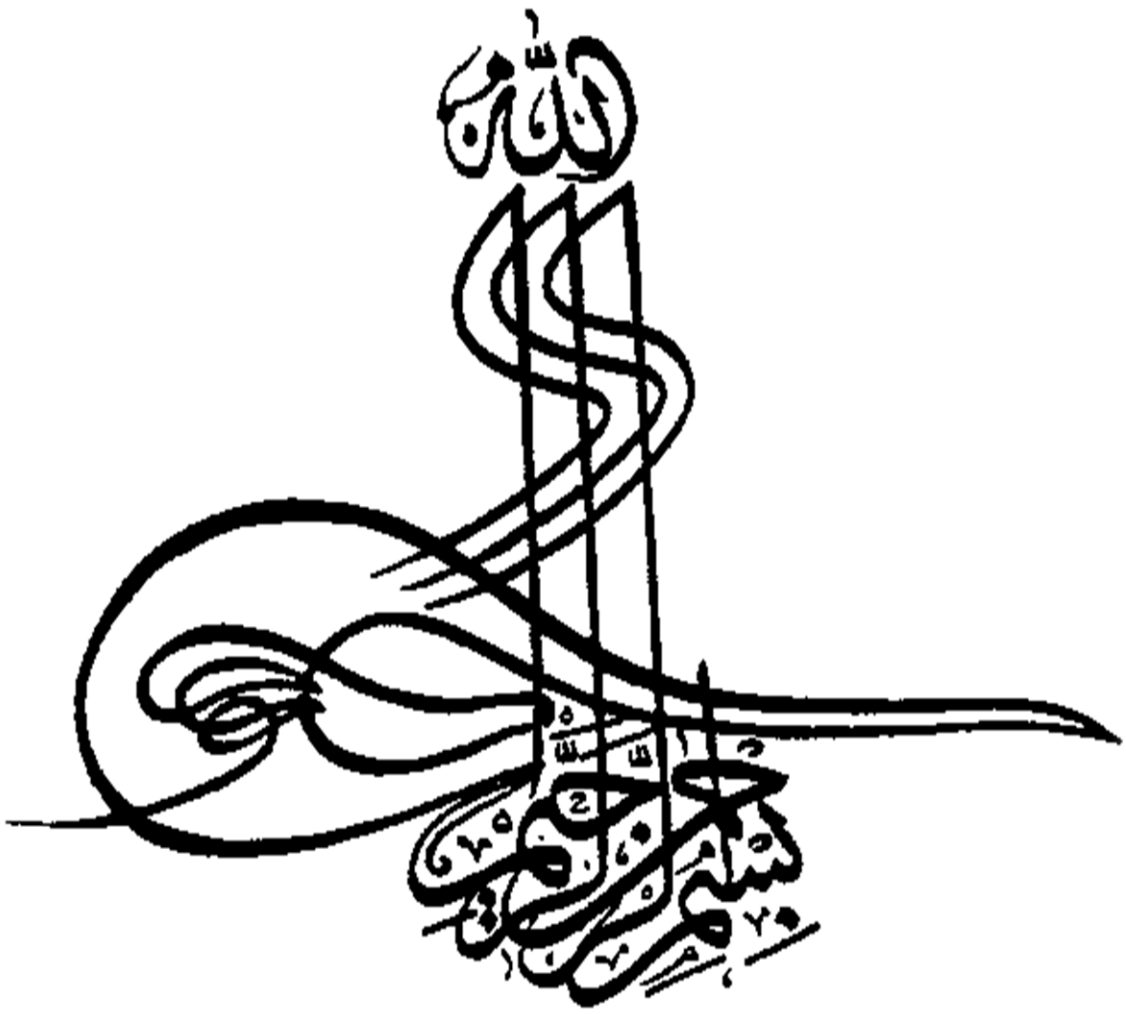

بسم الله الرحمن الرحيم

دانشکده : فیزیک

گروه : فیزیک ذرات بنیادی

عنوان:

توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری

دانشجو :

شکوفه فرضی یکنمی

استاد راهنما :

دکتر حسین موحدیان

پایان نامه ارشد جهت اخذ درجه کارشناسی ارشد

بهمن ماه ۱۳۹۲

سپاس بی پایان از خدای من

خدایا رودی هستم که نام‌های تو را زمزمه می‌کنم و
می‌گذرم.
از این‌که جریان پیوسته دارم سپاس‌گذارم خدای من چنانم آفریدی که هیچ سنگی نمی‌تواند
راهم را به سوی تو سد کند سپاس‌گذارم خدای من سپاس گذارم.
راه‌های پر پیچ و خم را پشت سر می‌گذارم سپاس‌گذارم که از همه راه‌ها مرا
می‌گذرانی.
خدایا خداوندا شایستگی زمزمه‌های نورانی‌ات را از من دریغ مدار.
سروده رود جز دریا دریا دریا چه می‌تواند باشد.

تقدیم با تمام وجود

تقدیم با بوسه بر استوارترین تکیه گاهم دستان پر مهر پدرم که هر چه از او می‌گویم باز هم کم می‌آورم و سبزترین نگاه زندگیم نگاه مهربان مادرم که شوق زیبای نفس کشیدن است. آموزگارانی که برایم زندگی، بودن و انسان بودن را معنا کردند.

پروردگارا نه می‌توانم موهایشان را که در راه موفقیت من سفید شد سیاه کنم و نه بر دست‌های پینه بسته‌شان که ثمره تلاش برای افتخار من است مرهمی باشم پس توفیقم ده که هر لحظه شکرگذارشان باشم و ثانیه های عمرم را در عصای دست بودنشان بگذرانم.

تقدیر و تشکر

«ویزکیهم و یعلمهم الکتاب و الحکمه»

سپاس بیکران پروردگار را که هستی‌مان بخشید و به طریق علم و دانش رهنمونمان شد و به هم‌نشینی رهروان علم و دانش مفتخرمان نمود و خوشه چینی از علم و معرفت را روزیمان ساخت.

اکنون که با یاری خدای متعال موفق به اتمام این مقطع تحصیلی شده‌ام، بر خود لازم می‌دانم از زحمات استاد بزرگوار **جناب آقای دکتر موحدیان** که در کمال سعه صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه بر من دریغ ننمودند کمال تشکر و قدردانی را داشته باشم.

و از جناب پرفسور رجبی و جناب دکتر عنابستانی و جناب دکتر حسن حسن آبادی که با سعه‌ی صدر داوری این پایان نامه رو پذیرفتند کمال تشکر دارم.

و از تمام دوستانم و هم‌کلاسی‌های عزیز و خوبم به خاطر کمک‌ها و حمایت‌هایشان سپاسگزارم و از خداوند منان توفیق روزافزون آنان را خواستارم.

و در کلام آخر این مجموعه را به یکایک اعضای خانواده‌ام به پاس عاطفه سرشار و گرمای امید بخش وجودشان که بهترین پشتیبان زندگانی من است تقدیم می‌کنم.

تعهد نامه

اینجانب **شکوفه فرضی یکنمی** دانشجوی دوره کارشناسی ارشد **فیزیک ذرات بنیادی** دانشکده **فیزیک** دانشگاه **صنعتی شاهرود** نویسنده پایان نامه **توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری** تحت راهنمائی **آقای دکتر حسین موحدیان** متعهد می‌شوم.

- تحقیقات در این پایان نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است .
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است .
- مطالب مندرج در پایان نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است .
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می باشد و مقالات مستخرج با نام « دانشگاه صنعتی شاهرود » و یا « **Shahrood University of Technology** » به چاپ خواهد رسید .
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده اند در مقالات مستخرج از پایان نامه رعایت می گردد.
- در کلیه مراحل انجام این پایان نامه ، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است .
- در کلیه مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری ، ضوابط و اصول اخلاق انسانی رعایت شده است .

تاریخ

امضای دانشجو

مالکیت نتایج و حق نشر

- *کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج ، کتاب ، برنامه های رایانه ای ، نرم افزار ها و تجهیزات ساخته شده است) متعلق به دانشگاه صنعتی شاهرود می باشد . این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود .*
- *استفاده از اطلاعات و نتایج موجود در پایان نامه بدون ذکر مرجع مجاز نمی باشد.*

چکیده:

یکی از مهمترین مسائلی که در اطلاعات کوانتومی با آن مواجه هستیم، انتقال اطلاعات به صورت ایمن می‌باشد. ابتدا پروتکلی را معرفی می‌کنیم که همانند همه پروتکل‌های توزیع کلید کوانتومی (QKD)، امنیت آن مبتنی بر قوانین فیزیک کوانتومی است و دیگر این که هیچ اطلاعاتی از آزمایشگاه دو کاربر مرتبط فاش نمی‌شود. سپس پروتکل توزیع کلید کوانتومی مستقل از دستگاه (DIQKD) مطرح خواهیم کرد. اثبات ایمنی این پروتکل بر فرضیات کمتری استوار است، بدین معنی که دو کاربر مرتبط نه تنها از ساختار دستگاه‌هایشان به طور دقیق خبر ندارند بلکه به دستگاه‌هایشان هم اعتماد نخواهند کرد و یا اینکه فرض نمی‌کنیم که دستگاه‌های آلیس و باب مشخصه‌ی از قبل تعیین شده داشته باشند، چون ممکن است که دستگاه‌های اندازه‌گیری آلیس و باب توسط استراق‌سمع‌کننده (ایو) دستکاری شوند. اگر ایمنی این نوع پروتکل‌ها بر اساس نقض نامساوی بل اثبات شود [۱۴]، در آن صورت هر پروتکل توزیع کلید کوانتومی مستقل از دستگاه در مقایسه با پروتکل توزیع کلید کوانتومی ایمنی به مراتب قوی‌تری خواهد داشت. متاسفانه این پروتکل مستقل از دستگاه عملا امکان پذیر نیست زیرا به بازده آشکارسازی نزدیک واحد و آهنگ بسیار پایین تولید کلید در فاصله‌های عملی نیاز دارد [۱۳]. بنابراین ایده توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری را به عنوان یک راه حل ساده مطرح می‌کنیم. زیرا نقص‌هایی نظیر بازده آشکارسازی نزدیک واحد و آهنگ بسیار پایین تولید کلید در فاصله‌های عملی که در پروتکل مستقل از دستگاه وجود دارد را ندارد.

گذشته از این، این پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری نه تنها عامل حذف تمام کانال‌های جانبی آشکارساز است بلکه فاصله ایمن را با لیزرهای معمولی نیز دو برابر می‌کند. بنابراین هدف پروتکل‌های مستقل از دستگاه اندازه‌گیری که در اینجا تحلیل و بررسی می‌کنیم؛ توزیع کلید سری‌ای است که امنیت آن براساس قوانین فیزیک کوانتومی است، بنابراین در این طرح فرض می‌کنیم که بیت‌های رشته

کلید مستقل از هم باشند و با هم برهم‌کنش نداشته باشند، همچنین با یکدیگر فاصله فضاگونه داشته باشند و در نتیجه از آن برای تولید آهنگ کلید ایمن استفاده می‌کنیم.

واژگان کلیدی: توزیع کلید کوانتومی، توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری، حمله NOT کنترلی، BB۸۴، آهنگ کلید ایمن.

لیست مقالات مستخرج از پایان نامه

۱- شکوفه فرضی یکنمی، دکتر حسین موحدیان **"حمله NOT کنترلی در توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری"** کنفرانس فیزیک محاسباتی ایران، ۲-۱ بهمن ماه ۱۳۹۲

۲- شکوفه فرضی یکنمی، دکتر حسین موحدیان **"تغییر جهت قطبش در توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری"** کنفرانس فیزیک ذرات بنیادی و میدان‌ها، ۸-۷ بهمن ماه ۱۳۹۲

فهرست مطالب

فصل اول : رمزنگاری کوانتومی

فصل دوم : قرارداد BB۸۴

فصل سوم : بررسی حمله NOT کنترلی شخص ثالث در پروتکل MDI-QKD

فصل چهارم : پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری

فهرست اشکال

فهرست جداول

فصل اول

رمزنگاری کوانتومی

- مقدمه
- رمزنگاری
- رمزنگاری کوانتومی
- توزیع کلید کوانتومی
- نتیجه‌گیری

۱-۱- مقدمه:

رمزنگاری[۱] برگرفته از واژه یونانی به معنای محرمانه نوشتن می باشد. رمزنگاری با وجود یک تاریخچه رنگانگ تنها بخشی از تئوری اطلاعات است و یکی از شاخه‌های اصلی علوم رایانه‌ای می‌باشد. در رایانه‌ها جهت ایمنی شبکه‌ها و کنترل اطلاعات ایمن مورد استفاده قرار می‌گیرد در بسیاری از کابردهای روزمره قابل لمس است، از جمله ایمنی کارت‌های ATM،... پسوردهای رایانه‌ای، تجارت‌های الکترنیکی و غیره که همگی به رمزنگاری وابسته هستند.

ابتدایی‌ترین تکنیک‌های رمزنگاری سنتی، مربوط به عملکرد جابجایی‌سازی[۲] است که به عنوان ساده‌ترین نوع رمزنگاری مطرح می‌شود. در اینجا هریک از حروف یا علائم پیغام که با یکدیگر جابجا شده‌اند دوباره توسط گیرنده پیغام رمزگشایی می‌شود.

مثلا در نمونه زیر پیغام ارسالی در تکنیک‌های سنتی با عملکرد جابجاسازی رمزنگاری شده است:

Help me ⟶ ehpl me

نوع دیگر تکنیک رمزنگاری سنتی با عملکرد جانشین‌سازی[۳] است، یعنی هر یک از حروف یا علائم پیغام به شکل ویژه‌ای که برای گیرنده پیغام قابل درک باشد تغییراتی داده شود.

مانند:

fly a once ⟶ gmz bu padf

---

۱. cryptography

۲. Transposition

جولیوس سزار متون رمزی در تکنیک جابجاسازی را در طول لشکرکشی نظامی‌اش مورد استفاده قرار می‌داد.

۳. Substitution

به عنوان نمونه دیگر از رمزنگاری در تکنیک جانشین سازی می‌توان به رمزنگاری مسیحیان در متون مذهبی از کتابشان را نام برد.

تکنیک‌های رمزنگاری مدرن در اوایل قرن بیستم به همراه چندین شیوه و روش رمزگذاری و رمزگشایی ریاضی اختراع شد؛ مشهورترین آن‌ها ماشین اینگما[1] بود. این ماشین توسط آلمان‌ها در جنگ جهانی دوم استفاده شد. پیشرفت رایانه‌های دیجیتالی و الکترونیکی بعد از جنگ جهانی دوم رمزنگاری بسیار پیچیده‌تر را امکان پذیر نمود؛ که بسیاری از رمزنگاری‌های رایانه‌ای می‌تواند در رشته‌هایی از بیت‌های باینری مشخص شوند، رایانه‌ها حوزه‌های رمزنگاری را به صورت پیچیده‌تر مهیا ساخته‌اند، به وسیله این تکنیک‌های مدرن و پیشرفته امنیت و ایمنی کار رمزنگاری بر الگوریتم‌های پیچیده مسائل محاسباتی بسیار مشکل و دیر حل شدنی تکیه دارد، که شکستن این گونه رمزنگاری مدرن کاری بس غیر مؤثر و ناکارآمد است و نیاز به تلاش بسیار زیادی دارد.

رمزنگاری به طور عمده قبل از اوایل قرن بیستم با الگوهای زبان شناسی رابطه داشت و پس از آن تغییر نموده و بعد از آن رمزنگاری استفاده وسیعی از ریاضیات شامل جنبه‌های اطلاعاتی، محاسبات پیچیده، آمار و ترکیبات، جبر مطلق و تئوری اعداد را دارد.

امروزه تکنیک‌های رمزنگاری کوانتومی به گونه‌ای است که استراق‌سمع‌کنندگان، محدودیتی در علم، تکنولوژی و قدرت محاسباتی ندارند. مهندسین علم رمزنگاری همواره سعی دارند فعال‌تر و هوشمندتر از استراق‌سمع‌کنندگان باشند و تحقق این کارها هنگامی صورت می‌گیرد که آن‌ها استراق‌سمع‌کنندگان دارای علم و تکنولوژی نامحدود را به مبارزه بطلبند. در این صورت بهترین روش این است که در پی جستجوی رابطه‌ای بین رمزنگاری ایمن با علم فیزیک کوانتومی باشیم، که امروزه تحقیقات فراوانی توسط دانشمندان فیزیک کوانتومی در این زمینه صورت گرفته و با فرض بالا پروتکل‌های رمزنگاری ایمن را به دنیای اطلاعات محرمانه عرضه داشته‌اند.

---

[1] Enigma

۱-۲- رمزنگاری:

رمزنگاری فرآیندی است که اجازه می‌دهد دو کاربر مرتبط با یک کانال ارتباطی ساختاری از اطلاعات محرمانه و مشترک را به وجود آورند. در نوشته‌های رمزشناسی، اطلاعاتی که باید رمزنگاری شوند به عنوان متن قابل درک (پیغام) شناخته می‌شوند؛ پارامترهای ویژه‌ای به نام کلید رمز وجود دارند که به صورت رشته بیت‌های تصادفی هستند که باعث تغییر شکل متن قابل درک می‌شوند و آنها را به کدهای محرمانه تبدیل می‌کند؛ این کدها عموما به شکل رشته بیت‌هایی است که می‌تواند به عنوان کد محرمانه برای روابط امنیتی مورد استفاده قرار گیرد. در حقیقت رمزنگاری هنر تقسیم و ارتباط بین کدهای محرمانه و کلید رمز بین دو کاربر است. تجزیه و تحلیل این رمزها هنر شکستن آن‌ها می‌باشد. رمزشناسی ترکیبی از آن دو می‌باشد.

امروزه رمزنگاری تقریبا منحصر به رمزگذاری و رمزگشایی است. رمزگذاری یعنی فرآیند تبدیل اطلاعات مثلا 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 رمزگذاری و دیگری برای رمزگشایی که این الگوریتم‌ها طوری طراحی شده‌اند که اطلاعات را بدون هیچ گونه کار اضافی رمزگذاری و رمزگشایی می‌کنند. در اصل امنیت یک متن رمزگذاری شده بستگی به محرمانه بودن روش کار رمزگذاری و رمزگشایی دارد. امروزه از الگوریتم‌هایی برای رمزگذاری و رمزگشایی استفاده می‌کنیم که این الگوریتم‌ها می‌توانند بدون به مخاطره انداختن امنیت رمزنگاری در دسترس عموم قرار گیرند. با تعریف الگوریتم مناسب به همراه کلید رمز و متن قابل درک می‌توان آن‌ها را به کدهای رمز (متن رمزگذاری شده) تبدیل نمود که این دقیقا یک فرآیند رمزگذاری است. بنابرین با تعریف الگوریتم مناسب دیگر این متن رمزگذاری شده به وسیله کلید رمز، رمزگشایی نمود و پیغام را دریافت؛ رمزگذاری ضرورتا درمورد سه نفر است.

آلیس که می‌خواهد پیغامی محرمانه، بدون اطلاع هر استراق‌سمع‌کننده‌ای مانند ایو به شخصی به نام

باب برساند. در این صورت نیاز به این است که آلیس پیغام M و کلید K را برای تولید رمز C با استفاده از یک الگوریتم مناسب E رمزگذاری کند و برای باب بفرستد.

روش رمزگذاری را به صورت زیر نمایش می‌دهیم:

$C = E (M+K)$

و باب با استفاده از الگوریتم مناسب دیگر D و داشتن کلید رمز K که قبلا از طریق یک کانال کاملا خصوصی، توسط آلیس به باب ارسال شده است و متن رمزی آن را رمزگشایی می‌کند و سرانجام به صورت پیغام دریافت می‌نماید.

عمل رمزگشایی نیز مانند روش رمزگذاری به صورت زیر انجام می‌شود.

$M = D(C+K)$

در چنین سیستم‌های متداول و منظم آلیس و باب یک کلید رمز را مورد استفاده قرار می‌دهند، که به صورت بیت‌های تصادفی است که آلیس را قادر به رمزگذاری پیغام، و باب را قادر به رمزگشایی متن رمزی می‌نماید. بعد از اینکه تمام مراحل کار رمزنگاری به صورت ایمن توسط آلیس و باب انجام شد، مهمترین مسئله امنیت یک رمزنگاری، ایمن بودن کلید رمز است. پس باید در جستجوی روشی باشیم که کلید رمز بین دو کاربر ایمن بماند. زیرا اگر ایو با فرض داشتن علم و تکنولوژی بالا و قابل دسترس بودن الگوریتم‌های رمزگشایی کلید رمز را بدست آورد ایمنی رمزگشایی زیر سؤال خواهد رفت. بنابرین کلید رمز باید در روشی کاملا ایمن که کار نقشه استراق‌سمع‌کننده را خنثی می‌کند بین دو کاربر منتقل شود و این کاری بسیار مشکل خواهد بود[۱,۸,۹,۱۸].

۱-۳- رمزنگاری کوانتومی:

هدف رمزنگاری تدوین پروتکل‌هایی است که برای مبادله اطلاعات ایمن از یک مکان به مکان دیگر

صورت می‌گیرد. رمزنگاری را می‌توان به شیوه زیر تعریف کرد:

پیغام اصلی را M می‌نامیم، وقتی این پیغام رمزینه می‌شود تبدیل به $E_k(M)$ خواهد شد، K کلید مشترک بین فرستنده و گیرنده است

$$M \rightarrow E_k(M)$$

این سیستم باید دو شرط اساسی داشته باشد:

شرط ۱) از $E_k(M)$ نباید به رمز دسترسی پیدا کنیم

$$E_k(M) \nrightarrow M$$

شرط ۲) وقتی شخصی مشغول استراق‌سمع‌کردن است، باید بدون اینکه طرف‌های مرتبط اطلاع پیدا کنند که وی روی خط است، مرتب پیغام‌های $E_k(M_1)$, $E_k(M_2)$, ... دریافت کند ولی همچنان از M آگاهی ندارد. لذا با در اختیار داشتن مجموعه E_k ها، نباید k را پیدا کند، چون در این صورت کانال ناامن خواهد بود. وقتی پیام به دست شخص مورد نظر می‌رسد، این شخص با استفاده از نگاشت D_k رمز را باز می‌کند که دارای دو خاصیت زیر هستند:

$$D_k \circ E_k = I$$

که ∘ را عمل ضرب بین دو اپراتور تعریف می‌کنیم

$$D_k(E_k(M)) = M$$

M را رمزینه می‌کنند و آن را به صورت $E_k(M)$ در می‌آورند و بعد یک تابع معکوس روی آن اعمال می‌کنند و به رمز پی می‌برند که این اصل رمزنگاری است. به عنوان مثال:

پیغام را به صورت رشته‌ای از اعداد 1, 0 در می‌آوریم $M = 1001 \rightarrow$

رشته تصادفی 0,1 که بین آلیس و باب مشترک است $K = 0011 \rightarrow$

$E_k(M) = M \oplus K$

$\oplus$=XOR

$D_k(M) = K \oplus E_k(M) \rightarrow K \oplus K \oplus M = M$

همچنین $a \oplus a = 0$

سوال اینجاست که آلیس و باب چطور یک رشته تصادفی K بین خودشان به اشتراک می‌گذارند؟ مثلا یک روش این است که با هم قرار می‌گذارند که K یک صفحه از کتاب مشخص شده بین خودشان باشد و آن را به صورت 0,1 در بیاورند که این رمز بین آن‌ها باشد، البته این نوع اشتراک رمز خطراتی هم دارد! بدین‌گونه که اگر از این کد زیاد استفاده کنیم، عبارت‌ها و کلمه‌هایی تکرار می‌شود و ایو می‌تواند از همبستگی‌هایی که در آن وجود دارد استفاده کند و بنابراین آلیس و باب مجبورند مرتبا همدیگر را ملاقات کنند، چون نمی‌توانند از یک کلید به مدت طولانی استفاده کنند. در نتیجه در دهه ۷۰ میلادی منجر به یک مسئله اساسی به نام مسئله توزیع کلید شد[۱۱].

۱-۴- توزیع کلید کوانتومی (QKD):

رایانه‌های کوانتومی، ابزارهای محاسباتی هستند که اصول فیزیک کوانتومی را برای انجام دادن محاسبات کارآمد بطور نامحدودی بکار می‌برند. می‌توانیم یک توزیع کلید ایمن را با بکار بردن اصول مکانیک کوانتومی بسازیم که به عنوان توزیع کلید کوانتومی QKD شناخته شده است. توزیع کلید کوانتومی، توان مکانیک کوانتومی را برای بدست آوردن توزیع کلیدی بکار می‌برد که در مقابل ایو با توان محاسباتی نامحدود ایمن می‌باشد. چنین عملی ماوراء توانایی فرایند اطلاعات کلاسیکی است. قدرتی که توسط بیت‌های کوانتومی بدست می‌آید نتیجه این حقیقت است که در مکانیک کوانتومی حالت یک چنین سیستمی کپی نمی‌شود.

کلید تولید شده با بکار بردن QKD امنیت روش بکار برده را تضمین می کند. بنابرین هر گونه تلاش

و عملی را که ایو برای دستیابی به اطلاعات روی بیت‌ها انجام دهد نه تنها ناموفق خواهد بود بلکه حضورش را هم آشکار خواهد ساخت.

هدف از طرح QKD این است که به دو نفر برای ارسال پیغام اجازه می‌دهد که یک کلید محرمانه با استفاده از قوانین فیزیک کوانتومی طراحی کنند. بدین شکل که برای ارسال پیغام، آن را همراه با یک کلید سری یا از طریق یک کانال کلاسیکی که همه به راحتی به آن دسترسی ندارند، یا از طریق کانال کوانتومی که یک کانال غیر امنیتی است، به این معنا که می‌توان به آن دسترسی داشت وحتی استراق‌سمع‌کننده می‌تواند سیگنال‌هایی را به درون آن بفرستد که از طریق فیزیک کوانتومی شناخته می‌شوند، اما نمی‌تواند در پیغام تغییری ایجاد کند، برای طرف دوم فرستاده می‌شود. البته قرارداد QKD نیاز به جفت ذرات درهم‌تنیده دارد چون ایو فقط در صورتی می‌تواند کشف رمز کند که جفت ذرات درهم‌تنیده[1] نباشند.

۱-۴-۱- ارسال سیگنال در طرح QKD در سه مرحله:

الف- مرحله تهیه و انتقال سیگنال: آلیس و باب به طور جداگانه تعدادی سیگنال‌های کلاسیکی و کوانتومی را ایجاد می‌کنند، تعدادی را نگه می‌دارند و تعدادی را به طرف دیگر از طریق کانال‌های کلاسیکی امن و کانال‌های کوانتومی غیر امن می‌فرستند. که این فرایند ممکن است چندین بار تکرار شود.

ب- مرحله کنترل و کیفیت سیگنال: در این مرحله درستی سیگنال‌هایی که از طریق کانال کوانتومی فرستاده می‌شود آزمایش می‌شود. از آنجایی که اندازه‌گیری کوانتومی برگشت پذیر نیست سیگنال‌های کوانتومی در مرحله کنترل کیفیت سیگنال‌ها از بین می‌روند. هدف از این آزمایش این است که میزان شلوغی کانال را برآورد کنند بنابرین بالاترین میزان تراز استراق‌سمع از طریق اندازه‌گیری کوانتومی

---

[1]. Entangled

بدست می‌آید. اگر در این آزمایش درستی سیگنال‌های کوانتومی باقی‌مانده به اندازه کافی بالا نباشد آنها را حذف و آزمایش را دوباره تکرار می‌کنند

پ- **مرحله تصحیح خطا**: آلیس و باب باید خطاهای باقی‌مانده در سیگنال‌ها را تصحیح کنند. علاوه بر آن هر اطلاعات باقی‌مانده‌ای که ممکن است استراق‌سمع‌کننده در آن مداخله کرده را حذف کنند. به عبارتی آلیس و باب می‌خواهند از سیگنال‌های کوانتومی آزمایش نشده باقی‌مانده یک زیرمجموعه را استخراج کنند که تقریبا کامل و بدون دخالت هیچ استراق‌سمع‌کننده‌ای باشد. در آخر آلیس و باب سیگنال‌های باقی‌مانده را برای ایجاد کلید رمز مشترک بکار می‌برند.

در سال ۱۹۸۰، دانشمندان کاربرد اصول مکانیک کوانتومی را برای پیغام‌هایی که به صورت رمز تبدیل شده‌اند پیشنهاد می‌کنند. قرارداد BB۸۴ مدلی از توزیع کلید کوانتومی است که در آن با استفاده از اصل عدم قطعیت در فیزیک کوانتومی، حضور استراق‌سمع‌کننده را در طول ارتباط آشکار خواهد ساخت. بر طبق این اصل اندازه‌گیری کردن کمیت‌های معینی به صورت همزمان غیر ممکن است، مانند مکان و اندازه حرکت یک ذره. فیزیکدان‌ها، جفت متغیرهایی مانند مکان و ذره حرکت را متغیرهای مزدوج می‌نامند.

در BB۸۴، این متغیرها برای نمایش دادن مقادیر باینری بکار می‌روند. بنابراین همواره یک جفت متغیر مزدوج وجود دارد که کامیوت نمی‌کنند به همین دلیل در BB۸۴ فضا، یک فضای دو بعدی است، بنابراین مبادله کردن رشته‌های بیتی مانند کلید رمز و حتی پیغام با یک روش بسیار ایمن امکان پذیر می‌باشد[۱۱].

۱-۵- نتیجه‌گیری:

رمزنگاری کلاسیکی، امروزه کاربردهای وسیعی در اطلاعات محرمانه دارد با این وجود این نوع رمزنگاری نمی‌تواند امنیت اطلاعات را به طور قطعی تضمین نماید. اخیرا فیزیکدانان با استفاده از تئوری کوانتومی و تئوری نسبیت توانسته‌اند ایمنی پروتکل‌های رمزنگاری را صد در صد تضمین نمایند. یعنی قوانین مکانیک کوانتومی هر گونه استراق‌سمع را به وسیله نوفه‌ای که در حالت کوانتومی سیستم‌های درهم‌تنیده ایجاد می‌کند آشکار کند این قوانین هرگز نمی‌تواند مانع از استراق‌سمع شود ولی ایمنی پروتکل را در مقابل استراق‌سمع تضمین می‌کند.

فصل دوم

قرارداد BB۸۴

- تعریف
- ایمنی پروتکل BB۸۴ در برابر ایو
- بیت‌های کوانتومی
- گیت
- گیت‌های کلاسیکی
- گیت‌های کوانتومی
- قضیه نوکلونینگ
- درهم‌تنیدگی
- موضعیت
- ناموضعیت
- کلید خام
- کدهای تصحیح خطا
- تصحیح خطای کلاسیکی
- تصحیح خطای کوانتومی
- کد سه کیوبیتی وارون بیتی
- آنتروپی شانون

۲-۱- تعریف قرارداد BB ۸۴:

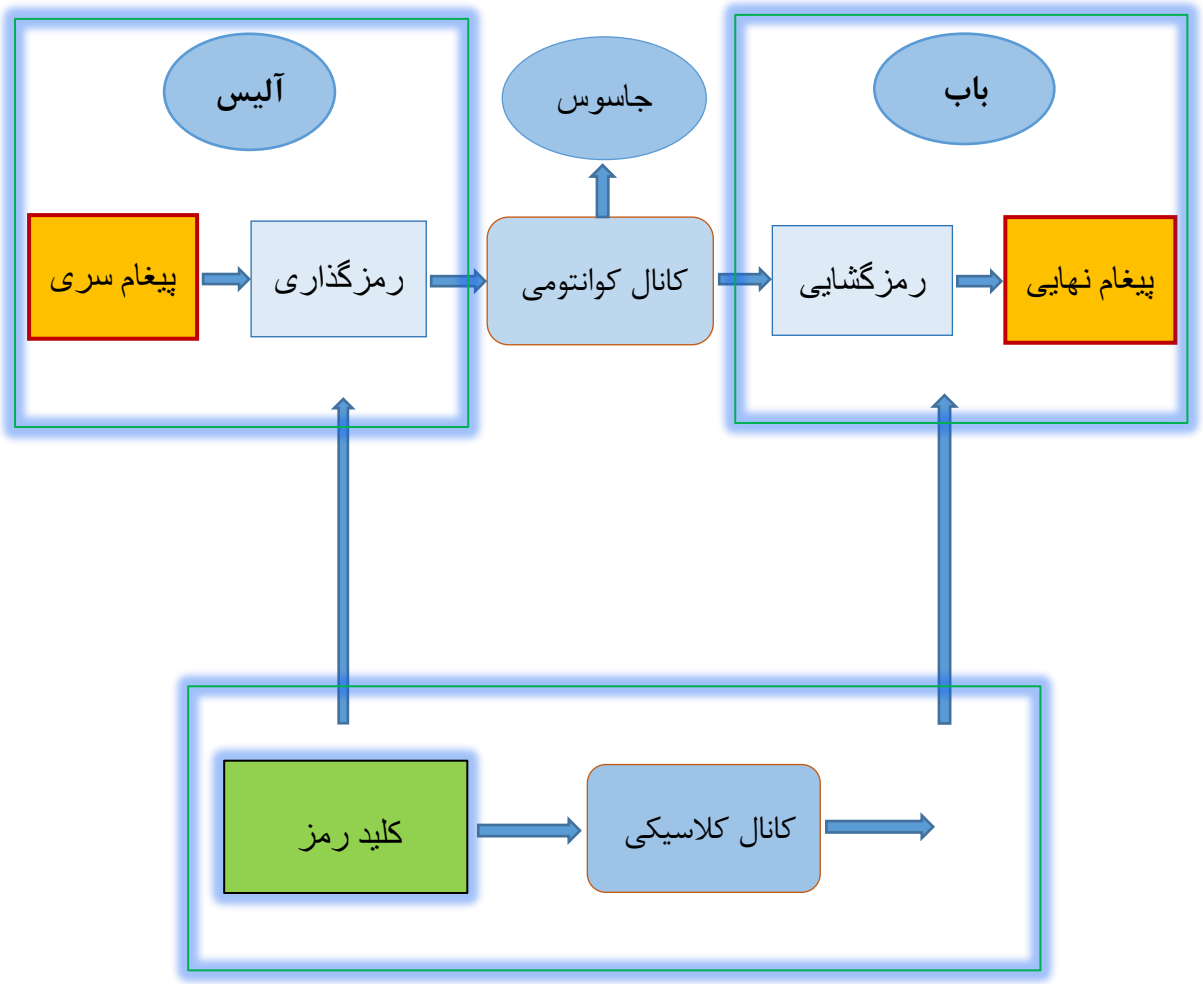
قرارداد BB۸۴، فرمول‌بندی ریاضی در یک فضای دو بعدی برای طراحی یک کلید رمز با استفاده از قوانین مکانیک کوانتومی است که این فضای دو بعدی می‌تواند هر سیستم دوحالته‌ای مانند: پلاریزاسیون نور و اسپین های الکترون، الکترون‌های یک اتم در حالت زمینه و برانگیخته، ... باشد.

پایه‌های چنین فضایی را بردارهای ویژه سیستم دو حالته مورد نظر تشکیل می‌دهد.

دو کاربر آلیس و باب را در نظر می‌گیریم. آلیس می‌خواهد پیغامی را برای باب ارسال کند. ابتدا یک کلید سری که بین آلیس و باب به اشتراک گذاشته شده، به شکل رمز درآورده سپس از طریق یک کانال کوانتومی برای باب می‌فرستد. کانال کوانتومی، یک کانال ارتباطی عمومی که هر کسی می‌تواند رمز را خوانده و آن را دستکاری نماید.

باب رمز را از طریق کانال کوانتومی دریافت کرده و با استفاده از یک کلید سری، پیغام را رمزگشایی می‌کند. آلیس و باب از طریق یک کانال کلاسیکی که می‌تواند تلفن، ایمیل و ... باشد، نتایج‌شان را برای طراحی یک کلید رمز مبادله می‌کنند. کانال کلاسیکی، خصوصی است یعنی اینکه حتی اگر اطلاعاتی هم از طریق این کانال در دسترس قرار بگیرد نمی‌توان پیغام‌های درون آن را دستکاری نمود. شخص سومی به نام ایو می‌خواهد به این اطلاعات دسترسی پیدا کند. او توان محاسباتی نامحدودی دارد و به هر دو کانال نیز دسترسی دارد ولی نمی‌تواند پیغامی که از کانال کلاسیکی می‌گذرد تغییر دهد (شکل۲-۱).

- هدف BB۸۴ طراحی چنین کلیدی است که بین آلیس و باب برای رمزگذاری و رمزگشایی قرارداد می‌شود.



شکل ۲-۱- نمایش تصویری چگونگی اجرای مراحل قرارداد BB۸۴

۲-۲- ایمنی پروتکل BB۸۴ در برابر ایو:

فرض کنید ایو بتواند کانال کوانتومی بین آلیس و باب را استراق‌سمع کند و فوتون را اندازه‌گیری کند، وقتی پایه‌هایی که در آن بیت‌ها کد[۱] شده‌اند را نمی‌داند سپس با احتمال ۱/۲ پایه‌های اشتباه را

[۱] code

اندازه‌گیری می‌کند (می‌دانیم که بیت‌های باب هم به طور تصادفی انتخاب شده‌اند)، حتی وقتی که باب در همان پایه‌هایی که آلیس برای کدکردن استفاده کرده باشد، اندازه‌گیری کند، به این دلیل که ایو نمی‌تواند حالت ارسالی آلیس را دریافت کرده و آنرا استراق‌سمع کند و مستقیما برای باب بفرستد (علت این است که بر اساس قضیه نوکلونینگ[۱] هیچ فرآیندی نمی‌تواند حالت‌های نامتعامد را کپی کند)، همچنان این خطاها حضور ایو را برای آلیس و باب آشکار می‌کنند و در نتیجه پروتکل متوقف می‌شود.

مسئله دیگر این است که ایو نیازی ندارد فوتونی را که از درون کانال کوانتومی عبور می‌کند اندازه‌گیری کند، اما می‌تواند حملات پیچیده‌تری انجام دهد، مثلا ایو می‌تواند سیستم را با فوتون درهم‌تنیده کند و آن را ذخیره کند و اندازه‌گیری که می‌خواهد انجام دهد را به تأخیر بیندازد و بعد از اینکه آلیس و باب پایه‌هایشان را برای کدگذاری آشکار کردند، اندازه‌گیری‌های خود را انجام دهد. اما مشکلاتی در این حین هم بوجود می‌آید و آن این‌که اجراسازی فیزیکی پروتکل کامل نخواهد بود.

علیرغم آن‌که همیشه ناخالصی شامل محیط وآشکارسازهای نامطمئن وجود دارد با وجود این ناخالصی‌ها همیشه می‌توان برای کانال یک کلید ایمن تولید کرد.

چند سال بعد از قرارداد BB۸۴ توسط بنت و براسارد، شخصی به نام ایکرت[۲] یک پروتکل توزیع کلید کوانتومی[۳] پیشنهاد کرد که براساس خواص فیزیکی کوانتومی است[۱۰].

در اصل هدف ما محدود کردن توانایی‌های محاسباتی و دسترسی شخص سوم (که همان ایو با استراق‌سمع‌کننده است) که می‌خواهد به اطلاعات ما دسترسی داشته باشد، است.

---

۱. No – Cloning

۲. Ekert

۳. Quantum key distribution

۲-۳- بیت‌های کوانتومی[۱]:

یکای غیر قابل تقسیم اطلاعات کلاسیکی، بیت[۲] است که یکی از دو مقدار {0,1} را می‌گیرد. یکای متناظر با اطلاعات کوانتومی، بیت کوانتومی نامیده می‌شود که حالتی را در ساده‌ترین سیستم کوانتومی توصیف می‌کند. کوچکترین فضای هیلبرت دوبعدی است. پایه‌های ارتونرمال برای فضای برداری دو بعدی را به شکل $\{|1\rangle , |0\rangle\}$ نمایش می‌دهیم. کـلی‌ترین حالت نرمالیزه شده به شکل زیر نمایش داده می‌شود:

$$a|0\rangle + b|1\rangle \qquad (۱-۲)$$

که در آن a و b اعداد مختلط هستند و در رابطه $|a|^2 + |b|^2 = 1$ صدق می‌کنند. بیت کوانتومی حالتی در فضای دوبعدی است که می‌تواند هر مقداری را که در معادله (۲-۱) صدق می‌کند بگیرد. وقتی اندازه‌گیری انجام می‌دهیم تصاویر آن روی پایه‌های $\{|1\rangle , |0\rangle\}$ بدست می‌آید. بنابراین $|0\rangle$ را با احتمال $|a|^2$ بدست می‌آوریم و $|1\rangle$ را با احتمال $|b|^2$ بدست می‌آوریم.

معادله (۲-۱) توصیف کننده سیستم دو حالته ذره‌ای با اسپین ۱/۲ است که در آن $|0\rangle$, $|1\rangle$ بردارهای پایه در امتداد محور Zها بصورت اسپین بالا[۳] $|\uparrow_z\rangle$ و اسپین پایین[۴] $|\downarrow_z\rangle$ هم نمایش داده می‌شود:

$$|\uparrow_z\rangle = |0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$$
$$|\downarrow_z\rangle = |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \qquad (۲-۲)$$

---

۱. Qubit

۲. bit

۳. up

۴. down

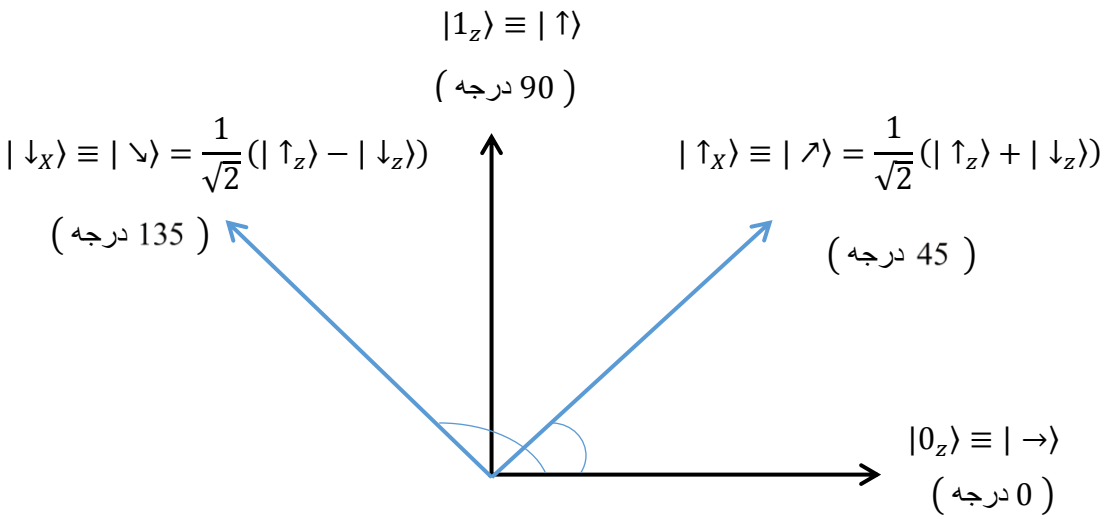
حال اگر در امتداد محور X ها اندازه‌گیری انجام بدهیم خواهیم داشت:

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\Rightarrow|\uparrow_x\rangle=\frac{1}{\sqrt{2}}(|\uparrow_z\rangle+|\downarrow_z\rangle)$$
$$|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\Rightarrow|\downarrow_x\rangle=\frac{1}{\sqrt{2}}(|\uparrow_z\rangle-|\downarrow_z\rangle) \qquad (۳-۲)$$

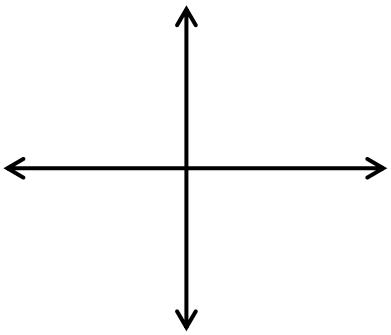
برای هر کدام از این حالت‌ها اگر اندازه‌گیری‌هایمان در امتداد محور Z ها باشد با احتمال ۱/۲، $|\uparrow_z\rangle$ را بدست خواهیم و با احتمال ۱/۲، $|\downarrow_z\rangle$ را بدست خواهیم آورد. معادله (۲-۱) می‌تواند توصیف کننده سیستم دوحالته پلاریزاسیون نور باشد که در ۴ قطبش ممکن افقی (0^0)، عمودی (90^0)، (45^0) و (135^0) را به عنوان پایه‌های قطبش در نظر گیرند، به این صورت که $\{0^0:|\rightarrow\rangle,90^0:|\uparrow\rangle\}$ پایه‌های راستگرد و $\{0^0:|\square\rangle,135^0:|\square\rangle\}$ پایه‌های قطری می‌باشند.

پایه	0	1
+	→	↑
×	↗	↘

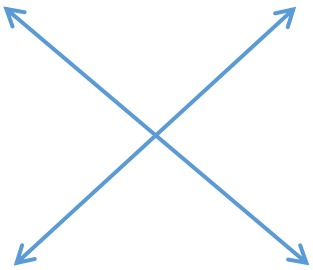
جدول ۲-۱- پایه‌های قطبش



قطبش فوتون



پایه‌های خطی



پایه‌های قطری

شکل ۲-۲- نحوه کدگذاری در پروتکل BB۸۴

آلیس یک بیت {0,1} و یک پایه را برای آن انتخاب می‌کند و قطبش مورد نظر را انجام داده و با استفاده از یک کانال کوانتومی برای باب می‌فرستد. آلیس این کار را چندین بار تکرار می‌کند و هر بار تمام اطلاعات را ثبت می‌کند. باب از پایه‌هایی که آلیس انتخاب کرده است اطلاعاتی ندارد. بنابرین تنها کاری که می‌تواند انجام دهد این است که برای هر مرحله پایه‌ای را به طور تصادفی برای اندازه‌گیری انتخاب کند آلیس و باب پایه‌های انتخابی‌شان را مقایسه می‌کنند و برای هر کدام که پایه‌های یکسانی به کار برده‌اند ولی مقادیر مختلفی بدست آورده‌اند حضور استراق‌سمع‌کننده را آشکار می‌سازند. در این حالت میزان نوفه کانال کوانتومی را برآورد می‌کنند و اگر این میزان با درصد بالایی زیاد باشد بیت‌ها را حذف می‌کنند و یکبار دیگر از ابتدا عمل را تکرار می‌کنند.

آلیس	پایه	+	x	x	x	+	x	+	x	+	x
	قطبش	↑	↖	↖	↗	↑	↖	→	↗	→	↗
	بیت	1	0	0	1	1	0	0	1	0	1
ایو	پایه	x	+	+	x	+	+	x	x	+	+
	بیت	1	0	1	1	1	1	0	1	0	0
باب	پایه	x	x	+	x	+	x	+	+	+	+
	بیت	1	0	1	1	1	1	1	0	0	0
		*	0	*	1	1	1	1	*	0	*

جدول ۲-۲- نحوه تبادل کلید در پروتکل BB۸۴

۲-۴-گیت (Gate):

فرایند انتقال بیت یا کیوبیت را توسط گیت نمایش می‌دهند.

۲-۴-۱-گیت‌های کلاسیکی:

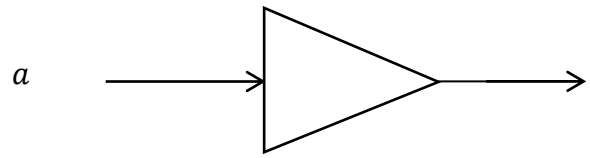
محاسبات کلاسیکی شامل فرایند تبدیل بیت کلاسیکی است. تنها عنصر اصلی این فرایند کلاسیکی بیت‌ها، گیت‌ها می‌باشند. یک پردازنده رایانه الکترونیکی جدید شامل صدها و میلیون‌ها گیت است، و هر کدام از گیت‌ها فرایند مخصوص به خود را انجام می‌دهند.

گیت‌های کلاسیکی بر طبق داده‌های ورودی به شکل زیر بیان می‌شوند:

گیت‌های تک ورودی کلاسیکی:

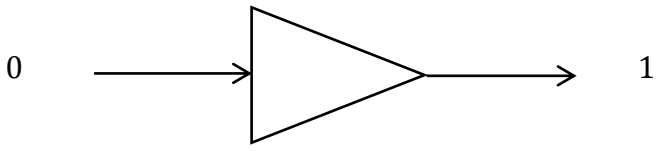
۱- گیت (NOT):

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



عملیات ریاضی آن به شکل زیر است.

(⊕ اشاره به باقی‌مانده حاصل جمع بر مبنای دو دارد)

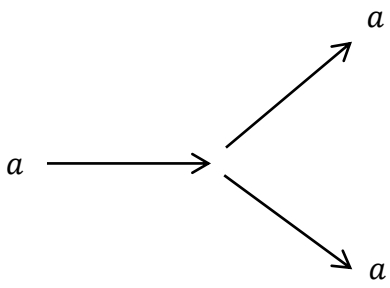


$\mathrm{NOT(a)} = 1 \oplus \mathrm{a}$; $(\oplus = \text{addition mod (2)})$

مثال: $\mathrm{NOT}(1) = 1 \oplus 1 = \mathrm{mod}\left(\frac{1+1}{2}\right) = 0$

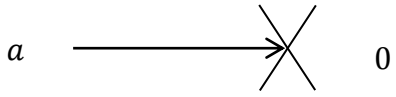
۲-گیت FANOUT (copy):

یک بیت ورودی می‌دهیم و دو بیت خروجی مشابه با بیت ورودی بدست می‌آوریم. در رایانه‌های کوانتومی این یک گیت برقرار نیست؛ یعنی فرایندی وجود ندارد که یک بیت به دو بیت مشابه با خود تبدیل شود.



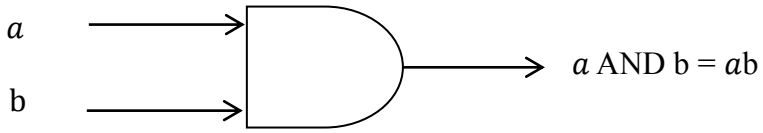
۳- گیت ERAS:

گیت ورودی را حذف می‌کند



گیت‌های دو ورودی کلاسیکی:

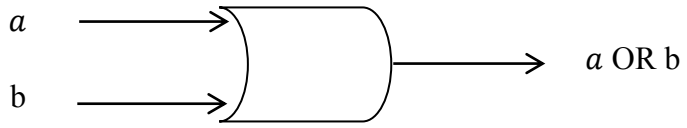
۱-گیت AND :



یک خروجی از دو ورودی بدست می‌آید و عملیات ریاضی آن مانند حاصل ضرب می‌باشد.

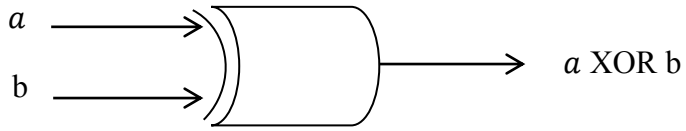
خروجی هنگامی یک است که هر دو ورودی یک باشند، در غیر این صورت خروجی برابر صفر خواهد شد.

۲-گیت OR:



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

۳-گیت XOR:



خروجی این نوع گیت برابر یک است اگر فقط یکی از ورودی‌ها مخالف هم باشند، در بقیه حالت‌ها خروجی برابر صفر است.

عملیات ریاضی آن به شکل زیر است:

$$a \text{ XOR } b = a \oplus b$$

گیت‌های دو ورودی را به راحتی می‌توان توسط جدول (۲-۳) نمایش داد.

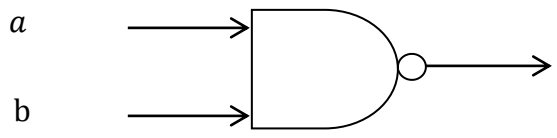
a	b	AND	OR	XOR
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

جدول ۲-۳- حاصل گیت‌های XOR ، OR ، AND برای بیت‌های مختلف

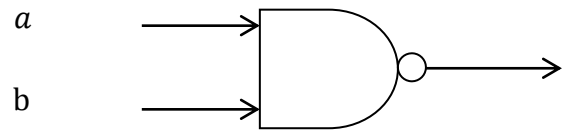
گیت OR می‌تواند از ترکیبی از AND و XOR ساخته شود.

a OR b = (a AND b) XOR (a XOR b)

۴-گیت NAND:



۵-گیت NOR:



۲-۴-۲-گیت‌های کوانتومی:

بیت‌های کوانتومی درست مانند بیت‌های کلاسیکی که تحت گیت‌های کلاسیکی تغییر می‌کنند، تحت گیت‌های کوانتومی تبدیل می‌شوند. که این تبدیلات در بردارنده تحولات زمانی سیستم کوانتومی تحت قوانین مکانیک کوانتومی هستند. بنابرین هر گیت کوانتومی متناظر با یک عملگر یکانی می‌باشد. بنابراین یک گیت کوانتومی که روی یک حالت چندگانه از بیت‌های کوانتومی اثر می‌کند به صورت زیر نمایش داده می‌شود:

$$|\psi_{in}\rangle \to |\psi_{out}\rangle = u|\psi_{in}\rangle$$

هر تحول یکانی داشته باشیم برگشت پذیر می‌باشد بنابراین:

$$|\psi_{in}\rangle = u^{\dagger}|\psi_{out}\rangle$$

ولی بعد از اندازه‌گیری نمی‌توانیم حالت قبل از اندازه‌گیری را داشته باشیم چون عملگر اندازه‌گیری، غیر یکانی می‌باشد. در مکانیک کوانتومی برای عملگرها نمایش ماتریسی داریم که اگر عملگر را بر حسب ویژه مقادیر خودش باشد، ماتریس قطری خواهیم داشت.

دسته‌بندی گیت‌های کوانتومی به صورت زیر می‌باشد:

گیت‌هایی با یک بیت کوانتومی ورودی:

۱-گیت NOT(X):

درست مانند گیت کلاسیکی NOT، برای گیت کوانتومی NOT داریم:

$$|0\rangle \to |1\rangle$$
$$|1\rangle \to |0\rangle$$

عملگر متناظر با این گیت، عملگر X می‌باشد که اگر در پایه‌های S_z نوشته شده باشد، ماتریس یکانی متناظر با آن به صورت زیر خواهد بود:

مثال:

$$X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

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

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

۲-گیت Z:

مطابق با این گیت داریم:

$$|0\rangle\rightarrow|0\rangle$$
$$|1\rangle\rightarrow-|1\rangle$$

وماتریس یکانی متناظر با این عملگر به صورت زیر نشان داده می‌شود:

$$z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

۳-گیت هادامارد (H):

با اعمال این گیت، یک حالت ویژه به یک برهم‌نهی تبدیل می‌شود،یعنی:

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

ماتریس یونیتاری متناظر با آن به صورت زیر تعریف می‌شود:

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\quad |x\rangle \;\text{——}\boxed{H}\text{——}\; (-1)^x|x\rangle+|1-x\rangle$$

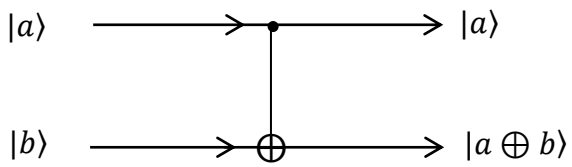
که H روی کیوبیتی در حالت $|x\rangle$ اعمال می‌شود که در آن $x=0,1$ است.

باید توجه داشت که گیت‌های H و Z مشابه کلاسیکی ندارند.

گیت با دو بیت کوانتومی ورودی:

۱-گیت Controlled NOT (C-NOT):

عمومی‌ترین گیت دو کیوبیتی گیت C-NOT است که به عنوان XOR یا گیت اندازه‌گیری هم شناخته می‌شود.



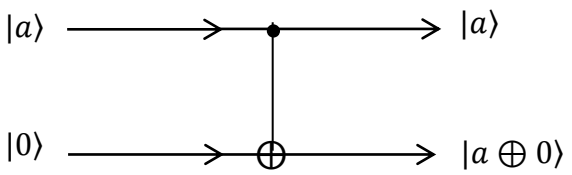
$$|a,b\rangle \xrightarrow{\text{C-NOT}} |a,a \oplus b\rangle$$

در آن a بیت کوانتومی کنترل و b بیت کوانتومی هدف نامیده می‌شود و در آن $a,b \in \{0,1\}$ هستند.

می‌توانیم پایه‌های محاسباتی دو بیت کوانتومی را به شکل زیر نیز نشان بدهیم:

$$|a,b\rangle = |a\rangle \otimes |b\rangle = |a\rangle|b\rangle$$

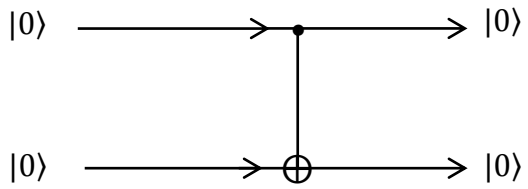
اگر b=0 باشد گیت بالا مانند کپی عمل می‌کند.



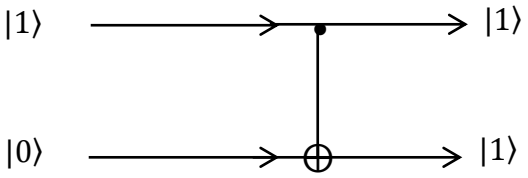
$$|a,0\rangle = |a\rangle|0\rangle = |a\rangle\otimes|0\rangle = \xrightarrow{\text{C-NOT}} |a\rangle|a\rangle$$

اعمال گیت C-NOT بر روی حالت‌های راست هنجار:

عمل کپی توسط گیت C-NOT بر روی حالت‌های راست هنجار زیر مشاهده می‌شود:



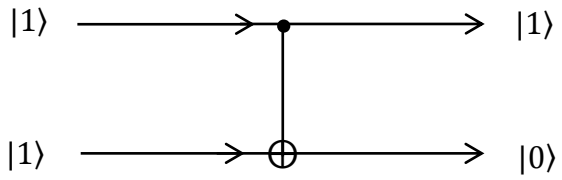
یعنی $|0\rangle|0\rangle \xrightarrow{C-NOT} |0\rangle|0\rangle$



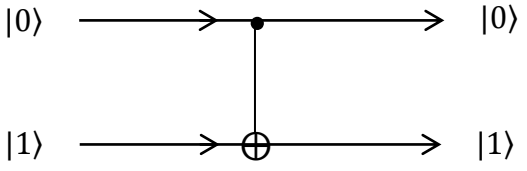
یعنی $|1\rangle|0\rangle \xrightarrow{C-NOT} |1\rangle|1\rangle$

اعمال گیت C-NOT در نمونه‌های دیگر:

همچنین عمل گیت C-NOT بر روی کیوبیت‌های زیر را نیز داریم:



یعنی $|1\rangle|1\rangle \xrightarrow{C-NOT} |1\rangle|0\rangle$

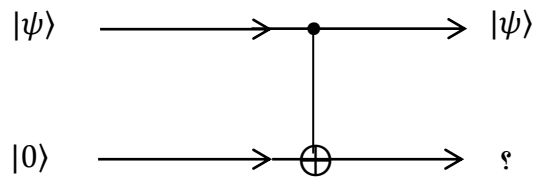


یعنی $|0\rangle|1\rangle \xrightarrow{C-NOT} |0\rangle|1\rangle$

گیتC-NOT یکی از مهمترین گیت‌های کوانتومی است.

۲-۵- تئوری نوکلونینگ[۱]:

در گیت (C-NOT) کپی برای حالت‌های پایه محاسباتی عمل می‌شود، 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؟ و چگونه گیت (C-NOT) بر حالت بالا عمل می‌کند؟



$$|\psi\rangle|0\rangle=|\psi\rangle\otimes|0\rangle=\alpha|0,0\rangle+\beta|1,0\rangle \xrightarrow{(\mathrm{C-NOT})} \alpha|0,0\rangle+\beta|1,1\rangle$$

به عبارت دیگر اگر کنترل کیوبیت به درستی کپی شود حالت نهایی می‌باید

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

فقط به ازای $\alpha=0$ یا $\beta=0$ این دو رابطه مشابه هم می‌شود، طوری که کیوبیت ورودی حالت‌های پایه محاسباتی باشد.

آیا امکان دارد گیت‌ها و مدارهای پیچیده‌تری استفاده شود که هر حالت کوانتومی دلخواه را کپی کند؟ با توجه به گیت‌های کوانتومی و خطی، جواب، نه می‌باشد؛ که این نتیجه از تئوری نوکلونینک می‌باشد.

تئوری نوکلونینگ[۱۰,۱۱]:

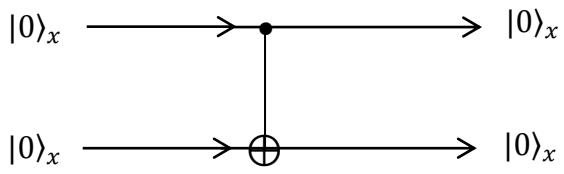
[۱]. No – Cloning theorem

«کپی شدن برای حالت‌های پایه راست هنجار امکان پذیر است نه برای هر حالت کوانتومی دلخواه» تئوری نوکلونینک به این معنی نیست که هرگز نمی‌توان کیوبیت‌هایی مانند $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ را کپی نمود بلکه اگر حالت راست هنجار برای آن وجود داشته باشد می‌توان با استفاده از تئوری کلونینک آن حالت را کپی نمود.

مثال (۱):

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

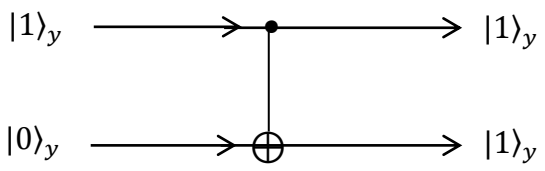
$$|\psi\rangle=|0\rangle_x$$



مثال (۲):

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

$$|\psi\rangle=|0\rangle_y$$



۲-۶- درهم‌تنیدگی[۱]:

درهم‌تنیدگی کوانتومی یکی از مفاهیم مهم مکانیک کوانتومی می‌باشد که مشابه کلاسیکی ندارد. با

[۱] Entanglement

بکارگیری حالات درهم‌تنیده‌ی کوانتومی قادر به انجام اموری می‌شویم که در دنیای کلاسیکی، سخت و یا غیر ممکن هستند. این مفهوم بیان می‌دارد که اگر دو ذره‌ی درهم‌تنیده را میلیون‌ها کیلومتر از یکدیگر دور کنیم و روی یکی از آن دو ذره اندازه‌گیری انجام دهیم، در همان لحظه (و به طور آنی)، حالت ذره‌ی دوم نیز تحت تأثیر قرار می‌گیرد. به عبارت دیگر، آن دو ذره (ظاهرا) با سرعتی بالاتر از سرعت نور و به آنی، تحت تأثیر یکدیگر قرار می‌گیرند و در عین حال این رویداد با پذیرفتن قضیه‌ی عدم علامت دهی[۱]، اصل نسبیت خاص اینشتین را نقض نمی‌کند. به عبارت دیگر، در این بین هیچ اطلاعاتی مبادله نمی‌شود و با اندازه‌گیری بر روی یکی از آن‌ها نمی‌توان هیچ گونه اطلاعاتی در مورد سیستم دیگر کسب نمود و تنها پیامد آن، تأثیر آنی بر روی حالت ذره‌ی دیگر است. انیشتن این موضوع را عملکرد شبح وار[۲] (روح مانند) در فواصل زیاد نامید که شبیه به ارتباط دو تکه‌ی درهم‌تنیده توسط سیم‌های نامرئی است که ما هیچ اطلاعی از آن‌ها نداریم، اما برای محاسبات کوانتومی یک اصل کلی به شمار می‌آیند.

پدیده‌ی شگفت انگیز درهم‌تنیدگی در نظریه‌ی کوانتومی تحول عظیمی به وجود آورده و به تبع آن، نتایجی را نیز در رایانه‌های کوانتومی به دنبال داشته است. از نتایج بسیار مهم پدیده‌ی درهم‌تنیدگی کوانتومی این است که موضعیت[۳] را نقض کرده و ثابت می‌کند که ماهیت نظریه‌ی کوانتومی، ناموضعی می‌باشد [۱۰].

دو سیستم مربوط به فضای هیلبرت $H_A \otimes H_B$ را در نظر بگیرید. یک حالت سیستم مربوط به این فضا به صورت زیر می‌باشد:

$$|\psi\rangle_A \otimes |\psi\rangle_B$$

---

۱. Signalling

۲. ghostly

۳. Localitiy

۳. منظور از موضعیت این است که قطبیدگی یک فوتون با اندازه‌گیری روی فوتون دیگری که در فاصله دور از هم هستند، اثر نمی‌گذارند.

سیستم فوق یک سیستم جداشدنی نامیده می‌شود. حال اگر $|i\rangle_A \in |\psi\rangle_A$ و $|j\rangle_B \in |\psi\rangle_B$ باشد، آنگاه بردارهای فضای هیلبرت $H_A \otimes H_B$ را می‌توان به صورت زیر نوشت:

$$|\psi\rangle_{AB} = \Sigma_{ij} c_{ij} |i\rangle_A \otimes |j\rangle_B \quad , \quad c_{ij} = c_i^A c_j^B$$

$|\psi\rangle_{AB}$ جدا شدنی است اگر $|\psi\rangle_A = \Sigma_i c_i^A |i\rangle_A$ و $|\psi\rangle_B = \Sigma_j c_j^B |j\rangle_B$ ، ولی اگر $c_{ij} \neq c_i^A c_j^B$ سیستم درهم‌تنیده نامیده می‌شود. به عنوان مثال، اگر $\{|0\rangle_A, |1\rangle_A\}$ مربوط به $|\psi\rangle_A$ و $\{|0\rangle_B, |1\rangle_B\}$ مربوط به $|\psi\rangle_B$ باشد، یکی از حالات درهم‌تنیده سیستم به صورت زیر خواهد بود:

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right)$$

اگر $|\psi\rangle_A$ اندازه‌گیری کند و $|0\rangle_A$ بدست آید حتما اندازه‌گیری $|\psi\rangle_B$ حالت $|1\rangle_B$ را خواهد داد و اگر $|\psi\rangle_A$ اندازه‌گیری کند $|1\rangle_A$ را بدست آورد اندازه‌گیری $|\psi\rangle_B$ حالت $|0\rangle_B$ را خواهد داد. عبارت فوق به این معنی است که اندازه‌گیری یکی به دیگری وابسته است.

یک حالت خالص[۱] $|\psi\rangle \in H_A \otimes H_B$ درهم‌تنیده است اگر نتوان آن را به فرم $|\psi\rangle \in |\psi\rangle_A \otimes |\psi\rangle_B$ نوشت که در آن $|\psi\rangle_A \in H_A$ و $|\psi\rangle_B \in H_B$ می‌باشد. یک حالت مخلوط[۲] ρ روی فضای هیلبرت $H_A \otimes H_B$ هنگامی درهم‌تنیده است که نتوان آن را به فرم زیر در آورد:

$$\rho = \Sigma_i \mathrm{P}_i \left|\psi_i^A\right\rangle\left\langle\psi_i^A\right| \otimes \left|\psi_i^B\right\rangle\left\langle\psi_i^B\right| \quad \rightarrow \quad \left|\psi_i^A\right\rangle \in H_B \quad , \quad \left|\psi_i^B\right\rangle \in H_B$$

که ماتریس چگالی ρ، یک ماتریس جدا شدنی است [۱۰,۱۱].

---

۱. Pure

۲. Mixed

۲-۷- موضعیت:

نتیجه و یا احتمال نتیجه یک اندازه‌گیری که روی قسمتی از یک سیستم مرکب با حالت $|\psi\rangle$ (سیستم ۱ + سیستم۲) انجام می‌شود مستقل از جنبه‌های مولفه‌های قسمت‌های دیگر است که آزمایشگر برای اندازه‌گیری انتخاب می‌کند. این به هیچ وجه به این معنی نیست که نتوان با بررسی سیستم۱ اطلاعاتی در مورد سیستم۲ بدست آورد. حالت $|\psi\rangle$ شامل اطلاعات مشترک مربوط به هر دو سیستم است و اندازه‌گیری روی یکی از این سیستم‌ها بخشی از این اطلاعات را آشکار می‌سازد. همچنین اگر یک اندازه‌گیری روی یک قسمت از سیستم مرکب انجام شود باعث اغتشاش موضعی آن قسمت می‌گردد و این با Locality مغایرتی ندارد.

آنچه که موضعیت می‌گوید اساسا این است که مقدار اندازه‌گیری شده یک کمیت در یک سیستم به طور علی نمی‌تواند متاثر از اندازه‌گیری یک کمیت روی سیستم دیگر باشد. زیرا وقتی که اندازه‌گیری انجام می‌شود فاصله سیستم‌ها فضا گونه است. لازم به توضیح است که فاصله سیستم‌ها فضا گونه است یعنی این‌که فاصله زمانی بین سیستم‌ها بیشتر از سرعت نور باشد.

۲-۸- ناموضعیت[۱]:

حالت یک جفت ذره را که در حالت بل هستند در نظر می‌گیریم:

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left(\left|\uparrow_z\right\rangle_A\left|\downarrow_z\right\rangle_B+\left|\downarrow_z\right\rangle_A\left|\uparrow_z\right\rangle_B\right)=\frac{1}{\sqrt{2}}\left(\left|\uparrow_x\right\rangle_A\left|\downarrow_x\right\rangle_B+\left|\downarrow_x\right\rangle_A\left|\uparrow_x\right\rangle_B\right)$$

آلیس و باب هر کدام ویژگی‌های ذره خود را اندازه‌گیری می‌کنند.

---

۱. Non - Locality

۱) فرض کنید آلیس ابتدا S_z را اندازه‌گیری می‌کند و بعد از اندازه‌گیری $\left|\downarrow_z\right\rangle_A$ را بدست آورد، باتوجه به حالت $|\psi\rangle$، حالت ذره باب، $\left|\uparrow_z\right\rangle_B$ خواهد شد.

۲) فرض کنید آلیس، S_x را اندازه‌گیری 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 کنید باب، S_x را اندازه‌گیری کند. می‌خواهیم ببینیم با چه احتمالی $\left|\downarrow_x\right\rangle_B$ و $\left|\uparrow_x\right\rangle_B$ را بدست می‌آورد؟ در حالت ۱ با احتمال ۱/۲ $\left|\downarrow_x\right\rangle_B$ را بدست می‌آورد و در حالت ۲ با احتمال ۱، $\left|\downarrow_x\right\rangle_B$ را بدست می‌آورد. احتمال اینکه خروجی باب چه باشد بستگی به این دارد که آلیس چه چیزی را اندازه‌گیری می‌کند، که این Non-Locality می‌باشد [۵,۱۰,۱۱].

۲-۹- معاوضه درهم‌تنیدگی[۱]:

با توجه به تعریف جالب دوربری[۲] ما می‌توانیم کاری کنیم دو ذره‌ای که هرگز برهم‌کنش نداشته‌اند درهم‌تنیده شوند. این ممکن است، حتی اگر ذرات میلیون‌ها کیلومتر از هم فاصله داشته باشند که این خاصیت teleportation است. معاوضه درهم‌تنیدگی را با دو زوج درهم‌تنیده شروع می‌کنیم. ما چهار ذره یا کیوبیت ۱، ۲، ۳ و ۴ داریم ذره ۱ و ۴ نزد آلیس و ذره ۲ و ۳ نزد باب وجود دارد ذره ۱ آلیس با ذره ۲ باب درهم‌تنیده است که حالت درهم‌تنیدگی به صورت زیر نمایش داده می‌شود

$$\left|\beta_{00}\right\rangle_{12}=\frac{\left|00\right\rangle_{12}+\left|11\right\rangle_{12}}{\sqrt{2}}$$

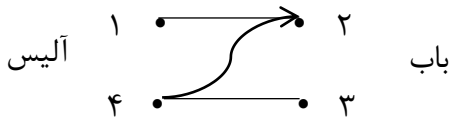
۱. Entanglement Swapping

۲. teleportation

ذره ۴ آلیس با ذره ۳ باب درهم‌تنیده است

$$|\beta_{00}\rangle_{34} = \frac{|00\rangle_{34} + |11\rangle_{34}}{\sqrt{2}}$$

آلیس می‌خواهد با teleportation ذره ۴ خود را به ذره ۲ باب بفرستد با این ارسال ذره ۴ آلیس منطبق بر ذره ۲ باب می‌شود و در نتیجه ذره ۲ و ۳ باب با یکدیگر درهم‌تنیده می‌شوند بدون این که درهم‌تنیدگی داشته باشند.



ضرب دو حالت در هم‌تنیده بالا را به صورت زیر انجام می‌دهیم:

$$|\psi\rangle = |\beta_{00}\rangle_{12}|\beta_{00}\rangle_{34} = \frac{1}{\sqrt{2}}\left(|00\rangle_{12} + |11\rangle_{12}\right) \otimes \frac{1}{\sqrt{2}}\left(|00\rangle_{34} + |11\rangle_{34}\right) =$$
$$\frac{1}{2}\left(|00\rangle_{12}|00\rangle_{34} + |00\rangle_{12}|11\rangle_{34} + |11\rangle_{12}|00\rangle_{34} + |11\rangle_{12}|11\rangle_{34}\right)$$

آلیس روی ذرات خود (۴،۱) اندازه‌گیری بل انجام می‌دهد اگر $|\psi\rangle$ را در پایه‌های آلیس بازنویسی کنیم داریم:

$$|\beta_{00}\rangle_{12}|\beta_{00}\rangle_{34} = \frac{1}{2}\left(|00\rangle_{14}|00\rangle_{23} + |01\rangle_{14}|01\rangle_{23} + |10\rangle_{14}|10\rangle_{23} + |11\rangle_{14}|11\rangle_{23}\right) \qquad (۴-۲)$$

این حالت (۲-۴) را دوباره در پایه‌های بل بازنویسی می‌کنیم:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \quad , \quad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \quad , \quad |\beta_{10}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$\begin{cases} |00\rangle = \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle + |\beta_{10}\rangle\right) \\ |01\rangle = \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle + |\beta_{11}\rangle\right) \end{cases} \qquad \begin{cases} |10\rangle = \frac{1}{\sqrt{2}}\left(|\beta_{10}\rangle - |\beta_{11}\rangle\right) \\ |11\rangle = \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle - |\beta_{10}\rangle\right) \end{cases}$$

$$\Rightarrow |\psi\rangle = \frac{1}{2}\{\ \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle + |\beta_{11}\rangle\right)_{14} \otimes \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle + |\beta_{11}\rangle\right)_{23} + \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle + |\beta_{10}\rangle\right)_{14} \otimes \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle + |\beta_{10}\rangle\right)_{23}$$

$$+ \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle - |\beta_{10}\rangle\right)_{14} \otimes \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle - |\beta_{10}\rangle\right)_{23} + \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle - |\beta_{11}\rangle\right)_{14} \otimes \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle - |\beta_{11}\rangle\right)_{23}\ \}$$

$$= \left(|\beta_{00}\rangle_{14}|\beta_{00}\rangle_{23} + |\beta_{01}\rangle_{14}|\beta_{01}\rangle_{23} + |\beta_{10}\rangle_{14}|\beta_{10}\rangle_{23} + |\beta_{11}\rangle_{14}|\beta_{11}\rangle_{23}\right)$$

$$= \left(|\varphi^+\rangle_{14}|\varphi^+\rangle_{23} + |\psi^+\rangle_{14}|\psi^+\rangle_{23} + |\psi^-\rangle_{14}|\psi^-\rangle_{23} + |\varphi^-\rangle_{14}|\varphi^-\rangle_{23}\right) \qquad (۵-۲)$$

اگر محاسبات بالا را به نحوی دیگر انجام دهیم یعنی آلیس روی ذرات خود (۱،۴) اندازه‌گیری بل انجام دهد ولی ذرات باب به صورت قبلی نوشته شود یعنی بدون اندازه‌گیری در پایه‌های بل باز نتایج یکسانی خواهیم داشت. با مقایسه فرمول (۲-۴)

$$\Rightarrow |\psi\rangle = \frac{1}{2}\{\ \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle + |\beta_{11}\rangle\right)_{14} \otimes |00\rangle_{23} + \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle + |\beta_{10}\rangle\right)_{14} \otimes |01\rangle_{23}$$

$$+ \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle - |\beta_{10}\rangle\right)_{14} \otimes |10\rangle_{23} + \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle - |\beta_{11}\rangle\right)_{14} \otimes |11\rangle_{23}\ \} =$$

$$\frac{1}{2\sqrt{2}}\left(|\beta_{00}\rangle_{14}|00\rangle_{23} + |\beta_{11}\rangle_{14}|00\rangle_{23} + |\beta_{01}\rangle_{14}|01\rangle_{23} + |\beta_{01}\rangle_{14}|01\rangle_{23} - |\beta_{10}\rangle_{14}|10\rangle_{23} + |\beta_{00}\rangle_{14}|11\rangle_{23} - |\beta_{11}\rangle_{14}|11\rangle_{23}\right)$$

$$= \frac{1}{2}\left\{|\beta_{00}\rangle_{14}\left(\frac{|00\rangle_{23} + |11\rangle_{23}}{\sqrt{2}}\right) + |\beta_{11}\rangle_{14}\left(\frac{|00\rangle_{23} - |11\rangle_{23}}{\sqrt{2}}\right) + |\beta_{01}\rangle_{14}\left(\frac{|01\rangle_{23} + |10\rangle_{23}}{\sqrt{2}}\right) + |\beta_{01}\rangle_{14}\left(\frac{|01\rangle_{23} - |10\rangle_{23}}{\sqrt{2}}\right)\right\}$$

$$= \left(|\beta_{00}\rangle_{14}|\beta_{00}\rangle_{23} + |\beta_{01}\rangle_{14}|\beta_{01}\rangle_{23} + |\beta_{10}\rangle_{14}|\beta_{10}\rangle_{23} + |\beta_{11}\rangle_{14}|\beta_{11}\rangle_{23}\right)$$

$$= \left(|\varphi^+\rangle_{14}|\varphi^+\rangle_{23} + |\psi^+\rangle_{14}|\psi^+\rangle_{23} + |\psi^-\rangle_{14}|\psi^-\rangle_{23} + |\varphi^-\rangle_{14}|\varphi^-\rangle_{23}\right) \qquad (۶-۲)$$

نتایج یکسان (۲-۵) و(۲-۶) نشان می‌دهد که اگر آلیس در پایه‌های بل اندازه‌گیری کند به طور آنی ذرات باب نیز در پایه‌های بل اندازه‌گیری خواهد شد در این حالت ماکزیمم درهم‌تنیدگی بین ذرات آلیس و باب به وجود خواهد آمد بدون اینکه این ذرات از قبل باهم درهم‌تنیده باشند.

۲-۱۰- کلید خام:

وقتی که یک رشته بیت از درون کانال کوانتومی (کانالی است که بین آلیس و باب به اشتراک گذاشته است) به باب ارسال می‌شود، به دلیل وجود عوامل مختلفی از قبیل نوفه درون کانال که در اثر حضور ایو به وجود آمده است یا ویژگی‌های کانال و یا نوع پروتکل، ممکن است رشته‌ی بین آلیس و رشته‌ی بین باب با یکدیگر یکسان نباشند و تنها بخشی از رشته بیت آن دو نفر برابر باشند که از آن رشته کلید یکسان به عنوان کلید خام استفاده خواهد شد.

۲-۱۱- کدهای تصحیح خطا:

وقتی که بیت‌های کلاسیک از یک کانال کلاسیک عبور می‌کنند همواره ممکن است دچار خطا شوند. این خطاها هنگام پردازش اطلاعات در یک کامپیوتر کلاسیک نیز می‌توانند رخ دهند. بنابراین لفظ کانال در این جا به یک معنای عام بکار می‌رود که الزاما به معنای آن نیست که بیت یک فاصله مکانی طولانی را طی می‌کند. این اتفاق برای کیوبیت‌ها نیز می‌تواند رخ دهد یعنی کیوبیت‌ها نیز وقتی که از یک کانال کوانتومی عبور می‌کنند ممکن است دچار خطا شوند. یک کامپیوتر کوانتومی وقتی می‌تواند به خوبی کار کند که به توانیم خطاهای ایجاد شده در کیوبیت‌ها را آشکار ساخته و تصحیح کنیم. این امر همچنین برای ارسال اطلاعات کوانتومی توسط کیوبیت‌ها ضرورت دارد. از این به بعد لفظ کانال کلاسیک یا کانال کوانتومی را همواره به یک معنای عام بکار می‌بریم. چند تفاوت مهم بین خطاهای

کلاسیک و کوانتومی وجود دارد و به نظر می‌رسد که خطاهای کوانتومی را واقعا نمی‌توان آشکار و تصحیح کرد:

۱- یک بیت کلاسیک می‌تواند ولتاژ یک نقطه و یا جریان عبور کننده از یک نقطه و یا مغناطش یک حوزه مغناطیسی باشد و اگرچه از نظر ماکروسکوپی کوچک است ولی از نظر میکروسکوپی هنوز از میلیاردها اتم تشکیل شده است و امکان بروز خطا در آن بسیار کم است. در حالی که یک کیوبیت واقعا میکروسکوپی است و نشان دهنده حالت یک اتم یا اسپین یا یون است و براحتی می‌تواند دچار خطا شود.

۲- خطای ایجاد شده در یک بیت کلاسیک یک خطای گسسته است که در آن مقدار $0\ (1)$ به مقدار $1\ (0)$ تبدیل می‌شود و حال آن که خطای ایجاد شده در یک کیوبیت پیوسته است و بردار حالت بیت کوانتومی می‌تواند به طور پیوسته تغییر کند.

۳- می‌توان یک بیت کلاسیک را مشاهده کرد و از خطای ایجاد شده در آن آگاهی یافت ولی یک بیت کوانتومی (کیوبیت) را به راحتی نمی‌توان مشاهده کرد زیرا مشاهده آن عموما منجر به رمبش تابع حالت و از بین رفتن حالت اولیه می‌شود.

۴- کپی‌های متعددی می‌توان از یک بیت کلاسیک تهیه کرد که در صورت بروز خطا در این بیت‌های کلاسیک با استفاده از رأی اکثریت[۱] (که بیشترین احتمال وجود خطا در بیت را بیان می‌کند) می‌توان به بروز خطا در آن‌ها پی برد و حال آن که بنابر قضیه عدم کپی برداری نمی‌توان یک حالت کوانتومی را تکثیر کرد و کپی از آن تهیه کرد.

این تفاوت‌ها در سال‌های اولیه طرح نظریه کامپیوترها و اطلاعات کوانتومی باعث شده بود که عده‌ای

---

۱. Majority voting

گمان کنند کامپیوترهای کوانتومی یا مخابره اطلاعات کوانتومی هرگز به عمل نزدیک نخواهد شد زیرا هرگز نمی‌توان خطاهای کوانتومی را تصحیح کرد. خوشبختانه امروزه یک نظریه کامل برای آشکارسازی و تصحیح خطاهای کوانتومی تدوین شده است که می‌تواند تمام این موانع را از سر راه بردارد و محاسبه و مخابره اطلاعات کوانتومی را به طوری که از خطا مصون باشد، امکان پذیر کند. در این قسمت ابتدا درباره تصحیح خطاهای کلاسیکی یا به اصطلاح کدهای تصحیح کننده خطاهای کلاسیکی بحث می‌کنیم و سپس به بررسی تصحیح خطاهای کوانتومی می‌پردازیم.

۲-۱۲- تصحیح خطای کلاسیکی:

می‌دانیم که هر نوع اطلاعات کلاسیکی به صورت رشته‌ای از علائم $0,1$ نوشته می‌شود. این نوع کدگذاری اصطلاحا کدگذاری منبع[۱] نامیده می‌شود و هدف آن تنها این است که اطلاعاتی که به صورت متن، صدا یا تصویر است به صورت رشته‌ای از علائم ساده و قابل حمل در بیت‌های کلاسیکی تبدیل شود. در کدگذاری منبع مسئله‌ای به نام تصحیح خطا جود ندارد زیرا هنوز اطلاعات به درون کانال (جایی که خطا در آن صورت می‌گیرد) ارسال نشده است. به عنوان مثال فرض کنید که منبع ما از چهار حرف A ، B ، C ، D تشکیل شده است. یک راه برای کدکردن منبع آن است که این حروف را به رشته‌های زیر کد کنیم:

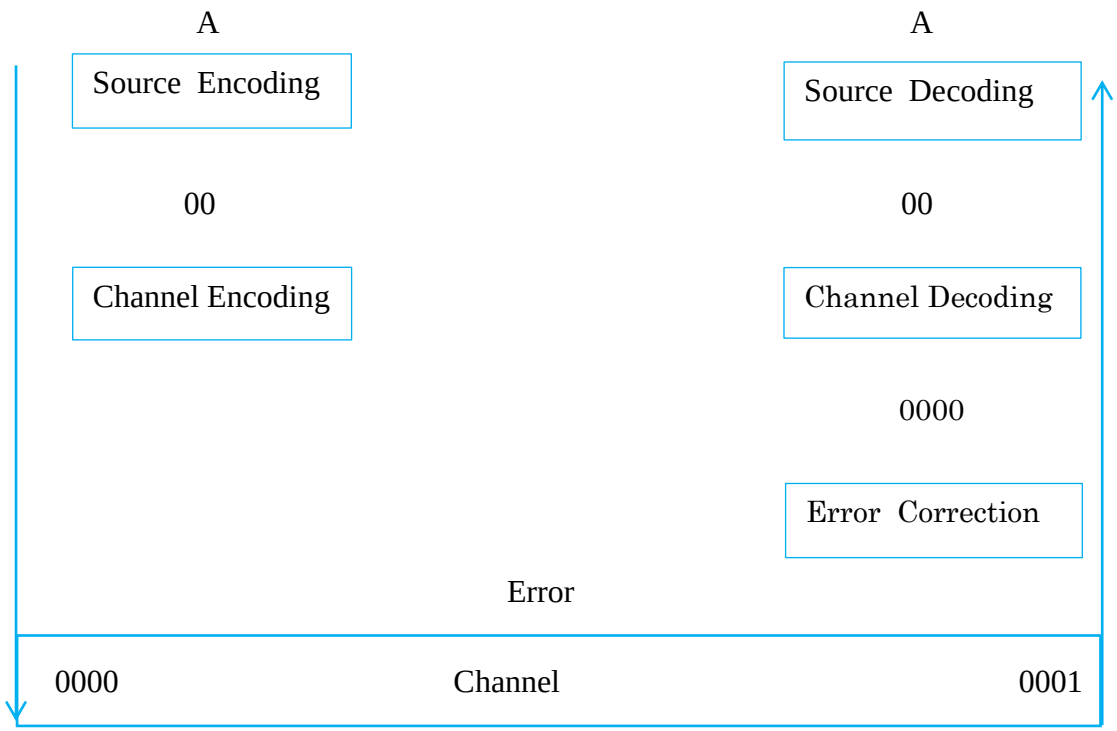
$$\begin{aligned} A &\to 00 \\ B &\to 01 \\ C &\to 10 \\ D &\to 11 \end{aligned} \qquad (۷-۲)$$

در مقصد نیز وقتی که این رشته‌ها به دست گیرنده می‌رسد او نیز همین روش را برای گشودن کد

[۱] Source coding

بکار می‌برد که به آن کدگشایی منبع[۱] می‌گوییم. کدگذاری (۲-۷) به صورت زیر کدگشایی می‌شود:

$$\begin{aligned} 00 &\rightarrow A \\ 01 &\rightarrow B \\ 10 &\rightarrow C \\ 11 &\rightarrow D \end{aligned} \qquad (۲-۸)$$



شکل ۲-۳- مراحل مختلف کدگذاری و کدگشایی یک پیام

اما وقتی که همین رشته‌ها را درون کانال می‌فرستیم دچار خطا می‌شوند. به عنوان مثال 01 می‌تواند در اثر ظاهر شدن یک خطا در بیت اول تبدیل به 11 شود که در مقصد به صورت حرف D تعبیر خواهد شد. بنابراین برای تصحیح این گونه خطاها که در کانال اتفاق می‌افتد می‌بایست در ابتدای

[۱]. source decoding

کانال یک نوع کدگذاری به نام کدگذاری کانال[۱] بکار برد.

$$\begin{aligned} 00 &\rightarrow 0000 \\ 01 &\rightarrow 0101 \\ 10 &\rightarrow 1010 \\ 11 &\rightarrow 1111 \end{aligned} \qquad (۹-۲)$$

رشته‌هایی که به صورت رابطه (۲-۹) کدگذاری کردیم به صورت زیر کدگشایی[۲] می‌کنیم

$$\begin{aligned} 0000 &\rightarrow 00 \\ 0101 &\rightarrow 01 \\ 1010 &\rightarrow 10 \\ 1111 &\rightarrow 11 \end{aligned} \qquad (۱۰-۲)$$

مراحل چهارگانه بالا در شکل (۲-۳) نشان داده است.

۲-۱۳- تصحیح خطای کوانتومی:

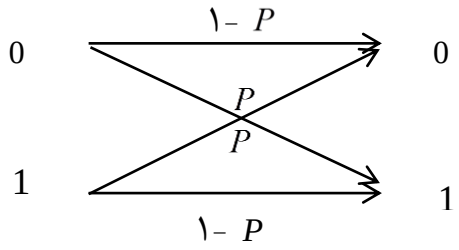
از مسائل اساسی در سیستم‌های اطلاعاتی، نوفه و از اهداف مهم، حفظ اطلاعات از دسترس این نوفه‌ها می‌باشد. نظریه اساسی و کلیدی برای حفظ و بدست آوردن اطلاعات درست و بدون نوفه، افزودن اطلاعات به پیغام اصلی است. در این روش حتی اگر بعضی از اطلاعات در اثر نوفه از بین رفته باشند، با استفاده از اطلاعات افزودنی، اطلاعات اولیه بازیافت شده و پیغام اصلی بدست می‌آید. به عنوان مثال، فرض می‌کنیم بیتی را از یک مکان به مکان دیگر از طریق یک کانال نوفه ارسال کنیم. اگر اثر نوفه در کانال با احتمال P رخ دهد، احتمال اینکه بیت بدون هیچ خطایی ارسال شود P -۱ خواهد بود. حال فرض می‌کنیم بیت 0 را منتقل کرده‌ایم. اثر نوفه به صورت تبدیل این بیت به بیت 1 با

---

۱. Channel Encoding

۲. Channel Decoding

احتمال P و در صورت تغییر نکردن (به صورت 0) با احتمال P -۱ می‌باشند.



شکل ۲-۴- کانال متقارن باینری

اگر کانالی که این بیت از آن عبور داده می‌شود فقط با احتمال P آن را به بیت 1 و P -۱ به بیت 0 تبدیل کند، کانال متقارن باینری[۱] نامیده می‌شود.

با عبور بیت 0 و تبدیل آن به بیت 1 با احتمال P، خطایی رخ داده که برای مقابله با این خطا کافی است به جای این که فقط یک بیت 0 را ارسال کنیم، سه بیت 0 را ارسال کنیم و یا این که به جای یک بیت 1 سه بیت 1 را ارسال کنیم.

$0 \rightarrow 000$

$1 \rightarrow 111$

بیت‌های افزودنی 000 و 111 را بیت‌های منطقی[۱] 0 و 1 می‌نامند. منظور از بیت منطقی 0 این است که به عنوان مثال به جای یک بیت 0، سه تا بیت 0 ارسال شده است.

$0 \rightarrow 000$

---

۱. Binary symmetric channel

۲. Logical bits

بیت خروجی برای این مثال می‌تواند یکی از فرم‌های شکل زیر را داشته باشد:

000	100	011	111
	010	101	
	110	001	

آن دسته از بیت‌هایی در بالا قابل قبول هستند که بیشترین احتمال را داشته باشند. در این مثال آن دسته از بیت‌هایی قابل قبول است که فقط یکی از بیت‌های ارسالی تبدیل شده باشد. در غیر این صورت فرآیند مردود شناخته می‌شود. فرض کنیم که 000 فرستاده شده و بیت خروجی 001 باشد. دریافت کننده می‌خواهد بیت اولیه را تشخیص بدهد، با توجه به بیت خروجی، احتمال P زیاد بالا نیست. بنابراین تشخیص می‌دهد که بیت سوم تغییر کرده و بیت اصلی صفر است. این روش تشخیص بیت اولیه روش رأی اکثریت نام دارد. در این روش اگر برای این مثال دو تا یا بیشتر از بیت‌ها تغییر کرده باشند رأی مردود شناخته می‌شود. در غیر این صورت قابل قبول می‌شود. در این مثال بیت صفر را به صورت سه تا بیت صفر ارسال کرده‌ایم بنابراین احتمال این که دو تا یا هر سه تا بیت تبدیل شوند به صورت زیر محاسبه خواهد شد.

$$\left.\begin{array}{l} 0\xrightarrow{P}1 \\ 0\xrightarrow{P}1 \\ 0\xrightarrow{P}1 \end{array}\right\}\Rightarrow \quad \text{با احتمال } P^3 \text{ هر سه تا بیت تبدیل شده‌اند.} \qquad (۱۱\text{-}۲)$$

برای این که دو تا از بیت‌ها تبدیل شود و یکی بدون تغییر باقی بماند سه حالت داریم:

$$\left.\begin{array}{lll} 0\xrightarrow{1-P}0 & 0\xrightarrow{P}1 & 0\xrightarrow{P}1 \\ 0\xrightarrow{P}1 & 0\xrightarrow{1-P}0 & 0\xrightarrow{P}1 \\ 0\xrightarrow{P}1 & 0\xrightarrow{P}1 & 0\xrightarrow{1-P}0 \end{array}\right\}\Rightarrow \qquad (۱۲\text{-}۲)$$

در رابطه (۲-۱۲) دو تا از بیت‌ها با احتمال کل $3P^2(1-P)$ تبدیل شده‌اند.

با توجه به روابط (۲-۱۱) و (۲-۱۲)، احتمال کل که در آن روش رأی اکثریت مردود می‌شود، $3P^2(1-P)+P^3$ است که با P_e نشان می‌دهیم که داریم:

$$P_e = 3P^2(1-P)+P^3 = 3P^2-3P^3+P^3 = 3P^2-2P^3$$

اگر فقط یک بیت 0را ارسال کنیم با احتمال P به 1 تبدیل می‌شود، اما در حالتی که به جای یک بیت 0، سه تا بیت 0را ارسال کنیم این احتمال برابر $P_e = 3P^2-2P^3$ است. و اگر احتمال P به صورتی باشد که کوچکتر از $\frac{1}{2}$ است در این صورت $P_e \langle P$ خواهد شد.

این روش کدگذاری، تکرار کد[۱] نامیده می‌شود که در این روش پیغام با تکرار هر بیت آن در یک تعداد معین تبدیل و سپس ارسال می‌گردد [۶,۷,۸].

۲-۱۳-۱- کد سه کیوبیتی وارون بیتی[۲]:

این روش کد گذاری، در کلاسیک قابل انجام است، اما در مکانیک کوانتومی با سه مشکل عمده روبرو هستیم:

۱- **نوکلونینگ:** اگر بخواهیم روش تکرار کد را در مکانیک کوانتومی بکار ببریم با تبدیل یک حالت کوانتومی به ۳ حالت یا بیشتر قضیه نوکلونینگ مانع از آن خواهد شد. حتی اگر کلونینگ هم ممکن باشد اندازه‌گیری کردن و مقایسه ۳ حالت کوانتومی خروجی از یک کانال ممکن نخواهد بود.

۲- **پیوستگی خطاها:** ممکن است خطاهای مختلف به طور پیوسته روی یک بیت منفرد رخ دهد و برای تعیین کردن خطاها و تصحیح آن‌ها به یک دقت نامحدود و در نتیجه منابع نامحدود نیازمندیم.

---

۱. Repetition code

۲. Bit flip codes

۳- تخریب خطاها در اثر اندازه‌گیری: در تصحیح خطای کلاسیکی، خروجی از کانال را مشاهده کرده و تصمیم می‌گیریم چه نوع فرآیند رمزگشایی را انتخاب کنیم. اما در مکانیک کوانتومی مشاهده، حالت کوانتومی را تخریب می‌کند و بازیافت حالت اولیه را غیر ممکن می‌سازد.

البته این سه مشکل قابل حل می‌باشد. در فرآیند اطلاعات، سیستم دو حالته است و یکی از دو مقدار 0 و 1 را دارد، بنابراین اطلاعات اصلی، رشته‌ای از 0 و 1ها می باشند. نوفه‌هایی هم که روی این اطلاعات اثر می‌کنند، به صورت تبدیل $|0\rangle$به $|1\rangle$ و یا $|1\rangle$ به $|0\rangle$ ظاهر خواهند شد و در این حالت می‌گوییم که خطای وارون بیتی[۱] رخ داده است. یا اینکه $a|0\rangle+b|1\rangle$ را به حالت $a|0\rangle-b|1\rangle$تبدیل کند که در این حالت می‌گوییم خطای فازی[۲] رخ داده است.

فرض کنید کیوبیت را از یک کانال نویزی ارسال می‌کنیم به طوری که با احتمال P -۱ بدون تغییر باقی بماند و با احتمال P خطای وارون بیتی رخ دهد. به این صورت که با احتمال P ، حالت $|\psi\rangle$ را به حالت $X|\psi\rangle$ تبدیل کند. عملگر X، عملگر پاولی σ_X می‌باشد که به آن عملگر وارون بیتی هم می‌گوییم. کانالی که در آن این نوع خطا رخ بدهد کانال وارون بیتی نامیده می‌شود.

فرض می‌کنیم کیوبیت منفرد $a|0\rangle+b|1\rangle$ را در سه تا کیوبیت کدگذاری گردد:

$$\left.\begin{array}{l}|0\rangle\to|000\rangle=|0_L\rangle\\|1\rangle\to|111\rangle=|1_L\rangle\end{array}\right\}\Rightarrow a|000\rangle+b|111\rangle$$

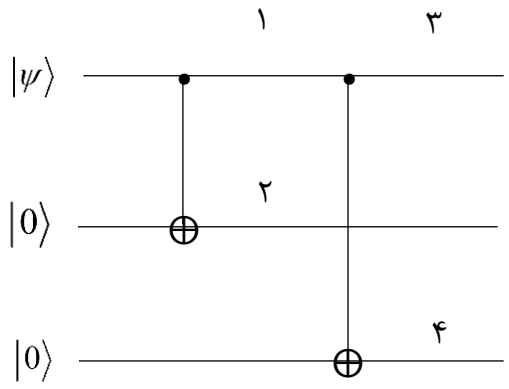
که L نشانگر $\text{logical}|0\rangle$ برای $|0\rangle$، $\text{logical}|1\rangle$ برای $|1\rangle$ می‌باشد. هر کدام از این ۳ کیوبیت از میان یک کپی مستقل از کانال وارون بیتی عبور داده می‌شود.

---

۱. Bit flip error

۲. Phase error

عمل کدگذاری: مدار ۱ عمل کدگذاری $|0\rangle \to |0_L\rangle$، $|1\rangle \to |1_L\rangle$ را انجام می‌دهد:



شکل۲-۵- مدار کدگذاری سه کیوبیت وارون بیتی

در شکل (۲-۵) نقاط توپر مربوط به تغییر فاز هستند. $\oplus$ مدول۲ را نشان می‌دهد. اگر در حالت کلی $|\psi\rangle = a|0\rangle + b|1\rangle$ باشند به $|\psi\rangle = a|000\rangle + b|111\rangle$ تبدیل می‌شوند، یعنی:

$$\big(a|00\rangle + b|11\rangle\big)|0\rangle = a|00\rangle|0\rangle + b|11\rangle|0\rangle \Rightarrow a|00\rangle|0\oplus 0\rangle + b|11\rangle|1\oplus 0\rangle = a|000\rangle + b|111\rangle$$

$$|\psi\rangle|0\rangle = \big(a|0\rangle + b|1\rangle\big)|0\rangle = a|0\rangle|0\rangle + b|1\rangle|0\rangle \Rightarrow$$

$$a|0\rangle|0\oplus 0\rangle + b|1\rangle|1\oplus 0\rangle = a|0\rangle|0\rangle + b|1\rangle|1\rangle = a|00\rangle + b|11\rangle$$

فرض کنید خطای وارون بیتی روی یکی از این کیوبیت‌ها اثر کند. دو مرحله ساده برای تصحیح خطا وجود دارد که می‌تواند حالت کوانتومی صحیح را بازیافت کند.

۱- آشکارسازی خطا یا فرآیند تشخیص مشکل: وقتی اندازه‌گیری صورت می‌گیرد، نوع خطا مشخص می‌شود و نتیجه اندازه‌گیری فرآیند خطا را نشان می‌دهد. برای کانال وارون بیتی، چهار فرآیند تشخیص خطا وجود دارد که با چهار عملگر تصویری متناظر است:

بدون خطا $P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$

وارون بیتی روی کیوبیت اول $P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$

وارون بیتی روی کیوبیت دوم $P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$

وارون بیتی روی کیوبیت سوم $P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$

فرض کنید یک خطای وارون بیتی روی کیوبیت اول روی دهد، در این حالت، حالت $a|000\rangle + b|111\rangle$ به حالت $a|100\rangle + b|011\rangle$ تبدیل می‌شود. باید توجه داشت که $\langle\psi|P_1|\psi\rangle = 1$ و بنابراین خروجی نتیجه اندازه‌گیری هم دقیقا ۱ است. به علاوه روند اندازه‌گیری هیچ تغییری در حالت ایجاد نمی‌کند، بنابراین قبل و بعد از اندازه‌گیری در حالت $a|100\rangle + b|011\rangle$ هستیم. باید توجه کرد که روند اندازه‌گیری فقط دربردارنده اطلاعاتی در مورد خطا می‌باشد و مقادیر a و b را تعیین نمی‌کند.

۲- بازیافت: مقداری را که در نتیجه روند اندازه‌گیری خطا بدست می‌آید، نوع فرآیندی را که باید برای بازیافت حالت اولیه انتخاب کنیم، نشان می‌دهد. برای مثال اگر روند خطا ۱ باشد، وارون بیتی روی کیوبیت اول رخ داده، بنابراین اگر کیوبیت اول را وارونه نماییم حالت اولیه $a|000\rangle + b|111\rangle$ بدست خواهد آمد. مقادیری که در نتیجه اعمال چهار عملگر فرآیند خطا بدست می‌آید و فرآیند بازیافت مربوط به آن‌ها به قرار زیر می‌باشد:

اگر مقدار صفر باشد یعنی خطایی رخ نداده است. اگر مقدار ۱ را بدست آوریم به معنی آن است که روی کیوبیت اول وارون بیتی رخ داده و کافی است که کیوبیت اول را وارونه کنیم. اگر مقدار ۲ بدست آید یعنی روی کیوبیت دوم وارون بیتی رخ داده و کافی است که کیوبیت دوم وارونه شود و اگر مقدار ۳ بدست آید یعنی روی کیوبیت سوم وارون بیتی رخ داده و کافی است که کیوبیت سوم وارونه شود و حالت اولیه بدست آید.

حالت اولیه $|\psi\rangle$ را در نظر می‌گیریم:

$$|\psi\rangle = a|000\rangle + b|111\rangle$$

فرض می‌کنیم که حالت نهایی بدست آمده به صورت $a|100\rangle + b|011\rangle$ باشد در این حالت با اعمال چهار عملگر P_0، P_1، P_2 و P_3 روی حالت نهایی نوع خطا و فرآیندی را که برای بازیافت خطا باید اعمال شود، تعیین می‌کنیم.

$$\langle\psi|P_0|\psi\rangle = \left(a^*\langle 100| + b^*\langle 011|\right)\left(|000\rangle\langle 000| + |111\rangle\langle 111|\right)\left(a|100\rangle + b|011\rangle\right) =$$

$$\left(a^*\langle 100| + b^*\langle 011|\right)\left(a|000\rangle\langle 000|100\rangle + b|000\rangle\langle 000|011\rangle + a|111\rangle\langle 111|100\rangle + b|111\rangle\langle 111|011\rangle\right) = 0$$

با توجه به شرایط تعامد داریم:

$$\langle 000|000\rangle = \langle 111|111\rangle = 1$$

$$\langle 000|111\rangle = \langle 111|000\rangle = 0$$

$$\langle\psi|P_1|\psi\rangle = \left(a^*\langle 100| + b^*\langle 011|\right)\left(a|100\rangle + b|011\rangle\right) = a^2 + b^2 = 1$$

$$\langle\psi|P_2|\psi\rangle = 0$$

$$\langle\psi|P_3|\psi\rangle = 0$$

نتایج بدست آمده بیانگر این مسئله است که وارون بیتی روی کیوبیت اول رخ داده، بنابراین کیوبیت اول را وارون می‌کنیم تا حالت اولیه بدست آید.

۲-۱۴- آنتروپی شانون:

اطلاعات تابعی از احتمالات است؛ از دیدگاه فیزیک، آنتروپی وابسته به توزیع احتمالات است. آنتروپی مفهوم کلیدی تئوری کوانتومی است که اطلاعات موجود در حالت فیزیکی را اندازه‌گیری می‌کند و

می‌توان این اطلاعات را فشرده کرد، بدون این که به محتوی آن لطمه‌ای وارد کرد. همچنین نوفه یک کانال کوانتومی، مقداری از اطلاعات کوانتومی فرستاده شده را از بین می‌برد که ما می‌توانیم مقادیر این اطلاعات را با تابع آنتروپی زیر تخمین بزنیم

$$H(A)=\sum_i P(a_i)h\left[P(a_i)\right]=-K\sum_i P(a_i)\log P(a_i)$$

این تابع $H(A)$، تابع آنتروپی شانون است که یک تابع مثبت است. آنتروپی شانون مربوط به متغیر تصادفی a_i، بیانگر میزان اطلاعاتی است که ما با آگاه شدن از متغیر تصادفی a_i کسب می‌کنیم، به عبارت دیگر آنتروپی شانون نشان دهنده میزان ناآگاهی ما از متغیر a_i قبل از دانستن مقدار آن است که این a_i می‌تواند مقادیر مختلفی را کسب کند این دو دیدگاه مکمل هم هستند، یعنی می‌توان آنتروپی را به عنوان ناآگاهی قبل از اندازه‌گیری متغیر a_i، یا اطلاعات بدست آمده بعد از اندازه‌گیری آن تعبیر و تفسیر کرد. به عنوان مثال متغیر تصادفی A که مقادیر « شیر یا خط » را با احتمالات P و ۱-P می‌پذیرد و متغییر تصادفی B که مقادیر « 0 یا 1 » را با احتمالات P و ۱-P می‌پذیرد، حاوی اطلاعات یکسانی بوده و آنتروپی یکسانی خواهند داشت.

فصل سوم

بررسی حمله NOT کنترلی شخص ثالث در پروتکل MDI-QKD

- مقدمه
- حمله NOT کنترلی در MDI-QKD
- پروتکل MDI-QKD
- حمله NOT کنترلی
- حمله NOT کنترلی متقارن
- الگوریتم کامل هادامارد تقویت کننده حمله NOT کنترلی
- نتیجه‌گیری

۳-۱- مقدمه:

در این بخش ما به بررسی حمله NOT کنترلی در پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI-QKD) می‌پردازیم. و یک روش استراق‌سمع را مطالعه می‌کنیم که می‌توان به طور مناسب در پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری نمایش داد. پروتکل‌های اخیر[۲,۳] از مقاومت در برابر حملات کانال جانبی، باعث شده‌اند که یک شخص ثالث غیر قابل اعتماد در پروتکل منظور شود. به ویژه در [۳] ایده توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری برای مقاومت در برابر حملات کانال جانبی آشکارساز، مطرح شده است. ما نشان خواهیم داد که ایده بنیادی حمله NOT کنترلی به طور مناسبی با تطبیق در این سناریو اصلاح شده است. این پروتکل اخیر برای یک چنین حمله‌ای علیرغم پیشرفت چشم‌گیر علم هنوز به طور دقیق مطالعه نشده است. حمله NOT کنترلی ذاتا نامتقارن است. بنابراین ما گیت هادامارد را درباره یک حمله NOT کنترلی متقارن بکار می‌بریم. در پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری [۳] نیازی نیست که آلیس و باب هیچ کیوبیتی را اندازه‌گیری کنند همه اندازه‌گیری‌ها در محل ایو (شخص ثالث غیر قابل اعتماد) انجام شده است. بنابراین، برای ترفندهای استراق‌سمع طبیعی است بررسی کنیم که ایو خودش تلاش می‌کند تا اطلاعات درباره کلید سری قرارداد شده بین آلیس و باب را بدست آورد. این حمله، حمله شخص ثالث نامیده می‌شود. حال در اینجا یک سری نمادگذاری‌هایی که می‌خواهیم بکار ببریم تعریف می‌کنیم.

BER_{AB} آهنگ خطای بیت برای بیت‌های کلید بین آلیس و باب را نمایش می‌دهد.

P_E احتمال موفقیت ایو در حدس صحیح بیتی است که آلیس برای باب به صورت کیوبیت فرستاده است را نمایش می‌دهد.

روش استراق‌سمعی (که در اینجا مطرح می‌کنیم) نشان می‌دهد که ایو اطلاعات کامل درباره بیت

بدست می‌آورد که در این صورت P_E=۱ است یا به طور کلی او هیچ اطلاعاتی غیر از حدس‌های تصادفی‌اش بدست نمی‌آورد که در این صورت P_E=۱/۲ . هر چند در حالت دوم ایو مقداری اطلاعات به شرح زیر بدست خواهد آورد:

π_E احتمال موفقیت ایو در حدس صحیح خطایی است که در مدت ارتباط بین آلیس و باب بوجود آمده را نمایش می‌دهد.

که در این مورد ایو ممکن است هیچ اطلاعاتی درباره مقدار بیت نداشته باشد اما او دقیقا می‌داند که یک خطا در طول ارتباط بین آلیس و باب رخ داده است یا نه که در این صورت $\pi_E = ۱$ است.

۳-۲- حمله NOT کنترلی در توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری:

ما از حالت‌های بل، حالت‌های درهم‌تنیده دوکیوبیتی استفاده می‌کنیم. چهار حالت بل را به صورت زیر داریم

$$\left|\varphi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \quad , \quad \left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)$$

ایو (شخص ثالث غیر قابل اعتماد) حالت‌های دریافتی از آلیس و باب را در این پایه‌ها اندازه‌گیری می‌کند و نتیجه اندازه‌گیری را به آن‌ها اطلاع می‌دهد. برای اهداف جاسوسی، تعدادی اندازه‌گیری دیگر توسط ایو را بررسی می‌کنیم که در این اندازه‌گیری‌ها کیوبیت‌های ایو با کیوبیت‌های فرستاده شده توسط آلیس و باب برهم‌کنش دارند. برای این جاسوسی‌ها، مبنی بر حالتی که بین آلیس و باب است ایو در پایه‌های بل یا در پایه‌های محاسباتی $\left(|00\rangle,|01\rangle,|10\rangle,|11\rangle\right)$ اندازه‌گیری می‌کند.

قبل از پرداختن به جزئیات بیشتر، نخست پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI-QKD) [۳] را شرح می‌دهیم.

۳-۳- پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI-QKD):

۱) آلیس و باب رشته بیت‌ها را به صورت تصادفی انتخاب می‌کنند و بیت‌ها را به صورت تصادفی در پایه‌های Z و X کد گذاری می‌کنند و آن‌ها را برای ایو می‌فرستند.

۲) ایو جفت کیوبیت‌ها را (یکی از آلیس و یکی از باب) دریافت می‌کند و آن‌ها را در پایه‌های بل اندازه‌گیری می‌کند. نتایج آشکارسازی به طور علنی منتشر می‌شود.

۳) برای حالت‌هایی که پایه‌های آلیس و باب مطابقت دارند

الف) اگر کیوبیت‌های آلیس و باب در پایه Z باشد و نتایج اندازه‌گیری ایو $\left|\psi^{\pm}\right\rangle$ باشد یک نفر از آلیس یا باب باید بیت را برگرداند؛

ب) اگر کیوبیت‌های آلیس و باب در پایه X باشد و نتیجه اندازه‌گیری ایو $\left|\psi^{-}\right\rangle$ یا $\left|\varphi^{-}\right\rangle$ باشد یک نفر از آلیس یا باب باید بیت را برگرداند؛

۴) اصلاح اطلاعات (استفاده کدهای تصحیح خطا) و تقویت خصوصی به وسیله آلیس و باب در n بیت باقی‌مانده (که کلید خام می‌نامیم) با بدست آوردن m بیت کلید مشترک (کلید پایانی) انجام شده است.

در عمل، ایو فقط دو حالت $\left|\psi^{\pm}\right\rangle$ از چهار حالت بل را مشخص می‌کند که برای اثبات ایمنی[۳] کافی است. تمام موارد مذکور به طور کلی به استثنای هنگامی که آلیس و باب کیوبیت‌ها را در پایه‌های

مختلف اندازه‌گیری می‌کنند و سپس این جفت کیوبیت‌ها را دور می‌اندازند در جدول (۳-۱) توضیح داده شده است.

by Qubit sent		Probability (Eve's end)				Flip
Alice	Bob	$\|\varphi^+\rangle$	$\|\varphi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	
$\|0\rangle$	$\|0\rangle$	1/2	1/2	0	0	No
$\|0\rangle$	$\|1\rangle$	0	0	1/2	1/2	Yes
$\|1\rangle$	$\|0\rangle$	0	0	1/2	1/2	Yes
$\|1\rangle$	$\|1\rangle$	1/2	1/2	0	0	No
$\|+\rangle$	$\|+\rangle$	1/2	0	1/2	0	No
$\|+\rangle$	$\|-\rangle$	0	1/2	0	1/2	Yes
$\|-\rangle$	$\|+\rangle$	0	1/2	0	1/2	Yes
$\|-\rangle$	$\|-\rangle$	1/2	0	1/2	0	No

جدول ۳-۱- برگرداندن بیت متناسب با پایه اندازه‌گیری آلیس و باب و نتایج اندازه‌گیری ایو

۳-۴- حمله NOT کنترلی:

مدل استراق‌سمع در این حالت به شرح زیر است که ایو (شخص ثالث غیر قابل اعتماد) تلاش می‌کند تا اطلاعات را بدست بیاورد. ایو کیوبیت‌ها را از آلیس و باب می‌گیرد و هر یک از این کیوبیت‌ها را در ورودی کنترل یک گیت NOT کنترلی ثبت می‌کند و او $|0\rangle$ را از کیوبیت‌های هدف بکار می‌گیرد. خروجی‌های مربوط به کیوبیت‌های کنترل گیت‌های NOT کنترلی در پایه‌های بل به وسیله ایو اندازه‌گیری خواهد شد و نتیجه با آلیس و باب مرتبط خواهد بود. ایو خروجی مربوط به هدف را در حافظه کوانتومی‌اش ذخیره می‌کند. سپس آلیس و باب پایه‌هایشان را اعلان می‌کنند. ایو تلاش خواهد کرد تا اطلاعات را از خروجی‌های مربوط به کیوبیت‌های هدف گیت‌های NOT کنترلی استخراج کند. اگر آلیس و باب پایه Z را برای ارتباط انتخاب کنند. در این حالت، ایو قادر خواهد بود کیوبیت‌ها را به طور کامل با استفاده گیت‌های NOT کنترلی بدون ایجاد هیچ اختلالی برای کیوبیت‌های فرستاده شده به وسیله آلیس و باب کپی کند. اگر بعد از اندازه‌گیری حالت ایو $|\varphi^{\pm}\rangle$ باشد بنابراین بیت‌های آلیس و باب مطابقت دارند. به طور مشابه اگر خروجی اندازه‌گیری ایو $|\psi^{\pm}\rangle$ باشد سپس بیت‌های آلیس و باب مطابقت ندارند بنابراین در این حالت ایو همه اطلاعات را بدون ایجاد هیچ اختلالی بدست خواهد آورد. توجه کنیم که در این حالت، ایو کیوبیت هدف‌اش را در پایه‌های محاسباتی $(|11\rangle+|10\rangle+|00\rangle+|01\rangle)$ اندازه‌گیری می‌کند. هنگامی که آلیس و باب در پایه‌های X با یکدیگر ارتباط برقرار می‌کنند بنابراین خطا توسط حمله NOT کنترلی بروز می‌کند و این شرایط به عنوان یک نمونه معاوضه درهم‌تنیدگی[۴] درنظر گرفته شده است. کاربرد معاوضه درهم‌تنیدگی در این پروتکل‌ها (همچنین در طرح یا در تحلیل) به سبب پیچیدگی شخص ثالث مشهود است. حالا یک حالت خاص را در اینجا بررسی می‌کنیم. و حالت‌های دیگر نیز به طور مشابه بررسی خواهند شد. آلیس و باب هر دو $|+\rangle$ را می‌فرستند. بنابراین بعد از استفاده گیت‌های NOT کنترلی توسط ایو حالت‌های درهم‌تنیده آلیس با ایو و باب با ایو به ترتیب به صورت $\frac{|0_A 0_{E_1}\rangle+|1_A 1_{E_1}\rangle}{\sqrt{2}}$ و

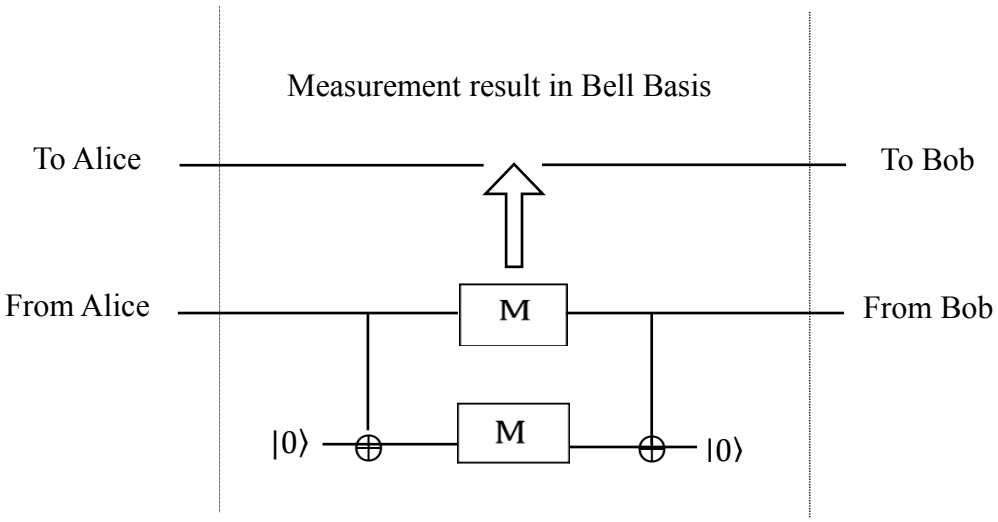
$\frac{\left|0_B 0_{E_2}\right\rangle+\left|1_B 1_{E_2}\right\rangle}{\sqrt{2}}$ خواهند بود. ضرب حالت‌های درهم‌تنیده را به صورت $\left(\frac{\left|0_A 0_{E_1}\right\rangle+\left|1_A 1_{E_1}\right\rangle}{\sqrt{2}}\right)\otimes\left(\frac{\left|0_B 0_{E_2}\right\rangle+\left|1_B 1_{E_2}\right\rangle}{\sqrt{2}}\right)$ داریم که این حالت سیستم مرکب آلیس، باب و ایو است که با بازنویسی در پایه ایو و سپس اندازه‌گیری در پایه‌های بل به صورت زیر نوشته می‌شود

$$\frac{1}{\sqrt{2}}\left(\left|\varphi^{+}{}_{AB}\right\rangle\left|\varphi^{+}{}_{E_1E_2}\right\rangle+\left|\varphi_{AB}{}^{-}\right\rangle\left|\varphi^{-}{}_{E_1E_2}\right\rangle+\left|\psi^{+}{}_{AB}\right\rangle\left|\psi^{+}{}_{E_1E_2}\right\rangle+\left|\psi^{-}{}_{AB}\right\rangle\left|\psi^{-}{}_{E_1E_2}\right\rangle\right).$$

اندازه‌گیری صحیح در این حالت $\left|\varphi^{+}{}_{AB}\right\rangle$ یا $\left|\psi^{+}{}_{AB}\right\rangle$ است که با احتمال ۱/۲ رخ می‌دهد که این حالت بعد از پایه‌های آلیس و باب اعلان می‌شود، ایو همچنین $\left|\varphi^{+}{}_{E_1E_2}\right\rangle$ یا $\left|\psi^{+}{}_{E_1E_2}\right\rangle$ را اندازه‌گیری خواهد کرد و او قادر خواهد بود بفهمد که بدون خطا منتشر شده‌اند. هر چند اگر نتیجه اندازه‌گیری $\left|\varphi^{-}{}_{E_1E_2}\right\rangle$ یا $\left|\psi^{-}{}_{E_1E_2}\right\rangle$ شود (این حالت نیز با احتمال ۱/۲ رخ می‌دهد)، سپس ایو متوجه می‌شود که یک خطا ایجاد شده و او قادر نیست بیت سری را بدست آورد. حالت‌های دیگر نیز به طور نمونه بررسی می‌شوند که در جدول (۳-۳) نشان داده شده است. بعد از این که آلیس و باب به طور علنی پایه‌هایشان را اعلان کنند اگر پایه اندازه‌گیری‌شان Z باشد ایو همه اطلاعات را بدون ایجاد هیچ خطایی به وسیله اندازه‌گیری در پایه‌های محاسباتی $\left(\left|11\right\rangle+\left|10\right\rangle+\left|00\right\rangle+\left|01\right\rangle\right)$ بدست می‌آورد. اگر پایه X باشد برهم‌کنش ایو خطایی با آهنگ ۱/۲ ایجاد می‌کند اما ایو هیچ اطلاعاتی درباره بیت‌های سری به دست نمی‌آورد که در جدول (۳-۲) نشان داده شده است. در این حالت اگر اندازه‌گیری ایو $\left|\varphi^{+}{}_{E_1E_2}\right\rangle$ یا $\left|\psi^{+}{}_{E_1E_2}\right\rangle$ باشد بنابراین او متوجه می‌شود که بدون اختلال منتشر شده است. اگر اندازه‌گیری ایو $\left|\varphi^{-}{}_{E_1E_2}\right\rangle$ یا $\left|\psi^{-}{}_{E_1E_2}\right\rangle$ باشد او متوجه می‌شود که خطا ایجاد شده است. یعنی این که آلیس و باب در یک مقدار بیت مکمل در این مکان کلید سری را بکار خواهند برد. حالت‌های مذکور به طور خلاصه در شکل (۳-۱) و جدول (۳-۳) نشان داده شده است.

Basis (Alice , Bob)	Operation by Eve	BER_{AB}	P_E	π_E
Z	C-NOT	0	1	1
X	C-NOT	0.5	0.5	1

جدول ۳-۲- احتمال موفقیت ایو با عمل C-NOT در حدس صحیح بیت بین آلیس و باب



شکل ۳-۱- حمله C-NOT در MDI-QKD

Alice , Bob	Eve (after C-NOT attack)
$\|+\rangle,\|+\rangle$	$\frac{1}{\sqrt{2}}\left(\|\varphi^+{}_{AB}\rangle\|\varphi^+{}_{E_1E_2}\rangle+\|\varphi_{AB}{}^-\rangle\|\varphi^-{}_{E_1E_2}\rangle+\|\psi^+{}_{AB}\rangle\|\psi^+{}_{E_1E_2}\rangle+\|\psi^-{}_{AB}\rangle\|\psi^-{}_{E_1E_2}\rangle\right)$
$\|+\rangle,\|-\rangle$	$\frac{1}{\sqrt{2}}\left(\|\varphi^+{}_{AB}\rangle\|\varphi^-{}_{E_1E_2}\rangle+\|\varphi_{AB}{}^-\rangle\|\varphi^+{}_{E_1E_2}\rangle-\|\psi^+{}_{AB}\rangle\|\psi^-{}_{E_1E_2}\rangle-\|\psi^-{}_{AB}\rangle\|\psi^+{}_{E_1E_2}\rangle\right)$
$\|-\rangle,\|+\rangle$	$\frac{1}{\sqrt{2}}\left(\|\varphi^+{}_{AB}\rangle\|\varphi^-{}_{E_1E_2}\rangle+\|\varphi_{AB}{}^-\rangle\|\varphi^+{}_{E_1E_2}\rangle+\|\psi^+{}_{AB}\rangle\|\psi^-{}_{E_1E_2}\rangle+\|\psi^-{}_{AB}\rangle\|\psi^+{}_{E_1E_2}\rangle\right)$
$\|-\rangle,\|-\rangle$	$\frac{1}{\sqrt{2}}\left(\|\varphi^+{}_{AB}\rangle\|\varphi^+{}_{E_1E_2}\rangle+\|\varphi_{AB}{}^-\rangle\|\varphi^-{}_{E_1E_2}\rangle-\|\psi^+{}_{AB}\rangle\|\psi^+{}_{E_1E_2}\rangle+\|\psi^-{}_{AB}\rangle\|\psi^-{}_{E_1E_2}\rangle\right)$

جدول ۳-۳- حالت ایجاد شده با ایو بعد از حمله NOT کنترلی

یک حالت از جدول (۳-۳) را بررسی می‌کنیم و بقیه حالت‌ها نیز به طور مشابه بررسی می‌شوند

آلیس و باب هر دو حالت $|+\rangle$ را انتخاب می‌کنند

$$|+\rangle_A=\frac{1}{\sqrt{2}}\left(|0\rangle_A+|1\rangle_A\right)$$

$$|+\rangle_B=\frac{1}{\sqrt{2}}\left(|0\rangle_B+|1\rangle_B\right)$$

ایو حالت $|0\rangle_E$ را انتخاب می‌کند و یک بار با آلیس حالت درهم‌تنیده ایجاد می‌کند و یک بار با باب.

حالت درهم‌تنیده بین پایه‌های ایو و آلیس:

$$|+\rangle_A|0\rangle_{E_1}=\frac{1}{\sqrt{2}}\left(|0\rangle_A+|1\rangle_A\right)\otimes|0\rangle_{E_1}=\frac{|00\rangle_{AE_1}+|10\rangle_{AE_1}}{\sqrt{2}}\xrightarrow{C-NOT}\frac{|00\rangle_{AE_1}+|11\rangle_{AE_1}}{\sqrt{2}}$$

حالت درهم‌تنیده بین پایه‌های ایو با باب:

$$|+\rangle_B|0\rangle_{E_2}=\frac{1}{\sqrt{2}}\left(|0\rangle_B+|1\rangle_B\right)\otimes|0\rangle_{E_2}=\frac{|00\rangle_{BE_2}+|10\rangle_{BE_2}}{\sqrt{2}}\xrightarrow{C-NOT}\frac{|00\rangle_{BE_2}+|11\rangle_{BE_2}}{\sqrt{2}}$$

ضرب دو حالت درهم‌تنیده بالا بین پایه‌های ایو با آلیس و ایو با باب را به صورت زیر انجام می‌دهیم:

$$|\psi\rangle=\frac{|00\rangle_{AE_1}+|11\rangle_{AE_1}}{\sqrt{2}}\otimes\frac{|00\rangle_{BE_2}+|11\rangle_{BE_2}}{\sqrt{2}}=\frac{1}{2}\left(|00\rangle_{AE_1}|00\rangle_{BE_2}+|00\rangle_{AE_1}|11\rangle_{BE_2}+|11\rangle_{AE_1}|00\rangle_{BE_2}+|11\rangle_{AE_1}|11\rangle_{BE_2}\right)$$

$|\psi\rangle$ را به صورت زیر در پایه‌های ایو بازنویسی می‌کنیم:

$$|\psi\rangle=\frac{1}{2}\left(|00\rangle_{AB}|00\rangle_{E_1E_2}+|01\rangle_{AB}|01\rangle_{E_1E_2}+|10\rangle_{AB}|10\rangle_{E_1E_2}+|11\rangle_{AB}|11\rangle_{E_1E_2}\right)$$

حالت بازنویسی شده پایه‌های ایو را دوباره با استفاده از حالت‌های بل که در فصل دوم بیان کردیم در پایه‌های بل می‌نویسیم و در انتها به جواب نهایی زیر می‌رسیم:

$$\Rightarrow|\psi\rangle=\frac{1}{2}\{\ \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle+|\beta_{11}\rangle\right)_{AB}\otimes\frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle+|\beta_{11}\rangle\right)_{E_1E_2}+\frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle+|\beta_{10}\rangle\right)_{AB}\otimes\frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle+|\beta_{10}\rangle\right)_{E_1E_2}$$

$$+\frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle_-|\beta_{10}\rangle\right)_{AB}\otimes\frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle-|\beta_{10}\rangle\right)_{E_1E_2}+\frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle-|\beta_{11}\rangle\right)_{AB}\otimes\frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle-|\beta_{11}\rangle\right)_{E_1E_2}\ \}$$

$$=\frac{1}{2}\left(|\beta_{00}\rangle_{AB}|\beta_{00}\rangle_{E_1E_2}+|\beta_{11}\rangle_{AB}|\beta_{11}\rangle_{E_1E_2}+|\beta_{01}\rangle_{AB}|\beta_{01}\rangle_{E_1E_2}+|\beta_{10}\rangle_{AB}|\beta_{10}\rangle_{E_1E_2}\right)$$

$$=\frac{1}{2}\left(|\varphi^+\rangle_{AB}|\varphi^+\rangle_{E_1E_2}+|\varphi^-\rangle_{AB}|\varphi^-\rangle_{E_1E_2}+|\psi^+\rangle_{AB}|\psi^+\rangle_{E_1E_2}+|\psi^-\rangle_{AB}|\psi^-\rangle_{E_1E_2}\right).$$

که حالت‌های β_{ij} همان حالت‌های بل هستند.

۳-۵- حمله NOT کنترلی متقارن:

ما در بخش قبلی دیدیم حمله NOT کنترلی شخص ثالث هیچ خطایی در پایه Z ایجاد نمی‌کند، اما

خطاهایی در نصف حالت‌ها در پایه X موجب می‌شود. بنابراین این حمله NOT کنترلی استراق‌سمع، نامتقارن است. با آماده سازی یک حمله NOT کنترلی متقارن، ما اصلاح زیر را انجام می‌دهیم.

H گیت هادامارد و I گیت همانی است و C گیت NOT کنترلی می‌باشد. به صورت زیر تعریف داریم

$$\mathrm{P}_u = (H \otimes I)^u \, C \, (H \otimes I)^u \qquad \text{for} \quad u = 0,1$$

با این تعریف حالت‌های زیر را بررسی می‌کنیم

$$\mathrm{P}_0(|00\rangle) = |00\rangle \quad , \quad \mathrm{P}_0(|10\rangle) = |11\rangle$$

$$\mathrm{P}_0(|+0\rangle) = \frac{|++\rangle + |--\rangle}{\sqrt{2}} \quad , \quad \mathrm{P}_0(|-0\rangle) = \frac{|+-\rangle + |-+\rangle}{\sqrt{2}}$$

$$\mathrm{P}_1(|00\rangle) = \frac{|0+\rangle + |1-\rangle}{\sqrt{2}} \quad , \quad \mathrm{P}_1(|10\rangle) = \frac{|0-\rangle + |1+\rangle}{\sqrt{2}}$$

$$\mathrm{P}_1(|+0\rangle) = |+0\rangle \quad , \quad \mathrm{P}_1(|-0\rangle) = |-1\rangle$$

با تعریفی که از صفحه قبل داریم موارد بالا را به صورت زیر بررسی می‌کنیم:

$$\mathrm{P}_u = (H \otimes I)^u \, C \, (H \otimes I)^u \qquad \text{for} \quad u = 0,1$$

1) $u = 0 \quad \Rightarrow \quad \mathrm{P}_0 = C$

2) $u = 1 \quad \Rightarrow \quad \mathrm{P}_1 = (H \otimes I) C (H \otimes I)$

1) $$\mathrm{P}_0(|+0\rangle) = C(|+0\rangle) = C(|+\rangle|0\rangle) = C\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = C\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2}}\left(\frac{|+\rangle+|-\rangle}{\sqrt{2}}\otimes\frac{|+\rangle+|-\rangle}{\sqrt{2}}+\frac{|+\rangle-|-\rangle}{\sqrt{2}}\otimes\frac{|+\rangle-|-\rangle}{\sqrt{2}}\right)=$$

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

$$\Rightarrow \mathrm{P}_0\left(|+0\rangle\right)=\frac{|++\rangle+|--\rangle}{\sqrt{2}}$$

$\mathrm{P}_0\left(|-0\rangle\right)=\frac{|+-\rangle+|-+\rangle}{\sqrt{2}}$ نیز مانند حالت قبلی بررسی می‌شود.

---

2) $\mathrm{P}_1\left(|00\rangle\right)=(H\otimes I)C(H\otimes I)|00\rangle=(H\otimes I)C\left(H|0\rangle\right)\left(I|0\rangle\right)=(H\otimes I)C\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle=$

$$(H\otimes I)C\left(\frac{|00\rangle+|10\rangle}{\sqrt{2}}\right)=(H\otimes I)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)=\frac{\left(H|0\rangle\right)\left(I|0\rangle\right)+\left(H|1\rangle\right)\left(I|1\rangle\right)}{\sqrt{2}}=\frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|0\rangle+\frac{|0\rangle-|1\rangle}{\sqrt{2}}\otimes|1\rangle\right)=$$

$$\frac{1}{\sqrt{2}\sqrt{2}}\left(|00\rangle+|10\rangle+|01\rangle-|11\rangle\right)=\frac{1}{\sqrt{2}}\left(|0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)+|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right)=\frac{1}{\sqrt{2}}\left(|0\rangle|+\rangle+|1\rangle|-\rangle\right)=\frac{|0+\rangle+|1-\rangle}{\sqrt{2}}$$

$$\Rightarrow \mathrm{P}_1\left(|00\rangle\right)=\frac{|0+\rangle+|1-\rangle}{\sqrt{2}}$$

$\mathrm{P}_1\left(|10\rangle\right)=\frac{|0-\rangle+|1+\rangle}{\sqrt{2}}$ را می‌توانیم به صورت حالت قبلی بررسی کنیم.

$$P_1(|+0\rangle)=(H\otimes I)C(H\otimes I)|+0\rangle=(H\otimes I)C(H\otimes I)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle=(H\otimes I)C(H\otimes I)\left(\frac{|00\rangle+|10\rangle}{\sqrt{2}}\right)=$$

$$(H\otimes I)C\left(\frac{(H|0\rangle)(I|0\rangle)+(H|1\rangle)(I|0\rangle)}{\sqrt{2}}\right)=((H\otimes I)C)\frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|0\rangle+\frac{|0\rangle-|1\rangle}{\sqrt{2}}\otimes|0\rangle+\right)=$$

$$((H\otimes I)C)\frac{1}{\sqrt{2}}\left(\frac{|00\rangle+|10\rangle}{\sqrt{2}}+\frac{|00\rangle-|10\rangle}{\sqrt{2}}\right)=\frac{(H\otimes I)}{\sqrt{2}}\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}+\frac{|00\rangle-|11\rangle}{\sqrt{2}}\right)=$$

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

$$\frac{1}{2}\left(\frac{|00\rangle+|10\rangle}{\sqrt{2}}+\frac{|01\rangle-|11\rangle}{\sqrt{2}}+\frac{|00\rangle+|10\rangle}{\sqrt{2}}-\frac{|01\rangle-|11\rangle}{\sqrt{2}}\right)=\frac{|00\rangle+|10\rangle}{\sqrt{2}}=\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle=|+0\rangle$$

$$\Rightarrow P_1(|+0\rangle)=|+0\rangle$$

با توجه به روش بالا $P_1(|-0\rangle)=|-1\rangle$ را نیز می‌توانیم بدست آوریم.

ایو P_0 یا P_1را اعمال می‌کند. اعمال $P_0(C-NOT)$ برای هر یک از حالت‌های آلیس و باب در بخش قبلی شرح داده شده است.

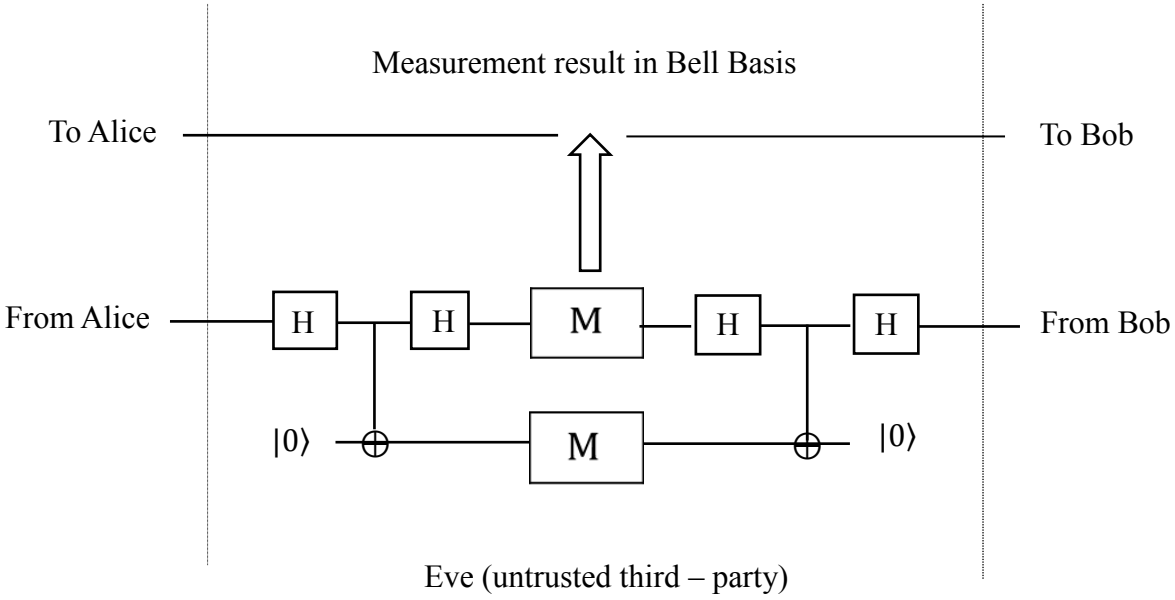
برای حالتی که P_1 اعمال می‌شود و آلیس و باب هر دو پایه X را برای ارتباط انتخاب کنند ایو قادر

خواهد بود بیت‌های سری را بدون ایجاد هیچ اختلالی به وسیله اندازه‌گیری کیوبیت‌های هدف‌اش در پایه‌های محاسباتی $\left(|00\rangle,|01\rangle,|10\rangle,|11\rangle\right)$ بدست آورد.

آلیس و باب پایه Z را برای ارتباط انتخاب کنند و P_1 اعمال شود ایو فقط قادر خواهد بود بیت سری را با حدس تصادفی پیش بینی کند (یعنی این که با احتمال ۱/۲)، ولی او قادر خواهد بود خطای ایجاد شده را تشخیص دهد. این حالت شبیه به این است که آلیس و باب پایه X را برای ارتباط انتخاب کنند و P_0 اعمال شود. حالت‌های مختلف در شکل (۳-۲) و جدول (۳-۵) شرح داده شده است بنابراین، P_0 و P_1 به طور تصادفی با احتمال ۱/۲ اعمال می‌شوند، ما نتایج را در جدول (۳-۴) نشان دادیم.

Basis (Alice , Bob)	Operation By Eve	BER_{AB}	P_E	π_E
Z	P_0	0	1	1
X	P_0	0.5	0.5	1
Z	P_1	0.5	0.5	1
X	P_1	0	1	1

جدول ۳-۴- احتمال موفقیت ایو با عمل P_0 , P_1 در حدس صحیح بیت بین آلیس و باب



شکل ۳-۲- هادامارد تقویت کننده‌ی حمله NOT کنترلی در MDI-QKD

Alice , Bob	Eve (after Hadamard assisted C-NOT attack, i.e.,with P_1)
$\|0\rangle,\|0\rangle$	$\frac{1}{\sqrt{2}}\left(\|\varphi^+_{AB}\rangle\|\varphi^+_{E_1E_2}\rangle+\|\varphi^-_{AB}\rangle\|\psi^+_{E_1E_2}\rangle+\|\psi^+_{AB}\rangle\|\varphi^-_{E_1E_2}\rangle-\|\psi^-_{AB}\rangle\|\psi^-_{E_1E_2}\rangle\right)$
$\|1\rangle,\|0\rangle$	$\frac{1}{\sqrt{2}}\left(\|\varphi^+_{AB}\rangle\|\varphi^-_{E_1E_2}\rangle-\|\varphi^-_{AB}\rangle\|\psi^-_{E_1E_2}\rangle+\|\psi^+_{AB}\rangle\|\varphi^+_{E_1E_2}\rangle+\|\psi^-_{AB}\rangle\|\psi^+_{E_1E_2}\rangle\right)$
$\|1\rangle,\|0\rangle$	$\frac{1}{\sqrt{2}}\left(\|\varphi^+_{AB}\rangle\|\varphi^-_{E_1E_2}\rangle+\|\varphi^-_{AB}\rangle\|\psi^-_{E_1E_2}\rangle+\|\psi^+_{AB}\rangle\|\varphi^+_{E_1E_2}\rangle+\|\psi^-_{AB}\rangle\|\psi^+_{E_1E_2}\rangle\right)$
$\|1\rangle,\|1\rangle$	$\frac{1}{\sqrt{2}}\left(\|\varphi^+_{AB}\rangle\|\varphi^+_{E_1E_2}\rangle-\|\varphi^-_{AB}\rangle\|\psi^+_{E_1E_2}\rangle+\|\psi^+_{AB}\rangle\|\varphi^-_{E_1E_2}\rangle+\|\psi^-_{AB}\rangle\|\psi^-_{E_1E_2}\rangle\right)$

جدول ۳-۵- حالت ایجاد شده با ایو بعد از هادامارد تقویت کننده ی حمله NOT کنترلی

۳-۵-۱- الگوریتم کامل هادامارد برای تقویت حمله N0T کنترلی:

۱) ایو P_0 یا P_1 را بر کیوبیت‌های $|\mu_A\rangle,|\mu_B\rangle$ (حالتی که توسط آلیس و باب به ایو مرتبط شده است) و $|0\rangle$ (منبع کمکی به وسیله ایو) برای هر دو حالت اعمال می‌کند.

۲) حالت دوکیوبیتی (خروجی‌های مربوط به $|\mu_A\rangle,|\mu_B\rangle$) در پایه بل اندازه‌گیری شده و نتیجه اندازه‌گیری با آلیس و باب مرتبط است. این دو خروجی مربوط به کیوبیت‌های $|0\rangle$ (از کیوبیت‌های هدف) با ایو در نظر گرفته شده‌اند.

۳) بعد از اعلان حالت بین آلیس و باب، ایو درباره حالت‌هایی که آلیس و باب پایه‌های یکسان دارند را می‌فهمد و حالت‌هایی که آلیس و باب پایه‌های مختلف دارند را دور می‌اندازد.

۴) اگر آلیس و باب هر دو کیوبیت‌هایی در پایه Z (X) انتخاب کنند و ایو P_0 (P_1) را اعمال کند سپس ایو بیت رمز متناظر را بدون ایجاد هیچ خطایی به وسیله اندازه‌گیری جفت کیوبیت‌ها در پایه‌های محاسباتی به دست می‌آورد.

۵) اگر آلیس و باب هر دو کیوبیت‌هایی در پایه Z (X) انتخاب کنند و ایو P_1 (P_0) اعمال کند ایو فقط می‌تواند بیت بین آلیس و باب را با احتمال ۱/۲ و با آهنگ خطای بیت ۱/۲ حدس بزند.

در این حالت‌ها ایو کیوبیت‌هایش را در پایه بل اندازه‌گیری می‌کند و اگر خروجی اندازه‌گیری ایو $|\varphi^+_{E_1E_2}\rangle$ یا $|\psi^+_{E_1E_2}\rangle$ باشد ($|\varphi^-_{E_1E_2}\rangle$ یا $|\psi^-_{E_1E_2}\rangle$) بنابراین ایو می‌داندکه در طول ارتباط خطا نبوده است (بوده است).

چنانکه آلیس و باب با احتمال مساوی بر پایه‌های X یا Z توافق کنند، و ایو P_0 یا P_1 را اعمال کند، آهنگ خطا در هر دو پایه X و Z برابر خواهد بود. بنابراین حمله یک حمله متقارن است.

۳-۶- نتیجه‌گیری:

ما در این قسمت بررسی کردیم برای این‌که حمله NOT کنترلی در پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری [۳] اعمال شود نیاز به یک شخص ثالث دارد تا حمله را با استفاده از معاوضه درهم‌تنیدگی اجرا کند. از طریق این نوع استراق‌سمع ایو به طور دقیق حدود نصف بیت‌های سری بین طرفین ارتباط (آلیس و باب) را به دست می‌آورد. برای بقیه بیت‌ها ایو فقط قادر خواهد بود مقادیر بیت را به طور حدسی پیش بینی کند. هر چند ایو پی خواهد برد که برهم‌کنش او خطایی بین آلیس و باب ایجاد خواهد کرد.

فصل چهارم

توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری

- مقدمه
- پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری
- آهنگ تولید کلید
- روش تخمین
- آهنگ کلید تحلیلی
- آهنگ کلید تخمینی
- نتیجه‌گیری
- پیشنهاد

۴-۱- مقدمه

ایمنی همه پروتکل‌های رمزنگاری توزیع کلید کوانتومی متکی بر چندین فرض است.

فرض اول – استراق‌سمع‌کننده که معمولا آن را (ایو) می‌نامند صرف نظر از قدرتش، باید از قوانین فیزیک کوانتومی تبعیت کند.

فرض دوم - فرضی که همیشه در مبادله کلید بین دو نفر برقرار است، این است که آزمایشگاه‌های آلیس و باب ایمن هستند. یعنی هیچ اطلاعاتی از آزمایشگاه دو طرف پروتکل که آن‌ها را آلیس و باب می‌نامیم فاش نمی‌شود و در این صورت وضعیت فیزیکی آن‌ها ایمن خواهد بود. مثلا اگر آلیس در کامپیوترش در حال تایپ کردن پیغام سری به باب است به طوری که ایو بدون اطلاع آلیس در حال مشاهده کردن پیغام وی باشد، و یا اگر دستگاه فیزیکی فرستنده رشته‌های اطلاعاتی را به ایو ارسال کند، در این صورت واضح است که هیچ امنیتی وجود ندارد البته این فرض خیلی حساس است.

فرض سوم - آلیس و باب اعداد تصادفی را به صورت ایمن تولید می‌کنند و از نتایج خروجی‌شان به عنوان کلید استفاده می‌کنند، به طوری که می‌توانند پایه‌های اندازه‌گیری خود را به صورت اتفاقی و مستقل از ایو انتخاب کنند. واضح است که اگر ایو پیشاپیش پایه‌های اندازه‌گیری را بداند، احتمال یک حمله موفقیت آمیز امکان پذیر است.

فرض چهارم – که ضروری‌ترین نیاز برای تحلیل ایمنی توزیع کلید کوانتومی است، این است که آلیس و باب کنترل کامل و دقیقی روی دستگاه‌های کوانتومی خود که از آن برای توزیع همبستگی استفاده می‌شود را دارند، و دقت و ویژگی کامل دستگاه را به خوبی می‌دانند در صورتی که تنها کانال کوانتومی نقص دارد. به عنوان مثال فرض می‌کنیم که دستگاه، یک فوتونی را که با یک بیت کد شده باشد، منتشر کند و در مکانی که این بیت کد شده منتشر می‌شود، هیچ فوتون کد شده دیگری نتواند عبور کند. نقض این فرض منجر به حملات ممکن روی طرح توزیع کلید کوانتومی می‌شود. البته این

فرض اغلب نقض می‌شود، مثلا اگر آلیس و باب به جای کیوبیت‌هایشان، سیستم‌های چهار بعدی را به اشتراک بگذارند، در این صورت امنیت پروتکل BB۸۴ به طور کامل دچار خطر کشف رمز قرار می‌گیرد. اگر اجرای توزیع کوانتومی کلید این شرایط را برآورده نکند، مثلا در پروتکل توزیع کوانتومی کلید BB۸۴، اگر منبع به جای یک فوتون چندین فوتون را منتشر کند و یا دستگاه‌ها به جای اندازه‌گیری کردن در دو پایه مختلف، از یک پایه استفاده کنند، امنیت این پروتکل به طور کامل ناامن خواهد شد.

در توزیع کلید کوانتومی، آلیس و باب ذرات درهم‌تنیده‌ای که از منبع عمومی منتشر می‌شود، دریافت می‌کنند و هر کدام از این ذرات منتشر شده را در پایه‌های تصادفی اندازه‌گیری می‌کنند. اندازه‌گیری‌های خروجی کلید خام را به وجود می‌آورد.

حال منبع ذرات را به صورت مراکزی در نظر می‌گیریم که ذرات درهم‌تنیده را توزیع می‌کنند و بین دستگاه‌های ایمن آلیس و باب قرار گرفته‌اند. بنابراین این منابع ممکن است تحت کنترل ایو که همان استراق‌سمع‌کننده است، باشد که تحت این شرط دیگر ایمن نمی‌باشد. مثلا ایو می‌تواند این منبع اصلی را تغییر دهد، یعنی اطلاعاتی که آلیس و باب در مورد نتایج اندازه‌گیری خود بدست آورده‌اند، مستقیما به دست ایو برسد، سپس ایو این اطلاعات را برای باب بفرستد. در نهایت آلیس و باب با مقایسه نتایج‌شان، حالت کوانتومی‌ای که دریافت کرده‌اند را به عنوان کلید سری بکار ببرند و به این موضوع پی نبرند که این حالت‌ها را ایو برای آلیس و باب توزیع کرده است. بنابراین این کلید سری دارای ایمنی مورد دلخواه ما نخواهد بود که این مشکل به‌خاطر این است که اجراسازی QKD در زندگی واقعی متفاوت با طرح ایده‌آل است. مثلا دستگاه‌های کوانتومی ممکن است در اثر برهم‌کنش با محیط دچار نوفه شوند. لذا ایمنی این نوع پروتکل‌های QKD تضمین نمی‌شود، پس انگیزه‌ای برای معرفی پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه (DIQKD) را داریم که شکل ایمنی قویتری را ارائه می‌دهند مشروط بر آن‌که از نقض نامساوی بل استفاده شود[۱۴]. ایمنی این نوع

پروتکل‌ها مبتنی بر فرضیات کمتری است یعنی بر خلاف QKD که فرض شده بود حالت فرستاده شده برای آلیس و باب از قبل درهم‌تنیده کامل است، ولی در این نوع پروتکل‌های مستقل از دستگاه حالت فرستاده شده ممکن است درهم‌تنیده کامل نباشد، و آن حالت کوانتومی توسط ایو به آلیس و باب فرستاده شود، بدین گونه که منبع همان استراق‌سمع‌کننده (ایو) باشد. پروتکل توزیع کلید کوانتومی مستقل از دستگاه همانند طرح توزیع کلید کوانتومی که براساس قوانین فیزیک کوانتومی می‌باشد، نیز باید از قوانین فیزیک کوانتومی تبعیت کند.

با تمام این شرایط پروتکل توزیع کلید کوانتومی مستقل از دستگاه (DIQKD) متاسفانه عملا امکان پذیر نیست زیرا به آشکارسازهایی با بازده آشکارسازی نزدیک واحد و آهنگ بسیار پایین تولید کلید در فاصله‌های عملی [۱۳] نیاز دارد. پس انگیزه‌ای برای معرفی پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI-QKD) پیدا می‌کنیم که عملا امکان پذیر است که در ساده‌ترین شکل فرمول‌بندی ممکن نسبت به پروتکل توزیع کلید کوانتومی مستقل از دستگاه نیاز به این فرض دارد که آلیس و باب تقریبا حالت‌هایشان را به طور کامل آماده‌سازی می‌کنند.

۴-۲- پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری:

ما می‌خواهیم حملات کانال جانبی آشکارساز را که مسئله‌ای بسیار مهم در رمزنگاری کوانتومی است حذف کنیم. یک راه حل ساده این مسئله - پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری را پیشنهاد می‌کنیم. این پروتکل نه تنها عامل حذف تمام کانال‌های جانبی آشکارساز است بلکه فاصله ایمن را با لیزرهای معمولی نیز دو برابر می‌کند. طرح پیشنهادی ما با راندمان پایین آشکارسازی و کانال‌های با نوفه زیاد انجام می‌شود که نشان می‌دهد طرح بسیار خوبی است که با این شرایط خاص (راندمان پایین آشکارسازی و کانال‌های با نوفه زیاد) قابل اجرا است.

در اینجا می‌خواهیم یک توضیح مفید و مختصر درباره حملات کانال جانبی داشته باشیم.

حملات کانال جانبی:

آشکارسازها هرگز رفتار بی‌عیب و نقصی ندارند و به همین دلیل اطمینان کامل از آشکارسازها کاهش می‌یابد که به مفهوم این است که می‌توان آشکارسازها را فریفت تا یک رشته بیت‌های از پیش تعیین شده را بسازند که این یکی از راه‌های نفوذ نوفه (که ایو کلید دلخواه خودش را به آلیس و باب می‌دهد) در آشکارسازهاست. این گونه نفوذها با نام حمله‌های کانال جانبی شناخته می‌شوند. طرح QKD درباره عملکرد آشکارسازها فرض‌های ایده‌آل درنظر می‌گیرد که در عمل می‌بینیم آشکارسازها ایده‌آل نیستند: مثلا آشکارسازها نمی‌توانند پالس‌های تک فوتونی و چند فوتونی را از هم تشخیص دهند و همچنین لحظه‌ای پس از هر آشکارسازی، عملکردشان را از دست می‌دهند. بنابراین با در نظر گرفتن این دو ویژگی، می‌توان آشکارسازها را از اجرای عمل‌شان دور کرد تا بیت‌های مورد نظر را بسازند. تمام حملات کانال جانبی در QKD به گونه‌ای مبتنی بر فریفتن آشکارسازها در نظر گرفته شده‌اند. پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری‌ای که من مطالعه و بررسی می‌کنم به آشکارسازهایی با بازده آشکارسازی نزدیک واحد و آهنگ بسیار پایین تولیدکلید در فاصله‌های عملی نیاز ندارد. و نتایج نشان می‌دهد که رمزنگاری کوانتومی برای فاصله طولانی بیشتر از ۲۰۰ کیلومتر حتی با نقص مهم آشکارسازها ایمن باقی خواهد ماند.

توزیع کلید کوانتومی به دو طرف (نوعا آلیس و باب نامیده می‌شوند) اجازه می‌دهد تا رشته مشترک بیت‌های ایمن، که کلید ایمن نام دارد در حضور ایو تولید کنند[۱۳]. این کلید برای کارهایی مانند ارتباطات ایمن و معتبر استفاده می‌شود. متاسفانه در اینجا یک شکاف بزرگ بین تئوری توزیع کلید کوانتومی و آزمایش‌های مربوط به آن وجود دارد. در اصل، ایمنی غیر شرطی توزیع کلید کوانتومی مبتنی بر قانون‌های فیزیک تضمین می‌شود[۱۶,۱۹]. هر چند در اجرای واقعی توزیع کلید کوانتومی فرضیات ایده‌آلی در نظر گرفته شده است اما در عمل این فرضیات ایده‌آل برقرار نیستند با آشکار شدن نقص‌ها در آشکارسازها حملات متفاوتی به طور موفقیت آمیز بر ضد سیستم‌های توزیع کلید

کوانتومی تجاری[۱] [۱۷] اعمال شده است که ارتباط بین آلیس و باب را کشف کرده‌اند و از این طریق مشکلات مربوط به این توزیع کلید کوانتومی را نشان داده‌اند.

برای ارتباط تئوری و عملی توزیع کلید کوانتومی، چندین روش پیشنهاد شده است.

۱) روش اول، تشخیص دادن دستگاه‌های کاملا واقعی و در نظر گرفتن آن برای همه کانال‌های جانبی است.

۲) روش دوم، ترفند دوربری[۲] است [۱۳,۲۰].

۳) سومین راه حل، توزیع کلید کوانتومی مستقل از دستگاه است[۱۴].

روش سوم نیازی ندارد به طور دقیق بررسی شود که چگونه دستگاه‌های توزیع کلید کوانتومی کار می‌کنند بلکه ایمنی آن بر اساس نقض نامساوی بل اثبات می‌شود. متاسفانه توزیع کلید کوانتومی مستقل از دستگاه عملا امکان پذیر نیست چون به آشکارسازهایی نزدیک بازده آشکارسازی واحد و آهنگ بسیار پایین تولید کلید در فاصله‌های عملی نیاز دارد [۱۳].

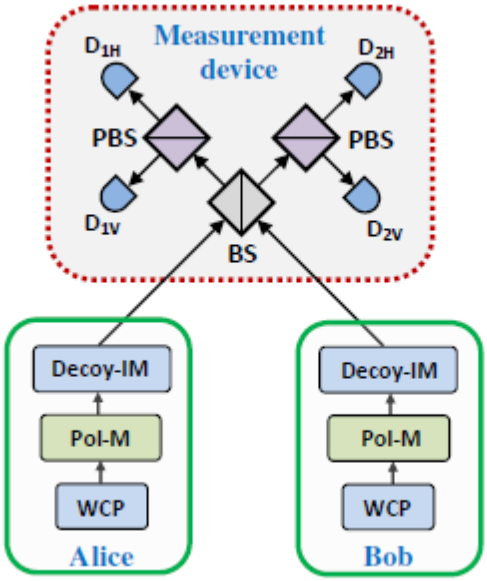
در اینجا ایده پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری را به عنوان یک راه حل ساده مطرح می‌کنیم تا تمام کانال‌های جانبی آشکارساز را [۱۳]، به طور تقریبی بحرانی‌ترین بخش اجرا، که نشان می‌دهد این پروتکل هم ایمنی و هم عملکرد بسیار خوب دارد را برطرف کنیم. علاوه بر این، پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری قدرت دو برابر کردن فاصله انتقال را دارد که با فرض‌های توزیع کلید کوانتومی که به طور قراردادی دیودهای لیزری را بکار می‌گیرد پوشش داده می‌شود. در مقایسه با توزیع کلید کوانتومی مستقل از دستگاه، در ساده‌ترین شکل فرمول بندی توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری نیاز به این فرض دارد که

---

۱. commercial

۲. teleportation trick

آلیس و باب تقریبا حالت‌هایشان را به صورت کامل آماده سازی کنند. هر چند ما معتقدیم که این فقط یک مانع جزئی است زیرا چشمه‌های سیگنال آلیس و باب که پالس‌های لیزر را کاهش می‌دهند توسط خود آلیس و باب تهیه می‌شوند. حالت‌های آلیس و باب از میان نمونه‌های تصادفی به طور تجربی در یک محیط آزمایشگاه کاملا محافظت شده از برهم‌کنش ایو بررسی می‌شوند.



شکل۴-۱- مدل سیستم توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری.

یک مثال ساده روش ما، توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI-QKD) در شکل (۴-۱) می‌باشد. آلیس و باب پالس‌های همدوس ضعیف[۱] تصادفی فاز را در چهار حالت قطبش ممکن BB۸۴ آماده می‌کنند و آن‌ها را برای ایو می‌فرستند. ایو باید یک اندازه‌گیری حالت بل انجام دهد و نتیجه اندازه‌گیری را منتشر کند برای این قبیل اندازه‌گیری‌ها در عمل ایو فقط دو حالت از چهار حالت

[۱] Weak coherent pulse (WCP)

بل را می‌تواند تشخیص دهد که این دو حالت برای اثبات ایمنی کافی است. و چون دستگاه اندازه‌گیری در پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری قبل از انتخاب درهم‌تنیدگی بین آلیس و باب بکار برده شده است. دستگاه کوانتومی می‌تواند به عنوان یک جعبه سیاه[۱] واقعی در نظر گرفته شود (خصلت این جعبه‌های سیاه این است: یک تابعی را برای ما محاسبه می‌کنند که فقط به ورودی و خروجی آن دسترسی داریم و همچنین از درون این جعبه سیاه اطلاعی نداریم) که نشان می‌دهد توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری با همه حملات در سیستم آشکارسازی ایمن است. این یک موفقیت بزرگ است به طوری که توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری به کاربران مرتبط اجازه می‌دهد نه تنها با ارسال‌های غیر قابل اعتماد ارتباطات کوانتومی ایمن [۱۶] انجام دهند همچنین تولید آشکارسازهای بدون منبع را با سازندگان غیر قابل اعتماد نیز داشته باشند.

توجه می‌کنیم که آشکارسازها اغلب تکنیکی‌ترین قطعات مورد نیاز سیستم QKD هستند، در حالی که چشمه‌ها از لیزرهای ساده که به هم فشرده‌اند ساخته شده‌اند و ارزان قیمت نیز هستند [۱۹]. بنابراین آلیس و باب حالت‌های به دام انداخته[۲] را بکار می‌گیرند [۱۵] تا بهره و آهنگ خطای بیت کوانتومی (QBER) را برای تعداد فوتون ورودی گوناگون تخمین بزنند. لازم به توضیح است که حالت‌های به دام انداخته حالت‌هایی هستند که به علت نبودن چشمه‌های کامل فوتون تنها، پالس‌های همدوس ضعیف که توسط آلیس و باب آماده می‌شوند وارد تلفیق کننده قطبش می‌شوند و تلفیق کننده قطبش حالت‌هایی تولید می‌کند که این حالت‌ها را حالت‌های به دام انداخته گویند. به محض این‌که ارتباط کوانتومی انجام شود، ایو یک کانال عمومی بکار می‌گیرد تا وقایعی که او نتیجه‌ای موفقیت آمیز از آلیس و باب بدست آورده را همراه با نتیجه اندازه‌گیری‌اش منتشر کند. آلیس و باب

---

۱. Black box or Oracle در اصطلاح کامپیوتر

۲. Decoy state method

داده‌هایی که با این نتایج مطابقت دارند را نگه می‌دارند و بقیه را دور می‌اندازند. بنابراین در BB۸۴، آلیس و باب وقایعی را انتخاب می‌کنند که در انتقال از طریق کانال عمومی از پایه یکسان استفاده شده باشد. سرانجام با اطمینان از این که رشته بیت‌هایشان به طور صحیح همبسته[۱] است، هر کدام از آلیس و باب به اجبار به جز برای حالت‌هایی که هر دو پایه قطری را انتخاب می‌کنند یک وارون بیتی بکار می‌گیرند و ایو یک نتیجه اندازه‌گیری موفقیت آمیز با یک حالت سه تایه را بدست می‌آورد (جدول(۴-۱) را ببینید).

آلیس و باب	$\|\psi\rangle^-$ خروجی رله	$\|\psi\rangle^+$ خروجی رله
پایه خطی (Z)	Bit flip	Bit flip
پایه قطری (X)	Bit flip	-

جدول ۴-۱- وارون بیتی در پایه خطی وقطری

برای سادگی اطلاعاتی که آلیس و باب به دو پایه به طور جداگانه می‌فرستند را بررسی می‌کنیم. پایه خطی (Z) برای تولید کلید بکار برده شده است در صورتی که پایه قطری (X) فقط برای آزمایش در برابر تحریف و هدف سنجیدن مقدار تقویت خصوصی لازم استفاده شده است.

۴-۳- آهنگ تولید کلید:

آهنگ تولید کلید ایمن توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری در حالت نامتقارن [۱۶]

---

۱. Correlated

به صورت زیر نوشته می‌شود:

$$R = Q_Z^{1,1}\left[1 - H_2\left(e_X^{1,1}\right)\right] - Q_Z f_e\left(E_Z\right) H_2\left(E_Z\right) \qquad (۱-۴)$$

$$Q_Z^{1,1} = P_Z^{1,1} Y_Z^{1,1}$$

که $Y_z^{1,1}$ و $e_X^{1,1}$ به ترتیب بازده در پایه خطی (Z) و آهنگ خطا در پایه قطری (X) است هنگامی که آلیس و باب هر دو حالت‌های فوتون تنها را بکار می‌گیرند ($P_Z^{1,1}$ احتمال در پایه Z)؛ H_2 تابع آنتروپی $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ است؛ Q_Z و E_Z به ترتیب بهره و آهنگ خطای بیت کوانتومی (QBER) در پایه Z و $f \geq 1$ تابع با بازدهی کم برای فرآیند تصحیح خطا است. اینجا پایه Z را برای تولید کلید و پایه X را فقط برای آزمایش استفاده می‌کنیم. در عمل Q_Z و E_Z مستقیما از آزمایش اندازه‌گیری می‌شوند، در حالی که $Y_z^{1,1}$ و $e_X^{1,1}$ با روش حالت به‌دام انداخته محدود تخمین زده می‌شوند [۱۳,۱۶].

در این بخش باید به دو نکته توجه داشته باشیم :

۱- نخست ما به طور ضمنی فرض کردیم که روش حالت به دام انداخته با تخمین بهره $Q_Z^{1,1}$ و آهنگ خطای بیت کوانتومی $e_X^{1,1}$ بکار گرفته شده است.

۲- دوم این که، ما نیاز داریم آهنگ کلید ایمن را از معادله (۴-۱) ارزیابی کنیم این نشان می‌دهد روش تخمین پارامترهای مربوط در فرمول آهنگ کلید با بکارگیری سیستم‌های QKD حالت به دام انداخته معادل است.

ایده توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری را می‌توانیم به صورت زیر تعمیم دهیم.

الف- توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری حالتی را بکار می‌گیرد که آلیس و باب از چشمه‌های جفت فوتون درهم‌تنیده استفاده می‌کنند.

ب- توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری حتی فرآیند آماده سازی ناقص آلیس و باب را بکار می‌گیرد چون چشمه‌های سیگنال آلیس و باب که پالس‌های لیزر را کاهش می‌دهند توسط خود آلیس و باب تهیه می‌شوند [۱۳].

پ- توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری حتی بدون تحلیل داده‌های تصفیه شده نیز استفاده می‌شود.

ت- توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری همچنین برای دیگر پروتکل‌های QKD (E91، BB92، ...) [۲۱] بکار گرفته می‌شود.

به طور خلاصه ما پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری را پیشنهاد می‌کنیم. این پروتکل مزیت‌هایی نظیر حذف همه کانال‌های جانبی آشکارساز را دارد و همچنین فاصله انتقالی ایمن را با استفاده از پالس‌های همدوس ضعیف با فرض‌های توزیع کلید کوانتومی دو برابر می‌کند. علاوه براین، این پروتکل آهنگ نسبتا زیاد تولید کلید دارد که این آهنگ تولید کلید اندازه مرتبه‌های بزرگتر از روش توزیع کلید کوانتومی مستقل از دستگاه است. پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری با آشکارسازهای آستانه که راندمان پایین آشکارسازی دارند و کانال‌های با نوفه زیاد قابل اجراست. نظر به ایمنی بسیار خوب، اجرا و پیاده سازی پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری ما معتقد هستیم که این پروتکل یک گام بلند رو به جلو برای اتصال تئوری توزیع کلید کوانتومی و آزمایش‌های مربوط به آن است. و ما انتظار داریم سیستم‌های توزیع کلید کوانتومی را در آینده بکار ببریم.

۴-۴- روش تخمین:

روش حالت به دام انداخته کاربردی را برای توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI-QKD) مطرح می‌کنیم که به آلیس و باب اجازه می‌دهد تا پارامترهای مربوط را با ارزیابی

فرمول کلید ایمن در سیستم نامتقارن تخمین بزنند. و بهره در پایه خطی $Q_Z^{1,1}$ و آهنگ خطای بیت کوانتومی در پایه قطری $e_X^{1,1}$ را بدست آورند. و همچنین بازده Y_n و آهنگ خطا e_n را برای n فوتون سیگنال [۱۵] تخمین بزنند.

مجموعه معادلات خطی:

$$Q^i = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y_n \qquad (۲-۴)$$

$$Q^i E^i = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y_n e_n \qquad (۳-۴)$$

که Q^i بهره زمینه به دام انداخته مختلف است که توسط آلیس استفاده شده است.

معادلات خطی در پروتکل MDI-QKD را به صورت زیر دنبال می‌کنیم:

$$Q_Z^{i,j} = \sum_{n,m=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} e^{-\mu_j} \frac{\mu_j^n}{m!} Y_Z^{n,m} \qquad (۴-۴)$$

$$Q_X^{i,j} = \sum_{n,m=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} e^{-\mu_j} \frac{\mu_j^n}{m!} Y_X^{n,m} \qquad (۵-۴)$$

که $Q_Z^{i,j}$ $\left(Q_X^{i,j}\right)$ بهره زمینه‌های به دام انداخته مختلف در پایه خطی (پایه قطری) است که توسط آلیس و باب استفاده شده است.

$$Q_Z^{i,j} E_Z^{i,j} = \sum_{n,m=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} e^{-\mu_j} \frac{\mu_j^n}{m!} Y_Z^{n,m} e_Z^{n,m}$$

$$Q_X^{i,j} E_X^{i,j} = \sum_{n,m=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} e^{-\mu_j} \frac{\mu_j^n}{m!} Y_X^{n,m} e_X^{n,m}$$

اندیس‌های i و j به ترتیب زمینه‌های به دام انداخته مختلف را نمایش می‌دهند که به وسیله آلیس و باب استفاده شده است.

n و m تعداد فوتونی است که توسط آلیس و باب استفاده شده است.

ابتدا از کمیت ${Q_Z}^{i,j}$ شروع می‌کنیم:

$${Q_Z}^{i,j} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{{\mu_i}^n}{n!} {Y_{n;Z,}}^{j} \qquad (۶-۴)$$

که

$${Y_{n;Z}}^{j} = \sum_{m=0}^{\infty} e^{-\mu_j} \frac{{\mu_j}^m}{m!} {Y_Z}^{n,m} \qquad (۷-۴)$$

برای j ثابت و i متغیر معادله (۴-۶) با معادله (۴-۲) معادل است که به این معنی است که آلیس و باب می‌توانند پارامترهای ${Y_{n;Z}}^{j}$ را بزنند. این معادله با (۴-۷) نشان داده شده که با معادله (۴-۲) معادل است و کاربرهای مرتبط می‌توانند پارامترهای ${Y_Z}^{n,m}$ و به طور مشابه ${Y_X}^{n,m}$ را تخمین بزنند. حالا روی ${E_Z}^{i,j}$ آهنگ خطای بیت کوانتومی تمرکز می‌کنیم که عبارت است از:

$${Q_Z}^{i,j}{E_Z}^{i,j} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{{\mu_i}^n}{n!} {W_{n,Z}}^{j} \qquad (۸-۴)$$

که

$${W_{n,Z}}^{j} = \sum_{m=0}^{\infty} e^{-\mu_j} \frac{{\mu_j}^n}{m!} {Y_Z}^{n,m} {e_Z}^{n,m} \qquad (۹-۴)$$

برای j ثابت و i متغیر معادله (۴-۸) را داریم که با معادله (۴-۲) معادل است بنابراین آلیس و باب می‌توانند پارامترهای ${W_{n,Z}}^{j}$ را تخمین بزنند که در معادله (۴-۹) نشان داده‌ایم که با معادله (۴-۳) با بازده ${Y_Z}^{n,m}$ که از قبل می‌دانیم معادل است. این بدان معنی است که آلیس و باب می‌توانند ${e_Z}^{n,m}$ و همچنین به طور مشابه ${e_X}^{n,m}$ را تخمین بزنند. ما نشان دادیم که آلیس و باب می‌توانند پارامترهای ${Y_Z}^{n,m}$، ${Y_X}^{n,m}$، ${e_Z}^{n,m}$ و ${e_X}^{n,m}$ را برای کل n و m در حالت‌های نامتقارن تخمین بزنند و همچنین کمیت‌های مناسب ${Y_Z}^{1,1}$ و ${e_X}^{1,1}$ را بدست آورند. بهره ${Q_Z}^{1,1}$ به صورت معادله (۴-۱۰)

$Q_Z^{1,1} = \mu_a \mu_b e^{-(\mu_a+\mu_b)} Y_z^{1,1}$ بدست می‌آید که μ_a و μ_b به ترتیب تعداد فوتون سیگنال آلیس و باب را نشان می‌دهد [۲۴،۲۵].

۴-۵- آهنگ تولید کلید تحلیلی:

در این بخش یک روش تحلیلی را با مدل کد گذاری قطبش سیستم توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI-QKD) مورد بحث قرار می‌دهیم و پارامترهای $Y_z^{1,1}$، $e_X^{1,1}$، Q_Z و E_Z را بدست می‌آوریم و سپس آهنگ کلید چشمداشتی را از معادله (۴-۱) تخمین می‌زنیم.

۱. محاسبه $Y_z^{1,1}, e_X^{1,1}$:

$Y_z^{1,1}$ و $e_X^{1,1}$ در معادله (۴-۱) به صورت زیر تخمین زده شده‌اند.

$$e_X^{1,1} = \frac{1}{2} - \frac{t_a t_b \eta_d^2 (1-e_d)^2 (1-Y_0)^2}{4 Y_X^{1,1}}$$

$$Y_Z^{1,1} = (1-Y_0)^2 \left[4Y_0^2 (1-t_a\eta_d)(1-t_b\eta_d) + 2Y_0 (t_a\eta_d + t_b\eta_d - 3t_a t_b \eta_d^2) + t_a t_b \eta_d^2 / 2 \right] \quad (۱۱-۴)$$

که $Y_X^{1,1} = Y_Z^{1,1}$ و $t_a (t_b)$ انتقال پذیری[۱] کانال آلیس (باب) را نشان می‌دهد. با چشم پوشی از نقص‌های سیستم از قبیل تغییر جهت قطبش و شمارش‌های زمینه[۲] $(e_d = 0, Y_0 = 0)$ $e_X^{1,1}$ صفر است در حالی‌که $\left(P_z^{1,1} = \mu_a \mu_b e^{-(\mu_a+\mu_b)}\right)$ $Q_Z^{1,1} = P_Z^{1,1} Y_Z^{1,1} \left(P_Z^{1,1} = \mu_a \mu_b e^{-(\mu_a+\mu_b)}\right)$ با $\mu_a = \mu_b$ بیشینه می‌شود.

۲. محاسبه Q_Z, E_Z:

قطبش‌های {افقی، عمودی، ۴۵درجه و ۱۳۵درجه} را استفاده می‌کنیم تا حالت‌های قطبش BB۸۴ را نمایش دهیم. همچنین $\{HH, HV, ++, +-\}$ روش‌های کدگذاری آلیس و باب را نشان می‌کند.

حال پارامترهای زیر را تعریف می‌کنیم

$$\gamma_a = \sqrt{\mu_a t_a \eta_a} \qquad \gamma_b = \sqrt{\mu_b t_b \eta_b} \qquad \beta = \gamma_a \gamma_b$$

$$\lambda = {\gamma_a}^2 + {\gamma_b}^2 \qquad \lambda = \gamma_a \gamma_b \sqrt{e_K (1-e_d)} \qquad \omega = {\gamma_a}^2 + e_d \left({\gamma_b}^2 - {\gamma_a}^2\right)$$

الف. محاسبه Q_Z^{HH}:

نخست آلیس و باب حالت‌هایشان را با H (حالت قطبش افقی) (متقارن با V(حالت قطبش عمودی)) کدگذاری می‌کنند. فرض می‌کنیم چرخش قطبش به گونه‌ای باشد که $\theta_1\theta_2\rangle 0$ باشد.

شدت‌های نوری در آزمایشگاه ایو بعد از عبور از جدا کننده باریکه[۳] وارد جدا کننده باریکه قطبش[۴] می‌شوند سپس بوسیله هرکدام از آشکارساز فوتون تنها[۵] دریافت شده‌اند که داریم:

$$D_{2H} : |A|^2 = \frac{(1-e_d)\left({\gamma_a}^2 + {\gamma_b}^2\right) - 2\gamma_a\gamma_b \cos(\phi)(1-e_d)}{2}$$

$$D_{1H} : |C|^2 = \frac{(1-e_d)\left({\gamma_a}^2 + {\gamma_b}^2\right) + 2\gamma_a\gamma_b \cos(\phi)(1-e_d)}{2}$$

$$D_{2V} : |B|^2 = \frac{e_d\left({\gamma_a}^2 + {\gamma_b}^2\right) - 2\gamma_a\gamma_b \cos(\phi)e_d}{2}$$

$$D_{1V} : |D|^2 = \frac{e_d\left({\gamma_a}^2 + {\gamma_b}^2\right) + 2\gamma_a\gamma_b \cos(\phi)e_d}{2} \qquad (۱۲-۴)$$

---

۱. Channel transmittance

۲. background counts

۳. beam splitter (BS)

۴. polarization beam splitter (PBS)

۵. single – photon detector (SPD)

که ϕ فاز نسبی بین حالت‌های همدوس ضعیف آلیس و باب را مشخص می‌کند. بنابراین احتمال آشکارسازی عبارت است از:

$$P_V = 1-(1-Y_0)e^{-|V|^2}$$

$$V = A, B, C, D \qquad (۱۳-۴)$$

سپس شمارش‌های منطبق[۱] برهم را به صورت زیر داریم:

$$Q_Z^{HH,\psi^+} = 2P_A P_B (1-P_c)(1-P_D)$$

$$Q_Z^{HH,\psi^-} = 2P_A P_B (1-P_B)(1-P_c)$$

که Q_Z^{HH,ψ^+} و Q_Z^{HH,ψ^-} به ترتیب احتمال تصویر در حالت سه تایه $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|H,V\rangle + |V,H\rangle)$ و در حالت تک تایه $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H,V\rangle - |V,H\rangle)$ را مشخص می‌کنند.

از شکل (۴-۱)، سه تایه یعنی این‌که، آشکارسازی‌های منطبق برهم $\{D_{2H} \,\&\, D_{2V}\}$ یا $\{D_{1H} \,\&\, D_{1V}\}$ است و حالت تک تایه، آشکارسازی‌های منطبق برهم $\{D_{2H} \,\&\, D_{1V}\}$ یا $\{D_{2V} \,\&\, D_{1H}\}$ است.

بعد از متوسط‌گیری فازنسبی ϕ (انتگرال‌گیری در محدوده $[0, 2\pi]$) داریم:

$$Q_Z^{HH,\psi^+} = 2e^{-\frac{\gamma}{2}}(1-Y_0)^2\left[I_0(\beta) + (1-Y_0)^2 e^{-\frac{\gamma}{2}} - (1-Y_0)e^{-\frac{\gamma(1-e_d)}{2}} I_0(e_d\beta) - (1-Y_0)e^{-\frac{\gamma e_d}{2}} I_0(\beta - e_d\beta)\right]$$

$$Q_Z^{HH,\psi^-} = 2e^{-\frac{\gamma}{2}}(1-Y_0)^2\left[I_0(\beta - 2\beta e_d) + (1-Y_0)^2 e^{-\frac{\gamma}{2}} - (1-Y_0)e^{-\frac{\gamma(1-e_d)}{2}} I_0(e_d\beta) - (1-Y_0)e^{-\frac{\gamma e_d}{2}} I_0(\beta - e_d\beta)\right]$$

(۱۴-۴)

۱. Coincident counts

که $I_0(.)$ تابع بسل اصلاح شده است. بنابراین به صورت زیر داریم:

$$Q_Z^{HH} = Q_z^{HH,\psi^+} + Q_Z^{HH,\psi^-} \qquad (۱۵-۴)$$

با ساده سازی معادله (۴-۱۴) و چشم پوشی از شمارش‌های زمینه یعنی $Y_0 = 0$ (به طوری که β,γ هر دو برحسب 0.01 هستند) به طوری که

$$I_0(\beta) = 1 + \frac{\beta^2}{4} + \mathrm{O}(\beta^4)$$

$$e^{\gamma} = 1 + \gamma + \frac{\gamma^2}{2} + \mathrm{O}(\gamma^3)$$

سپس معادله (۴-۱۴) را به صورت زیر بدست می‌آوریم:

$$Q_z^{HH,\psi^+} = \frac{\gamma^2 e_d(1-e_d)}{2} + \beta^2 e_d(1-e_d)$$

$$Q_z^{HH,\psi^-} = \frac{\gamma^2 e_d(1-e_d)}{2} - \beta^2 e_d(1-e_d) \qquad (۱۶-۴)$$

و در انتها خواهیم داشت:

$$Q_z^{HH} = Q_z^{HH,\psi^+} + Q_z^{HH,\psi^-} = \gamma^2 e_d(1-e_d)$$

ب. محاسبه Q_z^{HV} :

آلیس (باب) حالتش را با مد $H(V)$ کدگذاری می‌کند (متقارن با $V(H)$). شدت‌های نوری دریافت شده از آزمایشگاه ایو عبارتند از:

$$|A'|^2 = \frac{(1-e_d)\gamma_a{}^2 + e_d\gamma_b{}^2 - 2\lambda\cos(\phi)}{2}$$

$$|B'|^2 = \frac{e_d\gamma_a{}^2 + (1-e_d)\gamma_b{}^2 - 2\lambda\cos(\phi)}{2}$$

$$\left|C'\right|^2 = \frac{\left(1-e_d\right)\gamma_a{}^2 + e_d\gamma_b{}^2 + 2\lambda\cos\left(\phi\right)}{2}$$

$$\left|D'\right|^2 = \frac{e_d\gamma_a{}^2 + \left(1-e_d\right)\gamma_b{}^2 + 2\lambda\cos\left(\phi\right)}{2}$$

Q_z^{HV,ψ^+} و Q_z^{HV,ψ^-} مشابه معادله (۴-۱۴) محاسبه می‌شود. بعد از متوسط‌گیری نتایج به صورت زیر بدست خواهد آمد.

$$Q_Z^{HH,\psi^+} = 2e^{-\frac{\gamma}{2}}\left(1-Y_0\right)^2\left[I_0\left(2\lambda\right)+\left(1-Y_0\right)^2 e^{-\frac{\gamma}{2}} - \left(1-Y_0\right)e^{-\frac{\omega}{2}}I_0\left(\lambda\right) - \left(1-Y_0\right)e^{-\frac{\gamma-\omega}{2}}I_0\left(\lambda\right)\right]$$

$$Q_Z^{HH,\psi^-} = 2e^{-\frac{\gamma}{2}}\left(1-Y_0\right)^2\left[1+\left(1-Y_0\right)^2 e^{-\frac{\gamma}{2}} - \left(1-Y_0\right)e^{-\frac{\omega}{2}}I_0\left(\lambda\right) - \left(1-Y_0\right)e^{-\frac{\gamma-\omega}{2}}I_0\left(\lambda\right)\right]$$

(۴-۱۷)

بنابراین Q_Z^{HV} را به صورت زیر داریم:

$$Q_z^{HV} = Q_z^{HH,\psi^+} + Q_z^{HH,\psi^-} \qquad (۴-۱۸)$$

با ساده‌سازی معادله (۴-۱۷) و چشم پوشی از شمارش‌های زمینه داریم:

$$Q_z^{HV,\psi^+} = \frac{\omega\left(\gamma-\omega\right)}{2} + \lambda^2$$

$$Q_z^{HV,\psi^-} = \frac{\omega\left(\gamma-\omega\right)}{2} - \lambda^2 \qquad (۴-۱۹)$$

که در انتها Q_Z^{HV} داریم:

$$Q_z^{HV} = Q_z^{HH,\psi^+} + Q_z^{HH,\psi^-} = \omega\left(\gamma-\omega\right)$$

پ. محاسبه Q_Z, E_Z :

و سرانجام Q_Z, E_Z به صورت زیر بیان می‌شوند:

$$Q_z = \frac{Q_z^{HH} + Q_z^{HV}}{2}$$

$$E_z = \frac{Q_z^{HH}}{Q_z^{HH} + Q_z^{HV}} \qquad (۲۰-۴)$$

با استفاده از معادله‌های (۴-۱۸,۱۷,۱۵,۱۴) همرا با معادله (۴-۱۱) ما می‌توانیم آهنگ تولید کلید تحلیلی معادله (۴-۱) را بدست آوردیم.

با چشم پوشی از شمارش‌های زمینه معادله‌های (۴-۱۹,۱۶)، Q_Z و E_Z را به صورت زیر بدست می‌آوریم:

$$Q_z = \frac{\beta^2 + e_d\left(1 - \frac{e_d}{2}\right)\left(\gamma^2 - 2\beta^2\right)}{2}$$

$$E_z = \frac{\gamma^2 e_d\left(1 - \frac{e_d}{2}\right)}{4Q_z} \qquad (۲۱-۴)$$

ت. محاسبه Q_Z و E_Z با زاویه قطبش مخالف :

فرض می‌کنیم چرخش قطبش به گونه‌ای باشد که $\theta_1\theta_2 \langle 0$ باشد آنگاه معادله (۴-۱۲) به صورت زیر تغییر می‌کند.

$$|A|^2 = \frac{(1-e_d)\left(\gamma_a{}^2 + \gamma_b{}^2\right) - 2\gamma_a\gamma_b\cos(\phi)(1-e_d)}{2}$$

$$|B|^2 = \frac{e_d\left(\gamma_a{}^2 + \gamma_b{}^2\right) + 2\gamma_a\gamma_b\cos(\phi)e_d}{2}$$

$$|C|^2 = \frac{(1-e_d)\left(\gamma_a{}^2 + \gamma_b{}^2\right) + 2\gamma_a\gamma_b\cos(\phi)(1-e_d)}{2}$$

$$|D|^2 = \frac{e_d\left(\gamma_a{}^2 + \gamma_b{}^2\right) - 2\gamma_a\gamma_b\cos(\phi)e_d}{2}$$

بعد از انجام روش‌های مشابه از بخش(۴-۵) - ب معادله (۴-۱۶) به صورت زیر تغییر می‌یابد:

$$Q_z^{HH,\psi^+} = \frac{\gamma^2 e_d(1-e_d)}{2} - \beta^2 e_d(1-e_d)$$

$$Q_z^{HH,\psi^-} = \frac{\gamma^2 e_d(1-e_d)}{2} + \beta^2 e_d(1-e_d) \qquad (۲۲-۴)$$

چون آهنگ خطای بیت کوانتومی (QBER) بوسیله Q_Z^{HH} مشخص شده است از مقایسه معادله (۴-۱۶) با (۴-۲۲) نتیجه این‌که:

$0\rangle\theta_1\theta_2$: تصویر روی $\left|\psi^+\right\rangle$ در یک آهنگ خطای بیت کوانتومی بزرگتر از تصویر روی $\left|\psi^-\right\rangle$ را نتیجه می‌دهد.

$0\rangle\theta_1\theta_2$: تصویر روی $\left|\psi^+\right\rangle$ در یک آهنگ خطای بیت کوانتومی کمتر از تصویر روی $\left|\psi^-\right\rangle$ را نتیجه می‌دهد.

سپس Q_Z^{HV} با یک تحلیل مشابه و با توجه به بخش (۴-۵) - ب و معادله (۴-۱۹) به صورت زیر تغییر می‌یابد.

$$Q_z^{HV,\psi^+} = \frac{\omega(\gamma-\omega)}{2} - \lambda^2$$

$$Q_z^{HV,\psi^-} = \frac{\omega(\gamma-\omega)}{2} + \lambda^2 \qquad (۲۳-۴)$$

بنابراین آهنگ‌های کلید R^{ψ^-} و R^{ψ^+} به جهت نسبی زوایای چرخش بستگی دارند در حالی که آهنگ کلید کل R $\left(R = R^{\psi^-} + R^{\psi^+}\right)$ مستقل از جهت نسبی زوایای چرخش است.

ملاحظه می‌کنیم که در یک کدگذاری قطبش عملی سیستم توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری زاویه چرخش قطبش مربوط به هر کدام از کانال کوانتومی (θ_2 یا θ_1) را می‌توان با یک توزیع گاوسی با یک ریشه استاندارد $\theta_K^{std} = ark\sin\left(\sqrt{e_K}\right)(K=1,2)$ مدل سازی کرد که به این معنی است که هم θ_1 و هم θ_2 (اساسا) در یک زاویه $\left[-3\theta_K^{std}, 3\theta_K^{std}\right]$ توزیع شده‌اند و جهت نسبی بین آن‌ها همچنین به صورت تصادفی بین $0\rangle\theta_1\theta_2$ و $\theta_1\theta_2\langle 0$ توزیع می‌شود. بنابراین اثر تغییر جهت قطبش برای R^{ψ^-} و R^{ψ^+} یکسان است یعنی این که هم R^{ψ^-} و هم R^{ψ^+} مستقل از تغییر جهت قطبش کل هستند که ما می‌توانیم به طور تجربی اندازه‌گیری حالت تک تایه یا حالت سه تایه را فقط با دو آشکارساز [۲۲,۲۳] انتخاب کنیم.

۴-۶- آهنگ تولید کلید تخمینی R_{est}:

آهنگ تولید کلید تخمینی R_{est} تحت شرایطی که شمارش‌های زمینه چشم پوشی شود تعریف می‌شود که برای فاصله انتقالی کوتاه یک فرض معقولی است.

با چشم پوشی از Y_0، $e_X^{1,1}$ و $Q_Z^{1,1} = P^{1,1}Y^{1,1}$ (معادله (۴-۱۱) را ببینید) به صورت زیر داریم:

$$e_X^{1,1} = e_d - \frac{e_d^2}{2}$$

$$P^{1,1}Y^{1,1} = \frac{\mu_a t_a \mu_b t_b e^{-(\mu_a+\mu_b)}\eta_d^2}{2}$$

Q_Z و E_Z نیز به صورت زیر بدست می‌آیند (معادله (۴-۲۱) را ببینید):

$$Q_Z = \frac{t_a^2\eta_d^2\left[2x\mu_a\mu_b + \left(\mu_b^2 + x^2\mu_a^2\right)\left(2e_d - e_d^2\right)\right]}{4}$$

$$E_Z = \frac{\left(\mu_b + x\mu_a\right)^2\left(2e_d - e_d^2\right)}{2\left[2x\mu_a\mu_b + \left(\mu_b^2 + x^2\mu_a^2\right)\left(2e_d - e_d^2\right)\right]}$$

و با ترکیب دو معادله بالا با معادله (۴-۱) داریم:

$$R_{est} = \frac{t_b^2 \eta_d^2}{2} x \mu_a \mu_b e^{-(\mu_a+\mu_b)} \left[1 - H_2\left(e_d - \frac{e_d^2}{2}\right)\right] - \frac{2x\mu_a\mu_b + \left(\mu_a^2 + x^2\mu_b^2\right)\left(2e_d - e_d^2\right)}{2} f_e H_2\left(E_Z\right)$$

R_{est} آهنگ کلید تخمین زده شده یا آهنگ کلید کل است.

۴-۷- نتیجه‌گیری

در پروتکل رایج و متداول توزیع کلید کوانتومی (QKD)، فرض شده است که پایه‌های آلیس و باب ایمن هستند. اما دستگاه‌های کوانتومی در پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری (MDI-QKD)، قابل اطمینان نیستند. یک فرض کلیدی در پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری [۱۶] این است که آلیس و باب به دستگاه‌های تولید حالت‌هایشان اعتماد می‌کنند یعنی این‌که آن‌ها حالت‌های کوانتومی ایده‌آل خود را مشابه پروتکل BB۸۴ تولید می‌کنند. یک روش حذف این فرض تعیین کردن نقص‌ها در قسمت آماده سازی حالت است و ما معتقد هستیم که این فرض عملی است زیرا آلیس و باب خودشان حالت‌های کوانتومی‌شان را آماده می‌کنند. بنابراین حالت‌های کوانتومی آلیس و باب می‌توانند به صورت تجربی در یک محیط آزمایشگاه کاملا محافظت شده از برهم‌کنش ایو تحقق یابند. در این نوع پروتکل‌ها آلیس و باب فقط به آشکارسازهایشان که اعداد تصادفی را بوجود می‌آورند، اطمینان دارند، یعنی این‌که ایو به همه اطلاعات دسترسی دارد، تنها چیزی که از آن اطلاع ندارد فقط ارتباط بین ورودی‌ها و خروجی‌های دستگاه‌های آلیس و باب است.

یک طرح جالب دیگر [۱۳] که مطرح شده این است که آلیس و باب هر کدام از چشمه فوتون درهم‌تنیده (به جای پالس‌های همدوس ضعیف) استفاده می‌کنند و نقص‌های آماده سازی حالت را از طریق نمونه تصادفی مشخص می‌کنند. و یک آزمون بل موضعی در این نمونه‌ها انجام می‌دهند. یک چنین طرحی در فاصله‌های عملی نوید بخش یک روش مستقل از دستگاه است. بنابراین برای این‌که یک چنین طرحی را بدون این‌که محدودیتی برای فاصله در نظر بگیریم، عملی کنیم پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری را مطرح می‌کنیم که این پروتکل نه تنها عامل حذف تمام کانال‌های جانبی آشکارساز است بلکه فاصله ایمن را با لیزرهای معمولی نیز دو برابر می‌کند. و با راندمان پایین آشکارسازی و کانال‌های نوفه‌دار انجام می‌شود که نشان می‌دهد در شرایط خاص نیز

عملا امکان‌پذیر است.

هدف پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری، بوجود آوردن کلید سری بین دو کاربر مرتبط است. ایمنی این پروتکل به احتمال اندازه‌گیری‌ها بستگی ندارد (احتمال این‌که آلیس چه اندازه‌گیری‌ای انجام دهد و باب چه نتایجی را بوجود آورد، به یکدیگر وابسته نیست). آلیس و باب از پایه‌های اندازه‌گیری تصادفی استفاده می‌کنند و نتایجی را بوجود می‌آورند که برای استراق‌سمع‌کننده نامشخص خواهد بود. این نتایج اندازه‌گیری کلید خام را تشکیل می‌دهند.

۴-۸- پیشنهاد

کم کردن فرضیات کوانتومی برای ایمنی توزیع کلید کوانتومی مسئله‌ای است که توجه فیزیک دانان را به خود جلب کرده است و با توجه به حداقل رساندن فرضیات، ایمنی نرخ کلید را بیشتر و بیشتر افزایش خواهند داد. بنابراین می‌توان پروتکل توزیع کلید کوانتومی مستقل از دستگاه را تعمیم داد و نتایج معقولی را بدست آورد که این ایده منجر به ایمنی بیشتر خواهد شد.

ولی متاسفانه این پروتکل عملا امکان‌پذیر نیست زیرا به آشکارسازهایی نزدیک بازده آشکارسازی واحد (برای کاهش خطا در آزمایش) و آهنگ بسیار پایین تولید کلید در فاصله‌های عملی نیاز دارد [۱۳]. بنابراین ما پروتکل توزیع کلید کوانتومی مستقل از دستگاه اندازه‌گیری را پیشنهاد می‌کنیم که نه تنها شرط فاصله در این پروتکل مهم نیست بلکه این پروتکل فاصله ایمن را با لیزرهای معمولی نیز دو برابر می‌کند. و به آشکارسازهایی نزدیک بازده آشکارسازی واحد و آهنگ بسیار پایین تولید کلید در فاصله‌های عملی نیاز ندارد.

مراجع :

[1] H.Lo, M.Curty, H.F.Chau, M.Arehali. **(2006)** "Efficient quantum key distribution scheme and Proof of its unconditional security".

[2] A.Maitra. **(2012)** "Third-Party CNOT Attack on MDI-QKD" arxiv:**1208.5223v2** *[quant-ph]*.

[3] H.K. Lo, M.Curty, B.Qi. **(2012)**. Physical Review Letters, **108**, **130503**.

[4] M. Zukowski, A. Zeilinger, M. A. Horne, A. K. Ekert. Physical Review Letters, **71**, **4287–4290 (1993)**.

[5] Ashok Chatterjee, Theory Group, Saha Institute of Nuclear physics. **(2003)** "Introduction To Quantum Computation".

[6] M.A.Nielsen & I.L.Chuang. **(2000)** "Quantum Computation And Quantum Information" chapter **10**, **425-493**.

[7] E.Biham, M.Boyer, P.Oscar Boykin, T.Mor, V.Roychowdhury. **(1999)** "A proof of the security of quantum key distribution".

[8] A.R.Calderbank, P.W.Shor, M.Hill. **(1995)** "Good uantum error-correcting codes exist" *[Submitted September **12**]*.

[9] H.Inamori, N.Lutkenhaus, D.Mayers. **(2004)** "Unconditional security of practical quantum key distribution".

[10] C.H.Bennett, D.Divincenzo, W.K.Wootters. **(1996)** "Mixed state entanglement and quantum error correction".

[11] D.McMahon. **(2008)** "Quantum Computing Explained" chapter **1-11**, **1-249**.

[12] D.Gottesman, H.Lo, N.Lutkenhaus. **(2004)** "Security of Quantum Key Distribution with imperfect devices" Quant.Inf.Comput. **5**, **325-360**.

[13] H.Lo, M.Curty, B.Qi. **(2012)** "Measurement device independent quantum key distribution" Phys. Rev. Lett. **108**, **130503**.

[14] S.Pironio, A.Acin, N.Brunner, N.Gisin, S.Massar, V.Scarani. **(2009)** "Device-independent quantum key distribution secure against collective attacks" New J. Phys. **11**, **045021**.

[15] W.Hwang. Phys. Rev. Lett. **91**, **057901 (2003)**; H. Lo, X. Ma. Phys. Rev. Lett. **94**, **230504 (2005)**.

[16] F.Xu, M.Curty, B.Qi, H.Lo. **(2013)** "Practical Measurement-Device-Independent Quantum Key Distribution" Physical Review A **87**, **052329**.

[17] C. H.Fung. **(2007)**. Phys. Rev. A **75**, **032314**; F.Xu, B. Qi, H.Lo. **(2010)**. Phys. **12**, **113026**.

[18] S.Barnett. **(2009)** "Quantum Information" chapter **3**, **59-83**.

[19] F.Xu, B.Qi, Z.L, H.Lo. **(2013)** "Long distance measurement-device-independent quantum key distribution with entangled photon sources" Appl. Phys. Lett. **103**, **061101**.

[20] H.Lo, H. F. Chau. **(1999)**. Science **283**, **2050**. arxiv:**0704.3253v3** *[quant-ph]*.

[21] C. H. Bennett et al., IBM Technical Disclosure Bulletin **26**, **4363 (1984)**; D. Bruß, Phys. Rev. Lett. **81**, **3018 (1998).**

[22] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, arXiv preprint arXiv:**1304.2463 (2013)**.

[23] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.Lo, under preparation **(2013)**.

[24] X. Ma et al., Phys. Rev. A **72**, **012326 (2005)**; X.B.Wang, Phys. Rev. A **72**, **012322 (2005)**.

[25] Y. Zhao, B.Qi, X. Ma, H. Lo, L. Qian, Phys. Rev. Lett. **96**, **070502 (2006)**.

Abstract

One of the most important problems in quantum information that we faced, is information transfer secured perfectly. Therefore we introduce the protocol in which, like all Quantum Key Distribution protocols (QKD), the security relies on the laws of quantum physics and another thing is that no-information leakage from the legal parties labs. This scheme is named quantum key distribution protocol which is Device-Independent (DIQKD). The security proof is based on the minimal assumption rather than quantum distribution schemes, it means that two parties would not only have no knowledge about the structure of their quantum devices but they would also distrust their measuring apparatuses or we don't assume that Alice and Bob's devices behave according to predetermined specifications, because the measuring devices may be modified by eavesdropper (Eve). If the security of this kind of Device- Independent protocols comparable to those of standard schemes is more secure, if it is based on the observation of a Bell inequality violation. Unfortunately, DIQKD is highly impractical because it needs near unity detection efficiency, and generates an extremely low key rate at practical distances [10]. In contrast to the device independent QKD protocol, measurement device independent quantum distribution does not require detectors of near unity detection efficiency, and generates an extremely low key rate at practical distances. The aim of this protocol that we consider here, is distributing a secret key whose security relies on the laws of quantum physics, so in this scheme we make this assumption that bits of key sequence are mutually independent and have no interaction with each other, one could also defines space-like separated events and in consequence we use this, to generate the secret key rate.

Key Words: Quantum key distribution (QKD), Measurement device independent quantum key distribution (MDI-QKD), BB84, CNOT Attack, Secret key rate

Shahrood University of Technology

Faculty of physics

Master of Science Thesis

Measurement device independent quantum key distribution

Shokoofeh farzi Yeknami

Supervisor:

Dr. H. Movahhdian

February – 2014