مقدمه

از اوایل قرن بیستم، دو نظریه بزرگ، نسبیت و مکانیک کوانتومی، برای پاسخ گویی به مشکلات(قوانین نیوتن) و مسایلی که تا آن زمان گریبان گیر مکانیک کلاسیکی بود و توجیهی برای آن وجودنداشت، پا به عرصه وجود نهادند؛ و سیر تکاملی خود را طی کردند. نظریه نسبیت وکوانتوم هر دودر توجیه پدیده های حوزه خود از توانایی خوبی برخوردار بودند، نخست نسبیت خاص در سال ۱۹۰۵ تنها در محدوده دستگاههای لخت بکار گرفته شد، و در سال ۱۹۱۵ تحت عنوان نسبیت عام، در دستگاههای شتاب دار گسترش یافت، و مکانیک کوانتومی قدیم در سال ۱۹۰۰ با طرح کوانتومی در دهه ۱۹۲۰ سیر تکاملی خود را پیمود. همواره این سؤال مطرح بود که آیا این دو نظریه بزرگ را می توان با هم ترکیب کرد؟ دیراک توانست نسبیت خاص و مکانیک کوانتومی را به صورت مکانیک کوانتوم نسبیتی با هم ادغام کند[۱۱].

نسبیت خاص، دارای یک محدودیت اساسی بود؛ این محدودیت ناشی از آن بود که رویدادهای فیزیکی را در دستگاههای لخت مورد بررسی قرار می داد، در حالی که در جهان واقعی دستگاهها شتاب دار هستند. انیشتین در سال ۱۹۱۵ نسبیت عام را ارائه کرد، و نسبیت خاص را به عنوان حالت خاصی از نسبیت عام مطرح نمود.

مکانیک کوانتومی ساختار ریز و کوانتومی کمیت ها و واکنش های متقابل آنها را مورد بررسی قرار می دهد، به عبارت دیگر نگرش مکانیک کوانتومی بر مبنای کوانتومی (ناپیوستگی) شکل گرفته است. در این زمینه تا جایی پیش رفته که حتی اندازه حرکت و برخی دیگر از کمیتها را کوانتومی معرفی می کند. این نتایج بر مبنای یک سری شواهد تجربی مطرح شده و قابل پذیرش است. علاوه بر آن تلاش زیادی انجام می شود تا پدیده های بزرگ جهان را با قوانین شناخته شده در مکانیک کوانتومی توجیه کند، حال به نسبیت توجه کنید که فضا - زمان را پیوسته در نظر می گیرد؛ بنابراین نسبیت با مکانیک کوانتومی ناسازگار است. تلاش های زیادی انجام شده تا به طریقی یک هماهنگی منطقی و قابل قبول بین نسبیت و مکانیک کوانتومی ایجاد شود، در این

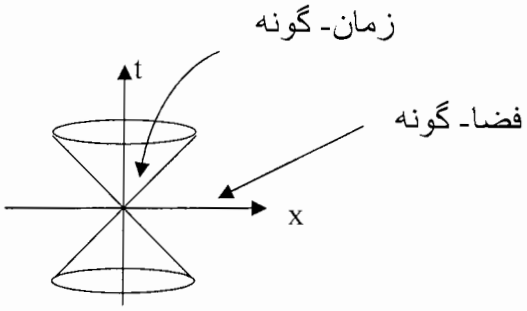
مورد کارهای دیراک شایان توجه است که مکانیک کوانتومی نسبیتی را پایه گـذاری کـرد و آن را توسعه داد.

تئوری کوانتومی که به مفهوم تکامل و تغییر تدریجی حالات کوانتومی محض است نیاز به منظـور کردن یا مجاز دانستن علامت دهی مافوق نور[1] را ندارد. اگر تئوری کوانتومی نسبیت را مجاز ندانـد در این صورت تئوری نسبیت را مختل می کند؛ یعنی علامت دهـی مـافوق نـور بـا اصـل نـسبیت سازگار نیست. تئوری کوانتومی هنگامی که اصـل نـسبیت و اصـل علیـت مینکوسـکی را در نظـر می گیرد سیگنال دهی مافوق نور را مجاز نمی داند،بنابراین در فصل ابتدا بـه صـورت اجمـالی بـه بررسی تئوری نسبیت می پردازیم و در تئوری کوانتومی اعتبار تئوری نسبیت یعنی علامت دهی[2] و ناعلامت دهی را در تئوری کوانتومی را بررسی می کنیم و ماشینی را معرفی خـواهیم نمـود کـه درآن دو تئوری کوانتومی و نسبیت با هم سازگارند و سرانجام نمونه کوانتومی را مطرح می نماییم که در آن علامت دهی با سرعت بیشتر از نور امکان پذیر نیست.

[1] No Signaling
[2] Signaling

۳-۲- بررسی رابطه علیت و نسبیت

رویدادهایی که در خارج از مخروط نوری قرار دارند (فضا گونه) نمی توانند بر رویدادهای واقع بر رأس مخروط مؤثر باشند؛ زیرا در این صورت علامت دهی نور باید با سرعت بیش از C حرکت کند. در این صورت، رویداد، کاملاً غیرفیزیکی است و ترتیب زمانی مطلق برای رویدادها در این ناحیه وجود ندارد؛ البته این نکته به این معنا نیست که علیت نقض می شود، بلکه اصلاً نمی توان علیت را در این ناحیه آزمایش نمود. در ضمن، تمام رویدادهایی که در داخل مخروط نوری هستند می توانند به طور علّی به یک رویداد در رأس مخروط مربوط شود.



۳-۳- علامت دهی و نا علامت دهی

هنگامی که حالت کوانتومی درهم تنیده دو ذره مفروض باشد و دو ذره از لحاظ فضایی از یکدیگر جدا باشند و اندازه گیری روی یکی از دو ذره انجام گیرد حالت کوانتومی ذرات در اثر برهم کنش با عملگر اندازه گیری کننده (دستگاه اندازه گیری) به طور آنی به حالت های دیگر فروپاشی می شود ممکن است دراین مورد تئوری کوانتومی، تئوری نسبیت را مجاز داند یعنی علامت دهی از ذره اندازه گیری شده به ذره دیگر با سرعت بیشتر از نور صورت گرفته است؛ این بدان معنا است که تئوری کوانتومی نیاز به مجاز دانستن تئوری نسبیت ندارد ولی اگر در تئوری کوانتومی تئوری نسبیت را مجاز بدانیم فروپاشی حالت کوانتومی دراثر اندازه گیری با آن که برای ذره اندازه گیری شده آناً صورت می گیرد ولی علامت دهی دو ذره به یکدیگر با حداکثر با سرعت نور امکان پذیر است که این مفهومی از نا علامت دهی است.

بـرای سـاده سـازی در نمادگـذاری فـرض مـی کنـیم ذرات در مکانهـای $x_1, x_2, \ldots, x_n$ در دستگاه مختصات لخت (x,t) قرار داشته باشند. تابع موج فضایی ذرات در سراسـر بحـث دارای گستردگی ناچیزی باشند. تابع موج این ذرات را که در هم تنیده می باشند در لحظه $t = 0$ بصورت زیر تعریف می کنیم:

$$|\psi(0)\rangle = \sum_{i_1 \cdots i_n} a_{i_1 \cdots i_n} |i_1\rangle_1 \cdots |i_n\rangle_n \qquad (۱-۳)$$

همچنین فرض می کنیم که ذرات با یکدیگر برهم کنش نداشته باشند، و نیز داریم:

$$|\psi(t)\rangle = |\psi(0)\rangle \quad \text{for} \quad -T < t < t_1 \qquad (۲-۳)$$

که در آن :

$$T \geq \max_{ij} \| \underline{x}_i - \underline{x}_j \| \qquad (۳-۳)$$

در لحظه $t = 0$ حالت ذره ۱ به صورت زیر است:

$$\rho_1(0) = tr_{2\cdots n}(|\psi(0)\rangle\langle\psi(0)|) \qquad (۴-۳)$$

فرض می کنیم یک اندازه گیری روی ذره دوم در لحظه $t_1 > 0$ صورت می گیـرد. اگـر ذره دوم در حالت $|j\rangle_2$ باشد، عملگر p^j را به صورت $p^j = |j\rangle_{22}\langle j|$ تعریف می کنیم. وقتی که این عملگر که روی حالت $|\psi(0)\rangle$ اثر می کند به صورت $p_2^j = 1 \otimes p_j \otimes 1 \cdots \otimes 1$ در می آید . در این صورت خواهیم داشت:

$$|\psi(t_1)\rangle = p_2^j |\psi(0)\rangle \qquad (۵-۳)$$

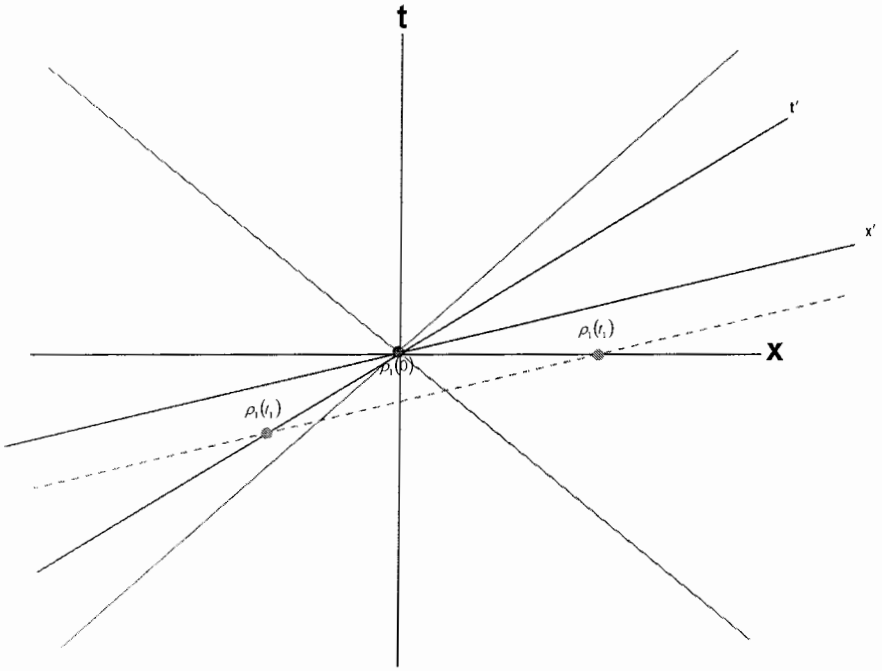
بنابراین حالت ذره ۱ به صورت زیر در می آید:

$$\rho_1(t_1) = tr_{2\cdots n}(|\psi(t_1)\rangle\langle\psi(t_1)|) \qquad (۶-۳)$$

به طور کلی $\rho_1(0)$ ، $\rho_1(t_1)$ متفاوت از هم هستند، با توجه به اندازه کوانتومی و ناموضعیـت حالت های در هم تنیده، هنگامی که ذره دوم اندازه گیری اش را انجام می دهد به طـور آنـی (بـا سرعت بینهایـت $\rho_1(0)$ به $\rho_1(t_1)$ تبدیل می شود.) زیرا حالت $|\psi_{(t=0)}\rangle$ در اثـر انـدازه گیـری بـه حالت $|\psi_{(t_i)}\rangle$ به طور آنی فرو پاشی می شود.

از این رو نمی توانیم هم اصول نسبیتی را حفظ کنیم و هم حالت ذره (۱) را به صورتی که در محاسبات تعریف شد به عنوان یک نمایش از واقعیت عینی در نظر بگیریم. از آن گذشته اگر فرض کنیم یک دستگاه فرضی مقدار حالت را به همان صورت که تعریف شده است بازخوانی کند در این حالت باید فرض کنیم که دستگاه نسبت به یک چارچوب مرجع کار می کند، بنابراین علامت دهی آنی وجود دارد صرف نظر از آنکه فاصله آنها چقدر باشد.

طبق نظریه EPR که در فصل چهارم به آن اشاره می شود،حالت فیزیکی ذره (۱) واقعاً بعد از اندازه گیری با $\rho_1(t_1)$ تعریف می شود نه $\rho_1(t=0)$ یعنی احتمال های خروجی مربوط به اندازه گیری روی ذره (۱) از $\rho_1(t_1)$ بدست می آید. بنابراین $\rho_1(t_1)$ بهترین توصیف فیزیکی قابل دسترس مربوط به حالت ذره (۱) است.



شکل (۳-۱): سازگاری تئوری کوانتومی با تئوری نسبیت توصیف حالت کوانتومی ذره (۱) در زمان های متفاوت

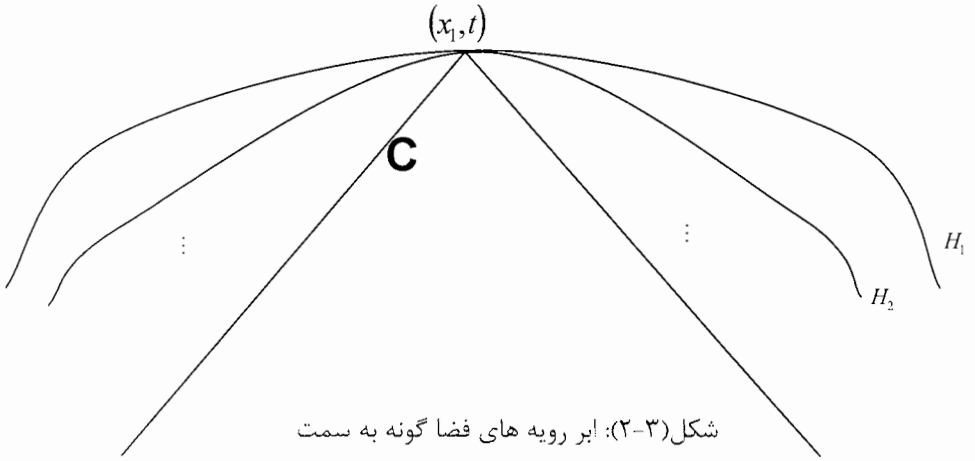
حال طبق اصول نسبیتی حالت ذره (۱) قبل از زمان t_1 هم $\rho_1(t_1)$ می تواند باشدشکل(۳-۱).

این مسئله ما را به متغیرهای نهانی موضعی که در دیدگاه دیوید بوهمی مطرح می شود هدایت می کند[۹]. نظریه بل با توجه به طرح نامساوی اش با فرض اینگونه متغیرها این خط فکری را رد

می کند[فصل چهارم،۱۰]. متغیرهای نهانی موضعی توانایی آن را ندارند که حالت در هم تنیده را دوباره ایجاد کنند و در این صورت علامت دهی مافوق نور نمی تواند وجود داشته باشد.

برای حل این مشکل می توان به شکل زیر عمل کرد:

چون سرعت نور در هر چارچوب مرجع لخت ثابت است بنابراین رویدادهایی که روی مخروط نوری هستند، در تمام چارچوب های مرجع روی همین مخروط نوری می باشند و تغییر نمی کنند. با در نظر گرفتن ذره (۱) در زمان t مربوط به ناحیه گذشته مطابق شکل زیر است.



شکل(۳-۲): ابر رویه های فضا گونه به سمت مخروط نوری زمان گذشته میل می کنند.

H_n که ابر رویه های فضا گونه ذره هستند که (x_1,t) از نقطه می گذرند که $|\psi^n\rangle$ بردار حالت سیستم روی H_n می باشد. در نتیجه:

$$\rho^n = tr_{2,\dots,n}(|\psi^n\rangle\langle\psi^n| \qquad (۳-۷)$$

بالاخره حالت موضعی ذره (۱) در زمان t به صورت زیر تعریف می شود.

$$\rho_1^{loc} = \lim_{n\to\infty} \rho^n \qquad (۳-۸)$$

وقتی که H_nها به سمت C میل می کند یعنی همه روی رویه C قرار می گیرند چون سرعت روی آن ثابت است و نمی تواند بیشتر از سرعت نور باشد بنابراین علامت دهی مافوق نور نداریم. در نتیجه بهترین توصیف ممکن برای حالت قابل دسترس که در مکان (x_1,t)موضعیت پیدا کرده است $\rho_1^{loc}(x_1,t)$ می باشد[۱۴].

۳-۴- ماشین حالت خوان [1]

می خواهیم تئوری بسازیم که در آن ارتباط با سرعت بیشتر از سرعت نور امکانپذیر نیست و با تئوری کوانتومی هم سازگار نمی باشد.

سالهای زیادی روی ماشینی کار شده است که بتواند حالتهای کوانتومی را بخواند. حالت خوان یک ماشین فرضی است و دراینجا به عنوان یک ناظر هم نظر گرفته می شود که نسبیت خاص ونسبیت عام را قویاً قبول دارد اما نسبت به تئوری کوانتومی شکاک می باشد.

به عنوان آزمایش یک حالت کوانتومی رادر آزمایشگاه ایجاد می کنیم:

$$|\psi\rangle = a|\uparrow_z\rangle + b|\downarrow_z\rangle \qquad (۹-۳)$$

aعددحقیقی مثبت و b عدد مختلط است . این حالت را به ورودی ماشین حالت خوان می دهیم خروجی ماشین برابر است:

$$a|\uparrow_z\rangle + b|\downarrow_z\rangle \qquad (۱۰-۳)$$

در اینجا احتمال اینکه خروجی $|\psi\rangle$ ، p_ψ باشد یک است.

توجه باید داشته باشیم که شخص اول ماشین حالت خوان و شخص دوم ما هستیم .

حال فرض می کنیم شخص سومی که در محل دیگر اقامت دارد نیز در این آزمایش شرکت می کند، اگر بعدازظهر امروز یک جفت ذره را در حالت منفرد ایجاد کند:

$$\frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle_A|\downarrow_z\rangle_B - |\downarrow_z\rangle_A|\uparrow_z\rangle_B\right) \qquad (۱۱-۳)$$

ذره دوم را برای ما به عنوان شخص دوم بفرستد ، فردا ظهر ساعت ۱۲:۰۰یک اندازه گیری راروی پایه های انتخابی اش برای ذره اول انجام می دهد. اگر نتیجه را بلافاصله با بی سیم گزارش کند علامت رادیویی در ساعت ۱:۰۰بعدازظهر به ما خواهد رسید، اما از او می خواهیم که علامت رادیویی را ساعت ۱۲:۳۰ارسال کند . بعد، حالت در هم تنیده را به ماشین ورودی می دهیم خروجی زیر را نشان می دهد:

$$\frac{1}{2}\left(|\uparrow_z\rangle_B\langle\uparrow_z| + |\downarrow_z\rangle_B\langle\downarrow_z|\right) \qquad (۱۲-۳)$$

---

[1] Zweisteine

دوباره این عمل را درساعت ۱۲:۰۱تکرار می کنیم خروجی بدست آمده باز هم به همان صورت قبلی است.

حالت در یک حالت محض است نه در حالت آمیخته این موضوع رابا شخص سوم در میان می گذاریم ، او می گوید هنوز آزمایش را ادامه بده.بنابراین ساعت ۱۲:۵۹آزمایش را دوباره تکرار می کنیم و دوباره همان حالت محض بدست می آید.ساعت ۱:۰۱دوباره آزمایش را تکرار می کنیم اما این بار می بینیم که در کمال تعجب خروجی به صورت زیر در می آید:

$$c\left|\uparrow_z\right\rangle + d\left|\downarrow_z\right\rangle \qquad (۱۳-۳)$$

وقتی پیام رادیویی شخص سوم آزمایشگرساعت ۱:۳۰می رسد، متوجه می شویم که او در پایه های زیر اندازه گیری هایش را انجام داده است:

$$\begin{matrix} c\left|\uparrow_z\right\rangle + d\left|\downarrow_z\right\rangle \\ \bar{d}\left|\uparrow_z\right\rangle - \bar{c}\left|\downarrow_z\right\rangle \end{matrix} \qquad (۱۴-۳)$$

و دومین حالت را بدست آورده است. یعنی :

$$\bar{d}\left|\uparrow_z\right\rangle - \bar{c}\left|\downarrow_z\right\rangle \qquad (۱۵-۳)$$

چگونه می توان حالت محض خروجی دستگاه را توصیف کرد؟؟؟

ماشین حالت خوان ، برای حالتهای محض به عنوان ماشین خروجی خوان حالت کوانتومی واقعی بکار می رود.وقتی هم با یک قسمت از سیستم در هم تنیده ظاهر می شود ، به عنوان ماشینی برای تشخیص اینکه سیستم در هم تنیده است یا خیر بکار می رود. به هر حال ماشین از فاصله فضایی بین دستگاههای اندازه گیری بی اطلاع است[۱۴].

۳-۵- علامت دهی با سرعت بیشتر از نور [1]

حالت محض دو طرفه در هم تنیده $|\psi\rangle_{AB}$ با تفکیک اشمیت زیر در نظر می گیریم:

$$|\psi\rangle_{AB}=\frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle_A|\uparrow_z\rangle_B+|\downarrow_z\rangle_A|\downarrow_z\rangle_B\right) \qquad (۱۶-۳)$$

چگالی ماتریس حالت (سیستم)A را به صورت زیر تعریف می شود:

$$\rho_A=\frac{1}{2}\left(|\uparrow_z\rangle_{A\,A}\langle\uparrow_z|+|\downarrow_z\rangle_{A\,A}\langle\downarrow_z|\right) \qquad (۱۷-۳)$$

بنابراین آنسامبل ρ_A که درآن احتمال $|\uparrow_z\rangle_A$ یا $|\downarrow_z\rangle_A$ هرکدام $\frac{1}{2}$ باشد را می توان با اندازه گیری سیستم B فراهم آورد .

سیستم B رادر پایه های $\{|\uparrow_z\rangle_B,|\downarrow_z\rangle_B\}$ اندازه گیری می کنیم:

اگر نتیجه اندازه گیری $|\uparrow_z\rangle_B$ باشد، برای سیستم A با توجه به حالت کوانتومی (کیوبیت) $|\psi\rangle_{AB}$، $|\uparrow_z\rangle_A$ بدست می آید.

اگر نتیجه اندازه گیری $|\downarrow_z\rangle_A$ باشد سیستم A در حالت $|\downarrow_z\rangle_B$ خواهد بود.

هر بردار یکانی n (با سه مولفه) ، $|\psi\rangle_{AB}$ یک تفکیک اشمیت به صورت زیر خواهد داشت :

$$|\psi\rangle_{AB}=1/\sqrt{2}\left(|\uparrow_n\rangle_A|\uparrow_n\rangle_B+|\downarrow_n\rangle_A|\downarrow_n\rangle_B\right) \qquad (۱۸-۳)$$

مشاهده می شود که با اندازه گیری سیستم B دریک پایه مناسب ، می توانیم هر توصیفی از ρ_A را به عنوان یک آنسامبل از دو حالت محض بدست آورد. بنابراین ممکن است این تصور پیش آید که در نظریه کوانتومی ارسال اطلاعات با سرعتی بیش از سرعت نور امکانپذیر است.

فرض می کنیم آلیس و باب در فاصله ای فضا گونه باشند. باب می خواهد پیغامی را به آلیس برساند . وقتی باب اندازه گیری اش را انجام می دهد پایه های مربوط به σ_z , σ_x را برای تمام اسپین هایش انتخاب می کند.

---

[1] Faster than light

بنابراین حالت اسپن آلیس در پایه های $\{|\downarrow_z\rangle_A, |\uparrow_z\rangle_A\}$ یا $\{|\downarrow_x\rangle_A, |\uparrow_x\rangle_A\}$ پیدا خواهد شد.

بعد ازاینکه باب خبر می دهد که اندازه گیری اش را انجام داده است ، آلیس فوراً اسپین اش را اندازه گیری می کند تا ببیند در کدام یک از این آنسامبل ها قراردارد . در این طرح نقطه منفی دیده می شود. اگرچه این دو روش مطمئناً متفاوت هستند ، ولی ماتریس چگالی مربوط به هر دو آنسامبل ها دقیقاً یکی است . بنابراین روشی وجود ندارد که آلیس دو تا آنسامبل را از هم جدا کند و هیچ راهی هم وجود ندارد که آلیس بفهمد عمل باب چه بوده است. بنابراین پیغام غیر قابل خواندن است. راه حل چیست؟

فرض کنیم باب اندازه گیری اش را در یکی از دو حالت زیر انجام دهد :

۱- اندازه گیری تمام اسپین هایش را در امتداد محور Z ها انجام می دهد.

۲- اندازه گیری تمام اسپین هایش را در امتداد محور X ها انجام می دهد.

باب از طریق تلفن یا بی سیم به آلیس نیتجه اندازه گیریش رااطلاع می دهد.

(به عنوان مثال اولی را بالا و دومی را پایین بدست آورده است و غیره). اما درمورد اینکه کدام دو روش (۱یا۲) را انتخاب کرده است چیزی نمی گوید. حا ل آلیس یکی از دوروش ۱یا ۲ رابرای اندازه گیری روی اسپین هایش انتخاب می کند.

اگر هم آلیس و هم باب هردو در امتداد یک محوراندازه گیری راانجام دهند، آلیس هریک ازنتیجه های اندازه گیری اش را موافق با آنچه که باب بدست آورده، بدست می آورد.اما اگر آلیس و باب اندازه گیری هایشان در امتداد محورهایی با جهت های مختلف باشد،آلیس نمی تواند بین نتایج اش و آنچه که باب بدست آورده ،رابطه ای پیدا کند. حدود نیمی از اندازه گیریهایش موافق با اندازه گیریهای باب و نیمی دیگر مخالف با آن است . اگر باب قول بدهد که یکی از دوروش (۱یا۲) را انجام بدهد و فرض می کنیم هیچ نوع خطایی نباشد.

آلیس با همان سرعتی نتیجه اندازه گیری را پیدا می کند با همان سرعت هم متوجه خواهد شد که باب، σ_x یا σ_z را اندازه گیری کرده است.

بنا براین آلیس راهی برای تشخیص روشی که باب به کاربرده است، خواهد داشت اما در این حالت سرعت انتقال اطلاعات کمتر یا حداکثر مساوی سرعت نور است. به این دلیل که آلیس مجبور است از طریق تماس تلفنی یا بی سیم ... از باب نتیجه اندازه گیری را بگیرد.
بنابراین ارتباطی با سرعت بیش از سرعت نور وجود ندارد[۲].

۳-۶- نتیجه گیری

در چارچوب نظریه کوانتومی موجود در صورتی که فیزیک نسبیتی را در نظر نگیریم علامت دهی مافوق سرعت نور وجود دارد. ولی در صورتی که بخواهیم اصول فیزیک نسبیتی را ارضاء کنیم علامت دهی مافوق سرعت نور امکان پذیر نیست؛ بنابراین اعتبار تئوری نسبیتی نظریه مکانیک کوانتومی را مُلزم می دارد که نا علامت دهی را بپذیرد و آن خدشه ای در تئوری کوانتومی وارد نمی کند. نا علامت دهی بیان می دارد که رویدادهای دو سیستم فضا گونه مستقل از هم و حداکثر سرعت بین دو رویداد برابر سرعت نور است، این به معنای آن نیست که ناموضعیت در تئوری کوانتومی نقض شود بلکه موضعیت چیزی جدا از ناعلامت دهی است که به طور خلاصه موضعیت احتمال یا نتیجه احتمال اندازه گیری دو رویداد فضاگونه را مستقل از یکدیگر می داند که در فصل چهارم به مفصل به آن می پردازیم.

فصل۴:

قضیه EPR و نا مساوی بِل

- مقدمه
- موجبیت
- موضعیت
- متغیر های پنهانی
- قضیه EPR
- قضیه بِل
- تعمیم های دیگر نامساوی بِل
- اثبات نا مساوی بِل و نقض آن
- نتیجه گیری

۴-۱- مقدمه

پدیده در هم تنیده ابتـدا توسـط انیـشتین ، روزن و پودولـسکی بـه صـورت یـک پـارادوکس (باطلنما) در رد نظریه کوانتومی مطرح شد آنها نظریه EPR را مطرح نمودند و اعتقاد داشتند نظریه کوانتومی ناقص است و توصیف واقعیت در نظریه کوانتومی با استفاده از تابع موج کامل نیست و در صدد توصیف واقعیت در نظریه کوانتومی بودند و آنها همواره در پی نقض اصل عدم قطعیت تـلاش می نمودند[۳۵].

قضیه EPR در سال ۱۹۳۵ ارائه شد و شرط لازم و کافی را بـرای کامـل بـودن یـک تئـوری و تعریف عنصری از واقعیت فیزیک را مورد بررسی قرار داد. قضیه بـل درسـال ۱۹۶۴ باعـث نزدیـک شدن موضوع به مرحله آزمایش و بررسی بیشتر گردید. بِل بـا اسـتفاده از فـرض هـای : موضـعیت، موجبیت، متغیرهای نهانی بدست آورد. و تعارض بین ایـن نامـساوی بـا پـیش بینـی هـای آمـاری مکانیک کوانتومی را نشان داد؛ سرانجام نقض این نامساوی در پـیش بینـی هـای تجربـی بـه نفـع مکانیک کوانتومی تمام شد[۳۶،۹].

کلوزر و هورن... در سال ۱۹۷۴، هانری استاپ در سال ۱۹۸۸ تعمیم ها و مدل های دیگـر از قـضیه بل را مطرح کردند که ظاهراً بدون فرض هایی نظیر موجبیت و متغیرهای نهانی بـود. تعـارض بـین نتایج آماری مکانیک کوانتومی و این مدل های تعمیم یافته را نشان دادند...

نامساوی بل در آزمایش های مربوط به فوتون ها و یون ها و نیز در فیزیک انرژی بالا با مزون هـا و ... نقض شده اند.

۴-۲- موجبیت

مکانیک کوانتومی نظریه ای نامتعین است. یعنی اندازه گیریهای فیزیکی وجود دارد که تا قبل از انجام آنها نتایجشان از روی حالت دستگاه (سیستم) به طور قطعی معین نمی شود. دست کم تا حد امکان مشاهده آن حالت قبل از انجام اندازه گیری ممکن نیست. اگر درست قبل از اندازه گیری تابع موج دستگاه، ویژه تابعی از عملگری که مشاهده پذیریش را می خواهیم اندازه گیری می کنیم نباشد آنگاه نتیجهٔ اندازه گیری قطعاً قابل پیش گویی نیست و تنها می توان احتمال نتایج مختلف را تعیین نمود.

برای مثال آزمایش اشترن گرلاخ را به یاد آورید. اگر باریکه ای از ذرات با اسپین $\frac{1}{2}$ از دستگاهی که سمتگیری آن در راستای z است عبور کند، باریکه در دو سمتگیری ممکن، برای S_z جدا می شود. اگر آن باریکه که حاوی ذرات با اسپین $S_z = \frac{\hbar}{2}$ است از دستگاهی که مؤلفه اسپین را در راستای دیگر اندازه می گیرد عبور کند باز هم باریکه در دو مؤلفه $\frac{\hbar}{2}$,$-\frac{\hbar}{2}$ جدا می شود. احتمال این دو نتیجه را می توان محاسبه کرد امّا نمی توان پیشگویی کرد آیا ذره ای اسپین بالا خواهد داشت یا اسپین پایین.

نامتعین بودن مکانیک کوانتومی با موجبیت مکانیک کلاسیکی در تضاد است. زیرا در مکانیک کلاسیکی تحول هر دستگاه با حالت اولیه و نیرو های وارد بر آن دقیقاً معین می شود. حتی حالت نهایی یک آزمایش کاتوره ای خاص نظیر پرتاب سکه را می توان تعیین نمود. در صورتی که موقعیت- سرعت- تکانه زاویه ای اولیه سکه و همچنین نیروی گرانی و اصطکاکی را که روی آن عمل می کند بدانیم. با این حال کاتوره ای بودن مکانیک کوانتومی خصلتی کاملاً متفاوت دارد؛ نتایج اندازه گیری پیامد روشنی از حالت قبلی دستگاه نیست. این واقعیت که ذرات اسپین $\frac{1}{2}$ ویژه حالتهای S_z هستند به طور کامل بخش منتسب به اسپین توابع موج را تعیین می کنند و این ذرات یکسانند با این وجود هرگاه مؤلفهٔ دیگر از اسپین اندازه گیری شود همین ذرات ممکن است به صورت متفاوت عمل کنند. برای مثال ذره ای در ویژه حالت S_z باید مقدار ثابتی از S_x داشته باشد، حتی اگر نتوان این مقدار را اندازه گرفت نظریه هایی که بر این چنین فرض هایی استوار اند نظریه متغیر پنهان نامیده می شود[۹].

۴-۳- موضعیت[1]

مسئله دوم در مکانیک کوانتومی نظریه موضعیت می باشد هنگامی که در مورد ذرات صحبت می کنیم فرض ما بر این است که آن ها نقطه گونه اند و یا حداقل به قدر کافی کوچکتر از ابعاد دستگاه تحت بررسی هستند پیامد غیرموضعی بودن درمکانیک کوانتومی ، رفتار ذراتی است که در فضا از هم جدا هستند اما خواص آنها به نوعی به هم وابسته است. دستگاهی از این نوع در ابتدا به وسیله انیشتن،پودولسکی و روزن مورد بحث قرار گرفت.

برای روشن شدن این بحث آزمایش ذهنی بوهم را مورد بررسی قرار می دهیم:

یک جفت ذره، هر یک با اسپین $\frac{1}{2}$ و اسپین کل صفر که هر یک تکانه زاویه ای مداری صفر دارند در نظر می گیریم جفت ذراتی که این خواص را دارند هنگامی که از هم دور می شوند.مؤلفهٔ مثلاً Z اسپین ذره اول (S_{1z}) و سپس همان مؤلفهٔ از ذره دوم (S_{2z}) می گیرند از آنجا که اسپین کل صفر است این مؤلفه باید مختلف العلامه باشند. $S_{1z}=\frac{1}{2}, S_{2z}=-\frac{1}{2}$. پس اندازه گیری دوم غیر ضروری است زیرا S_{2z} را می توان از مقدار S_{1z} بدست آورد. پس از اندازه گیری S_{1z} ، ذره دوم در ویژه حالتی از S_{2z} قرار می گیرد این موضوع به معنی تعبیر در احتمال اندازه گیری مؤلفهٔ دیگری از اسپین ذره دوم نیز هست.

بنابراین نتیجه اندازه گیری اسپین ذره دوم متأثر از اندازه گیری اسپین ذره اول است. البته ذرات باید دور از هم و بدون بر هم کنش باشند.طبق مکانیک کوانتومی، دو ذره در حالتی از این نوع مستقل از یکدیگرند بنابراین اگر آنها را مستقل از هم در نظر بگیریم باید در نظریه ای از نوع متغیر پنهان در این مورد بنا نماییم[۲].

کوشش هایی برای توسعهٔ نظریه ای که قادر باشد با حفظ موجبیت و موضعیت تمام نتایجی از مکانیک کوانتومی را که به تجربه نیز اثبات شده است به دست آورد صورت گرفته است اخیراً معلوم شده است که چنین نظریه ای امکان ناپذیر است.

حال تعریف دقیقتری از موضعیت ارائه می دهیم:

---

[1] Locality

۴-۳-۱- موضعیت

نتیجه و یا احتمال یک نتیجه اندازه گیری که روی قسمتی از یک سیستم مرکب باحالت $|\psi\rangle$ (سیستم۱ + سیستم۲) انجام می شود مستقل از جنبه های مولفه های قسمت های دیگر است که آزمایشگر برای اندازه گیری انتخاب می کند. این به هیچ وجه به این معنی نیست که نتوان با بررسی سیستم ۱ اطلاعاتی در مورد سیستم ۲بدست آورد.

حالت $|\psi\rangle$ شامل اطلاعات مشترک مربوط به هر دو سیستم است و اندازه گیری روی یکی از این سیستم ها بخشی از این اطلاعات را آشکار می سازد. همچنین اگر یک اندازه گیری روی یک قسمت از سیستم مرکب انجام شود باعث اغتشاش موضعی آن قسمت می گردد و این با موضعیت مغایرتی ندارد[۳۵].

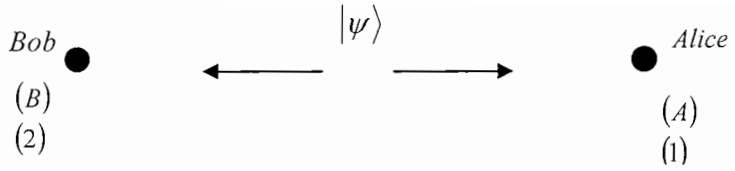
۴-۳-۲- بررسی ناموضعیت[1] با استفاده از حالت های در هم تنیده دو طرفه

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle_A|\downarrow_z\rangle_B + |\downarrow_z\rangle_A|\uparrow_z\rangle_B\right) \qquad (۱-۴)$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_x\rangle_A|\downarrow_x\rangle_B + |\downarrow_x\rangle_A|\uparrow_x\rangle_B\right) \qquad (۲-۴)$$

حالت درهم تنیده دو طرفه $|\psi\rangle$ که حالت های اسپینی در راستای محور X,Z می باشد. آلیس(A) و (B) باب به عنوان دو ناظر که یک سری اندازه گیری اسپینی در راستای محور X,Z روی $|\psi\rangle$ انجام می دهند. هر کدام ویژگیهای ذره خود را اندازه گیری می کنند. فرض بر اینکه سیستم شامل دو ذره (۱) و(۲) مربوط به آلیس و باب در فاصله بسیار دوری از هم قرار داشته باشند، و هیچ بر هم کنشی بین آنها وجود نداشته باشد.

[1] Non- Locality



شکل(۴-۱) کیوبیت درهم تنیده به سوی دو کاربر فرستاده می شود

دو وضعیت زیر را در نظر می گیریم :

۱- اگر آلیس ابتدا S_z رااندازه گیری کند و بعداز اندازه گیری $\left|\uparrow_z\right\rangle_A$ را بدست آورد؛ با توجه به حالت $|\psi\rangle$ ، حالت ذره باب $\left|\downarrow_z\right\rangle_B$ خواهد شد. زیرا با اندازه گیری S_Z روی حالت $|\psi\rangle$ ،حالت $|\psi\rangle$ به حالت $\left|\downarrow_z\right\rangle_B\left|\uparrow_z\right\rangle_A$ فرو پاشی می کند.

۲- اگرآلیس S_x را اندازه گیری کند و $\left|\uparrow_x\right\rangle_A$را بدست آورد، آنگاه با توجه به حالت $|\psi\rangle$ ، حالت ذره باب $\left|\downarrow_x\right\rangle_B$خواهد شد. فرض کنیم باب ، S_x را می خواهد اندازه بگیرد. می خواهیم ببینیم با چه احتمالی $\left|\downarrow_x\right\rangle_A\left|\uparrow_x\right\rangle_B$ را بدست می آورد؟

در حالت ۱ با احتمال $\frac{1}{2}$ ، $\left|\downarrow_x\right\rangle_B$ را بدست می آورد. زیرا رابطه زیر برقرار است:

$$\left|\downarrow_z\right\rangle_B=\frac{1}{\sqrt{2}}\left(\left|\uparrow_x\right\rangle_B+\left|\downarrow_x\right\rangle_B\right) \qquad (۳-۴)$$

در حالت ۲ با احتمال 1 , $\left|\downarrow_x\right\rangle_B$ را بدست می آورد.

احتمال اینکه خروجی باب چه باشد بستگی به این دارد، که آلیس چه چیزی را اندازه گیری می کند، که این با اصل موضعیت تناقض دارد. در نتیجه با بررسی این نمونه حالت در هم تنیده دو طرفه به ناموضعیت می رسیم[۹،۲].

آزمایش ذهنی بوهم یکی دیگر از آزمایشاتی است که مکانیک کوانتومی در نظریه متغیرهای پنهان نتایج متفاوتی می دهد.

۴-۴- بررسی آزمایش ذهنی بوهم:

در این آزمایش حالت در هم تنیده حامل کیوبیت $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$ را در نظر می گیریم. برای نشان دادن این تناقض ابتدا باید پشگویی های کمّی مکانیک کوانتومی را برای اندازه گیری مؤلفه اسپینی $S_{2\phi}$ ذرهٔ دوم در زاویه ϕ نسبت به محور X در صورتی که قبلاً مؤلفه S_{1z} ذره اول تعیین شده باشد و نتایج اندازه گیری اول مقدار $\frac{\hbar}{2}$ باشد S_{2z} لزوماً منفی است؛ بنابراین قسمت اسپینی تابع موج ذره دوم برابر است با:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (۴-۴)$$

عملگر $\hat{S}_\phi$ که نشان دهنده مؤلفه ای از اسپین در زاویه ϕ نسبت به محور Z عبارت است از:

$$\hat{S}_\phi = \hat{S}_z Cos\phi + \hat{S}_x Sin\phi = \frac{\hbar}{2}\begin{pmatrix} Cos\phi & Sin\phi \\ Sin\phi & -Cos\phi \end{pmatrix} \qquad (۴-۵)$$

ویژه مقادیر $\hat{S}_\phi$، $\frac{\hbar}{2}, -\frac{\hbar}{2}$ و ویژه بردارهای متناظر با آن $\begin{pmatrix} Cos\frac{\phi}{2} \\ Sin\frac{\phi}{2} \end{pmatrix}$ و $\begin{pmatrix} -Sin\frac{\phi}{2} \\ Cos\frac{\phi}{2} \end{pmatrix}$ هستند تابع موج $|1\rangle$ را به صورت خطی از این دو ویژه بردار بسط می دهیم:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = Sin\frac{\phi}{2}\begin{pmatrix} Cos\frac{\phi}{2} \\ Sin\frac{\phi}{2} \end{pmatrix} + Cos\frac{\phi}{2}\begin{pmatrix} -Sin\frac{\phi}{2} \\ Cos\frac{\phi}{2} \end{pmatrix} \qquad (۴-۶)$$

بنابراین احتمال آنکه نتیجه اندازه گیری دوم مقداری مثبت باشد.

$$P_{++} = Sin^2\frac{\phi}{2} \qquad (۴-۷)$$

به این ترتیب احتمال های P_{-+}, P_{+-} و P_{--} را برای نتایج ممکنه مختلف از هر دو آزمایش به صورت زیر تعریف می کنیم.

$$P_{++}(\phi) = Sin^2\frac{\phi}{2} \qquad P_{+-}(\phi) = Cos^2\frac{\phi}{2}$$
$$P_{-+}(\phi) = Cos^2\frac{\phi}{2} \qquad P_{--}(\phi) = Sin^2\frac{\phi}{2} \qquad (۴-۸)$$

ضریب همبستگی $C(\phi)$ را به صورت مقدار میـانگین حاصـل ضـرب $\langle S_{z1}S_{\phi 2}\rangle_{\psi}$ کـه روی تعـداد زیادی از چنین زوج ذراتی انجام شده ثبت و تعریف می کنیم. پس داریم:

$$C(\phi)=\frac{\hbar^2}{8}\left(P_{++}(\phi)-P_{+-}(\phi)-P_{-+}(\phi)+P_{--}(\phi)\right)$$
$$=\frac{\hbar^2}{4}\left(Sin^2\frac{\phi}{2}-Cos^2\frac{\phi}{2}\right)=-\frac{\hbar^2}{4}Cos\phi \qquad (۹-۴)$$

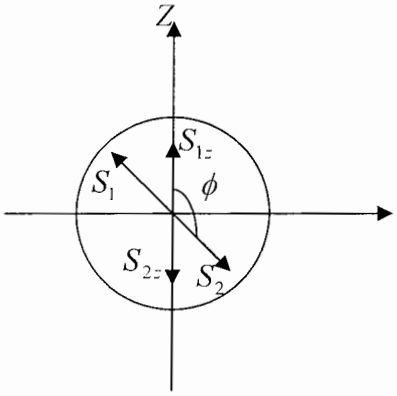
اینک آزمایش ذهنی بوهم را طبق نظریه متغیرهـای پنهـانی بررسـی مـی نمـایم کـه در آن فـرض می شود تمام اسپین (که در هر لحظه فقط یکـی از آنهـا قابـل تعیـین اسـت) مقـادیر معـین ولـی نامعلومی داشته باشند. یعنی همچون بردار تکانه زاویه ای کلاسـیکی بایـد اسـپین حقیقـی وجـود داشته باشد. به عبارت دیگر بردار اسپین حقیقی دو ذره در هنگام دور شدن باید مقدار یکسان ولـی در خلاف جهت هم داشته باشند.

در مکانیک کوانتومی در هر لحظه فقط یک مؤلفهٔ اسپینی ذره قابل تعین است و تنها نتیجه ممکن برای آن مؤلفه $\frac{\hbar}{2}$ است می توان مؤلفه های دیگر را که اندازه گیری نشده اند متغیـر پنهـان تـصور کرد.

با فرض اینکه بردار اسپین حقیقی ذره را با S نشان دهیم بردار اسپین S با ابزار آزمایش باید چنـان بر هم کنش کند که اطمینان حاصل شود مقدار اندازه گیری شده مؤلفهٔ اسپین همواره $\pm\frac{\hbar}{2}$ اسـت. هر چند مؤلفهٔ اسپین S ممکن است مقدار دیگری داشته باشد. در نظریه متغیر های پنهان اگر S_z اندازه گیری شود مؤلفهٔ S_x, S_y نیز موجودند کـه بـه همـراه S_z اسـپین حقیقـی کـل را تـشکیل می دهند. بنابراین مفهوم اسپین حقیقی را با این پیش فرض ها در نظر می گیریم.

حال نشان می دهیم که این مفهوم تابع همبستگی $C'(\phi)$ برای مؤلفه های اسپین دو ذره با نتـایج حاصل از مکانیک کوانتومی متفاوت است. اگر در آزمایش فرضی بالا مقدار $S_{1z}=\frac{\hbar}{2}$ برای ذره اول بدست آید مؤلفهٔ Z اسپین ذره دوم مقداری منفی است بنابراین بردار اسپین حقیقـی ذره دوم بایـد در نیم کره پایینی با محور تقارن Z باشد. اگر ذره دوم در راستایی بـا زاویـه ϕنـسبت بـه محـور Z

باشد. احتمال $P'_{++}(\phi)$ برای آنکه S_{1z} و $S_{2\phi}$ به طور هم زمان مثبت باشند با حجم حاصل از هم پوشان دو نیم کره متناسب است.



$$P'_{++}(\phi)=1 \qquad (۱۰-۴)$$

شکل(۴-۲) مفهوم بردار اسپین حقیقی طبق نظریه متغیرهای پنهانی

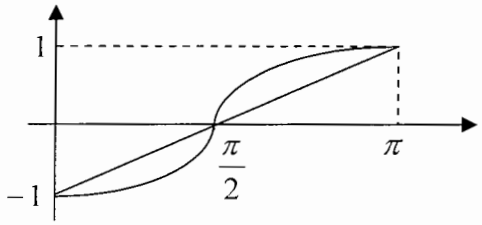
بنابراین داریم:

$$P'_{++}(\phi)=\frac{\phi}{\pi} \qquad P'_{+-}(\phi)=1-\frac{\phi}{\pi}$$
$$P'_{--}(\phi)=\frac{\phi}{\pi} \qquad P'_{-+}(\phi)=1-\frac{\phi}{\pi} \qquad (۱۱-۴)$$

در نظریه متغیرهای پنهان ضریب همبستگی $C'(\phi)$ که به صورت میانگین حاصل ضرب مؤلفه های اسپین اندازه گیری شده هر دو ذره تعریف می شود برابر است با :

$$C'(\phi)=\frac{\hbar^2}{4}(\frac{2\phi}{\pi}-1) \qquad (۱۲-۴)$$

این رابطه با رابطه مکانیک کوانتومی فقط در $\phi=0,\phi=\frac{\pi}{2},\phi=\pi$ توافق دارد؛ در سمتگیریهای متفاوت از آرایش آزمایشی نتایج اختلاف قابل ملاحظه ای دارند.



شکل(۴-۳)مقایسه تابع همبستگی مکا نیک کوانتومی و نظریه متغیر پنهان

در ادامه نشان خواهیم داد که هر نظریه متغیرهای پنهان با پیش گویهایی از نتایج تجربی در مکانیک کوانتومی تناقض دارد[۲۹].

۴-۵- قضیه EPR:

قضیه EPR امیدوار است که تفسیر جدیدی از مکانیک کوانتومی را مطرح کند یعنی توصیفی از واقعیت توسط متغیرهای پنهانی با پارامترهای غیر قابل اندازه گیری ارائه دهد؛ که در سطح آماری نتایج آن با نتایج مکانیک کوانتومی آزمایشگاهی یکسان باشد.در این بخش به این موضوع خواهیم پرداخت که با وجود آنکه تابع موج توصیف کاملی از واقعیت را ارائه نمی دهد معتقدیم چنین توصیف کاملی امکان پذیر نیست.

آنچه که موضعیت می گوید اساساً این است که مقدار اندازه گیری شده یک کمیت در یک سیستم به طور علّی نمی تواند متأثر از اندازه گیری یک کمیت روی سیستم دیگر باشد. زیرا وقتی که اندازه گیری انجام می شود فاصله سیستم ها فضا گونه است، یعنی بسیار دوراز هم قرار دارند و هیچ بر هم کنشی بین آنها وجود ندارد.

اصل عدم قطعیت هایزنبرگ ($\Delta x.\Delta p \geq \hbar$) بیان می کند که دو کمیت فیزیکی که با هم کامیوت نمی کنند($[p,x]=i\hbar$)به طور دقیق اندازه گیری نمی شوند. یعنی طبق اصل عدم قطیت هیچگاه نمی توان اطلاعات کاملی از رفتار اشیاء بسیار کوچک را دریافت نمود. در نظریه EPR برای نقض عدم قطعیت از حالت های در هم تنیده معروف به حالت های EPR استفاده نمودند. با تعریف حالت های در هم تنیده به شکل زیر برای دو ذره (۱و۲):

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left(|+\rangle_1|-\rangle_2+|-\rangle_1|+\rangle_2\right) \qquad (۱۳-۴)$$

که این حالت می تواند واپاشی ذره به دو قسمت مساوی (۱) و (۲) مانند یکی از موارد زیر باشد:

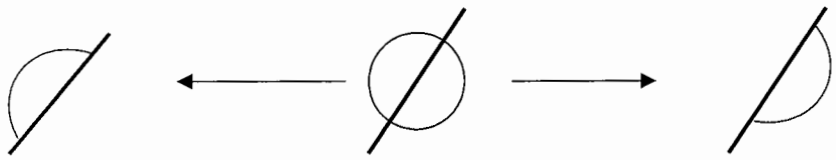
۱- واپاشی ذره پای π

۲- تولید زوج

۳- نابودی زوج

و غیره

به صورتی که اندازه حرکت کل ذره یا فوتون ها قبل از واپاشی صفر می باشد.



(۱) شکل(۴-۴) طرح ساده از ذرات در هم تنیده (۲)

دو کمیت فیزیکی مانند P, X (مکان و اندازه حرکت ذرات) را در نظر گرفتند و با تعریف اصل موضعیت EPR یک سیستم S_2 در فضای R_2 به هیچ طریقی نمی تواند با چیزی که در سیستم S_1 در فضای R_1 انجام می شود مختل شود وقتی که دو سیستم از قبل از نظر مکانی از هم جدا شده اند. وضعیت واقعی سیستم S_1 مستقل از چیزی است که در S_2 انجام می شود. بنابراین با اندازه گیری در سیستم S_2 می توان مقادیری را برای S_1 بدون مختل کردن سیستم با قطعیت مشخص کرد. ولی نظریه کوانتومی طبق اصل عدم قطعیت هایزنبرگ نمی تواند چنین مقادیری را مشخص کند. از این رو EPR آن را مبنی بر ناقص بودن نظریه کوانتومی می داند.

برای نمونه آنها بیان نمودند که با داشتن تابع حالت در هم تنیده و اندازه گیری اندازه حرکت ذره (۲) و اصل پایستگی اندازه حرکت می توان دقیقاً اندازه حرکت ذره (۱) را بدست آورد، یعنی بدون آنکه ذره (۱) اندازه گیری شود و سیستم آن مختل گردد مقدار اندازه حرکت آن تعیین شده است.با اندازه گیری مکان ذره (۱) همزمان با اندازه گیری اندازه گیری اندازه حرکت ذره (۲) می توان اصل عدم قطعیت ($\Delta x.\Delta p \geq \hbar$) را نقض کرد. زیرا در لحظه دو کمیت فیزیکی P,X که با هم کامیوت نمی کنند ($[p,x]=i\hbar$) به طور دقیق اندازه گیری شده اند.

ولی آنها دو نکته بسیار مهم را در نظر نداشته اند:

۱- اصل موضعیت در مکانیک کوانتومی نقض می شود، یعنی حالت های در هم تنیده اصل موضعیت را نقض می کنند.

۲- هنگامی که ذره (۲) توسط عملگر اندازه حرکت اندازه گیری می شود تابع حالت در هم تنیده به تابع حالت اندازه حرکت فروپاشی می شود در این صورت اندازه گیری دقیق مکان در تابع حالت اندازه حرکت امکان پذیر نیست.

نتیجه بحث این است کـه ناموضـعیت مکانیـک کوانتـومی نظریـه EPR رابـه باطنمـا EPR تبـدیل می نمود[۳۵].

۴-۶- قضیه بِل

جهت دست یابی به اثبات عمومی تر ابتدا باید حداقل فرض های لازم نظریه متغیر پنهان موجبتی موضعیتی را برای آزمایش فرضی بوهم بیان نماییم.پس از آنکه دو ذره از هم جدا شده اند، دستگاه باید دارای خاصیتی باشد که پیشایش نتیجه اندازه گیری مؤلفـهٔ اسـپین هـر ذره را تعیـین نماید.

در مثال قبلی این خاصیت با وجود اسپین حقیقی ایجاد شده بود اما در حالت کلی لازم نیست کـه متغیر پنهان متناظر پارامتری از مدل فیزیکی خاصی باشد.

بنابراین نتیجه اندازه گیری مؤلفهٔ Z اسپین S اولین ذره را به صورت $S_{1z}(\lambda)$ نمایش می دهیم که در آن تنها مقادیر مجاز برای S_{1z} ، $\pm\frac{\hbar}{2}$ بوده و λ نمایشگر متغیرپنهـانی اسـت. چنـین نظریـه ای موجبتی است. زیرا مقادیر S_{1z} و S_{2z} از مقدار λ بدست می آید و موضعی است برای آنکـه نتیجـه هر آزمایش مستقل از آزمایش تعیین مقدار اسپین ذرات دیگر است.

هر ذوج ذره مقدار معینی از λ دارد و چگالی احتمال $\rho(\lambda)$ یعنی احتمـال آن کـه ذره مقـدار λ بین λ تا $\lambda+d\lambda$ داشته باشند برابر است با:

$$\int\rho(\lambda)d\lambda \qquad (۱۴-۴)$$

$$\int\rho(\lambda)d\lambda=1 \qquad (۱۵-۴)$$

با تعریف شرط بهنجارش داریم:

اینک آزمایش تعیین مؤلفهٔ اسپین S_{1z} و S_{2z} تعـداد زیـادی جفـت ذره در هـم تنیـده را در نظـر می گیریم؛ مقدار(مقدار انتظاری) $C''(\phi)$ برای حاصلضرب های $\langle S_{2\phi}S_{1z}\rangle$ عبارت است از:

$$C''(\phi)=\int S_{z1}(\lambda)S_{\phi 2}(\lambda)\rho(\lambda)d\lambda \qquad (۱۶-۴)$$

حال آزمایشی را در نظر می گیریم که همانند قبل مؤلفهٔ Z ذره اول را اندازه می گیرد. اما ایـن بـار اسباب اندازه گیری در زاویه θ نسبت به محور Z قرار گرفته است. در نتیجه عبارت مـشابهی بـرای ضریب همبستگی $C''(\theta)$ بدست می آوریم که عبارت است از :

$$C''(\phi)-C''(\theta)=\int[S_{z1}(\lambda)S_{\phi 2}(\lambda)-S_{z1}(\lambda)S_{\theta 2}]\rho(\lambda)d\lambda \qquad (۱۷-۴)$$

می دانیم که اسپین هر دو ذره مفروض اندازه ای برابر ولی در جهت خلاف هم دارند پس داریم:

$$S_{\theta 1}(\lambda)=-S_{\theta 2}(\lambda) \quad , \quad S_{\phi 1}(\lambda)=-S_{\phi 2}(\lambda) \qquad (۱۸-۴)$$

با جای گذاری (۴-۱۸) در (۴-۱۷) بدست می آوریم:

$$\begin{aligned} C''(\phi)-C''(\theta) &= -\int[S_{z1}(\lambda)S_{\phi 1}(\lambda)-S_{z1}(\lambda)S_{\theta 1}(\lambda)]\rho(\lambda)d\lambda \\ &= -\int S_{z1}\left(S_{\phi 1}(\lambda)-S_{\theta 1}(\lambda)\right)\rho(\lambda)d\lambda \\ &= -\int S_{z1}\left(S_{\phi 1}(\lambda)-\frac{4}{\hbar^2}S^2{}_{\phi 1}(\lambda)S_{\theta 1}(\lambda)\right)\rho(\lambda)d\lambda \end{aligned} \qquad (۱۹-۴)$$

مقدار $\left\langle S^2{}_{\phi 1}(\lambda)\right\rangle=\frac{\hbar}{2}$ همواره برقرار است بنابراین $\frac{4}{\hbar^2}S^2{}_{\phi 1}(\lambda)=1$ و داریم:

$$C''(\phi)-C''(\theta)=-\int S_{z1}(\lambda)S_{\phi 1}(\lambda)\left(1-\frac{4}{\hbar^2}S_{\phi 1}(\lambda)S_{\theta 1}(\lambda)\right)\rho(\lambda)d\lambda \qquad (۲۰-۴)$$

در نتیجه اندازه معادله (۴-۲۰) را می توان به صورت عبارت تخمین زد:

$$\left|C''(\phi)-C''(\theta)\right|\le\int\left|S_{z1}(\lambda)S_{\phi 1}(\lambda)\left(1-\frac{4}{\hbar^2}S_{\phi 1}(\lambda)S_{\theta 1}(\lambda)\right)\right|\rho(\lambda)d\lambda \qquad (۲۱-۴)$$

از آنجاکه $\rho(\lambda)$ همواره مثبت است و اسپین تنها مقادیر $\pm\frac{\hbar}{2}$ را دارند پس داریم:

$$\left|S_{z1}(\lambda)S_{\phi 1}(\lambda)\right|=\frac{\hbar^2}{4} \qquad (۲۲-۴)$$

با اعمال (۴-۲۲) و (۴-۲۱) داریم:

$$\begin{aligned} &\left|C''(\phi)-C''(\theta)\right|\le\int\left|\left(\frac{\hbar^2}{4}-S_{\phi 1}(\lambda)S_{\theta 1}(\lambda)\right)\right|\rho(\lambda)d\lambda \\ &\left|C''(\phi)-C''(\theta)\right|\le\frac{\hbar^2}{4}+\int\left(S_{\phi 1}(\lambda)S_{\theta 1}(\lambda)\right)\rho(\lambda)d\lambda \\ &\left|C''(\phi)-C''(\theta)\right|\le\frac{\hbar^2}{4}+C''(\theta-\phi) \\ &\left|C''(\phi)-C''(\theta)\right|+C''(\theta-\phi)\le\frac{\hbar^2}{4} \end{aligned} \qquad (۲۳-۴)$$

در رابطه بالا فرض کنید که محور Z و راستاهایی که با θ,ϕ مشخص می شوند، در یک صحفه قرار داشته باشند. مقدار میانگین که در معادله (۴-۱۶) تعریف شده است می توان معادله بالا را با تابع همبستگی $C''(\theta-\phi)$ جایگزین نمود.

نامساوی(۴-۲۳) قضیه بِل نامیده می شود و نتیجه مستقیم هر نظریه متغیر پنهانِ موضعی ـ موجبتی است.

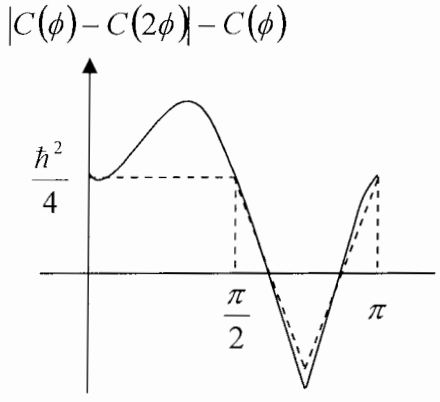
اکنون تحقیق می کنیم که آیا این نامساوی با پیشگویهای مکانیک کوانتومی توافق دارد یا خیر برای انجام این کار حالت خاص $\theta = 2\phi$ را بررسی می کنیم و دو تابع همبستگی را می توان به کمک (۴-۹) بدست آورد.

$$C(\phi) = -\frac{\hbar^2}{4}Cos\phi \quad , \quad C(2\phi) = -\frac{\hbar^2}{4}Cos2\phi \qquad (۲۴-۴)$$

با مقایسه (۴-۲۳) و (۴-۲۴) در می یابیم که مکانیک کوانتومی با در نظریه متغیر پنهان فقط وقتی سازگار است که رابطه زیر برقرار باشد.

$$\frac{\hbar^2}{4}\left(\left|Cos\phi - Cos2\phi\right| + Cos\phi\right) \le \frac{\hbar^2}{4} \qquad (۲۵-۴)$$

شکل(۴-۵) نشان می دهد که قضیه بِل در محدودهٔ $\frac{\pi}{2} \le \phi \le \pi$ برقرار است، هنگامی که $\phi = \frac{\pi}{3}$ باشد تابع بالا بیشنه ای با مقدار $\frac{3\hbar^2}{8}$ را دارد.



شکل(۴-۵): منحنی خط پر برپایه مکانیک کوانتومی و منحنی خط چین بر مبنای نظریه متغیر پنهان است

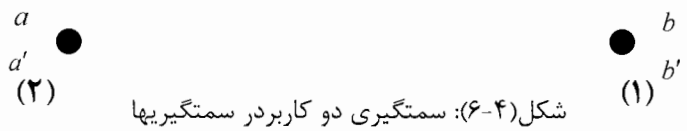
درضمن شکل (۴-۵) تابعی را هم که با استفاده از بحث قبلی نظریه بردار اسپین حقیقی محاسبه شده (۴-۱۲) نشان می دهد.(منحنی خط چین) البته این منحنی با قضیه بِل سازگار ولی با مکانیک کوانتومی ناسازگار است[۵،۹،۱۰،۱۳].

۴-۶-۱- تعمیم های دیگر نامساوی بِل

پس از آنکه جان بِل در سال۱۹۶۴ قضیه ای منتشر کرد که به نامساوی بل معروف بود. وی که در این نامساوی با استفاده از نظریه متغیرهای پنهانی موجبتی وموضعی انیشتین را یک شرط در اثبات این نامساوی قرار داد.. نامساوی بل با پیش بینی های نظریه کوانتومی نقض شد. طبیعت (آزمایشهای تجربی) به نفع نظریه کوانتومی نظریه کوانتومی رای داد.

موضعیت اینشتین مورد چالش قرار گرفت و ذات غیر موضعی طبیعت آشکار شد.

پس از بِل؛ کِلوزر،هورن،شیمونی و هالت[1] و بعد کِلوز و هورن[2] وکلوزر و شیمونی[3] این نامساوی را به کلی ترین حالت برای یک سیستم در هم تنیده (۱) و (۲) حامل کیوبیت بدست آوردند.که به صورت رندمی اندازه گیریهایی را روی ذرات خود می توانند داشته باشند.



شکل(۴-۶): سمتگیری دو کاربردر سمتگیریها متفاوت اندازه گیری ذرات

هر کدام از a,a' , b,b' هم می توانند دارای دو مقدار ± 1 باشند.

(CHSH) و (SH) با مقدار انتظاری و (CH) با احتمالات این نامساوی را تعمیم دادند[۹،۱۰،۱۲] .

اگر نتایج حاصل از اندازه گیرها در آزمایشات تجربی در این نا مساوی تعمیم یافته صدق می کرد نظریه کوانتومی ناسازگار و موضعیت در مکانیک کوانتومی بر قرار بود، که اینگونه نشد.

اکنون به چند نمونه از نامساویهای تعمیم یافته بِل اشاره می کنیم.

۴-۶-۲- اولین نامساوی تعمیم یافته بِل

این نامساوی همان نامساوی بِل است که به صورت مشابه طراحی شده است .

فرض می کنیم یک جفت اسپین ذرات نیم صحیح در حالت اسپین زیر منفرد وجود داشته باشد:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right)$$

این جفت ذرات حرکت آزادانه در خلاف جهت هم می توانند داشته باشند.

---

[1] Clouser-horne-shimony-halt (CHSH)
[2] (CH)
[3] (SH)

اندازه گیری توسط دستگاه اشترن گرلاخ روی گزینش مؤلفه های اسپینی انجام می گیرد.

نتیجه اندازه گیری A ، $\sigma_1 \cdot a$ به وسیله a و λ (متغیرهای پنهانی) مشخص می شود.

نتیجه اندازه گیری B ، $\sigma_2 \cdot b$ به وسیله b و λ (متغیرهای پنهانی) مشخص می شود.

$$A_a(\lambda_{HV}) = \pm 1 \quad , \quad B_b(\lambda_{HV}) = \pm 1 \qquad (۲۶-۴)$$

فرض کنیم که نتیجه اندازه گیری B روی ذره دوم وابسته به قرار گرفتن نتیجه a نیست و همچنین برای A به نتیجه حاصل از b بستگی ندارد و بر هم کنشی بین دو ذره وجود ندارد.

λ بی نهایت عدد با متغیر فیزیکی A,B می باشد که از قوانین حرکت معنا دار دینامیکی پیروی می کند.

مقدار انتظاری حاصل از اندازه گیری دو مؤلفه توسط دو کاربر با چگالی احتمال از $\rho(\lambda_{HV})$ برابر است:

$$C(a,b) = \int d\lambda_{HV} \rho(\lambda_{HV}) A_a(\lambda_{HV}) B_b(\lambda_{HV}) \qquad (۲۷-۴)$$

با فرض شرط بهنجارش:

$$\int d\lambda_{HV} \rho(\lambda_{HV}) = 1 \qquad (۲۸-۴)$$

و نیز داریم:

$$(۲۹-۴)$$

$$\langle C(a,b) \rangle_\psi = -a \cdot b \qquad (۳۰-۴)$$

$$\langle C(a,a) \rangle_\psi = -1 \Rightarrow A_a(\lambda_{HV}) = -B_a(\lambda_{HV})$$

$$C(a,b) = -\int d\lambda_{HV} \rho(\lambda_{HV}) A_a(\lambda_{HV}) A_b(\lambda_{HV}) \qquad (۳۱-۴)$$

$$C(a,b) - C(a,c) = -\int d\lambda_{HV} \rho(\lambda_{HV}) (A_a(\lambda_{HV}) A_b(\lambda_{HV}) - A_a(\lambda_{HV}) A_c(\lambda_{HV})) \qquad (۳۲-۴)$$

با توجه به اینکه:

$$\langle A_b(\lambda_{HV}) \rangle^2 = 1 \qquad \langle A_a(\lambda_{HV}) \rangle^2 = 1 \qquad (۳۳-۴)$$

$$C(a,b) - C(a,c) = -\int d\lambda_{HV} \rho(\lambda_{HV}) A_a(\lambda_{HV}) A_b(\lambda_{HV}) (1 - A_b(\lambda_{HV}) A_c(\lambda_{HV})) \qquad (۳۳-۴)$$

با برقراری روابط زیر:

$$A_b(\lambda_{HV'}) = -B_b(\lambda_{HV}) \qquad B_b(\lambda_{HV'}) = \pm 1 \quad , \quad A_a(\lambda_{HV}) = \pm 1 \qquad (۳۴-۴)$$

داریم:

$$|C(a,b) - C(a,c)| \le \int d\lambda_{HV}\, \rho(\lambda_{HV}) |(1 - A_b(\lambda_{HV}) A_c(\lambda_{HV}))|$$

$$|C(a,b) - C(a,c)| \le 1 + \int d\lambda_{HV}\, \rho(\lambda_{HV}) A_b(\lambda_{HV}) A_c(\lambda_{HV})$$

$$|C(a,b) - C(a,c)| \le 1 + C(b,c) \qquad (۳۵-۴)$$

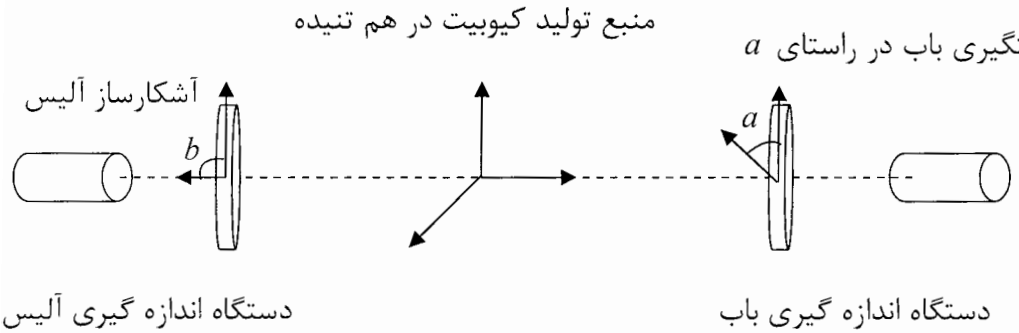
رابطه (۴-۳۵) معروف به اولین نامساوی تعمیم یافته بِل است.

می توان با فرض $\|a\| = \|b\| = \|c\| = 1$ و برقراری رابطه $_{\psi}\langle C(a,b)\rangle_{\psi} = -Cos\theta$ ناسازگاری این نامساوی را درمکانیک کوانتومی بررسی نمود[۲،۹،۱۰] .

بنابراین می توان نتیجه گرفت که هیچ متغیر پنهانِ موجبتی موضعی وجود ندارد که بتواند همان نتایج حاصل از مکانیک کوانتومی را برای آزمایش هایی از این نوع را بدست آورد. نظریه مکانیک کوانتومی با طبیعت سازگار است زیرا مکانیک کوانتومی بر پایهٔ شواهد تجربی استوار می باشد اما آزمایش های قبل از فرمول بندی قضیه بِل، سازگاری مکانیک کوانتومی را با این نکته خاص بررسی نکرده بودند در سال های اخیر آزمایش های متعددی برای آزمودن این مسئله انجام گرفته است هر چند آزمایش های اولیه نتایج سازگار با قضیه بِل را ارائه دادند که به تردیدی در اعتبار مکانیک کوانتومی انجامید. امّا آزمایش های بسیار دقیق دیگر نتایجی را در بر داشتند که با قضیه بِل ناسازگار ولی با پیشگوئیهای مکانیک کوانتومی در توافق بود. اغلب این آزمایش ها قطبش جفت فوتون های همبسته اندازه می گیرند در این حالت فرمول بندی اندکی با (۴-۹) متفاوت است ولی در بحث کلی اختلاف چندانی ندارد.

۴-۶-۳- دومین نامساوی تعمیم یافته بِل

این نامساوی با پیروی از ساختار اصلی قضیه بِل تعمیم داده شده است.



شکل(۴-۷): براساس طرحی از نامساوی CHSH

$$A_a(\lambda_{HV'}) = \pm 1 \quad , \quad B_b(\lambda_{HV}) = \pm 1 \qquad (۳۶-۴)$$

$$C(a,b) = \int d\lambda_{HV}\, \rho(\lambda_{HV}) A_a(\lambda_{HV}) B_b(\lambda_{HV}) \qquad (۳۷-۴)$$

در این نامساوی با تقسیم بندی فضای متغیرهای پنهانی به دو قسمت Λ^+, Λ^- داریم:

$$\Lambda_{HV'}^{\pm} \qquad A_{b'}(\lambda_{HV}) = \pm B_b(\lambda_{HV}) \qquad (۳۸-۴)$$

$$|C(a,b) - C(a,c)| \le 2 - C(b',b) - C(b',c) \qquad (۳۹-۴)$$

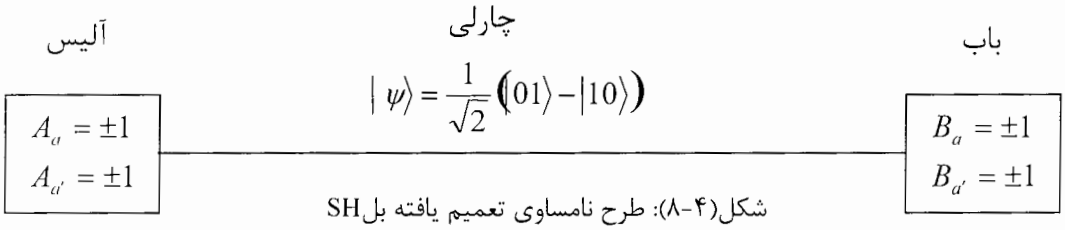
این نامساوی معروف به دومین نامساوی تعمیم یافته بِل است[۳۰،۹،۲] .

۴-۶-۴- سومین نامساوی تعمیم یافته بِل

اساس کار این نامساوی که معروف به نامساوی کلوزر و شیمونی است مانند قبل می باشد یعنی این نامساوی نیز براساس مقدار میانگین حاصل از اندازه گیریها عمل می کند. بنابراین مقدار انتظاری آن به صورت زیر می باشد[۳۶،۱۰،۹] :

$$C(a,b) = \int d\lambda_{HV'}\, \rho(\lambda_{HV}) \overline{A}_a(\lambda_{HV}) \overline{B}_b(\lambda_{HV})$$
$$A_a(\lambda_{HV'}) = \pm 1 \rightarrow |\overline{A}_a| \le 1$$
$$B_b(\lambda_{HV'}) = \pm 1 \rightarrow |\overline{B}_b| \le 1 \qquad (۴۰-۴)$$

اگر A,B سمتگیریهای a,b و a',b' را به طور رندمی در بر روی اسپین ذرات خود اندازه گیری انجام دهند.شکل(۴-۸)



شکل(۴-۸): طرح نامساوی تعمیم یافته بلSH

چارلی کیوبیت در هم تنیده (اسپینی ذره- قطبشی فوتون) را برای باب و آلیس تهیه می کند و به سوی آنها می فرستد. باب و آلیس قادرند بر روی کیو بیت های درهم تنیده خودکه به آنها می رسد اندازه گیری انجام دهند، آنها پایه های اندازه گیریشان را به ترتیب a,a' باب برای خود و b,b' آلیس برای خود انتخاب می کند و به طور رندمی آنها را اندازه گیری می کند.

دستگاه اشترن-گرلاخ را برای اندازه گیری اسپین بکار می گیریم. یک زوج بردار واحد a و a' را برای ناظر(۱) و زوج دیگر b و b' را برای ناظر(۲) در نظر می گیریم. یک سری اندازه گیری ها روی (مجموعه) سیستمها صورت می گیرد که در حالت کوانتومی یگانه قرار دارند یعنی:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle \otimes |-\rangle + |-\rangle \otimes |+\rangle) \qquad (۴۱-۴)$$

فرض کنید A_a به صورت $\frac{2}{\hbar}\vec{a}.\vec{s}$ متعلق به ذره(۱) در عنصر nام آنسامبل باشد. اگر $\vec{a}.\vec{s} = \pm\frac{\hbar}{2}$ آنگاه $A_a = \pm 1$ است.(۱+ برای اسپین بالا و ۱- برای اسپین پایین می باشد.)

فرض کنید B_b به صورت $\frac{2}{\hbar}\vec{b}.\vec{s}$ متعلق به ذره(۲) در عنصر n ام آنسامبل باشد. اگر $\vec{b}.\vec{s} = \pm\frac{\hbar}{2}$ آنگاه $B_b = \pm 1$ است.

$$C(a,b)-C(a,b')=\int d\lambda_{HV}\rho(\lambda_{HV})\left[\overline{A}_a(\lambda_{HV})\overline{B}_b(\lambda_{HV})-\overline{A}_a(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})\right]$$
$$=\int d\lambda_{HV}\rho(\lambda_{HV})\left[\overline{A}_a(\lambda_{HV})\overline{B}_b(\lambda_{HV})\pm\overline{A}_a(\lambda_{HV})\overline{B}_b(\lambda_{HV})\overline{A}_{a'}(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})\right.$$
$$\left.\mp\overline{A}_a(\lambda_{HV})\overline{B}_b(\lambda_{HV})\overline{A}_{a'}(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})-\overline{A}_a(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})\right]$$
$$=\int d\lambda_{HV}\rho(\lambda_{HV})\overline{A}_a(\lambda_{HV})\overline{B}_b(\lambda_{HV})\left[1\pm\overline{A}_{a'}(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})\right]$$
$$-\int d\lambda_{HV}\rho(\lambda_{HV})\overline{A}_a(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})\left[1\pm\overline{A}_{a'}(\lambda_{HV})\overline{B}_b(\lambda_{HV})\right]$$
$$\Rightarrow\left|C(a,b)-C(a,b')\right|=\int d\lambda_{HV}\rho(\lambda_{HV})\left|\overline{A}_a(\lambda_{HV})\overline{B}_b(\lambda_{HV})\right|\left[1\pm\overline{A}_{a'}(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})\right]$$
$$+\int d\lambda_{HV}\rho(\lambda_{HV})\left|\overline{A}_a(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})\right|\left[1\pm\overline{A}_{a'}(\lambda_{HV})\overline{B}_b(\lambda_{HV})\right] \qquad (۴۲-۴)$$

با توجه به (۴-۴۰) داریم:

$$\left|C(a,b)-C(a,b')\right|\le$$
$$=\int d\lambda_{HV}\rho(\lambda_{HV})\left[1\pm\overline{A}_{a'}(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})\right]$$
$$+\int d\lambda_{HV}\rho(\lambda_{HV})\left[1\pm\overline{A}_{a'}(\lambda_{HV})\overline{B}_b(\lambda_{HV})\right]$$
$$\Rightarrow\left|C(a,b)-C(a,b')\right|\le 1\pm\int d\lambda_{HV}\rho(\lambda_{HV})\overline{A}_{a'}(\lambda_{HV})\overline{B}_{b'}(\lambda_{HV})$$
$$1\pm\int d\lambda_{HV}\rho(\lambda_{HV})\overline{A}_{a'}(\lambda_{HV})\overline{B}_b(\lambda_{HV})$$
$$\Rightarrow\left|C(a,b)-C(a,b')\right|\le 2\pm\left(C(a',b')+C(a',b)\right)$$

$$\Rightarrow\left|C(a,b)-C(a,b')\right|+\left|\left(C(a',b')+C(a',b)\right)\right|\le 2 \qquad (۴۳-۴)$$

بنابراین داریم:

$$\left|C(a,b)-C(a,b')+\left(C(a',b')+C(a',b)\right)\right|\le 2 \qquad (۴۴-۴)$$

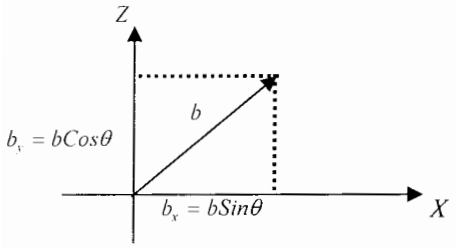
۴-۷- مثال نقض از سومین نامساوی تعمیم یافته بِل

به آسانی می توان در تئوری مکانیک کوانتومی مثالی آورد که سومین نا مساوی تعمیم یافته بِل (نامساوی کلوزر و شیمونی) در آن نقض می شود. ولی ابتدابا استفاده از مفاهیم بالا مقدار انتظاری $[C(a,b)]_{QM}$ را در تئوری مکانیک کوانتومی بار دیگر با روش مشابه دیگر بدست می آوریم.

در نتیجه شکل مکانیک کوانتومی تابع همبستگی:

$$C(a,b)=\left(\frac{2}{\hbar}\right)^2{}_{\psi}\left\langle \vec{a}\cdot\vec{s}_1\otimes\vec{a}\cdot\vec{s}_2\right\rangle_{\psi} \qquad (۴۵-۴)$$

برای محاسبه این همبستگی فرض می کنیم a در جهت Z باشد و b درصفحه XZو با a زاویه θ بسازد. در این صورت داریم:



$$\vec{s}_1=\frac{\hbar}{2}(\sigma_{1x}+\sigma_{1y}+\sigma_{1z}) \qquad (۴۶-۴)$$

$$\vec{s}_2=\frac{\hbar}{2}(\sigma_{2x}+\sigma_{2y}+\sigma_{2z}) \qquad (۴۷-۴)$$

$$\vec{a}\cdot\hat{s}_1=\frac{\hbar}{2}a_z\sigma_{1z} \qquad (۴۸-۴)$$

$$\vec{b}\cdot\hat{s}_2=\frac{\hbar}{2}(b_x\sigma_{2x}+b_z\sigma_{2z})=\frac{\hbar}{2}(\sigma_{2x}\sin\theta_{ab}+\sigma_{2z}\cos\theta_{ab}) \qquad (۴۹-۴)$$

$$C(\vec{a},\vec{b})=\left\langle\psi\left|\sigma_{1z}\otimes(\sigma_{2x}\sin\theta_{ab}+\sigma_{2z}\cos\theta_{ab})\right|\psi\right\rangle \qquad (۵۰-۴)$$

$$\sigma_Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\quad,\quad \sigma_X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$\sigma_{2X}Sin\theta_{ab}=\begin{pmatrix}0&1\\1&0\end{pmatrix}Sin\theta_{ab}=\begin{pmatrix}0&Sin\theta_{ab}\\Sin\theta_{ab}&0\end{pmatrix},\quad .....$$

$$\sigma_{1z}\otimes(\sigma_{2x}\sin\theta_{ab}+\sigma_{2z}\cos\theta_{ab})=$$
$$\begin{pmatrix}1&0\\0&-1\end{pmatrix}\otimes\begin{pmatrix}\cos\theta_{ab}&\sin\theta_{ab}\\\sin\theta_{ab}&-\cos\theta_{ab}\end{pmatrix}=$$
$$\begin{pmatrix}\cos\theta_{ab}&\sin\theta_{ab}&0&0\\\sin\theta_{ab}&-\cos\theta_{ab}&0&0\\0&0&-\cos\theta_{ab}&-\sin\theta_{ab}\\0&0&-\sin\theta_{ab}&\cos\theta_{ab}\end{pmatrix} \qquad (۵۱-۴)$$

با استفاده از روابط:

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

$$|+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{و} \quad |-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}] =$$

$$\frac{1}{\sqrt{2}}[\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}] = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \Rightarrow \langle\psi| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & -1 & 0 \end{pmatrix} \qquad (۵۲-۴)$$

بنابراین:

$$\langle\psi|\sigma_{1z} \otimes (\sigma_{2x}\sin\theta_{ab} + \sigma_{2z}\cos\theta_{ab})|\psi\rangle = ?$$

$$\frac{1}{2}\begin{pmatrix} 0 & 1 & -1 & 0 \end{pmatrix}\begin{pmatrix} \cos\theta_{ab} & \sin\theta_{ab} & 0 & 0 \\ \sin\theta_{ab} & -\cos\theta_{ab} & 0 & 0 \\ 0 & 0 & -\cos\theta_{ab} & -\sin\theta_{ab} \\ 0 & 0 & -\sin\theta_{ab} & \cos\theta_{ab} \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix} 0 & 1 & -1 & 0 \end{pmatrix}\begin{pmatrix} \sin\theta_{ab} \\ -\cos\theta_{ab} \\ \cos\theta_{ab} \\ \sin\theta_{ab} \end{pmatrix} = \frac{1}{2}(-\cos\theta_{ab} - \cos\theta_{ab}) = -\cos\theta_{ab}$$

(۵۳-۴)

به طریق مشابه:

$$C(\vec{a},\vec{b}') = -Cos\theta_{ab'}$$
$$C(\vec{a}',\vec{b}) = -Cos\theta_{a'b}$$
$$C(\vec{a}',\vec{b}') = -Cos\theta_{a'b'} \qquad (۵۴-۴)$$

در این صورت نا مساوی بِل با توجه به تابع همبستگی مکانیک کوانتومی و فرضیات بالا به شکل زیر می توان نوشت :

$$|Cos\theta_{ab} - Cos\theta_{ab'} + Cos\theta_{a'b} + Cos\theta_{a'b'}| \le 2$$

اکنون فرض کنیم که چارلی حالت درهم تنیده $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ را که حامل کیوبیت در هم تنیده است را فراهم کرده و به سوی آلیس و باب می فرستد و آنها اندازه گیریهایشان را مطابق شکل زیر برای سمتگیریهای a,a',b,b' انجام می دهند و θ زاویه بین آنها $\frac{\pi}{4}$ می باشد[۹،۱۰].

با یک محاسبات ساده می توان نشان داد که (۴-۴۴) برای نامساوی کلوزر و شیمونی در مکانیک کوانتومی برابراست با:

$$S = |C(a,b) - C(a,b') + C(a',b') + C(a',b)|_{QM}$$

$$C(a,b) = -Cos\frac{\pi}{4} = -\frac{\sqrt{2}}{2}$$

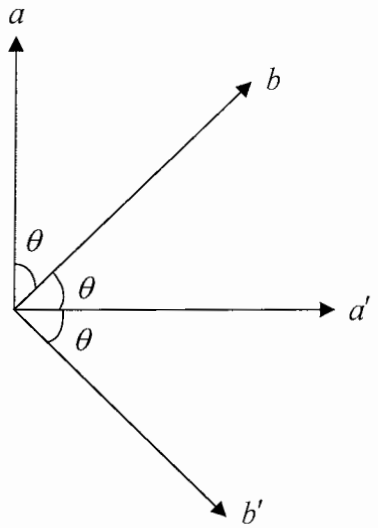
$$C(a,b') = -Cos\frac{3\pi}{4} = \frac{\sqrt{2}}{2}$$

$$C(a',b') = -Cos\frac{\pi}{4} = -\frac{\sqrt{2}}{2}$$

$$C(a',b) = -Cos(-\frac{\pi}{4}) = -\frac{\sqrt{2}}{2}$$

$$|C(a,b) - C(a,b') + C(a',b') + C(a',b)|_{QM}$$

$$\left|-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\right|_{QM} = 2\sqrt{2}$$



شکل(۴-۹): باانتخاب سمتگیریهای مناسب a,a',b,b' ونقض نامساوی تعمیم یافته

در اینجا پارامتر S را به صورت زیر تعریف می کنیم:

$$S = |C(a,b) - C(a,b') + C(a',b') + C(a',b)| \qquad (۵۵-۴)$$

۴-۷-۱- مثال نقض از نامساوی کلوزر و شیمونی درآزمایشگاه

بل و دیگران نشان دادند با نوعی آزمایش که پارامتری به اسم S را می سنجد، می شود بین مکانیک کوانتوم و این نظریه های متغیرهای نهانی فرق گذاشت. به بیان ساده، نظریه های موضعی پیش بینی می کنند S همواره کوچکتر از دو است، در حالیکه پیش بینی کوانتوم مکانیک S=Sqr(2)*2 است. وقتی S بزرگتر از ۲ می شود، می گویند نامساوی بل نقض شده است.

آزمایشی توسط برخورد شتابدهنده باریکه های الکترون و پوزیترون با هم برخورد می کنند و مزونها و پادذره هایشان را تولید می کنند که اینها هم به ذرات سبک دیگر واپاشی می شوند. زوج مزونها مثل زوج فوتون رفتار می کنند. اما گروه بله[1] ، به جای تحلیل هم بستگی بین جهت های قطبش، هم بسته گی های ذره-پادذره را با روشی به اسم برچسب طعم گذاری بررسی کردند[۱۱] و مقدار S=2.725 حساب کردند و خطای این سنجش چنان است که نامساوی تا حد سه انحراف معیار نقض می شود.بنابراین مکانیک کوانتومی در توصیف بنیادی طبیعت در بین آن ذرات همبستگی های ناموضعی دیده شود.

۴-۸- نتیجه گیری

در آزمون های نامساوی بل، ویژگی های زوج ذره هایی را می سنجند که فاصله آنها، از نظر نسبیت خاص، فضاگونه است؛ مکانیک کوانتوم پیش بینی می کند بین ذره ها هم بستگی های ناموضعی هم می تواند باشد. اما بعضی از فیزیک پیشه ها معتقدند این نمی تواند درست باشد، و ذره های کوانتومی باید کمیت های موضعی (به اسم متغیرهای نهانی) داشته باشند، که نمی توانیم آنها را بسنجیم. باید توجه داشت که اگر پیش بینی های مکانیک کوانتومی از نظر تجربی نامساوی بِل را نقض می کند باید غیر موضعیت را به عنوان یک هویت اساسی طبیعت بپذیریم.

غیر موضعیت یکی از وجوه اساسی طبیعت است و هر نظریه ای که ادعای توصیف طبیعت کوانتومی را داشته باشد باید غیر موضعی باشد.

در رفتار غیر موضعی طبیعت چند چیز جلب توجه می کند:

چطور دو شئ همبسته می توانند در آن واحد (با سرعتی بالاتر از سرعت نور) با هم ارتباط برقرار کنند.ذات این همبستگی است: اینکه دو شیء کوانتومی زمانی که با هم ترکیب می شوند، دیگر هیچ وقت از هم جدا نمی شوند. هر زوج ، زوج همبسته خود را می شناسد طوری که تنها این دو با هم ارتباط برقرار می کنند.

[1] Belle

فصل۵:

رمز نگاری کوانتومی

- مقدمه
- رمزنگاری
- توزیع کلید رمز محرمانه
- رمزنگاری کوانتومی وتاریخچه آن
- امنیت رمزنگاری کوانتومی درمقابل تهاجمات استراق سمع کنندگان
- ایده های اساسی در رمزنگاری کوانتومی
- پروتکل توزیع کلید کوانتومی محرمانه
- بیان یک نمونه از پروتکل رمزنگاری کوانتومی محرمانه
- نمونه هایی ازرمزنگاری کوانتومی در لوس آلاموس
- نتیجه گیری

۵-۱- مقدمه

رمزنگاری[1] برگرفته از واژه یونانی به معنای پنهان شده و نوشتن می باشد. رمزنگاری با وجود یک تاریخچه رنگارنگ تنها بخشی از تئوری اطلاعات است، امروزه هر کسی می تواند به طور خلاصه رمزنگاری را به عنوان یک سیستم ریاضی یا نظامی از روابط ریاضی مربوط به امنیت اطلاعات تعریف نماید و یکی از شاخه های اصلی علوم رایانه ای می باشد، د ررایانه ها جهت امنیت شبکه ها و کنترل اطلاعات محرمانه مورد استفاده قرار می گیرد. در بسیاری از کاربردهای روزمره قابل لمس است، از جمله امنیت کارت های ATM ،...، پسوردهای رایانه ای، تجارت های الکترونیکی و غیره که همگی به رمزنگاری وابسته هستند.

ابتدایی ترین تکنیک های رمزنگاری سنتی،مربوط به عملکردجابجایی[2] سازی است که به عنوان ساده ترین نوع رمزنگاری مطرح می شود، در اینجا هر یک از حروف یا علائم پیغام که با یکدیگر جابجا شده اند دوباره توسط گیرنده پیغام رمز گشایی می شود.

مثلاً در نمونه زیرپیغام ارسالی در تکنیک های سنتی با عملکرد جابجاسازی رمزنگاری شده است:

help me ⟶ ehpl em

نوع دیگر تکنیک رمز نگاری سنتی با عملکرد جانشین سازی[3] است یعنی هر یک از حروف یا علائم پیغام به شکل ویژه ای که برای گیرنده پیغام قابل درک باشد تغییراتی داده شود.

مانند:

fly a once ⟶ gmz bu padf

---

[1] Cryptography

[2] Transposition

جولیوس سزار متون رمزی در تکنیک جابجاسازی را طول لشکرکشی نظامی اش مورد استفاده قرار می داد.

[3] Substitution

نمونه دیگر از رمزنگاری در تکنیک جانشین سازی می توان به رمزنگاری مسیحیان در متون مذهبی از کتابشان را نام برد

تکنیک های رمزنگاری مدرن در اویل قرن بیستم به همراه چندین شیوه و روش رمز گذاری و رمز گشایی ریاضی اختراع شد؛ مشهورترین آنها ماشین اینگما[1] بود. این ماشین توسط آلمان ها در جنگ جهانی دوم استفاده شد.

پیشرفت رایانه های دیجیتالی و الکترونیکی بعد از جنگ جهانی دوم رمز نگاری بسیار پیچیده تر را امکان پذیر نمود؛ که بسیاری از رمز نگاری های رایانه ای می تواند در رشته هایی از بیت های باینری مشخص شوند، رایانه ها حوزه های رمز نگاری را به صورت پیچیده تر مهیا ساخته اند، به وسیله این تکنیک های مدرن و پیشرفته امنیت و ایمنی کار رمزنگاری بر الگوریتم های پیچیده و مسائل محاسباتی بسیار مشکل و دیر حل شدنی تکیه دارد، که شکستن این گونه رمزنگاری مدرن کاری بس غیر مؤثر و نا کار آمد است و نیاز به تلاش بسیار زیادی دارد.

تحقیقات آکادمی در مورد رمزنگاری در اواسط دهه ۱۹۷۰ با پایه گذاری استاندارد رمزنگاری اطلاعات و الگوریتم RSA آغاز شد؛ از این پس رمز نگاری یک ابزار کاربردی در ارتباطات، شبکه های رایانه ای و امنیت رایانه ها محسوب می شد.

رمزنگاری به طور عمده قبل از اویل قرن بیستم با اُلگوهای زبان شناسی رابطه داشت وپس از آن تغییر نموده و بعد از آن رمزنگاری استفاده وسیعی از ریاضیات شامل جنبه های اطلاعاتی، محاسبات پیچیده، آمار و ترکیبات،جبر مطلق و تئوری اعداد را دارد.

امروزه تکنیک های رمزنگاری به گونه ای است که برای استراق سمع کنندگان، محدودیتی در علم و تکنولوژی و قدرت محاسباتی آنها در نظر می گیرند؛ بنابراین برای استراق سمع کنندگان علم ،تکنولوژی وقدرت محاسباتی نامحدود دارند، هیچ گونه تضمینی برای امنیت آن وجود ندارد؛ مهندسین علم رمزنگاری همواره سعی دارند فعّال تر و هوشمندتر از استراق سمع کنندگان باشند و تحقق این کار هنگامی صورت می گیرد که آنها استراق سمع کنندگان دارای علم و تکنولوژی نامحدود را به مبارزه بطلبند. در اینصورت بهترین روش این است که در پی جستجوی رابطه ای بین رمزنگاری محرمانه و ایمن با علم فیزیک کوانتومی باشیم، که امروزه تحقیقات فراوانی توسط دانشمندان فیزیک کوانتومی در این زمینه صورت گرفته و با فرض بالا پروتکل های رمزنگاری بسیار ایمن را به دنیای اطلاعات محرمانه عرضه داشته اند.

---

[1] Enigma

۵-۲- رمزنگاری

رمزنگاری فرآیندی است که اجازه می دهد دو کاربر مرتبط با یک کانال ارتباطی ساختاری از اطلاعات محرمانه و مشترک را به وجود آورند. در نوشته های رمز شناسی، اطلاعاتی که باید رمزنگاری شوند به عنوان متن قابل درک[1] شناخته می شوند؛ پارامترهای ویژه بنام کلید رمز وجود دارند که به صورت رشته بیت های تصادفی هستند که باعث تغییر شکل متن قابل درک می شوند و آنها را به کد های محرمانه[2] تبدیل می کند؛ این کدها عموماً به شکل رشته بیت های است که می تواند به عنوان کد محرمانه برای روابط امنیتی مورد استفاده قرار می گیرد.درحقیقت رمزنگاری هنر تقسیم و ارتباط بین کدهای محرمانه و کلید رمز بین دو کاربر است، تجزیه و تحلیل این رمزها هنر شکستن آنها می باشد. رمز شناسی ترکیبی از آن دو می باشد.

امروزه رمزنگاری تقریباً منحصر به رمزگذاری ورمزگشایی است. رمزگذاری یعنی فرآیند تبدیل اطلاعات مثلاً یک متن قابل درک به یک متن رمزی غیر قابل خواندن و رمزگشایی یعنی فرآیند برگرداندن اطلاعات از حالت متن رمزی است. رمزنگاری دارای دو الگوریتم است یکی برای رمز گذاری ودیگری برای رمزگشایی که این الگوریتم ها طوری طراحی شده اند که اطلاعات رابدون هیچ گونه کار اضافی رمزگذاری ورمزگشایی می کنند. در اصل امنیت یک متن رمزگذاری شده بستگی به محرمانه بودن روش کار رمزگذاری و رمزگشایی دارد، درهر صورت امروزه کاراکترهای رمزگذاری شده از الگوریتم هایی برای رمزگذاری و رمزگشایی مورد استفاده قرار می گیرد که این الگوریتم ها می تواند بدون به مخاطره انداختن امنیت رمزنگاری در دسترس عموم قرار گیرد. با تعریف الگوریتم مناسب به همراه کلید رمز و متن قابل درک (پیغام) می توان آنها را به کدهای رمز (متن رمزگذاری شده)تبدیل نمود که این دقیقاً یک فرآیند رمز گذاری است؛ بنابراین با تعریف الگوریتم مناسب دیگر این متن رمزگذاری شده به وسیله کلید رمز، رمزگشایی نمود و پیغام را دریافت؛رمزنگاری ضرورتاً راجع به سه نفر است:

آلیس که می خواهد پیغامی محرمانه، بدون اطلاع هر استراق سمع کننده ای مانند ایو به شخصی به نام باب برساند.

---

[1] Plaintext
[2] Cipher

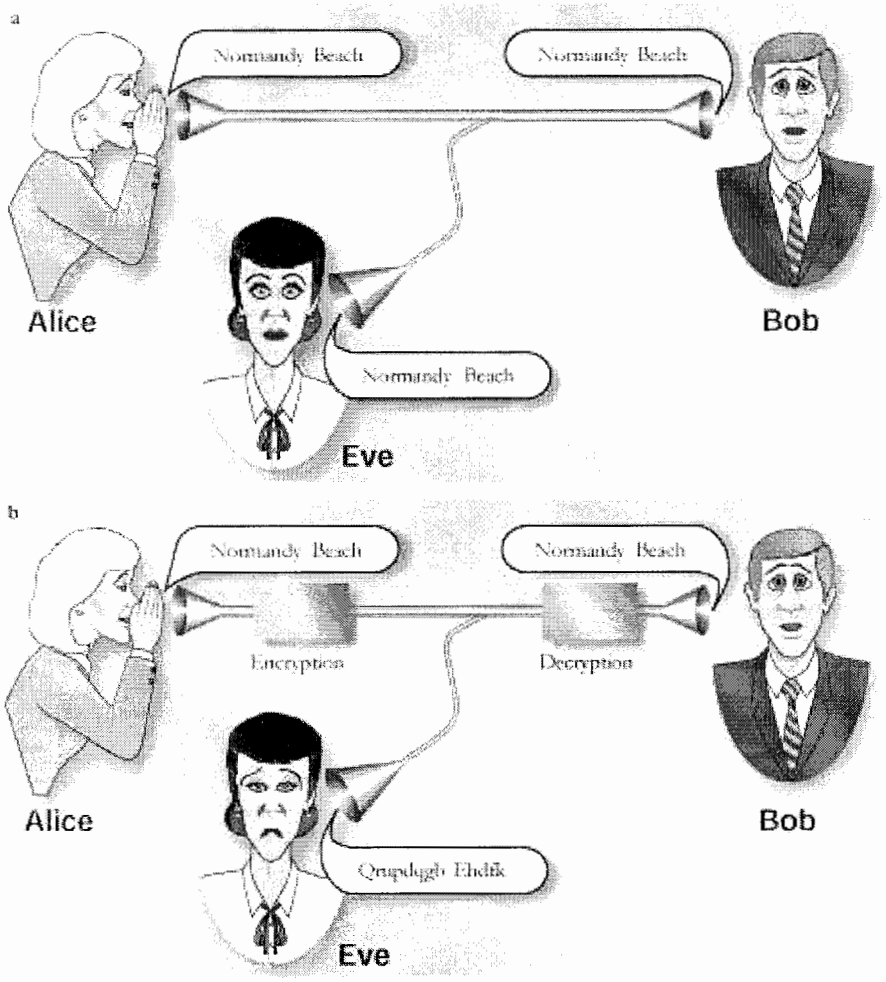
در این صورت نیاز به این است کـه آلـیس پیغـام را توسـط یـک کلیـد رمـز و الگـوریتم مناسـب رمزگذاری کند و برای باب بفرستد.

رمز گذاری C= Algorithms (M+K)

و باب با استفاده از الگوریتم مناسب دیگر و داشتن کلید رمز که قبلاً از طریـق یـک کانـال کـاملاً خصوصی، توسط آلیس به باب ارسال شده است و متن رمزی آن را رمزگشایی می کند و سـرانجام به صورت پیغام دریافت می نماید.

رمز گشایی

M=Algorithms (C+K)



شکل(۵-۱): پروتکل رمزنگاری کلاسیکی امن و نا امن

در این صورت ایو با استراق سمع در کانال عمومی و مشاهده متن رمزگذاری شده، اطلاعات قابل فهم دریافت نخواهد کرد. شکل (۵-۱)

در چنین سیستمهای متداول و منظم آلیس و باب یک کلید رمز را مورد استفاده قرار مـی دهنـد، که به صورت بیت های تصادفی است که آلیس را قـادر بـه رمزگـذاری پیغـام، و بـاب را قـادر بـه رمزگشایی متن رمزی می نماید.

بعد از آنکه تمام مراحل کار رمزنگاری به صورت محرمانه توسط آلیس و باب انجام شد، مهمتـرین مسئله امنیت یک رمزنگاری، محرمانه بودن کلید رمز است. و بایستی همواره در جستجوی روشـی باشیم که کلید رمز محرمانه بین دو کاربر مجاز (آلیس و باب) مورد توافق قرار گیرد. زیرا اگر کلید رمز به هر طریقی توسط ایو با فرض داشتن علم و تکنولوژی بالا و قابل دسـترس بـودن الگـوریتم های رمزگشایی، امنیت رمزنگاری زیر سؤال خواهد رفت؛ بنابراین کلید رمز بایـد در روشـی کـاملاً محرمانه که کار و نقشه استراق سمع کننده را خنثی می کند بـین دو کـاربر منتقـل شـود و ایـن کاری بسیار مشکل خواهد بود.

در نوشته های رمزشناسی این مسئله بـه عنـوان توزیـع کلیـد رمـز محرمانـه مطـرح مـی شـود و روش های گوناگونی در این زمینه به عنوان پروتکل بیان شده است.

در شکل زیر طرحی از رمزنگاری نشان داده شده است که توزیع کلید کوانتومی از طریق یک کانال کاملاً خصوصی بین دو کاربر منتقل می شود[۱۸،۹،۸،۱].

۵-۲-۱- توزیع کلید رمز محرمانه

اصول امنیت و ایمنی یک متن رمزگذاری شده بستگی به میزان محرمانه بـودن کامـلِ شـیوه رمزگذاری و رمزگشایی دارد؛ به هر حال امـروزه مـا از کلیـدهای رمـز اسـتفاده مـی کنـیم و نیـز می توانیم هر کدام از الگوریتم های مربوط به رمزگذاری و رمزگشایی را بدون بـه خطـر انـداختن امنیت رمزنگاری آشکار کنیم. در چنین حالتی کلیدهای رمز که یـک گـروه از پارامترهـای خـاص هستند و به همراه متن قابل درک به عنوان ورودی الگوریتم رمزنگاری می باشند. و نیز کلید رمـز به همراه پیام رمزی به عنوان ورودی به الگوریتم رمزگشایی فراهم آورده می شوند. ایـن الگـوریتم های رمزگذاری و رمزگشایی آشکارا در یک کانال عمومی معرفـی شـده، هـستند. در ایـن صـورت امنیت پیام رمزی کاملاً وابسته به میزان سری بودن کلید رمز خواهد بود. این کلیدها مـی بایـست

مرکب از بیت های انتخاب شده بدون ترتیب و تصادفی باشد. که به طـور کـافی رشـته طـویلی از بیت ها را ایجاد می کند.

هر گاه این کلید رمز پایه گذاری شده در یک کانال عمومی پی در پی ارسال شود در مقابل استراق سمع آسیب پذیر است. بنابراین بایستی مراحل ارتباطی از یک کانال کـاملاً قابـل اعتمـاد و بـسیار ایمن مورد استفاده قرار گیرد. این کار بسیار مشکل است، در اصل هر توزیع کلیـد رمـز کلاسـیکی هنگامی که بین دو کاربر منتقل می شود؛ تضمینی برای امنیت این کلید رمز در مقابل تهاجمـات استراق سمع کنندگان وجود ندارد. دانشمندان بخصوص ریاضی دانان تلاش بسیار زیادی در جهت حل این مسئله در توزیع کلید رمز محرمانه کرده اند.

در دهه ۱۹۷۰ یک دستاورد ریاضیاتیِ هوشمندانه به شکل سیستم های کلید رمز عمومی به منصه ظهور در آمد، در این سیستم ها کاربران نیاز به این داشتند که بر سر یک کلید رمز محرمانه قبـل از ارسال پیام به توافق برسند.

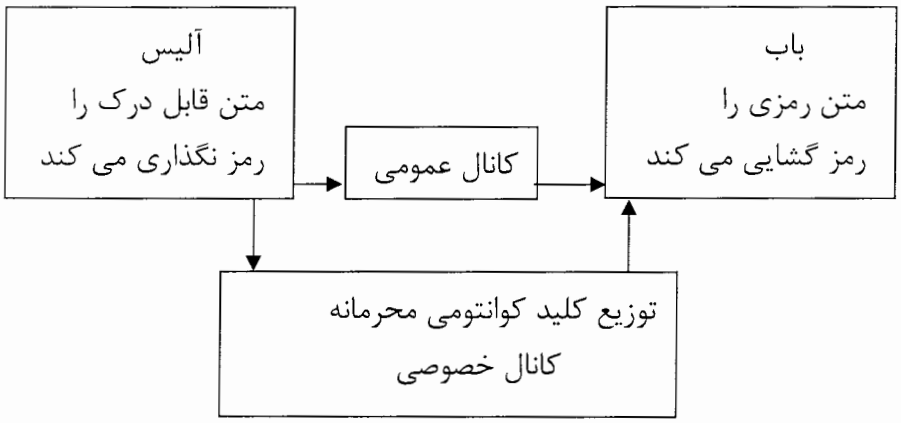
RSA مشهورترین پیام رمز کلید عمومی است، امنیتش را از مسئله تجزیه اعداد بزرگ بـه عوامـل اول بدست می آورد. با توجه به آنکه ریاضی دانان و دانـشمندان علـوم رایانـه توسـط شـیوه هـای هوشمندانه و سریع در زمینه تجزیه اعداد صحیح بزرگ به عامل های اول را نمی توان بسیار سریع انجام دهند و نیز علم و دانش و تکنولوژی استراق سمع کنندگان امروزی قادر به حـل سـریع ایـن مسائل مشکل ریاضی نیستند، امنیت این کلید توزیع عمومی در حال حاضر قابل قبول و در مراحل انجام کار می باشد. اگر شیوه های هوشمندانه و سریع در زمینه تجزیه اعداد صحیح بزرگ به عامل های اول وجود داشته باشد مانند رایانه های کونتومی که می تواند خیلی سریع تـر از رایانـه هـای کلاسیکی این عمل انجام دهنـد، در ایـن صـورت امنیـت و محرمیـت و آزادی عمـل سیـستمهای رمزنگاری کلید رمز عمومی خیلی زود از میان می رود[۹،۱].

۵-۳- رمزنگاری کوانتومی

از ویژگی های مهم رایانه های کوانتومی، تجزیه و تحلیل رمزنگاری است. زمانی که رایانه های کوانتومی ساخته شود بسیاری از پیامهای سرّی و محرمانه و کلیدهای رمـز عمـلاً در یـک معنـا و مفهوم به صورت ناامن و غیر ایمن مبدل می شوند؛ برای مثال هر پیام RSA رمزنگاری شـده کـه

امروزه ضبط و گزارش می شود، بعد از آنکه اولین ماشین تجزیه و تحلیل کوانتومی روشن گردد تبدیل به پیام قابل خواندن می شود. در این صورت RSA نمی تواند به طور ایمن جهت انتقال هرگونه اطلاعاتی که نیاز به سرّی و محرمانه بودن دارند مورد استفاده قرار گیرد[۱].

امروزه اطمینان و اعتماد در جریان ها آهسته که وابسته به تکنولوژی امروزی است امنیت موجود در سیستم RSA را تأمین می کند و تحت پوشش خود قرار می دهد. خوشبختانه با وجود اینکه رایانه کوانتومی رمز نگاری امروزی را محیطی ناامن و غیر ایمن تبدیل می کند ولی خود نیز پروتکل های رمز نگاری کوانتومی بسیار امن را به جهان اطلاعات عرضه می دارد. شکل(۵-۶) [۱۶،۱۵،۱۰،۲،۱]



شکل (۵-۲): طرح پروتکل رمزنگاری کوانتومی محرمانه

۵-۳-۱- تاریخچه رمزنگاری کوانتومی

رمزنگاری کوانتومی متدها و روش های جدیدی را در مورد ارتباط ایمن عرضه می دارد که مورد تهدید قدرت رایانه های کوانتومی قرار نمی دهد. بر خلاف تمام رمزنگاری کلاسیکی، این رمزنگاری به جای اینکه برای علم و تکنولوژی استراق سمع کنندگان محدودیتی قائل شود در عوض برای او دانش و تکنولوژی و تلاش بیش از اندازه و نامحدود در نظر می گیرد و اطمینان از امنیت رمزنگاری تکیه بر قوانین و تئوری فیزیکی می داند. رمزنگاری کوانتومی توسط استفان ویزنر[۱] کشف شد؛ پس در دانشگاه کلمبیا در شهر نیویرک، وی در اوایل دهه ۱۹۷۰ مفهوم

[۱] Stephen wiesner

کدگذاری شکل های متفاوت کوانتومی را معرفی کرد. او چگونگی نگهداری یا انتقال دو پیام را با کدگذاری آنها به دو شکل متفاوت و قابل مشاهده به نمایش گذاشت؛ از جمله آنها می توان به پلاریزه شدن مدور و خطی نور نام برد؛ به طوری که یکی از آنها نه هر دو ممکن است دریافت شود و رمزگشایی گردد. او ایده اش را به همراه یک طرح برای یادداشتهای بانکی غیر قابل تقلب به تصویر کشید. یک دهه بعد و پس از تحقیقات و فعالیت های متعدد بر سر این پروژه افرادی چون بنت[1] از مرکز تحقیقات وستون و براسارد[2] از دانشگاه مونترال یک روش را به منظور ایجاد ارتباط ایمن برای شکل های متفاوت قابل مشاهده ویزنر پیشنهاد دادند. در سال ۱۹۹۰ به طور مستقل و مقدماتی اِکرت[3] و سپس دانشگاه آکسورد یک دستآورد متفاوت از رمزنگاری کوانتومی بر اساس ارتباط کوانتومی ویژه و غیر عادی شناخته شده مانند در هم تنیدگی کوانتومی گسترش و توسعه دادند[۹].

۵-۴- امنیت رمزنگاری کوانتومی در مقابل تهاجمات استراق سمع

رمزنگاری کوانتومی می تواند انتظار سیستمهای ارتباطی امن را برآورده کند. به کمک تئوری های کوانتومی می توان کلید رمز را با امنیت صددرصد بین دو کاربر مبادله کرد و هر گونه شنود احتمالی یا استراق سمع را توسط کاربرهای غیر مجاز کشف نمود.

رایانه های کوانتومی در صورت ساخته شدن می توانند بهترین و امن ترین سیستمهای رمزنگاری را ایجاد کنند و باعث می شوند هر گونه استراق سمع در سیستمهای رمزنگاری کوانتومی خنثی شود. با توجه به اصل عدم قطعیت، اشاره دارد به این که هر وقت و در هر صورت یک کمیت با دقت بالا یا متوسط و یا پایین اندازه گیری شود باعث پارازیت[4] به کمیت مزدوج (همیوغ مختلط) آن اضافه می شود. یعنی این کمیت های مزدوج در اثر اندازه گیری آشفته می شوند، از این رو در اثر اندازه گیری بر روی کمیتهای کوانتومی پارازیتی از خود به جای می گذارد که باعث آشکارشدن استراق سمع و یا اندازه گیری غیر مجاز می شود[۹].

---

[1] Charles H.Bennett
[2] Gilles Brassard
[3] Artur Ekert
[4] noise

۵-۴-۱- بررسی امنیت در توزیع کلید کوانتومی درذرات با حالت کوانتومی S_x و S_z :

فرض کنیم قرار است آلیس و باب حالت اسپینی ذرات را مورد اندازه گیری قرار می دهند، به صورتی که آلیس فرستنده ذرات (الکترون) در حالت کوانتومی اسپینی باشد.

آلیس به طور رندمی حالت های کوانتومی اسپینی ذرات $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_x + |1\rangle_x)$ یا $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_z + |1\rangle_z)$ را با احتمال مساوی به سوی باب می فرستد به صورتی که قبل از فرستادن کیو بیت به طور رندمی بر روی پایه های اندازه گیریش S_x و S_z انجام می دهد و نیز باب به طور رندمی پایه های اندازه گیری S_x و S_z را برای سنجش حالت های کوانتومی فرستاده شده آلیس انتخاب می کند.

	آلیس	باب
$\|0\rangle_z$	$S_z\left[\frac{1}{\sqrt{2}}(\|0\rangle_z + \|1\rangle_z)\right] = \|0\rangle_z \ldots\ldots E_1 \ldots\ldots S_z\|0\rangle_z$	$\|0\rangle_z$
$\|1\rangle_z$	$S_z\left[\frac{1}{\sqrt{2}}(\|0\rangle_z + \|1\rangle_z)\right] = \|1\rangle_z \ldots\ldots E_2 \ldots\ldots S_x\|1\rangle_z$	$\%50\|1\rangle_x, \%50\|0\rangle_x$
$\|0\rangle_x$	$S_x\left[\frac{1}{\sqrt{2}}(\|0\rangle_z + \|1\rangle_z)\right] = \|0\rangle_x \ldots\ldots E_3 \ldots\ldots S_x\|0\rangle_x$	$\|0\rangle_x$
$\|1\rangle_x$	$S_x\left[\frac{1}{\sqrt{2}}(\|0\rangle_z + \|1\rangle_z)\right] = \|1\rangle_x \ldots\ldots E_4 \ldots\ldots S_z\|1\rangle_x$	$\%50\|1\rangle_z, \%50\|0\rangle_z$

طبق اصول موضوعه مکانیک کوانتومی احتمال اینکه باب کیو بیت $|0\rangle_z$ را در رویداد (۱) بدست آورد برابر یک است زیرا با اندازه گیری آلیس حالت کوانتومی اسپینی ذره به $|\psi\rangle = |0\rangle_z$ فروپاشی شده است. بنابراین می توان گفت که اگر آلیس و باب به طور رندمی پایه های اندازه گیریشان یکسان انتخاب شود آنها در کیو بیت هایی به صورت توافقی با هم مشترک می شوند می توان آنرا به عنوان توزیع کلید رمز بین دو کاربر در نظر گرفت.

انتخاب پایه های رندمی اندازه گیری آلیس و باب برای امنیت این توزیع کلید کوانتـومی ضـروری است، ایو نمی داند که پایه های اندازه گیریی که آلیس در نظـر گرفتـه اسـت چیـست بنـابراین او مجبور است که پایه های اندازه گیریش را به طور رندمی S_x و S_z انتخاب کند در این صـورت دو حالت زیر حتماً اتفاق می افتد:

۱) اگر پایه اندازگیری ایو با پایه اندازگیری آلیس یکسان باشد.

۲) اگر پایه اندازگیری ایو با پایه اندازگیری آلیس یکسان نباشد.

نویز در حالت دوم به صورت واضح در رویدادهای (۱) و (۳) مشاهده می شود:

باب آلیس

$$|0\rangle_z \qquad S_z\left[\frac{1}{\sqrt{2}}\left(|0\rangle_z+|1\rangle_z\right)\right]=|0\rangle_z \ldots\ldots\ldots E_1 \ldots\ldots\ldots$$

$$S_x|0\rangle_z=\left[\frac{1}{\sqrt{2}}\left(|0\rangle_x+|1\rangle_x\right)\right],\%50|0\rangle_x,\%50|1\rangle_x \ldots\ldots\ldots S_z|0\rangle_z \qquad \%50|1\rangle_z,\%50|0\rangle_z$$

یعنی ایو با استراق سمع در این رویداد کیو بیت اسپینی ذره را از پایه z به پایه x تبدیل می کنـد با استفاده از اصل عدم قطعیت $(\Delta S_x)_\psi$ مقدار دقیقی نخواهد داشت.

$$[S_x,S_z]=-i\hbar S_Y \qquad , \qquad (\Delta S_x)_\psi(\Delta S_z)_\psi \geq \frac{1}{2}\langle S_y\rangle \qquad (۱-۵)$$

این نویز ایجاد شده هنگامی که باب و آلیس بعضی از نتایجی که پایه های اندازه گیریشان یکـسان است را اعلام کنند آشکار می شود.

از این رو کدگذاری بیت ها در متغیرهای مزدوج با توجه به قوانین و تئـوری هـای اولیـه مکانیـک کوانتومی هر اندازه گیری با یک نویز یا پارازیت قابل ضمانت می باشد. مخـصوصاً اگریـک اسـتراق سمع کننده غیر مجاز سعی در استخراج اطلاعات از چنین کانـال کوانتـومی باشـد. در آن صـورت

ضرورتاً رابطه بیت های ورودی و خروجی را کاهش می دهد، بنابراین کاربر های قانونی می توانند حضور هر استراق سمع کننده را ردیابی کنند.

کانال کوانتومی برای فرستادن کلید رمز حامل رشته بیت های رندومی و تصادفی بدون اطلاعات استفاده می شوند. از این رو آلیس و باب به عنوان دو کاربر مجاز می توانند توسط رابطه کامل بین بیت هایشان که به یکدیگر منتقل شده متوجه شوند و کنترل نمایند که آیا این کلید محرمانه است یا خیر؟ و اگر استراق سمع صورت گیرد با ایجاد نویز را بطه منطقی بین بیت ها وجود نخواهد داشت. تا تمام این مراحل قبل از آنکه کلید رمز بین دو کاربر به صورت ایمن مبادله نشود آن کلید برای کدگذاری پیام استفاده نمی شود.

۵-۵- ایده های اساسی در رمزنگاری کوانتومی

در حین اینکه پیام رمزی کلاسیکی، تکنیک های ریاضیاتی متعددی را به منظور محدود کردن استراق سمع کنندگان از دریافتن محتویات پیام رمزگذاری شده به خدمت می گیرند، در مکانیک کوانتومی امنیت این اطلاعات توسط قوانین فیزیکی مورد حمایت قرارمی گیرد. در پیام های رمزی کلاسیکی ایمنی مطلق اطلاعات تضمین نمی گردد. اصل عدم قطعیت هایزنبرگ و در هم تنیدگی حالت های کوانتومی می تواند در سیستم های ارتباطی ایمن مورد استفاده قرار گیرد؛ اغلب به عنوان پیام رمزی کوانتومی ارجاع داده می شود. ارتباطات کوانتومی محرمانه معنایی را برای دو کاربر فراهم می کند و باعث تبادل کلید رمز بر فراز یک کانال خصوصی همراه با ایمنی کامل می شود.

حداقل سه نوع سیستم مهم رمزنگاری کوانتومی برای توزیع کلید رمز محرمانه وجود دارد. آنها عبارتند از:

الف) سیستم های پیام رمز همراه با رمزنگاری براساس دو مشاهده غیر مکرر که توسط ویزنر در سال ۱۹۷۰ و هچنین توسط بنت وبراسارد درسال ۱۹۸۴ پیشنهاد گردید[۲۰،۱۹].

ب) سیستم های پیام رمز همراه با رمزنگاری انجام شده بر روی جفت های کوانتومی و تئوری معادله بِل که توسط ایکرت در سال ۱۹۹۰ پیشنهاد گردی[۱۸].

پ) سیستم های پیام رمز همراه با رمزنگاری بر اساس بردارهای حالت غیر راست هنجار[1] گه توسط بنت در سال ۱۹۹۲ پیشنهاد گردید[۱۷].

۵-۵-۱- سیستم های پیام رمز همراه با رمزنگاری کوانتومی بر اساس ایده ویزنر

این سیستم های پیام رمز کوانتومی در بر دارنده یک فرستنده (آلیس) و یک گیرنده (باب) است.ارسال کننده از فرستنده ای(ماشینی) برای ارسال فوتون ها در یکی از حالت های قطبیدگی استفاده کند؛مانند: ۰، ۴۵، ۹۰، ۱۳۵ درجه. یک دریافت کننده در انتهای دیگر از گیرنده (ماشین) به منظور اندازه گیری قطبیدگی استفاده می کند. بر طبق قوانین مکانیک کوانتومی این گیرنده می تواند قطبش های مستقم الخط (۰ و ۹۰) را تشخیص دهد، یا اینکه گیرنده می تواند به سرعت جهت تشخیص دادن قطبش های قطری (۴۵ و ۱۳۵) دوباره تنظیم کند. این گیرنده هرگز نمی تواند هر دو نوع این قطبش ها را با هم اندازه گیری کند.

توزیع کلید رمز در این ایده چندین مرحله زیر را ملزم می دارد:

۱) ارسال کننده ، فوتون ها را در یکی از چهار قطبش هایی که بطور اتفاقی انتخاب می شود ارسال می کند.

۲)برای هر فوتون ورودی، گیرنده بطور اتفاقی نوع اندازه گیری را انتخاب می کند. یعنی پایه های اندازه گیری قطبش نوع مستقیم الخط یا نوع اُریب (قطری).

۳)گیرنده نتایج مورد نظر را ضبط وثبت می کند، امّا آنرا به صورت سرّی و محرمانه نگه می دارد.

۴)بطور پی در پی این گیرنده نوع قطبش اندازه گیری خود را آشکار و اعلام می کند، اما نتایج آن را همچنان محرمانه نگه می دارد.

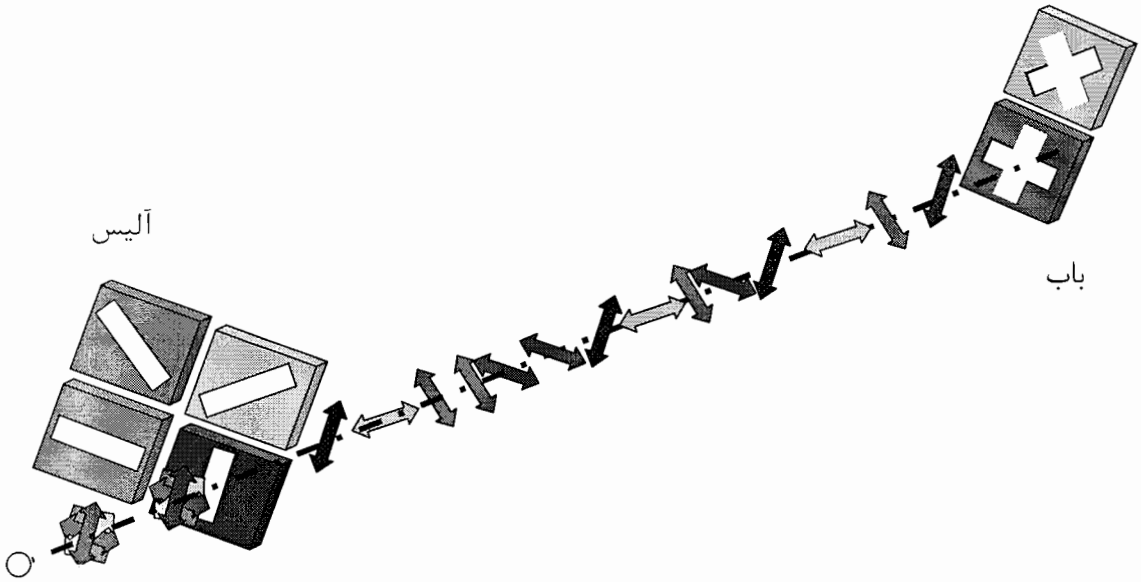
۵)ارسال کننده فوتون به گیرنده که فوتون را، مورد سنجش قرار می دهد، اطلاع می دهد که کدام نوع از اندازه گیری هایش موافق با نوع قطبش ارسالی انتخاب شده است.

۶)اعلام بعضی از نتایج از قطبش های که بطور صحیح بین دو کاربر به توافق رسیده، برای حفظ امنیت این پروتکل که آیا استراق سمع صورت گرفته است یا خیر؟

---

[1] Orthogonal

۷)این دو کاربر مجاز (فرستنده و گیرنده) نتایج اندازه گیری اعلام نشده فوتون های را که پایه های اندازه گیری آنها بطور یکسان و موافق با یکدیگر انتخاب شده اند به عنوان کلید رمز مشترک بین دو کاربر مجاز می باشد.



شکل(۵-۳): پرتوکل توزیع کلید کوانتومی بر اساس ایده ویزنر

در این ایده برای هر یک از قطبش ها کیو بیت زیر راتعریف می کنیم:

فوتون با قطبش مستقیم الخط ۰ درجه $|0\rangle_d$

فوتون با قطبش مستقیم الخط ۹۰ درجه $|1\rangle_d$

فوتون با قطبش قطری ۴۵ درجه $|0\rangle_o$

فوتون با قطبش قطری ۱۳۵ درجه $|0\rangle_o$

پایه های اندازه گیری آلیس و باب را می توان توسط دو ماتریس زیر نمایش داد:

$$\hat{d} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad , \quad \hat{o} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad (۲-۵)$$

d^0	$\|0\rangle_d$	E_1	$d^{0,90}\|0\rangle_d$
d^{90}	$\|1\rangle_d$	E_2	$d^{0,90}\|1\rangle_d$
d^0	$\|0\rangle_d$	E_3	$o^{45,135}\,\%50\|0\rangle_o,\%50\|1\rangle_o$
o^{45}	$\|1\rangle_o$	E_4	$d^{0,90}\,\%50\|0\rangle_d,\%50\|1\rangle_d$
o^{135}	$\|1\rangle_o$	E_5	$o^{45,135}\|1\rangle_o$
o^{135}	$\|1\rangle_o$	E_6	$d^{90}\,\%50\|0\rangle_d,\%50\|1\rangle_d$

رابطه زیر همواره کیوبیت های برقرار است:

$$|1\rangle_O = \frac{1}{\sqrt{2}}\left(|0\rangle_d - |1\rangle_d\right) \quad , \quad |0\rangle_O = \frac{1}{\sqrt{2}}\left(|0\rangle_d + |1\rangle_d\right) \tag{۳-۵}$$

بررسی رویداد (۱):

منبع فوتونی با قطبش دلخواه به سوی آلیس می فرستد و آلیس به طور رندمی بر روی یکی از چهار پایه قطبش گفته شده بالا اندازه گیری انجام می دهد که در نمونه یک آلیس پایه اندازه گیریش قطبش مستقم الخط با زاویه صفر درجه است و نتیجه کیوبیت مطابق زیراست:

$$\hat{d}|\psi\rangle = |0\rangle_d \tag{۴-۵}$$

در این نمونه باب همان پایه اندازه گیری را در نظر گرفته است بنابراین داریم:

$$\hat{d}|0\rangle_d = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle_d \tag{۵-۵}$$

بررسی رویداد (۳):

در این رویداد پایه های اندازه گیری آلیس و باب با یکدیگر متفاوت است با این توضیح که مانند رویداد (۱) آلیس ابتدا پایه اندازه گیریش قطبش مستقم الخط با زاویه صفر درجه کیو بیت $|0\rangle_d$ را بدست می آورد؛سپس باب با انتخاب پایه اندازه گیری قطبش قطری ۴۵و۱۳۵ درجه نتیجه زیر حاصل می شود.

$$\hat{o}|0\rangle_d = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle_o + |1\rangle_o\right) \tag{۶-۵}$$

این رویداد در توزیع کلید کوانتومی نقش خاصی را بر عهده ندارند و خود به خود از پروتکل توزیع کلید کوانتومی حذف می شوند.

همان گونه که مشاهده می شود در رویداد های (۱) و(۲) و(۵) که پایه های اندازه گیری آلیس و باب به طور رندمی یکسان انتخاب شده اند و نتایج اندازه گیری حاصل از آنها را می توان به عنوان توزیع کلید رمز مورد استفاده قرار گیرد، به شرط آنکه امنیت این کلید رمز کاملاً تضمین شود.

بررسی امنیت در مقابل تهاجمات استراق سمع ایو در رویداد (۱):

رویداد یک به علت رندمی بودن پایه های اندازه گیری قطبش مستقیم الخط و اُریب (قطری) به طور یقین در پرتوکل توزیع کلید کوانتومی مشاهده می شود، در صورتی که ایو بتواند

در این گونه رویدادها استراق سمع کند، آلیس وباب با اعلام بعـضی از نتـایج ایـن رویـداد پـی بـه استراق سمع ایو می برند. در زیر محاسباتی را انجام می دهیم که نویز ایجـاد شـده توسـط ایـو در رویداد (۱) قابل مشاهده است؛ اگرایو در رویداد (۱) استراق سمع انجام دهد و پایه اندازه گیریش با پایهٔ اندازه گیری آلیس یکسان نباشد،همان روابطی که در رویداد (۳) برای باب بدست آمده بـرای ایو حاصل می شود یعنی کیوبیت ها حاصل از اندازه گیری ایو $\frac{1}{\sqrt{2}}\left(|0\rangle_o + |1\rangle_o\right)$ می شود.

اگر ایو استراق سمع انجام ندهد باب با توجه آشکار بودن پایه های اندازه گیری خود و آلیس و بر طبق اصول تئوری کوانتومی می بایست کیوبیت $|0\rangle_d$ به طور یقین بدست آورد. حال با محاسبات ریاضی نشان می دهیم که نویز استراق سمع ایو در کیوبیت حاصـل از انـدازه گیـری بـاب آشـکار می شود و دو کاربر مجاز چگونه پی آن می برند.

$$\hat{d}\frac{1}{\sqrt{2}}\left(|0\rangle_o + |1\rangle_o\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}_o = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}_d$$
$$= \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix}_d + \begin{pmatrix}0\\-1\end{pmatrix}_d\right] = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix}_d - \begin{pmatrix}0\\1\end{pmatrix}_d\right] = \frac{1}{\sqrt{2}}\left(|0\rangle_d - |1\rangle_d\right) \qquad (۷-۵)$$

یعنی در این رویداد احتمال ۵۰٪ وجود دارد که باب کیوبیت $|0\rangle_d$ را بدست نیاورد در صورتی کـه چنین اتفاقی رخ دهد با توجه به مرحله (۶) که دو کاربر با اعلام بعضی از نتایجی کـه پایـه انـدازه گیری یکسانی دارند می توانند به نویز ایجاد شده در استراق سمع ایو پی ببرند.

پس از بررسی امنیت این پرتوکل نتایج اندازه گیریهای اعلام نشده در پایه های یکسان دو کاربر را می توان به صورت بیت هایی از صفر و یک در کلید رمز کد بندی نمود؛ در نتیجـه آن کلیـد رمـز شامل رشته هایی از صفر و یک می شود. امنیت این پروتکل در صورت استراق سـمع محـدود بـه معرفی خطا و اشتباه در نتایج اندازه گیری ها وکلید رمز می شود؛ زیرا با اندازه گیری استراق سمع کننده ونویز ایجاد شده در نوع قطبش هر فوتون به دو کاربر مجاز امکان این را می دهد که از استراق سمع کاربر غیر مجاز با خبر شوند.بنابراین هر کدام از فوتون های که بطور پی درپی بسوی گیرنده فرستاده می شود، به استراق سمع کننده اجازه دستیابی به مقادیر واضح مشاهده پذیر غیر مکرر را نمی دهد. دو کاربر مجاز در یک کانال کوانتومی با نشان دادن رشته ای از بیت های کلیـد مبادله شده بطور تصادفی و بررسی میزان خطا و تحصیح آن به استراق سمع احتمالی انجام شـده

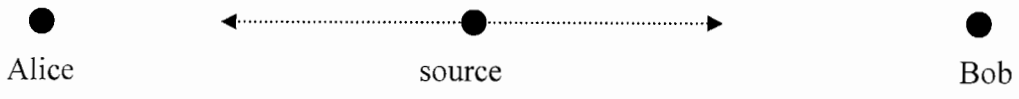
پی می برند. اگر چه نمی توان از فرآیند استراق سمع جلوگیری کرد، اما هرگز توسط استراق سمع کننده فریب خورده نمی شود. هر چه این فرآیندها پیچیده تر و حساس تر باشد تلاش استراق سمع کنندگان جهت گشودن این کانال مشکل تر خواهد بود.

زمانیکه ایمنی این کانال توسط استراق سمع کنندگان تهدید شود، دو کاربر مجاز برای توزیع کلید دوباره پروتکل را از ابتدا شروع به کار می کنند[۱،۷،۸،۱۰،۱۹] .

۵-۵-۲- پلارزاسیون فوتون بر اساس ایدهٔ بنت و براسارد

این طرح و برنامه رمزنگاری پالس های نوری پلاریزه شده که یک فوتون به همراه هر پالس استفاده می شود. دو نوع قطبش یا پلاریزه را در نظر گرفته می شود؛ نوع خطی و مدّور. قطبش خطی می تواند افقی یا عمودی باشد و قطبش مدّور می تواند خمیده در جهت راستگرد یا چپ گرد باشد؛ هر قطبش مربوط به یک فوتون منفرد می تواند یک بیت اطلاعات را رمزگذاری کند. برای مثال با قطبش عمودی برای کیو بیت $|0\rangle$ و قطبش افقی برای کیو بیت $|1\rangle$ یا قطبش چپ گرد برای کیو بیت $|0\rangle$ و قطبش راست گرد برای کیو بیت $|1\rangle$ مناسب می باشد. به منظور ایجاد یک کلید رمز اتفاقی و بدون ترتیب، آلیس باید هم قطبش افقی و هم قطبش عمودی را با احتمال مساوی ارسال نماید؛برای حفظ امنیت این رمز نگاری از استراق سمع ایو، همچنین آلیس باید بطور اتفاقی از قطبش متناوب مدوّر استفاده کند؛همین طور باید به طور رندومی فوتون ها را بین قطبش های مدوّر راست گر و چپ گر انتخاب نماید[۹،۲۰]. بطور مشابه پروتکل توزیع کلید کوانتومی محرمانه BB84 با استفاده از ایده بالا علاوه بر پلاریزاسیون فوتون می توان برای حالت های درهم تنیده اسپینی که از طرف منبع تولید این حالت به ترتیب به سوی آلیس و باب فرستاده می شود و انها به طور رندمی روی پایه های X,Z اندازه گیری انجام می دهند بکار برد که این پروتکل براساس تئوری مکانیک کوانتومی بطور قابل اثبات ایمن می باشد[۱،۲،۱۰،۱۷].

$$|\Psi_i\rangle = \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right)$$



شکل(۵-۴): کیوبیت درهم تنیده از منبع به سوی دو کاربر فرستاده می شود.

۵-۵-۳- ایده اساسی سیستم های رمزنگاری برروی جفت های کوانتومی و تئوری بِل

این ایده توسط اِکرت برای یک رشته از جفت ذرّات درهم تنیده با اسپین $\frac{1}{2}$ ارائه شده است که هر عضوی از این جفت ذرّات توسط دو کاربر مجاز مانند آلیس و باب مورد سنجش و بررسی قرار خواهند گرفت. این طرح و برنامه توسط اسپکت و همکارانش به عمل در آزمایشگاه توسط جفت های در هم تنیده فوتون به جای ذرات با اسپین $\frac{1}{2}$ انجام شده است؛ که در هر 10ns یک جفت فوتون در کاهش اتمی کلسیم منتشر می شد[۱۲]. مانند فوتون های معروف انیشتین،پودولسکی و روزن که قطبش های آنها توسط دو گروه (کاربر)مورد اندازه گیری قرار می گیرد. همچنین این جفت های در هم تنیده می توانند توسط آلیس و باب یا بعضی از منابع جدا از آن دو مثل استراق سمع کننده (ایو) تولید و ارسال شود. استراق سمع کننده بر روی ارتباط دو کاربر مجاز نیاز به بررسی یک ذره (فوتون) برای دریافت سیگنال (علامت مبادله شده بین دو کاربر) می باشد، همچنین باید دوباره آنرا ارسال نماید یا اینکه ذره یا فوتونی را جایگزین آن کند که این کار را به منظور ناشناس باقی ماند حضورش انجام می دهد. به هر حال عمل بررسی یک ذره از جفت ذرّات در هم تنیده ارتباط کوانتومیش را با ذره دیگر خراب می کند. دو کاربر مجاز به آسانی می توانند با نویز ایجاد شده صحت و سقم این ارتباط کوانتومی را از روی آشکار سازی بعضی نتایج اندازه گیری هایشان و بکار بردن نامساوی بِل و بررسی آن توسط تئوری بِل در یک کانال عمومی (باز) تعیین کنند و به استراق سمع ایو پی ببرند.

این طرح به سه ویژگی حالت های در هم تنیده تکیه دارد:

۱) اول اینکه می توانیم حالت های در هم تنیده را ایجاد کنیم و آن را در اختیار آلیس و باب قرار دهیم تا ذرّات یا فوتون ها خود را مورد سنجش قرار دهند، خواه این ذرّات دارای هر نوع مؤلفه اسپینی یا قطبشی باشند.

۲) این حالت های در هم تنیده دارای یک ویژگی مهم هستند که در تئوری مکانیک کوانتومی به ناموضعیت معروف هستند؛ بطوری که هیچ آنالوگی در فیزیک کلاسیک ندارند؛ یعنی اندازه گیری آلیس به طور صریح اندازه گیری باب را قیاس در می آورد و برعکس. این باعث ارتباط قوی بین دو کاربر می شود.

۳) براساس تئوری بِل هر گونه تلاش در جهت استراق سمع توسط ایو، ارتباطات بین دو کاربرمجاز را که توسط آلیس و باب مورد بررسی قرار می گیرد ضعیف خواهد کرد. یعنی با استفاده از نتایج اندازه گیری رندومی توسط دو کاربر و به کار بردن نامساوی بِل و بررسی آنها با یکدیگر به نویز ایجاد شده در این پروتکل توسط استراق سمع پی برده می شود و جایی برای استراق سمع باقی نمی گذارد.

۵-۵-۲-۱- پروتکل های توزیع کلید کوانتومی بر اساس ایده اِکرت:

۱- دو کاربر مجاز آلیس و باب در حالت های کوانتومی جفت ذرات با اسپین $\frac{1}{2}$ در حالت منفرد مشترک یا سهیم می شوند که حاصل کیوبیت های در هم تنیده زیر است:

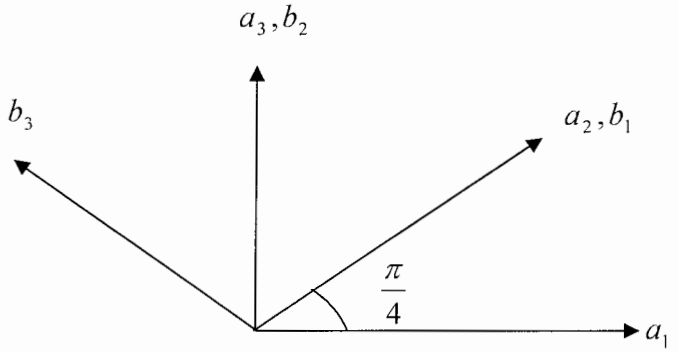
$$|\psi\rangle_i = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \qquad (۸-۵)$$

۲- این ذرات حامل کیوبیت های در هم تنیده به طور مجزا در امتداد محور z به سمت دو کاربر مجاز در یک کانال عمومی که امکان استراق سمع برای ایو به آسانی وجود دارد منتشر می شود.

۳- آلیس و باب بعد از اینکه ذرات از یکدیگر جدا شده اند اندازه گیریهای خود را در جهت مولفه های اسپینی در امتداد یکی از سه مسیر ارائه شده توسط بردارهای a_i و b_j $(i,j=1,2,3)$ در صحفه xy هستند که به طور عمود با خط مسیر ذرات قرار می گیرند. که هر کدام با زاویه ای در جهت ساعتگرد به شکل زیر است:

$$a_i : \phi_1{}^a = 0, \phi_2{}^a = \frac{\pi}{4}, \phi_3{}^a = \frac{\pi}{2} \quad ; \quad b_j : \phi_1{}^b = \frac{\pi}{4}, \phi_2{}^b = \frac{\pi}{2}, \phi_3{}^b = \frac{3\pi}{4}$$

b,a پایه های اندازه گیری آلیس و باب هستند زوایای ϕ از محور x اندازه گیری می شود شکل(۵-۵).



شکل (۵-۵): جهت پایه های اندازه گیری a_i, b_j در ایده توزیع کلید کوانتومی اِکرت

۴- کاربرهای مجاز پایه های اندازه گیریشان را به طور رندمی وابسته به هر یک از جفت ذرات وارد شده انتخاب می کنند؛هر اندازه گیری با فرض $\frac{\hbar}{2}=1$ می تواند دو مقدار ۱+ برای اسپین بالا و ۱- برای اسپین پایین به عنوان یک بیت از اطلاعات آشکار کند.

۵- پس از اندازه گیری دو کاربر جهت های پایه اندازه گیری که به صورت رندمی انتخاب شده است در یک کانال عمومی به اطلاع هم می رسانند.

۶- نتایج اندازه گیری پس از اعلام پایه های اندازه گیری به دو گروه تقسیم می شوند:

- گروه اول آن نتایجی هستند که دو کاربر مجاز از پایه های اندازه گیری در جهت های متفاوت استفاده نموده اند.
- گروه دوم آن نتایجی هستند که دو کاربر مجاز از پایه های اندازه گیری در جهت های یکسان استفاده نموده اند.

قبل از آنکه امنیت این پروتکل را مورد بررسی قرار دهیم کمیت $C(a_i,b_j)$ را به صورت زیر تعریف می کنیم:

$$C(a_i,b_j)=P_{++}(a_i,b_j)+P_{--}(a_i,b_j)-P_{+-}(a_i,b_j)-P_{-+}(a_i,b_j) \qquad (۱۰-۵)$$

این همان ضریب همبستگی(مقدار انتظاری حاصل از اندازه گیری دو کاربر مجاز) است که در فصل چهارم (۴-۴) به آن اشاره شده است؛ ضریب همبستگی حاصل از اندازه گیری انجام شده توسط آلیس در امتداد a_i و باب در امتداد b_i می باشد. در اینجا $P_{\pm\pm}(a_i,b_j)$ احتمال آن است که حاصل اندازه گیری باب در امتداد b_j، ±1 و برای آلیس در امتداد b_j ، ±1 باشد.

از طرفی همان طوری که بر طبق قوانین کوانتومی در فصل چهارم ثابت شد داریم :

$$C(a_i,b_j)=-a_i\cdot b_j \qquad (۱۱-۵)$$

برای مثال برای دو جفت از اندازه گیری با جهت های یکسان $(a_2,b_1;a_3,b_2)$ در تئوری مکانیک کوانتومی ضریب همبستگی نتایج بدست آمده توسط آلیس و باب به قرار فوق برابر است با:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

$$C(a_2,b_1) = P_{++}(a_2,b_1) + P_{--}(a_2,b_1) - P_{+-}(a_2,b_1) - P_{-+}(a_2,b_1)$$

$$C(a_2,b_1) = P_{+}(a_2)P_{+}(b_1) + P_{-}(a_2)P_{-}(b_1) - P_{+}(a_2)P_{-}(b_1) - P_{-}(a_2)P_{+}(b_1)$$

$$C(a_2,b_1) = \frac{1}{2}\times 0 + \frac{1}{2}\times 0 - \frac{1}{2}\times 1 - \frac{1}{2}\times 1 = -1$$

به طریق مشابه داریم:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

$$C(a_3,b_2) = P_{++}(a_3,b_2) + P_{--}(a_3,b_2) - P_{+-}(a_3,b_2) - P_{-+}(a_3,b_2)$$

$$C(a_3,b_2) = P_{+}(a_3)P_{+}(b_2) + P_{-}(a_3)P_{-}(b_2) - P_{+}(a_3)P_{-}(b_2) - P_{-}(a_3)P_{+}(b_2)$$

$$C(a_3,b_2) = \frac{1}{2}\times 0 + \frac{1}{2}\times 0 - \frac{1}{2}\times 1 - \frac{1}{2}\times 1 = -1$$

در اینجا $P_{+}(a_3), P_{+}(b_2)$ برای نمونه با محاسبات ریاضی بدست می آوریم:

$$a_3 = \hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad , \quad |0\rangle_z = \frac{1}{\sqrt{2}}\left(|0\rangle_y + i|1\rangle_y\right) \qquad (۱۲-۵)$$

$$a_3|\psi\rangle_i = \hat{Y}\otimes I\left(\frac{1}{\sqrt{2}}\left(|0\rangle_z|1\rangle_z - |1\rangle_z|0\rangle_z\right)\right) = \frac{1}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\left(|0\rangle_y + i|1\rangle_y\right)\otimes I|1\rangle_z$$

$$-\frac{1}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\left(|0\rangle_y - i|1\rangle_y\right)\otimes I|0\rangle_z = \frac{1}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} + i\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}\right)\otimes I|1\rangle_z$$

$$-\frac{1}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} - i\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}\right)\otimes I|0\rangle_z = \frac{1}{2}\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} + i\frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ i \end{pmatrix}\right)\otimes|1\rangle_z$$

$$-\frac{1}{2}\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} - i\frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ i \end{pmatrix}\right)\otimes|0\rangle_z = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|0\rangle_y - i|1\rangle_y\right)\right]\otimes|1\rangle_z$$

$$-\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|0\rangle_y + i|1\rangle_y\right)\right]\otimes|0\rangle_z = \frac{1}{\sqrt{2}}\left(|0\rangle_z|1\rangle_z - |1\rangle_z|0\rangle_z\right)$$

$$50\%|0\rangle_z, 50\%|1\rangle_z \Rightarrow P_{+}(a_3) = \frac{1}{2}$$

اگر آلیس در اندازه گیری اش در پایه a_3 کیوبیت $|0\rangle_z$ را بدست آورد، کیوبیت در هم تنیده $|\psi\rangle_1$ به کیوبیت $|0\rangle_z|0\rangle_z$ فروپاشی می شود در نتیجه طبق محاسبات زیر احتمال آنکه بـاب در انـدازه گیریش کیوبیت $|0\rangle_z$ را بدست آورد برابر صفر است.

$$P_+(b_2) = ?$$

$$I \otimes \hat{Y}|0\rangle_z|0\rangle_z = I|0\rangle_z \otimes \hat{Y}\left(\frac{1}{\sqrt{2}}\left(|0\rangle_y + i|1\rangle_y\right)\right)$$

$$= |0\rangle_z \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\ i\end{pmatrix} + i\begin{pmatrix}1\\ -i\end{pmatrix}\right]$$

$$= |0\rangle_z \otimes \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\ i\end{pmatrix} + i\begin{pmatrix}-1\\ i\end{pmatrix}\right] = |0\rangle_z \otimes \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left[|0\rangle_y - i|1\rangle_y\right]$$

$$= |0\rangle_z|1\rangle_z \qquad \%100, |1\rangle_z \Rightarrow \qquad P_+(b_2) = 0$$

a_i, b_j همانگونه که در فصل چهارم اشاره شد بردارهای واحد پایه های اندازه گیری آلـیس و بـاب هستند.بنابر این به طریق مشابه داریم:

$$C(a_2, b_1) = -a_2 \cdot b_1 = -|a_2||b_1|Cos\,0 = -1\times 1\times 1 = -1$$
$$C(a_3, b_2) = -a_3 \cdot b_2 = -|a_3||b_2|Cos\,0 = -1\times 1\times 1 = -1 \qquad (۱۳-۵)$$

در تعمیم نا مساوی بِل نظر خود را به نامساوی سوم کلوزر و شیمونی جلب مـی کنـیم؛ نامـساوی کلوزر و شیمونی مانند دیگر نا مساویهای بِل در مکانیک کوانتـومی نقـض شـد کـه نـشان دهنـده ناموضعی بودن تئوری مکانیک کوانتومی است بر اساس این ایده اگر ما بتوانیم پروتکل توزیع کلید کوانتومی مفروض را در محدوده ای از تئوری مکانیک کوانتومی که نامساوی بِل را نقض مـی کنـد در نظر بگیریم، می توانیم به نویز ایجاد شده درصورت استراق سمع ایو به آن پی ببریم.

به معرفی کمیت S که در فصل چهارم به آن اشاره شد می پردازیم:

کمیت S در این پروتکل شامل ضریب همبستگی هایی است که پایه های اندازه گیری آلیس و باب در جهت متفاوت هستند.

$$S = |C(a_1, b_1) - C(a_1, b_3) + C(a_3, b_1) + C(a_3, b_3)|_{QM} \qquad (۱۴-۵)$$

با توجه به شکل(۵-۵) می توان با بدست آوردن مقادیر ضریب همبستگی مقدار S را تعین نمود.

$$S = \left|C(a_1,b_1) - C(a_1,b_3) + C(a_3,b_1) + C(a_3,b_3)\right|_{QM}$$

$$C(a_1,b_1) = -a_1 \cdot b_1 = -|a_1||b_1| Cos\,\frac{\pi}{4} = -\frac{1}{\sqrt{2}}$$

$$C(a_1,b_3) = -a_1 \cdot b_3 = -|a_1||b_3| Cos\,\frac{3\pi}{4} = +\frac{1}{\sqrt{2}}$$

$$C(a_3,b_1) = -a_3 \cdot b_1 = -|a_3||b_1| Cos\,\frac{\pi}{4} = -\frac{1}{\sqrt{2}}$$

$$C(a_3,b_3) = -a_3 \cdot b_3 = -|a_3||b_3| Cos\,\frac{\pi}{4} = -\frac{1}{\sqrt{2}}$$

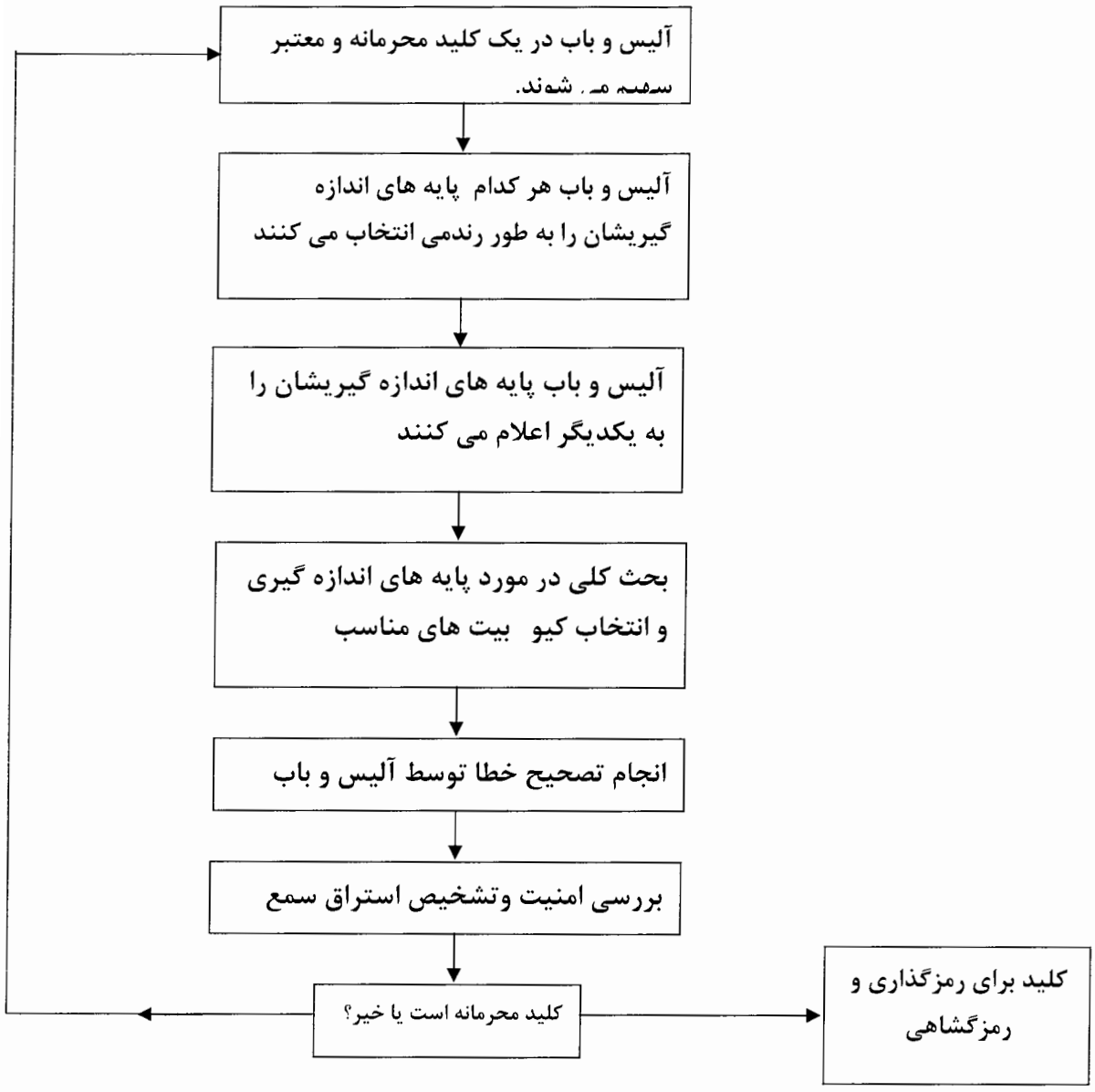
$$S = \left|-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right|_{QM} = \left|-\frac{4}{\sqrt{2}}\right| = 2\sqrt{2} \qquad (۱۵-۵)$$

۷- آلیس و باب نتایجی را که در گروه اول بدست آورده اند در کانال عمومی آشکار می کنند، این کار امنیت پروتکل را به هیچ عنوان تهدید نمی کند ولی به دو کاربر مجاز اجازه آنرا می دهد که مقدار S را تعین نمایند؛ اگر ذرات به طور مستقیم یا غیر مستقیم بهم ریخته نشوند بر طبق اصول تئوری مکانیک کوانتومی مقدار S بایستی در محدوده نقض نامساوی کلوزر و شیمونی برابر $2\sqrt{2}$ شود.در بررسی امنیت پروتکل توزیع کلید کوانتومی محرمانه در ایده اِکرت ناموضعیت در تئوری مکانیک کوانتومی نقش اساسی دارد.بنابریاین هرگاه دو کاربر مجاز مقدار $S = 2\sqrt{2}$ از روی نتایج اندازه گیریشان بدست آورده اند؛ آنها می توانند مطمئن شوند که نتایجی که در گروه دوم از اندازه گیری آنها بدست آمده است، کاملاً محرمانه و ایمن از هر گونه استراق سمع می باشد. رشته هایی از کیوبیت هایی که از نتایج گروه دوم می توان به عنوان کلید رمز محرمانه تبدیل شوند و در پروتکل رمزنگاری کوانتومی بین آلیس و باب از ان استفاده کرد[۱۸].

۵-۶- پروتکل های توزیع کلید کوانتومی

امروزه رمزنگاری کوانتومی به صورت کاربردی حداقل از نقطه نظر علم فیزیک و تئوری های کوانتومی امکان پذیر است.مسئله اصلی در رمزنگاری کوانتومی توزیع (انتشار) کلیدهای کوانتومی است که توسط ویژگی های تئوری فیزیکی به عنوان مثال می توان به ارسال فوتون در هم تنیده بین دو کاربر مجاز نام برد؛ امنیت آن در مقابل تهاجمات استراق سمع کننده قابل

ضمانت است یا حداقل ردیابی استراق سمع در این توزیع کلید کوانتومی وجود دارد. بنابراین باداشتن یک کلید کوانتومی کاملاً ایمن و با انجام کار بسیار اندک می توان رمز گذاری و رمزگشایی را توسط الگوریتم ها در مراحل بعدی رمزنگاری به انجام رساند. با توجه به ایده های رمزنگاری و توزیع کلید کوانتومی که در این بخش اشاره شد می توان طرح کلی و مراحل توزیع کلید کوانتومی را به شکل پروتکل های زیر نشان داد[۱۵]:



شکل(۵-۶): فرآیند توزیع کلید کوانتومی

۵-۷- بیان یک نمونه قابل ذکر از پروتکل رمزنگاری کوانتومی

اگر آلیس و باب بخواهند برای یکدیگر پیام رمزی بفرستند راهی که آنها بتوانند مطمئن شوند که کسی استراق سمع نمی کند استفاده از مسیرهای یکبار مصرف[1] می باشد. در غیر این صورت ممکن است یک استراق سمع کننده بتواند بعضی ازاطلاعات درباره پیام را به دست آورد. بنابراین باید بسیارسریع مورد استفاده قرار گیرد. آلیس و باب در یک کلید محرمانه (خصوصی) شریک می شوند که مرکب از بیت های تصادفی متوالی است که برای هر دوی آنها شناخته شده است.ولی برای دیگران قابل شناسایی نیست.سپس برای ارسال پیام،آلیس آن را به یک رشته از بیت ها تبدیل کرده و الگوریتمی مناسب برای مثال به ساده ترین شکل گیت XOR را بین هر یک از رشته های بیت های کلیدی اجرا می کند و سپس نتایج را برای باب می فرستد. این کار اینگونه انجام می شود که آلیس برای هر بیت پیام m به جای آن m+k می فرستد. در حالی که k یک بیت کلیدی است، (XOR یک باقی مانده مجموع اعداد بر مبنای دو[2] است، بنابراین اگر m وk هر دو یک باشند آلیس صفر را می فرستد).

از آنجاییکه باب هم بیت های کلیدی را می داند به راحتی می تواند با گرفتن گیت مناسب دیگر ، بیت دریافتیr با بیت کلیدی مناسب k ،پیام را رمز گشایی کند.

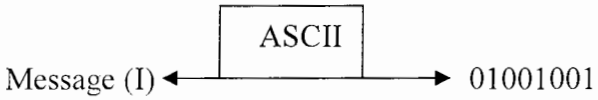
$$m= r+k$$

از طرف دیگر یک استراق سمع کننده مثلاً ایو، چیزی درباره k نمی داند. از آنجا که k یک بیت کاملاً تصادفی است بنابراین r هم یک بیت تصادفی است. بنابراین با نگاه کردن به r ایوچیزی درباره m نمی فهمد وایو چیزی درباره پیام نمی آموزد. در این بخش سعی بر ان است که پروتکل رمزنگاری کوانتومی به عنوان نمونه ارائه دهیم.

---

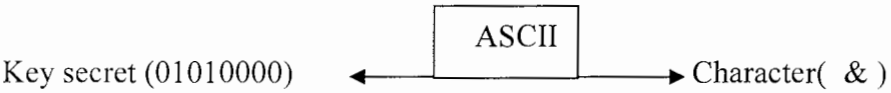
[1] One-time-pad
[2] Addition modulo 2

اکنون با استفاده از کلید رمز محرمانه به ادامه رمز نگاری کوانتومی می پردازیم آلیس به عنوان فرستنده پیغام و باب به عنوان گیرنده پیغام می باشد، فرض کنیم پیغام فقط یک کاراکتر مثلاً "I" باشد در طرح کد دهی ASCII نیاز به هشت بیت می باشد یعنی هر کاراکتر به صورت هشت بیت کوانتومی باشد.



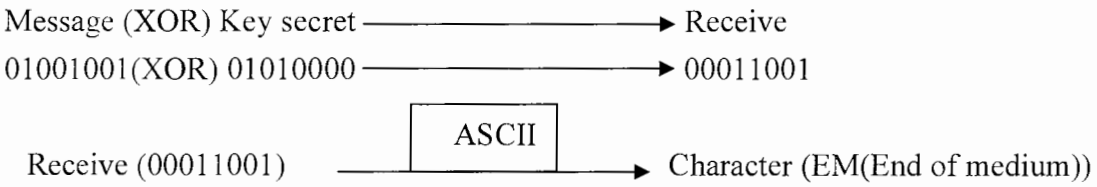
حال آلیس برای رمز گذاری نیاز به کلید رمز محرمانه دارد با توجه به مطالب بالا در بررسی امنیت پروتکلBB84 دو کاربر مجازدارای یک کلید رمز محرمانه مشترک به دور از هر گونه استراق سمعی هستند، بطوری که آنها می توانند ازهشت کیو بیت محرمانه مشترک اول برای کلید رمز استفاده کنند(انتخاب هشت کیوبیت به علت استفاده ازطرح کدهی ASCII می باشد).

حال فرض کنیم کلید رمز به صورت زیر باشد:



مطابق شکل بالا آلیس و باب داری یک کلید رمز محرمانه مشترک (01010000)هستند، که آلیس با تعریف یک الگوریتم مناسب، مثلاً گیتً XOR می تواند پیغام را با استفاده از کلید رمز به پیغام رمز گذاری شده برای در یافت باب آماده کند که با پیغام دریافتی نشان داده شده است.

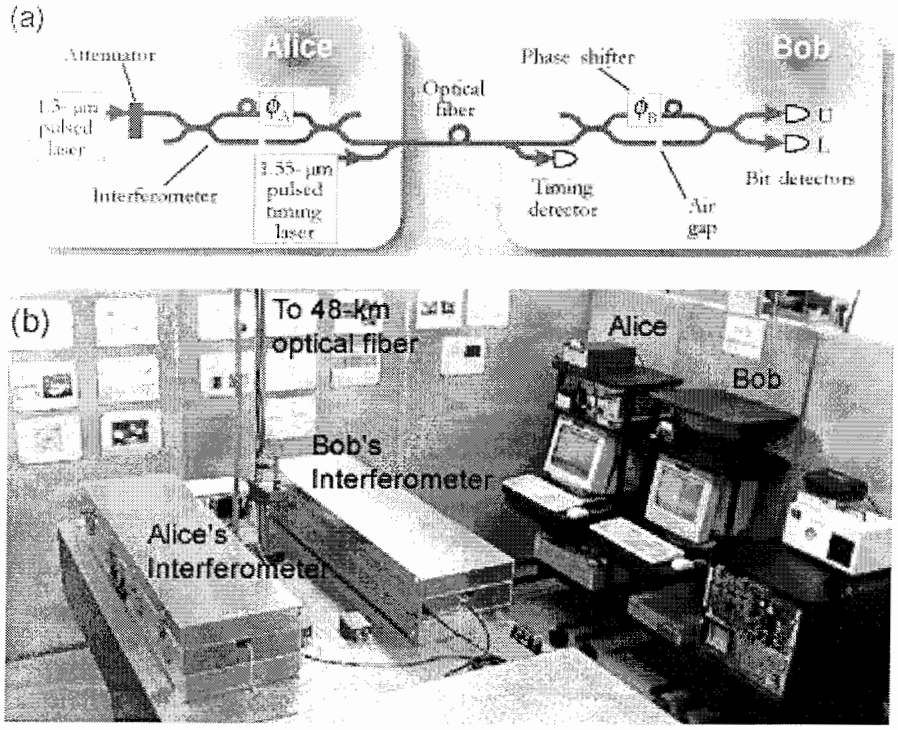
مطابق شکل زیر:



حال آلیس می تواند پیغام رمز گذاری شده را در یک کانال عمومی به باب برساند،در این صورت باب دارای یک کلید رمز محرمانه ویک پیغام رمز گذاری شده است که با استفاده از الگوریتم (گیت) مناسب وقابل توافق با آلیس می تواند و با اعمال یک الگوریتم یا برنامه نرم افزاری پیغام رمز گذاری شده را توسط کلید رمز،رمز گشایی کند.

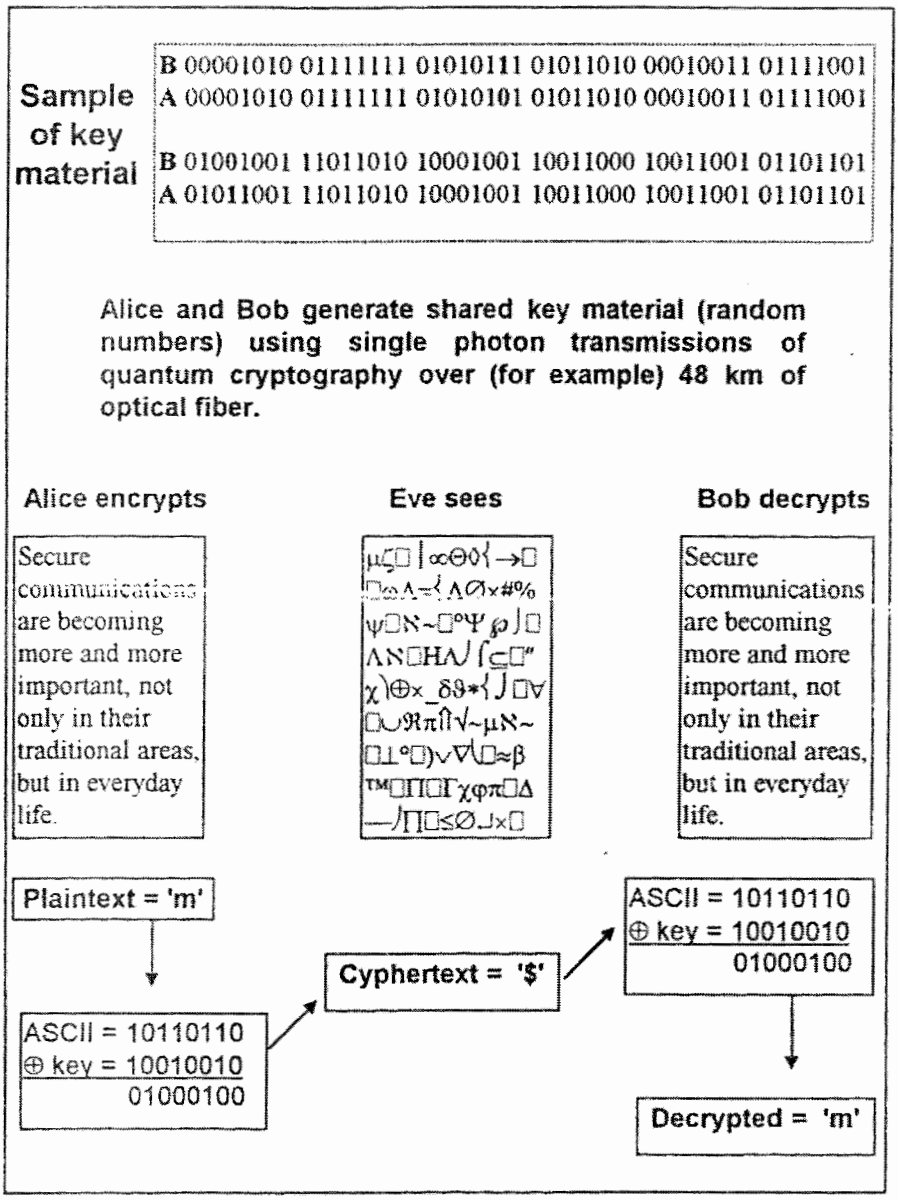
۵-۸- نمونه هایی از رمزنگاری کوانتومی

در لوس آلاموس، ما یک چشم انداز متفاوت تری در یک محیط کاملاً دانشگاهی رمزنگاری کوانتومی به شکل کاربردی از نقطه نظر علم فیزیک امکان پذیر مشاهده می کنیم، کانال کوانتومی استفاده شده برای مبادله یا انتقال بیت های کلید از یک فیبر نوری یا اتمسفر می باشد که استفاده کردن از طول موج ۱/۳ میکرون تا ۵۵ میکرون در یک فیبر نوری امکان پذیر است. در آخرین آزمایشات نشان داده شده است که اتمسفر یک کانال کوانتومی کاربردی است آزمایشاتی در آزمایشگاه دانشگاه لوس آلاموس برای انتقال فوتون ها مادون قرمز ۷۷۰ nm در فاصله یک کیلومتری در فضای آزاد با موفقیت انجام شد و رمزنگاری کوانتومی در ارسال فوتون های در هم تنیده در ۴۸ کیلو متری دو کاربر در آزمایش فیبر نوری نیز با موفقیت انجام گردید[۱۵].



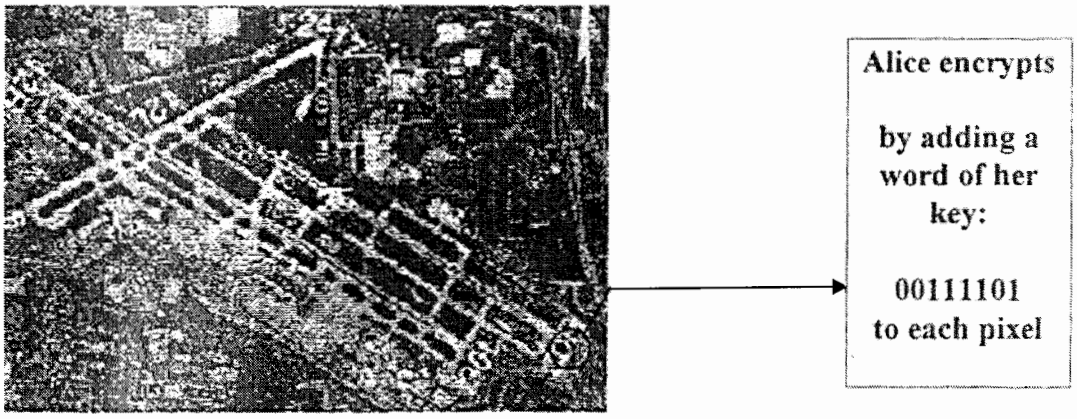
شکل (۵-۷) طرحی از آزمایشات در لوس آلاموس با استفاده از پروتکل مشهور B92 طی ۴۸ km از فیبر نوری ،نوری با طول موج ۱/۳ میکرو متر توسط یک منبع فوتون منفرد [۱۷].

نمونه ای از رمزنگاری در طرح وار زیر(شکل۵-۸) نشان داده شده است، در این نمونه توسط آلیس عبارت یا متن قابل درک را با اعمال گیت XOR بر روی هر یک از کاراکترهـای آن در کـد دهـی ASCII و اسناد کلید کوانتومی رمزگذاری می شود و نیز باب این رشته از بیت هارا بـا اسـتفاده از گیت مناسب دیگر وهمان کلید کوانتومی محرمانه مشترک رمزگشایی می کند[۱۵].

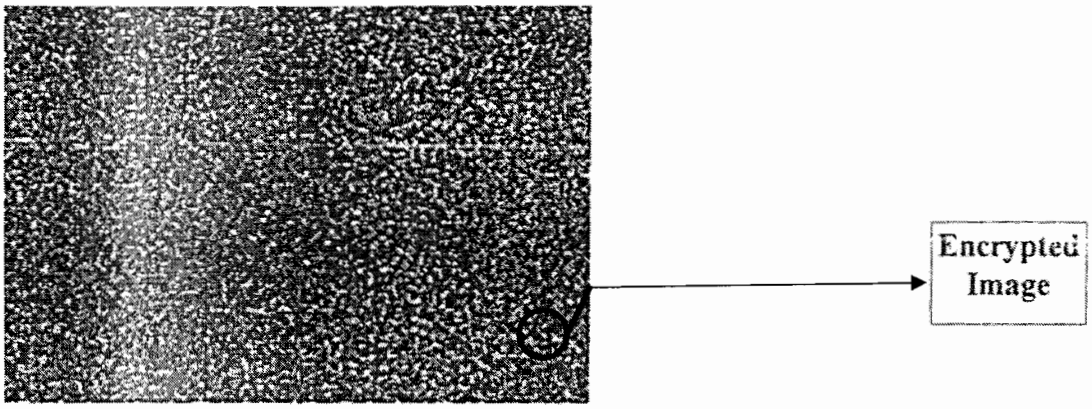


شکل(۵-۸): نمونه رمزنگاری کوانتومی

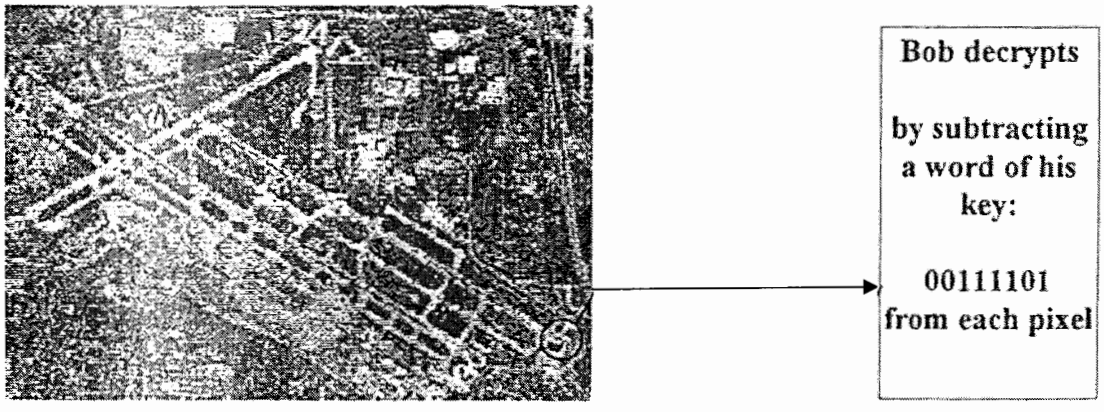
نمونه دیگر برای رمزنگاری یک تصویر از فرودگاه سنت لویز می باشد که هر پیکسل توسط با یک بایت نشان داده شده است در اینجا نیز کلید رمزکوانتومی توسط گیت XOR با هر یک از پیکسل ها رمزنگاری شده است و توسط باب با استفاده از کلید رمز کوانتومی و تصویر رمزگذاری شده رمزگشایی صورت می گیرد[۱۵].



شکل(۵-۹) تصویر ازفرودگاه سنت لویز



شکل (۵-۱۰) تصویر رمزگذاری شده



شکل (۵-۱۱) تصویر رمزگشایی شده

۵-۹- نتیجه گیری

رمزنگاری کلاسیکی، امروزه کاربردهای وسیعی در اطلاعات محرمانه دارند با این حال آنها نمی توانند امنیت اطلاعات را به طور قطعی تضمین نمایند. اخیراً فیزیکدانان با استفاده از تئوری کوانتومی و تئوری نسبیت معتبر توانسته اند پروتکل های رمزنگاری را امنیت صد درصد تضمین نمایند. یعنی قوانین مکانیک کوانتومی هر گونه استراق سمع را به وسیله نویزی که در حالت کوانتومی سیستم های درهم تنیده ایجاد می کند آشکار کند این قوانین هرگز نمی توانند مانع از استراق سمع شوند؛ ولی آنها ایمنی پروتکل را در مقابل استراق سمع تضمین می نمایند.

فصل ۶:

پروتکل توزیع کلید کوانتومی بیت محرمانه درچارچوب نظریه فرا کوانتومی

- مقدمه
- نظریه فراکوانتومی
- پروتکل توزیع بیت محرمانه فرا کوانتومی
- تهاجمات استراق سمع کننده
- اثبات ایمنی پروتکل
- نتیجه گیری
- پیشنهادات

۶-۱- مقدمه

اگر تئوری کوانتومی صحیح باشد پروتکل توزیع کلید کوانتومی استاندارد به طور قابل اثبات در مقابل تهاجمات استراق سمع کنندگان ایمن هستند، ما نیاز به فرض اعتبار تئوری کوانتومی برای اثبات امنیت توزیع کلید کوانتومی داریم یا اینکه امنیت را برمبنای اصول فیزیکی دیگر پایه ریزی کنیم، اگر مکانیک کوانتومی در تعدادی روش ناموفق بود به این دلیل است که استراق سمع کننده شاید می توانست از فیزیک فراکوانتومی برای استخراج اطلاعات از ارتباطات کوانتومی بدون آنکه ضرورتاً باعث اغتشاشات حالت کوانتومی شود که خود دلیل امنیت است استفاده کند. در اینجا یک طرح توزیع کلید ایمنی به طور قابل اثبات در مقابل تهاجمات کلی (عمومی) توسط یک استراق سمع کننده فرا کوانتومی که فقط با غیر ممکن بودن علامت دهی مافوق نور محدود می شود (علامت دهی بیشتر از سرعت نور امکان پذیر نباشد) را شرح می دهیم. امنیت این طرح از نقض نامساوی بل حاصل می شود.

با کشف رمزنگاری کوانتومی[۱۹] و توزیع کلید کوانتومی [۲۰،۱۸] که در فصل چهارم به طور مفصل به آن اشاره شد حالا به خوبی درک می شود که عملکردهای رمزنگاری می تواند با اصول فیزیکی تضمین شود. بنابراین ما دارای پروتکل هایی برای عملکردهای مختلف شامل توزیع کلید کوانتومی با فرض تئوری مکانیک کوانتومی معتبر به طور قابل اثبات ایمن می باشد [۲۴،۲۳،۲۲،۲۱].

در ضمن پروتکل های امن با ضمانتی مبنی بر غیر ممکن بودن علامت دهی ما فوق نور تولید شده اند[۲۵،۲۶].

امکان پایه ریزی امنیت رمزنگاری در قوانین شناخته شده فوق اخیراً بحث شده است. [۲۷] .

۶-۲- نظریه فرا کوانتومی

در این قسمت ما نظریه فراکوانتومی به شرح زیر را تحقیق می کنیم که آیا یک طرح توزیع کلید فراکوانتومی با علامت دهی مافوق نور غیر ممکن به طور قابل اثبات ایمن است یا خیر؟ ما استراق سمع کنندگان را مجاز می نماییم که بتوانند قوانین مکانیک کوانتومی را نقض نمایند ولی آنها نمی توانند علامت دهی مافوق نور داشته باشند(یعنی تئوری نسبیت نقض نمی شود).

به طور کلی این بدان معنا خواهد بود که ممکن است اثبات ایمنی پروتکل های توزیع کلید کوانتومی برای مدت طولانی تر معتبر نباشد و همچنین ما نمی توانیم برای مدت طولانی تر فرض کنیم که تئوری کوانتومی در ارتباطات اطلاعاتی معتبر باشد، یعنی ما نسبت به تئوری کوانتومی شکاک هستیم واعتقاد داریم ممکن است در آینده ثابت شود که تئوری کوانتومی معتبر نیست . نظریه فرا کوانتومی در توزیع کلید فراکوانتومی به این دلیل مطرح می شودکه اگر در آینده تئوری کوانتومی معتبر نباشد ما بتوانیم با ارائه نظریه فراکوانتومی که فقط بر اساس اعتبار تئوری نسبیت پایه ریزی شده است به طور قابل اثبات توزیع کلید فراکوانتومی بیت محرمانه داشته باشیم. با توجه به فصل پنجم لازم است بدانیم در نظریه کوانتومی اگر ایو بتواند اطلاعات را از کیو بیت ها استخراج کند و ضرورتاً بایستی در کیو بیت درهم تنیده اغتشاش ایجاد کند. (اغتشاش کیوبیت عامل اصلی پی بردن به امنیت توزیع کلید کوانتومی است).

اثبات های ایمنی موجود اعتبار تئوری کوانتومی را فرض می کند در عین حال تئوری کوانتومی در یک محدوده موثر از آزمایشات تایید گردیده است، این امر باورنکردنی وجود دارد که تعدادی از آزمایشات بعدی محدوده ای برای حوزه اعتبار تئوری کوانتومی را اثبات خواهد کرد. مسلماً این امر نیز امکان پذیر است که بعضی از آزمایشات بعدی بتواند امکان علامت دهی ما فوق نور را ثابت کند. اما این احتمالات به طور منطقی مستقل از هم هستند. تئوری کوانتومی می تواند بدون

نقض کردن خصوصیت علیت نسبیتی استاندارد رد شود و برعکس، یک طرح رمزنگاری مـی توانـد امنیت را به وسیله هر دو اصل (تئوری کوانتومی و تئوری نسبیتی) تضمین کند، موثق تر آن است که امنیت کاملاً روی یک اصل وابسته باشد.

همان طوری که در زیر نشان می دهیم یک امکان اتصال محرمانه بین این نوع پروتکـل در نظریـه فراکوانتومی نقض نامساوی بل می باشـد[۳۰،۲۹]. یعنـی امنیـت توزیـع کلیـد فـرا کوانتـومی در محدوده ای که نامساوی بل نقض می شود قابل اثبات است.

بنابراین روابط نا موضعیت (درمحدوده نقض نامساوی بل) و یک منبع قابل بهره برداری بـرای ایـن کار تشکیل می شود و تنها حالت های در هم تنیده منبعی برای توزیع کلید فراکوانتومی قراردادی می باشد. ما یک طرح فراکوانتومی را نشان می دهـیم کـه شـامل نقـض بـل در مقابـل تهاجمـات عمومی که توسط ایو و ناعلامت دهی (علامت دهی بیشتر از سرعت نور امکان پذیر نیـست) ایمـن می باشد.

۶-۳- پروتکل توزیع بیت محرمانه در نظریه فراکوانتومی

ما فرض می کنیم که آلیس و باب یک کانال کوانتومی نویز آزاد و یـک کانـال کلاسـیکی معتبر دارند. کانال نویز آزاد، کانالی است که هر شخصی مثـل ایـو بـه طـور آزادانـه مـی توانـد بـا اغتشاش سیستم یا حالت کوانتومی درآن استراق سمع کند و در آن پارازیت ایجاد کند. در پروتکل زیر ما نشان می دهیم که چگونه یک بیت محرمانه مشترک تولید می شود و امنیت آن در مقابـل تهاجمات استراق سمع کنندگان فراکوانتومی ضمانت می شود.

پایه های X_r برای عدد صحیح r به صورت زیر تعریف کنید:

$$X_r = \left\{ Cos\frac{r\pi}{2N}|0\rangle + Sin\frac{r\pi}{2N}|1\rangle, -Sin\frac{r\pi}{2N}|0\rangle + Cos\frac{r\pi}{2N}|1\rangle \right\} \qquad (۱-۶)$$

برای هر پایه، ما نتایج 0 و 1 را به ترتیب در تصاویر عناصر پایه اول و دوم تعیین کردیم.

بنابراین پایه X_{r+N} شامل بر مبنای مشابهی از پایه X_r با مجموعه نتایج معکوس[1] شده می باشد، که به آن پایه های مشابه با نتایج معکوس گویند؛ برای مثال پایه های مشابه X_{-1} و X_N با نتایج معکوس پایه های X_{N-1} و X_0 می باشدکه در زیر آنرا بررسی می کنیم:

$$X_r = \left\{ Cos\frac{r\pi}{2N}|0\rangle + Sin\frac{r\pi}{2N}|1\rangle, -Sin\frac{r\pi}{2N}|0\rangle + Cos\frac{r\pi}{2N}|1\rangle \right\}$$

$$X_{r+N} = \left\{ Cos\frac{(r+N)\pi}{2N}|0\rangle + Sin\frac{(r+N)\pi}{2N}|1\rangle, -Sin\frac{(r+N)\pi}{2N}|0\rangle + Cos\frac{(r+N)r\pi}{2N}|1\rangle \right\}$$

$$X_{r+N} = \left\{ Cos(\frac{r\pi}{2N}+\frac{\pi}{2})|0\rangle + Sin(\frac{r\pi}{2N}+\frac{\pi}{2})|1\rangle, -Sin(\frac{r\pi}{2N}+\frac{\pi}{2})|0\rangle + Cos(\frac{r\pi}{2N}+\frac{\pi}{2})|1\rangle \right\}$$

$$X_{r+N} = \left\{ -Sin(\frac{r\pi}{2N})|0\rangle + Cos(\frac{r\pi}{2N})|1\rangle, -Cos(\frac{r\pi}{2N})|0\rangle - Sin(\frac{r\pi}{2N})|1\rangle \right\}$$

$$X_{r+N} = \left\{ -Sin(\frac{r\pi}{2N})|0\rangle + Cos(\frac{r\pi}{2N})|1\rangle, -(Cos(\frac{r\pi}{2N})|0\rangle + Sin(\frac{r\pi}{2N})|1\rangle) \right\} \qquad (۲-۶)$$

در رابطه (۶-۲) منفی به عنوان عامل فـاز در حالـت کوانتـومی مـی باشـد و تـأثیری روی حالـت کوانتومی ندارد، بنابراین داریم:

$$X_{r+N} = \left\{ -Sin(\frac{r\pi}{2N})|0\rangle + Cos(\frac{r\pi}{2N})|1\rangle, Cos(\frac{r\pi}{2N})|0\rangle + Sin(\frac{r\pi}{2N})|1\rangle \right\} \qquad (۳-۶)$$

با استفاده از رابطه (۶-۱) و (۶-۳) داریم:

$$r = 0 \rightarrow \begin{cases} X_0 = \{|0\rangle, |1\rangle\} \\ X_N = \{|1\rangle, |0\rangle\} \end{cases} \qquad (۴-۶)$$

$$r = -1 \rightarrow \begin{cases} X_{-1} = \left\{ Cos(\frac{-1\pi}{2N})|0\rangle + Sin(\frac{-1\pi}{2N})|1\rangle, -Sin(\frac{-1\pi}{2N})|0\rangle + Cos(\frac{-1\pi}{2N})|1\rangle \right\} \\ X_{N-1} = \left\{ -Sin(\frac{-1\pi}{2N})|0\rangle + Cos(\frac{-1\pi}{2N})|1\rangle, Cos(\frac{-1\pi}{2N})|0\rangle + Sin(\frac{-1\pi}{2N})|1\rangle \right\} \end{cases}$$

$$N \rightarrow \infty \rightarrow \begin{cases} X_{-1} = \{|0\rangle, |1\rangle\} \\ X_{N-1} = \{|1\rangle, |0\rangle\} \end{cases} \qquad (۵-۶)$$

پارامترهای امنیتی N و M را برای اعداد صحیح مثبت بزرگ در ادامه تعریف می کنیم، برای ساده کردن این آنالیز ما $M \langle\langle\langle N$ را در نظر می گیریم.

---

[1] Reverse out come

۶-۳-۱- مراحل پروتکل توزیع بیت خصوصی(محرمانه):

۱- آلیس و باب $n = MN^2$ زوج سیستم هر یک در حالت درهم تنیده (کیوبیت در هم تنیده) $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ را به اشتراک گرفته اند.

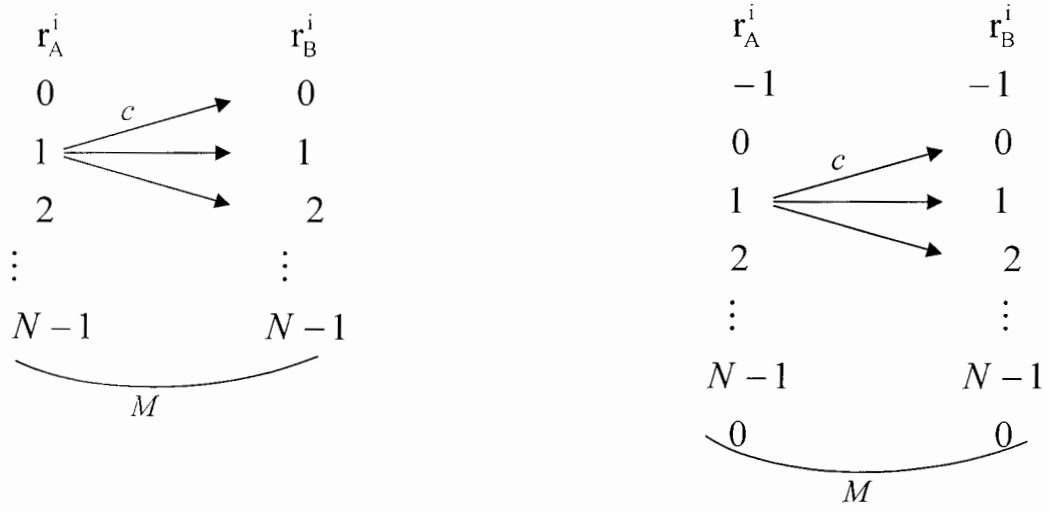
۲- آلیس و باب عناصر رندمی r_A^i, r_B^i را از مجموعه $\{0,1,2,....,N-1\}$ برای هر i ازتا MN^2 را کرده اند و i امین ذرهٔ آنها در پایه های $A_i = X_{r_A^i}, B_i = X_{r_B^i}$ اندازه گیری می کنند.

۳- وقتی تمام اندازه گیری آنها تکمیل شد، آلیس و باب پایه های اندازه گیریشان را در سراسر یک کانال عمومی تأئید شده و کلاسیک آشکار می کنند.

۴- آلیس و باب این پروتکل را ناتمام می گذارند و دوباره شروع به کار می کنند مگر اینکه:

$$2MN \le \sum_{i=1}^{MN^2} \sum_{c=-1,0,1} \left|\{j : A_j = X_i, B_j = X_{i+c}\}\right| \qquad (۶-۶)$$

رابطه سری $\sum_{i=1}^{MN^2} \sum_{c=-1,0,1} \left|\{j : A_j = X_i, B_j = X_{i+c}\}\right|$ را می توان به شکل زیر در نظر گرفت:



شکل(۶-۱):سری $\sum_{i=1}^{MN^2} \sum_{c=-1,0,1} \left|\{j : A_j = X_i, B_j = X_{i+c}\}\right|$ به ازای پارامترc به تعدادM بار تکرار می شود X_{-1}, X_N پایه های اندازه گیری مشابه با نتایج مختلف X_0, X_{N-1} هستند.

با توجه به شکل بالا تعداد حالات مجاز که توسط پارامتر c محدود شده است برابر است با 3MN می باشد.

مقدار انتظاری مجموعه سری بالا برابر 3MN می باشد. طبق رابطه زیر:

احتمال حالت انتخاب شده × تعداد کل حالات = مقدار انتظاری

می توانیم بنویسیم:

$$\text{Expectation value} = \sum_i \mathrm{n}_i P_i \qquad (۷-۶)$$

$$\text{Expectation value} = MN^2 \times \frac{3MN}{MN^2} = 3MN$$

امکان شرایط ناموفق از رده $e^{-\frac{MN}{6}}$ می باشد[۳۷] .

۵- نتایج برای یک جفت انتخاب شده بطور تصادفی مخفی نگه داشته می شود که پایه های انتخاب شده X_i, X_{i+c} برای بعضی i ، c= -1,0,1 بوده اند؛ ما پایه های این شکلی را همسایه $c = -1,1$ و مساوی $c = 0$ می نامیم. نتایج برای تمام جفت های باقی مانده اعلام می شود.

۶- آلیس و باب این پروتکل را ناتمام می گذارند اگر نتایج حاصل از اندازه گیری a,b آنها در تمام مواردی که آنها پایه های مجاور (همسایه) را انتخاب نموده اند نا مربوط شوند؛ یعنی با توجه به کیو بیت درهم تنیده نتایج مورد انتظار باید $a \neq b$ بدست آید.

۷- اگر این پروتکل به پایان رسانده شود و نتایج اندازه گیری اعلام نشدهٔ آنها بیت خصوصی را تعیین می کند، که برای آلیس معادل با نتیجه او و برای باب مخالف با نتیجه او می باشد.

۶-۴- تهاجمات استراق سمع کننده

برای تجزیه و تحلیل نمودن این پروتکل، ما باید رسماً عملکرد های موجود برای استراق سمع کنندگان فرا کوانتومی را شرح دهیم:

با دادن حداکثر توان به ایو، ما فرض می کنیم که هر جفت از سیستم ها در هم تنیده توسط یک منبع تحت کنترل او تولید می شود. در حالت کلی بطور پیوسته تهاجم ایو اینگونه است که با فراهم کردن 2n+1 سیستم در حالت فراکوانتومی λ و فرستادن n سیستم به سوی آلیس و n سیستم دیگر به سوی باب و نگه داشتن یکی از سیستم ها برای خود جهت استراق سمع می باشد.

احتمالات اندازه گیری حالت λ را تعریف می کند.

$$P_{\lambda} = (abe|ABE) \qquad (۸-۶)$$

در اینجا $A = \{A_1, A_2, ...A_n\}$ و $B = \{B_1, B_2, ...B_n\}$ مجموعه پایه های انتخاب شده رندمی ممکن برای اندازه گیری آلیس و باب هستند و $E = \{E_1\}$ مجموعه ای شامل یک پایه انتخاب شده توسط ایو برای اندازه گیری است با نتایج وابسته e, b, a می باشد.این حالت ممکن است غیر کوانتومی و ناموضعی باشد اما نباید علامت دهی (سرعت بیشتر از نور) را حتی در یک رشته مشترک مجاز بدانیم یعنی تئوری نسبیت همواره برقرار است. بنابراین با توجه به ناعلامت دهی و اعتبار تئوری نسبیت در نظریه فرا کوانتومی برای هر تفکیک $B = B^1 \cup B^2$ و $A = A^1 \cup A^2$ و $E = E^1 \cup E^2$ هر پایه اندازه گیری رندمی دیگر $\overline{A}^2$ و $\overline{B}^2$ و $\overline{E}^2$ داریم:

$$\sum_{a^2 b^2 e_2} P_{\lambda}(a^1 a^2 b^1 b^2 e_1 e_2 \left| A^1 A^2 B^1 B^2 E_1 E_2 \right.) = \sum_{\overline{a}^2 \overline{b}^2 \overline{e}_2} P_{\lambda}(a^1 \overline{a}^2 b^1 \overline{b}^2 e_1 \overline{e}_2 \left| A^1 \overline{A}^2 B^1 \overline{B}^2 E_1 \overline{E}_2 \right.) \qquad (۹-۶)$$

ایو ممکن است منتظر بماند تا اینکه تمام ارتباطات آلیس و باب قبل از اندازه گیری او تمام شود. محدوده اندازه گیریها قابل دسترس برای ایو و نتیجه احتمال آنها مستقل از زمان است و فرض می کنیم در تئوری فرا کوانتومی ،همچنین در تئوری کوانتومی ،اندازه گیریها در یک حالت مشترک نمی توانند برای فرستادن علامت دهی سرعت بیشتر از نور به طرفین استفاده شود، دراین تئوری، اطلاعات در پایه ها و نتایج اندازه گیریهای انجام شده توسط آلیس و باب که برای ایو حداکثربا سرعت نور منشر می شود را می پذیرد یعنی علامت دهی با سرعت بیشتر از نور وجود ندارد. در این صورت بایستی آنالیزهای امنیتی پروتکل توزیع کلید کوانتومی نیاز به اندازه گیریهای آلیس و باب دارد که کاملاً در مقابل تهاجمات ایو ایمن باشد. در فرضیه رمزنگاری فرا کوانتومی نیاز به پیروی قوانین کوانتومی نیست هدف تضمین توزیع کلید محرمانه در پروتکل بالا می باشد که فرض بر آن است که هیچ گونه اطلاعات شامل نتایج حاصل از اندازه گیری آلیس و باب متعاقباً به ایو منتشر نشود.

۶-۵- تصویرکیوبیت درهم تنیده در پایه اندازه گیری دو کاربر مجاز

در این بخش می خواهیم تصویرکیوبیت درهم تنیده $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ را در پایه های اندازه گیری آلیس و باب به عنوان دو کار بر مجاز بدست آوریم؛ X_r پایه اندازه گیری آلیس و باب می باشد که می توان این پایه ها را به صورت زیر برای آلیس و باب نمایش داد:

$$X_r = \left\{ Cos\frac{r\pi}{2N}|0\rangle + Sin\frac{r\pi}{2N}|1\rangle, -Sin\frac{r\pi}{2N}|0\rangle + Cos\frac{r\pi}{2N}|1\rangle \right\}$$

$$X_r^{1A} = \left\{ Cos\frac{r\pi}{2N}|0\rangle + Sin\frac{r\pi}{2N}|1\rangle \right\} \quad , \quad X_r^{1A} = \left\{ Cos\frac{r\pi}{2N}|0\rangle + Sin\frac{r\pi}{2N}|1\rangle \right\}$$

$$X_r^{2A} = \left\{ -Sin\frac{r\pi}{2N}|0\rangle + Cos\frac{r\pi}{2N}|1\rangle \right\} \quad , \quad X_r^{2A} = \left\{ -Sin\frac{r\pi}{2N}|0\rangle + Cos\frac{r\pi}{2N}|1\rangle \right\} \qquad (۱۰-۶)$$

برای کیوبیت درهم تنیده می توان رابطه زیر را نوشت:

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$

$$|0\rangle_A = \alpha_1 X_r^{1A} + \alpha_2 X_r^{2A} = \alpha_1\left[Cos\frac{r\pi}{2N}|0\rangle_A + Sin\frac{r\pi}{2N}|1\rangle_A \right] + \alpha_2\left[-Sin\frac{r\pi}{2N}|0\rangle_A + Cos\frac{r\pi}{2N}|1\rangle_A \right] \qquad (۱۱-۶)$$

به طریق مشابه داریم:

$$|1\rangle_A = \alpha_1 X_r^{1A} + \alpha_2 X_r^{2A} = \alpha_1\left[Cos\frac{r\pi}{2N}|0\rangle_A + Sin\frac{r\pi}{2N}|1\rangle_A \right] + \alpha_2\left[-Sin\frac{r\pi}{2N}|0\rangle_A + Cos\frac{r\pi}{2N}|1\rangle_A \right] \qquad (۱۲-۶)$$

$$|0\rangle_B = \alpha_1 X_r^{1B} + \alpha_2 X_r^{2B} = \alpha_1\left[Cos\frac{r\pi}{2N}|0\rangle_B + Sin\frac{r\pi}{2N}|1\rangle_B \right] + \alpha_2\left[-Sin\frac{r\pi}{2N}|0\rangle_B + Cos\frac{r\pi}{2N}|1\rangle_B \right] \qquad (۱۳-۶)$$

$$|0\rangle_B = \alpha_1 X_r^{1B} + \alpha_2 X_r^{2B} = \alpha_1\left[Cos\frac{r\pi}{2N}|0\rangle_B + Sin\frac{r\pi}{2N}|1\rangle_B \right] + \alpha_2\left[-Sin\frac{r\pi}{2N}|0\rangle_B + Cos\frac{r\pi}{2N}|1\rangle_B \right] \qquad (۱۴-۶)$$

۶-۶- اثبات امنیت پروتکل

ما A_j و B_j را بخاطر بودن پایه های اندازه گیری انتخابی آلیس و باب برای j امین جفت تعریف می کنیم که اینها متغیرهای رندمی هستند. هر اندازه گیری با احتمال $\frac{1}{N}$ پدید می آید. ما همچنین a_j و b_j را به عنوان نتایج اندازه گیری در نظر می گیریم و داریم:

$$t_j = \frac{1}{3N} \sum_{c=-1,0,1} \sum_{i=0}^{N-1} p_r\left(a_j \neq b_j \middle| A_j = X_i, B_j = X_{i+c}\right) \qquad (۱۵-۶)$$

بار دیگر یاد آوری می شود که X_N, X_{-1} با نتایج معکوس شده X_0, X_{N-1} هستند.

توجه داشته باشید که اگر λ موضعی باشد ما داریم:

$$t_j \leq 1 - \frac{2}{3N} \qquad (۱۶-۶)$$

این یک نامساوی تعمیم یافته بل می باشد. در واقع مشابه با نامساوی متسسّل بران استین و کیوز[۱] است[۳۲] .

اگر استراق سمع وجود نداشته باشد، و نیز دو کاربر در حالت منفرد (کیوبیت درهم تنیده) معتبر مشترک شوند، آنگاه در مکانیک کوانتومی مقدار t_j برابر است با:[۳۷]

$$t_j = 1 - o\left(\frac{1}{N^2}\right) \qquad (۱۷-۶)$$

برای تمام j ، نامساوی تعمیم یافته بل رابطه (۶-۱۶) برای N به اندازهٔ کافی بزرگ نقض می شود:

$$\begin{cases} \left[t_j\right]_{QM} = 1 - o\left(\frac{1}{N^2}\right) \\ \left[t_j\right]_{Local} \leq 1 - \frac{2}{3N} \end{cases} \xrightarrow{N \to \infty \Rightarrow \frac{1}{N^2} \to 0} \begin{cases} \left[t_j\right]_{QM} = 1 \\ \left[t_j\right]_{Local} \leq 1 - \frac{2}{3N} \langle 1 \end{cases} \qquad (۱۸-۶)$$

با نقض نامساوی بالا برای امنیت این پروتکل به طور قطعی برقرار است. یعنی نقض نامساوی بالا دانش ایو را در استراق سمع پروتکل برای محدود شدن مجاز می داند و در این صورت به ایو اجازه استراق سمع نخواهد داد.

---

[۱] Braunstein and caves

اکنون ما می خواهیم محدودهٔ پایین تری را در مقدار t_s برای جفت خصوصی S ارائه دهیم که آلیس و باب پروتکل را با موفقیت[1] به پایان می رسانند و ایو همیشه در استراق سمع این پروتکل ناموفق است. همچنین ما محدودهٔ پایین تر در t_s که به یک محدودهٔ بالاتر در اطلاعات ایو است اشاره می کنیم که می تواند بطور قرار دادی M کوچک و N بزرگ باشد.

از حالا ، ما فرض می کنیم که حداقل یک جفت برای اندازه گیری آلیس و باب که مجاور یا مساوی بوده اند وجود دارد، درغیر این صورت آنها بی نتیجه خواهند ماند. بیائید فرض کنیم که S یک متغیر تصادفی ضمیمهٔ جفت انتخاب شده برای تعیین کردن بیت خصوصی باشد. یک حالت فرا کوانتومی λ احتمال با موفقیت به پایان رسد با P_λ نشان می دهیم در زیر قضیه ای را ثابت می کنیم تا مقدار P_λ را بدست آوریم.

۶-۶-۱- قضیه

برای هر حالت فرکوانتومی λ چنانچه $P_\lambda(pass)\rangle\varepsilon$ ما داریم :

$$P_\lambda(a_s \neq b_s | pass)\rangle 1-\frac{1}{2MN\varepsilon} \qquad (۱۹-۶)$$

اثبات: اجازه دهید m متغیر رندمی ، تعداد جفت هایی باشد که اندازه گیریهای آنها مجاور یا مساوی می باشد. برای یک جفت ارائه شده بالا c در شرایطی که اندازه گیریهای آنها مجاور و مساوی با نتایج نامربوط هستند در نظر می گیریم. اگر جفت خصوصی برای c واجد شرایط باشد آنگاه آلیس و باب در مقدار بیت خصوصی توافق خواهند داشت. ما نماد #(c) را به معنای تعداد جفت هایی که در شرایط c قرار دارند نشان می دهیم؛ در زیر چهار رخداد منحصر به پروتکل توزیع بیت خصوصی در تئوری فرا کوانتومی را نشان می دهیم:

$$\begin{array}{ll} E_0 & m\langle 2MN \\ E_1 & m \geq 2MN \quad \text{and} \quad \#(c)\langle m-1 \\ E_2 & m \geq 2MN \quad \text{and} \quad \#(c)=m-1 \\ E_3 & m \geq 2MN \quad \text{and} \quad \#(c)=m \end{array} \qquad (۲۰-۶)$$

[1] pass

توجه داشته باشید که:

۱- اگر E_0 یا E_1 اتفاق اُفتد آنگاه آلیس و باب قطعاً به نتیجه نمی رسند و باید دوباره پروتکل تکرار شود.

۲- اگر E_3 پدید بیاید آلیس و باب به طور قطع به نتیجه خواهند رسید.

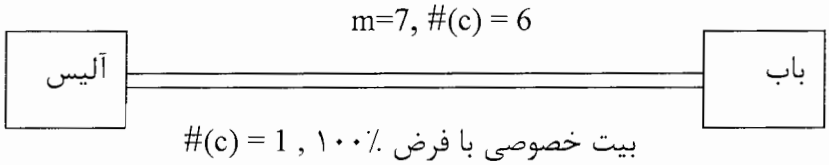
حالت فراکوانتومی λ احتمالی را برای هر یک از این چهار رخ داد مطابق رابطه زیر تعریف می کند:

$$P_\lambda(E_i) = q_i \qquad (۲۱-۶)$$

۳- اگر E_2 پدید بیاید، در صورتی این پروتکل با موفقیت به پایان می رسد که جفت خصوصی c را واجد شرایط نکند یعنی اینکه جفت خصوصی در رویداد E_2 شامل جفت c نباشد و آنرا دربرنگیرد.

به شکل خیلی ساده می توان رویداد های بالا را مانند طرح زیر شبیه سازی نمود:

فرض کنیم که پروتکل ما داری تعداد ۷ جفت با اندازه گیریهای مجاوریا مساوی هستند (m = ۷) در رویداد E_0 به طور قطع پروتکل به نتیجه نمی رسد زیرا این رویداد شرط اصلی در مرحله سوم پروتکل را ارضاء نمی کند و باید پروتکل دوباره باید تکرار شود.



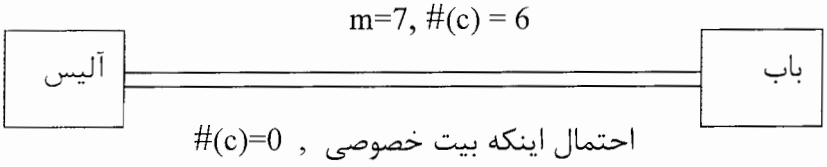
شکل(۶-۲) ؛ شبیه سازی رویداد E_3 m=#(c)

همان طوری که در شکل (۶-۲) مشاهد می شود؛ باب و آلیس با توجه به مرحله پنجم پروتکل توزیع بیت محرمانه یک بیت خصوصی از جفت های m را مخفی نگه می دارند و بقیه را به یکدیگر اعلام می کنند دو کاربرمجاز با اعلام نتایج متوجه می شوند که به جزء یک مورد همه دارای نتایج مخالف یکدیگر $(a \neq b)$ هستند بنابراین آنها می توانند با فرض اینکه بیت خصوصی مخفی نگه داشته شده نیز دارای نتیجه مخالف یکدیگر $(a_s \neq b_s)$ هستند رویداد E_3 را با موفقیت بدون استراق سمع ایو به پایان برسانند یعنی:

$$m = \#(c) = 7$$

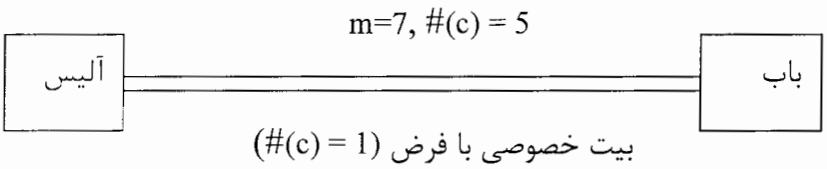
زیرا اگر ایو استراق سمع داشته باشد در آن صورت رابطه قبل برقرارنیست.

حال این سؤال پیش می آید که ممکن است آن بیت خصوصی دارای نتایج مخالف یکدیگر نباشد یعنی دقیق همان بیتی باشد که ایو استراق سمع نموده است. در این صورت رویداد E_2 شامل این مورد است.



شکل(۶-۳) ؛ شبیه سازی رویداد E_2 m-1=#(c)

رویداد E_1 در رخ دادن نیز پروتکل را به نتیجه نمی رساند زیرا دو کاربرمجاز پی به استراق سمع ایو می برند، حتی اگر بیت خصوصی نیزدارای نتیجه $a \neq b$ باشد باز هم مرحله ششم پروتکل شرط نتایج a , b را ارضاء نمی کند و حداقل در یک مورد نتیجه $a = b$ حاصل شده است.



شکل(۶-۴) ؛ شبیه سازی رویداد E_1 m-1>#(c)

با توجه به توضیحات بالا اکنون می توانیم رابطه زیر را برای احتمال آنکه چهار رویدادبالا رخ دهد وپروتکل با موفقیت به پایان رسد برابر است با:

$$P_\lambda(pass) = q_3 + q_2 P_\lambda(pass|E_2) \qquad (۲۲-۶)$$

در رابطه (۶-۲۲) عبارت $P_\lambda(pass|E_2)$ را در صورتی که در رویداد E_2 پروتکل با موفقیت به پایان رسد رابطه زیر را برای آن داریم:

$$P_\lambda(pass|E_2) = \sum_{i=2MN}^{MN^2} \frac{P(m=i|E_2)}{i} \qquad (۲۳-۶)$$

$$\text{Max}(P(m=i|E_2)) = 1$$

$$Min(i) = 2MN$$

$$P_\lambda(pass|E_2) = \sum_{i=2MN}^{MN^2} \frac{P(m=i|E_2)}{i} \leq \frac{1}{2MN} \qquad (۲۴-۶)$$

با توجه به فرض قضیه $P_{\lambda}(pass)\rangle\varepsilon$ باشد و روابط (۶-۲۲) و (۶-۲۴) ما می توانیم بنویسیم:

$$q_3\rangle\varepsilon-\frac{q_2}{2MN}$$

بنابراین حکم قضیه یعنی احتمال بیت خصوصی دارای نتایج مخالف یکدیگر باشند با شرط آنکه پروتکل با موفقیت به پایان رسد،با توجه به رابطه شرطی احتمال داریم:

$$P_{\lambda}(a_s\neq b_s|pass)=\frac{P_{\lambda}(a_s\neq b_s\wedge pass)}{P_{\lambda}(pass)}=\frac{q_3}{q_3+q_2P_{\lambda}(pass|E_2)}$$

رابطه بالا با افزایش q_3 به طور یکنواخت افزایش می یابد بنابراین داریم:

$$P_{\lambda}(a_s\neq b_s|pass)=\frac{q_3}{q_3+q_2P_{\lambda}(pass|E_2)}\rangle\frac{\varepsilon-\frac{q_2}{2MN}}{\varepsilon-\frac{q_2}{2MN}+\frac{q_2}{2MN}}=\frac{\varepsilon-\frac{q_2}{2MN}}{\varepsilon}$$

$$=1-\frac{q_2}{2MN\varepsilon}$$

$$\mathrm{Max}(q_2)=1$$

$$P_{\lambda}(a_s\neq b_s|pass)\rangle1-\frac{1}{2MN\varepsilon}$$

اگر این قضیه از شرط نا علامت دهی یعنی معتبر بودن تئوری نسبیت پیروی کند رابطه (۶-۹) و قانون تسسّل برای احتمالات نامعلوم با شرط آنکه پروتکل با موفقیت به پایان رسد برابر است با:

$$t_s\rangle1-\frac{1}{2MN\varepsilon}\qquad(۲۵-۶)$$

۶-۶-۲- مثال نقض

از حالا ما فرض می کنیم که این پروتکل با موفقیت به پایان می رسد، ما می توانیم بررسی نماییم که آلیس و باب و ایو هر سه سیستم مشترک دارند و معادله (۶-۲۵) نیز برقرار است. اکنون ما نشان می دهیم که این آگاهی یا استراق سمعی که ایو می تواند با انجام دادن یک اندازه گیری در سیستم خود بدست آورد اندک است.

ما این کار را توسط مثال نقض انجام می دهیم؛ بنابراین فرض می کنیم که با احتمال $0\langle\delta$ ایو نتیجه e_0 را بدست آورد بطوریکه داشته باشیم:

$$P_\lambda\left(a_s=b,b_s=\bar{b}\middle|A_s=X_k,B_s=X_{k+d},e_0\right)\rangle\frac{1}{2}\left(1+\delta'\right) \qquad (۲۶-۶)$$

رابطه (۶-۲۶) برای بعضی از $d=-1,0,1$; k که دراینجا $0\langle\delta'$ و $b\in\{0,1\}$ است و نیز داریم:

$$P_i^A\equiv P_\lambda\left(a_s=b\middle|A_s=X_i,e_0\right) \qquad (۲۷-۶)$$

$$P_i^B\equiv P_\lambda\left(b_s=\bar{b}\middle|B_s=X_i,e_0\right) \qquad (۲۸-۶)$$

شرایط ناعلامت دهی (۶-۹) با قاطعیت بیان می دارد که P_i^A مستقل از اندازه گیریی می باشد که باب انجام می دهد و بطور مشابه با آن P_i^B مستقل از اندازه گیریی است که آلیس انجام می دهد. این نکته ما را قادر می سازد که بنویسیم:

$$P_k^A,P_{k+d}^B\rangle\frac{1}{2}\left(1+\delta'\right) \qquad (۲۹-۶)$$

اثبات:

$$P_k^A\equiv P_\lambda\left(a_s=b\middle|A_s=X_k,e_0\right)\geq P_\lambda\left(a_s=b,b_s=\bar{b}\middle|A_s=X_k,B_s=X_{k+d},e_0\right)\rangle\frac{1}{2}\left(1+\delta'\right)$$

$$P_i^B\equiv P_\lambda\left(b_s=\bar{b}\middle|B_s=X_i,e_0\right)\geq P_\lambda\left(a_s=b,b_s=\bar{b}\middle|A_s=X_k,B_s=X_{k+d},e_0\right)\rangle\frac{1}{2}\left(1+\delta'\right)$$

حالا با توجه به مطلب بالا داریم:

$$P_\lambda\left(a_s=b,b_s=\bar{b}\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\leq P_\lambda\left(a_s=b\middle|A_s=X_i,e_0\right)=P_i^A \qquad (۳۰-۶)$$

$$P_\lambda\left(a_s=b,b_s=\bar{b}\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\leq P_\lambda\left(b_s=\bar{b}\middle|B_s=X_{i+c},e_0\right)=P_i^B \qquad (۳۱-۶)$$

$$P_\lambda\left(a_s=\bar{b},b_s=b\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\leq P_\lambda\left(a_s=\bar{b}\middle|A_s=X_i,e_0\right)=1-P_i^A \qquad (۳۲-۶)$$

$$P_\lambda\left(a_s=\bar{b},b_s=b\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\leq P_\lambda\left(b_s=b\middle|B_s=X_{i+c},e_0\right)=1-P_i^B \qquad (۳۳-۶)$$

$$P_\lambda\left(a_s\neq b_s\middle|A_s=X_i,B_s=X_{i+c},e_0\right)=P_\lambda\left(a_s=b,b_s=\bar{b}\middle|A_s=X_i,B_s=X_{i+c},e_0\right)+P_\lambda\left(a_s=\bar{b},b_s=b\middle|A_s=X_i,B_s=X_{i+c},e_0\right) \qquad (۳۴-۶)$$

با توجه به رابطه های (۶-۳۰)،(۶-۳۱)،(۶-۳۲)،(۶-۳۳) و (۶-۳۴) داریم:

$$P_\lambda\left(a_s\neq b_s\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\leq \mathrm{Min}\left(\mathrm{P_i^A},\mathrm{P_{i+c}^B}\right)+\mathrm{Min}\left(1-\mathrm{P_i^A},1-\mathrm{P_{i+c}^B}\right) \qquad (۳۵-۶)$$

سپس می توان به سادگی ثابت کرد:

$$\mathrm{Min}\left(\mathrm{P_i^A},\mathrm{P_{i+c}^B}\right)+\mathrm{Min}\left(1-\mathrm{P_i^A},1-\mathrm{P_{i+c}^B}\right)=1-\left|P_i^A-P_{i+c}^A\right| \qquad (۳۶-۶)$$

اثبات:

فرض می کنیم که $P_i^A\langle P_{i+c}^B$ باشد داریم:

$$\begin{cases}\mathrm{Min}\left(\mathrm{P_i^A},\mathrm{P_{i+c}^B}\right)=\mathrm{P_i^A}\\ \mathrm{Min}\left(1-\mathrm{P_i^A},1-\mathrm{P_{i+c}^B}\right)=1-\mathrm{P_{i+c}^B}\end{cases}\Rightarrow \mathrm{Min}\left(\mathrm{P_i^A},\mathrm{P_{i+c}^B}\right)+\mathrm{Min}\left(1-\mathrm{P_i^A},1-\mathrm{P_{i+c}^B}\right)$$
$$=\mathrm{P_i^A}+1-\mathrm{P_{i+c}^B}=1+\mathrm{P_i^A}-\mathrm{P_{i+c}^B} \quad ,\ \mathrm{P_i^A}-\mathrm{P_{i+c}^B}\langle 0 \qquad (۳۷-۶)$$

به طریق مشابه $P_{i+c}^B\langle P_i^A$ باشد داریم:

$$\begin{cases}\mathrm{Min}\left(\mathrm{P_i^A},\mathrm{P_{i+c}^B}\right)=\mathrm{P_{i+c}^B}\\ \mathrm{Min}\left(1-\mathrm{P_i^A},1-\mathrm{P_{i+c}^B}\right)=1-\mathrm{P_i^A}\end{cases}\Rightarrow \mathrm{Min}\left(\mathrm{P_i^A},\mathrm{P_{i+c}^B}\right)+\mathrm{Min}\left(1-\mathrm{P_i^A},1-\mathrm{P_{i+c}^B}\right)$$
$$=\mathrm{P_{i+c}^B}+1-\mathrm{P_i^A}=1+\mathrm{P_{i+c}^B}-\mathrm{P_i^A} \quad ,\ \mathrm{P_{i+c}^B}-\mathrm{P_i^A}\langle 0 \qquad (۳۸-۶)$$

بنابراین با استفاده از رابطه (۶-۳۵) و (۶-۳۶) رابطه (۶-۳۵) بدست می آید. بنابراین:

$$P_\lambda\left(a_s\neq b_s\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\le 1-\left|\mathrm{P_i^A}-\mathrm{P_{i+c}^B}\right|$$

حالا ما داریم:

$$\sum_{c=-1,0,1}\sum_{i=0}^{N-1}P_\lambda\left(a_s\neq b_s\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\le\sum_{c=-1,0,1}\sum_{i=0}^{N-1}\left[1-\left|\mathrm{P_i^A}-\mathrm{P_{i+c}^B}\right|\right] \qquad (۳۹-۶)$$

$$\sum_{c=-1,0,1}\sum_{i=0}^{N-1}P_\lambda\left(a_s\neq b_s\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\le\sum_{c=-1,0,1}\sum_{i=0}^{N-1}1-\sum_{c=-1,0,1}\sum_{i=0}^{N-1}\left|\mathrm{P_i^A}-\mathrm{P_{i+c}^B}\right|$$

$$\sum_{c=-1,0,1}\sum_{i=0}^{N-1}P_\lambda\left(a_s\neq b_s\middle|A_s=X_i,B_s=X_{i+c},e_0\right)\le 3N-\sum_{c=-1,0,1}\sum_{i=0}^{N-1}\left|\mathrm{P_i^A}-\mathrm{P_{i+c}^B}\right| \qquad (۴۰-۶)$$

از طرفی با توجه به ناعلامت دهی رابطه (۶-۹) داریم:

$$\begin{cases}\sum\mathrm{P_{i+c}^B}=\sum P_\lambda\left(b_s=\bar{b}\middle|B_s=X_{i+c},e_0\right)\\ \sum\mathrm{P_{i+c}^A}=\sum P_\lambda\left(a_s=b\middle|A_s=X_{i+c},e_0\right)\end{cases}\Rightarrow\sum\mathrm{P_{i+c}^B}=\sum\mathrm{P_{i+c}^A} \qquad (۴۱-۶)$$

$$3N-\sum_{c=-1,0,1}\sum_{i=0}^{N-1}\left|\mathrm{P_i^A}-\mathrm{P_{i+c}^B}\right|=3N-\sum_{c=-1,0,1}\sum_{i=0}^{N-1}\left|\mathrm{P_i^A}-\mathrm{P_{i+c}^A}\right|=$$

$$3N-\sum_{i=0}^{N-1}\left(\left|\mathrm{P_i^A}-\mathrm{P_{i-1}^A}\right|+\left|\mathrm{P_i^A}-\mathrm{P_i^A}\right|+\left|\mathrm{P_i^A}-\mathrm{P_{i+1}^A}\right|\right)\le 3N-\sum_{i=0}^{N-1}\left(\left|\mathrm{P_i^A}-\mathrm{P_{i+1}^A}\right|\right) \qquad (۴۲-۶)$$

زیرا رابطه زیر همواره برقرار است:

$$\sum_{i=0}^{N-1}\left(\left|P_i^A - P_{i-1}^A\right| + \left|P_i^A - P_i^A\right| + \left|P_i^A - P_{i+1}^A\right|\right) \geq \sum_{i=0}^{N-1}\left(\left|P_i^A - P_{i+1}^A\right|\right) \qquad (۴۳-۶)$$

از طرفی داریم:

$$\sum_{i=0}^{N-1}\left(\left|P_i^A - P_{i+1}^A\right|\right) = \left|P_0^A - P_1^A\right| + \left|P_1^A - P_2^A\right| + \ldots \left|P_k^A - P_{k+1}^A\right| \ldots + \left|P_{N-2}^A - P_{N-1}^A\right| \rangle \left|P_k^A - P_{k+1}^A\right|$$

$$, \quad P_1^A + P_2^A \ldots + P_{k+1}^A + \ldots + P_{N-1}^A = 1 \rightarrow P_{k+1}^A = 1 - P_1^A + P_2^A \ldots + P_k^A + \ldots + P_{N-1}^A$$

$$\left|P_k^A - P_{k+1}^A\right| = \left|P_k^A - \left(1 - P_1^A + P_2^A \ldots + P_k^A + \ldots + P_{N-1}^A\right)\right\rangle \left|P_k^A - \left(1 - P_k^A\right)\right\rangle$$

$$\sum_{i=0}^{N-1}\left(\left|P_i^A - P_{i+1}^A\right|\right)\rangle\left|2P_k^A - 1\right| \qquad (۴۴-۶)$$

با استفاده از رابطه (۶-۲۹) داریم:

$$P_i^A \rangle \frac{1}{2}(1+\delta') \rightarrow \delta' \langle 2P_i^A - 1 \rightarrow \sum_{i=0}^{N-1}\left(\left|P_i^A - P_{i+1}^A\right|\right)\rangle\left|2P_k^A - 1\right|\rangle\delta' \qquad (۴۵-۶)$$

بنابراین با استفاده از رابطه (۶-۴۲) در کل داریم:

$$\sum_{c=-1,0,1}\sum_{i=0}^{N-1} P_\lambda\left(a_s \neq b_s \middle| A_s = X_i, B_s = X_{i+c}, e_0\right) \leq 3N - \left|2P_k^A - 1\right| \leq 3N - \delta' \qquad (۴۶-۶)$$

نا مساوی بالا درشرایطی که ایو اندازه گیریش را انجام دهد پروتکل نیز با موفقیت بـه پایـان رسـد برابر است با :

$$t_s = \frac{1}{3N}\sum_{c=-1,0,1}\sum_{i=0}^{N-1} P_\lambda\left(a_s \neq b_s \middle| A_s = X_i, B_s = X_{i+c}, e_0\right) \leq 1 - \frac{(\delta\delta')}{3N}$$

$$\Rightarrow t_s \leq 1 - \frac{(\delta\delta')}{3N} \qquad (۴۷-۶)$$

برای هر مقدار ثابت $(\delta, \delta' \rangle 0)$ ما می توانیم مقادیر M, N, ε را انتخاب کنیم که روابط (۶-۲۵) بـا (۶-۴۷) متناقض باشد؛ یعنی اطلاعات حاصل از اندازه گیریی که ایو بدست آورده است با نقض این دو رابطه محدود می شود و امنیت با نقض آن تضمین می گردد.

برای مثال با فرض $\varepsilon = N^{-\frac{1}{4}}, M = N^{\frac{3}{4}}$ آنرا بررسی می کنیم:

مقادیر فرض شده بالا را دررابطه (۶-۲۵) جایگذاری می کنیم:

$$t_s \rangle 1 - \frac{1}{2MN\varepsilon} \rightarrow t_s \rangle 1 - \frac{1}{2N^{\frac{3}{4}} N N^{-\frac{1}{4}}} \rightarrow t_s \rangle 1 - \frac{1}{2N^{\frac{3}{2}}} \qquad (۴۸-۶)$$

این رابطه با فرض مقادیر بالا نشان می دهد که آلیس و باب دارای نتایج حاصل از اندازه گیریهای مخالف یکدیگرند و پروتکل با موفقیت به پایان رسیده است.

برای اینکه رابطه (۶-۴۸) و (۶-۴۷) یکدیگر را نقض کنند داریم:

$$1-\frac{\delta\delta'}{3N}\langle 1-\frac{1}{2N^{\frac{3}{2}}}\Rightarrow\frac{\delta\delta'}{3N}\rangle\frac{1}{2N^{\frac{3}{2}}}\rightarrow\delta\delta'\rangle\frac{3N}{2N^{\frac{3}{2}}}\rightarrow\delta\delta'\rangle\frac{3}{2N^{\frac{1}{2}}}\rightarrow N^{\frac{1}{2}}\rangle\frac{3}{2\delta\delta'}$$

$$\Rightarrow N\rangle(\frac{3}{2\delta\delta'})^2 \qquad (۴۹-۶)$$

با توجه به آنکه مقادیر ثابت $(\delta,\delta'\rangle 0)$ بسیار کوچک هستند به ازایN به اندازه کافی بزرگ با توجه به رابطه (۶-۴۹) دو رابطه (۶-۲۵) و (۶-۴۷) یکدیگر را نقض می کنند.

باید توجه داشت که اگر نتایج آلیس وباب به طور کلاسیکی در میان یک تئوری متغیر پنهانی موضعی مربوط شوند،فرصت اینکه پروتکل با موفقیت به پایان رسد بسیار اندک است وانتخاب پارامتر ها برای اینکه روابط (۶-۲۵) و (۶-۴۷) یکدیگر را نقض کنند وجود ندارد.

اگرچه ما پارامتر ایمنی $M\langle\langle N$ را برای ساده نمودن بحث محدود کرده ایم با این حال این پروتکل می تواند برای پذیرفتن M به طور قرار دادی بزرگ تعمیم داده شود[۳۷] .

۶-۷- نتیجه گیری

اثبات ایمنی پروتکل بالا آزمودن آلیس و باب در تعداد جفت هایی است که بایستی نتایج توافق شده یعنی مخالف یکدیگر داشته باشند و از طرفی با انتخاب پارامتر های مناسب دانش و آگاهی استراق سمع ایو در پروتکل محدود می شود،بنابراین امنیت آن را حتی در مقابل تهاجمات انبوه ایو در تئوری فرا کوانتومی تضمین می کند. در نتیجه این پروتکل به آلیس و باب اجازه آن را می دهد که آنها بیت مشترک محرمانه واحد را ایجاد کنند. این پروتکل می تواند برای ایجاد یک رشته بیت محرمانه مشترک با ضمانت مشابه تعمیم داده شود.

نا موضعیت برای موفقیت این پروتکل بسیارمهم است. این مورد به سادگی دیده می شود که اگر آلیس و باب نامساوی بل را نقض نمی کردند، آنگاه ایو می توانست کاملاً با آماده کردن هر جفت از سیستم ها در یک حالت فرا کوانتومی دترمینستیک (در اینجا به معنای تمام احتمالات توسط حالت های 0 و1 تعیین می شود) و موضعی اطلاعات لازم در مورد نتایج حاصل از اندازه گیری آلیس وباب را بدست آورد. به عبارت دیگر آلیس و باب نامساوی بل را نقض کنند آنگاه حداقل بعضی از حالت های فراکوانتومی فراهم شده توسط ایو باید ناموضعی باشد. از طرفی هر حالتی که دترمینستیک و ناموضعی باشد علامت دهی حداکثر با سرعت نور (اعتبار تئوری نسبیت) را مجاز می داند[۳۳] .بنابراین ما با طرح این پروتکل توزیع بیت محرمانه امنیت آنرا به طور قابل اثبات با فرض علامت دهی تضمین نموده ایم یعنی با اعتبار تئوری نسبیت استراق سمع کننده را مجاز نموده ایم که قادر باشد قوانین مکانیک کوانتومی را نقض نماید. بنابر این با این استراتژی آگاهی ایو از طریق استراق سمع در پروتکل غیر ممکن است. زیرا می توانیم بگوییم پروتکل وقتی در شرایط نا علامت دهی فرض شود روابط ناموضعیت را برای یک جفت در هم تنیده در تئوری کوانتومی ارضاء می کند[۳۱].

۶-۸- پیشنهادات

ناموضعیت یعنی نقض نامساوی بل برای موفقیت این پروتکل بسیارمهم است که تحمل آگاهی از نویز استراق سمع ایجاد شده به ۲۹/۳٪ می رسد اخیراً در مقاله ای مساوی و نامساویی در مقایسه با نامساوی های بل بدست آمده است که در آن نظریه کوانتومی موضعیت را با قدرت بیشتری نقض می کند و تحمل آگاهی از نویز استراق سمع کننده تقریباً دو برابر قبل یعنی به ۵۸/۶٪می رسد[۳۸] بنابراین می توان پروتکل توزیع کلید کوانتومی در چارچوب کوانتومی و فرا کوانتومی را با بکار بردن این مساوی و نامساوی ها تعمیم داد و نتایج بسیار خوبی را بدست آورد. جالب به نظر می رسد که عملکرد های دیگر از پروتکل توزیع کلید کوانتومی محرمانه نتایج اندازه گیریهای آنها توسط دو کاربر مجازشامل ناموضعیت نمی شود و امنیت آنها را بدون نقض نامساوی بل تضمین می شود مورد بررسی قرار گیرد [۳۴] .

منابع

[1].D.Mermin.2005.Lecture notes on Quantum Computation. Physics 481-681, CS 483.

[2].J.Perskill.2001.Lecture notes for Ph219/CS219

[3].A. Ekert, P. Hayden, and H.Inamori.2001.Basic concepts in quantum computation.quant-ph/0011013.

[4].A.Chatterjee.2003. Introduction to quantum computation. quant-ph/0312111.

[5].Sara M.McMurry.1993-94. Quantum Mechanics, pp.337-346.

[6].A.zeilinger.1997. A Fundamental Concept Finding its Applications, PP.12-18.C.Macchiavello, G.M.Palma, A.zeilinger.1999. , Quantum computation and Quantum Information.ISBN 981-02-4117-8.World scientific, Singapore. New Jersey. London. Hong Kong.

[7].G.Ribordy, N.Gisin, and H. Zbinden. Quantum key distirbution, PP.235-239.C.Macchiavello, G.M.Palma, A.zeilinger.1999. , Quantum computation and Quantum Information.ISBN 981-02-4117-8.World scientific, Singapore. New Jersey. London. Hong Kong.

[8].W.Tittle, G.Ribordy, and N.Gisin. Quantum Cryptography, PP.240-244.C.Macchiavello, G.M.Palma, A.zeilinger.1999. , Quantum computation and Quantum Information.ISBN 981-02-4117-8.World scientific, Singapore. New Jersey. London. Hong Kong.

[9].G. Auletta. 2001. Foundations and Interpretation of quantum mechanics. World scientific. Singapore. New Jersey. London. Hong Kong.

[10].Michael a. Neilson, and Isaac L. Chuang 2003. Quantum computation and Quantum Information. World scientific, Singapore.

[11]. F. Halzen, Alen D. martin. 1984. Quark and leptons: An Introduction course in modern particle physics.

[12]. J.J. Sakurai. 1982. Modern Quantum Mechanics.

[13]. A.Prers. 2002. Quantum Theory: Concepts and methods.Kluwer Academic publishers. Newyork, Boston, London, Moscow.

[14]. A. Kent. 2002. Non Linerarity with out superluminality.quan-ph/0204106.

[15]. Richard J.Hughes. 1998. Quantum Cryptography, PP.88-92. Quantum computing and communication.

[16]. A. Ekert.2004. Introduction and over view.

[17]. C. H. Bennett. 1992. Quantum Cryptography using any two Non Orthogonal states. Phys. Rev. Lett. 68. 3121-3124.

[18]. A.Ekert.1991. Quantum Cryptography Based on Bell's Theory. Phys. Rev. Lett. 67. 661-663.
[19]. S. Wiesner. 1983. Proc IEEE int. Conference on computer, system and signal processing. SIGACT News 15, 78.
[20]. C. H. Bennett, and G. Brassard. 1984. In proceeding of IEEE International Conference on computer, system and signal processing, P. 175.
[21]. M.Hillery, V. Buzek, and A. Berthiaume.1999. Quantum secret sharing. Phys. Rev. A 59. 1829-1834.
[22]. R.Cleve, D. Gottesman, and H.K.Lo. 1999. How to share a quantum secret. Phys. Rev. Lett. 83, 648-651.
[23]. A. Kent. 2003. Quantum Bit string commitment. Phys. Rev. Lett. 90. 237901.
[24]. L. Hardy, and A. Kent. 2004.Cheat sensitive quantum Bit commitment. Phys. Rev. Lett. 92. 157901.
[25]. A. Kent. 1999. Unconditionally secure Bit commitment. Phys. Rev. Lett. 83. 1447.
[26]. A. Kent. 2006. Secure classical Bit commitment using fixed capacity communication channels. quant-ph/9906103.
[27]. A. Kitaev, D.Mayers, and J. Perskill.2004. Superselection rule and quantum protocols. Phys. Rev . A 69. 052326.
[28]. F. Verstracte, and J. I. Cirac. 2003. Quantum Non locality in the presence of. Superselection rules and data hiding protocolls. Phys. Rev. Lett. 91. 10404.
[29].J. S. Bell.1964.Speakable and unspeakable in quantum mechanics. Phys.1, 195.
[30]. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt.1969. Proposed Experiment to test local hidden-variable theories. Phys. Rev. Lett. 23. 880.
[31]. J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. 2005. Non local correlation as an information-throretic resource. Phys. Rev. A 71. 22101.
[32] S. Braunstein and C. Caves. 1990. Wringing out better Bell Inequalities. Ann. Phys. 202. 22-56
[33] A. Valentini. 2002. Signal locality in hidden variables theories. Phys. Lett. A 297, 273.
[34] C. H. Bennett, G. Brassard, and N. D. Mermin. 1992. Quantum cryptography with out Bell's theorem. Phys.Rev. Lett. 68. 557.
[35].A. Einstein, B. Podolski, N.Rosen.1935. Pgys. Rev. 41. 1881.
[36]. J. F. Clauser, and A. Shimony.1978. . Rep. Prog . Phys. 41.1881.
[37].J. Barrett, L. Hardy, and A. Kent.2005. Non signaling and quantum key distribution. Phys. Rev. Lett. 95. 010503. quant-Ph/0405101.
[38]. H.Movahhedian.Stronger violation of local throries with equalities. J.Phys.A:Math.Theor.40,2839-2847(2007) . quant-ph/0611124.

Abstract:

Confidential information and its transfer safely has still been one of human mental disturbance during history. The Confidential information one transferred with relative acceptable Security regards to advancement of Science and technology and build of classical Computer; but this kind of information transfer isn't secured with 100 percent Safely. Theory – Maker physicists recently could offer cryptography protocols with confidential Quantum key distribution based Valid theory or physic principles to information world with provably secure; they have secured the security of quantum key distribution protocol in the basis on of quantum theory validity, relativity and other valid physic principle with certainty. In this study, we also encode confidential information in the from of quantum qubits in Quantum computers, so that , first we detected the structure of quantum computer using quantum theory and obtained entanglement qubit which is confidential information carrier between two allowed user by means of its two- input gates and then we paid to bipartite qubit applications which are the same entanglement quantum states in quantum computers, after that we considered them By use of quantum theory Compatibility and relativity that which maximum rate transfer in entanglement qubits equal to light speed and by expression EPR theorem, Because it can be better identified wonderful phenomenon of entanglement quantum states, Besides, we investigated on quantum theory- in detail – a bout subjects Such as causality, locality and hidden Variable, then assuming variables of Bell inequality Locality – causality. As a result, we achieved to quantum theory and applied some examples as a sample for violation of Bell inequality and its generalization. We introduced quantum cryptography protocols with confidential quantum key distribution by use of entanglement quantum states.

And we studied in detail the basic ideas for such protocols with its security which using uncertainty principle and Violation of bell inequality resulted from Noise that produced by eavesdropper in quantum state which is the original factor of quantum key distribution security. At last proceeded to Confidential quantum key distribution protocol in post quantum theory, so that; it just secures this Confidential key distribution Security Based on Validity of relatively theory.

This Mean that, it is assumed the maximum Signaling rate is equal to light speed and allow to eavesdropper to Continue eavesdropping By use of post quantum theory; as a result, we are doubtful relative to quantum theory in this protocol; so that, it never be used quantum theory Validity for security and we allow to eavesdropper who can violate quantum mechanic theory. As a consequence, we assured the security of this protocol by violation of bell inequality in non locality area provably secure.