
بسم الله الرحمن الرحيم

دانشکده : فیزیک

گروه :فیزیک

اثر وابستگی به زمینه در ایمنی توزیع کلید کوانتومی

دانشجو :

فاطمه محمدی پلارتی

استاد راهنما :

دکتر حسین موحدیان

شهریور ۱۳۹۰

تقدیم به:

پدر مهربان و مادر دلسوزم، که در تعلیم و تربیت من فداکارانـه از هـیچ کوشـشی دریـغ نکردند و در هر مرحله از زندگی مرا حمایت کردند. به پـاس ایـن زحمـات پایـان‌نامـه‌ی حاضر را به آنان تقدیم می‌کنم.

تشکر و قدردانی:

با نام خالق هستی راهی را آغاز نمودم که پیمودنش آسان نبود جز با نام و یاد او، و اکنون که به پایان راه رسیده‌ام سر به سجده‌ی شکر او فرو می‌برم.

در اینجا وظیفه‌ی خود می‌دانم استاد راهنمای گرامی خویش، جناب دکتر حسین موحدیان را سپاس گویم چرا که ایشان با راهنمایی‌هایشان، در تمام مراحل کار مرا یاری کردند و سپس از تمام کسانی که در این پایان‌نامه به گونه‌ای راهگشای من بودند، کمال تشکر و قدردانی را دارم.

تعهد نامه

اینجانب **فاطمه محمدی پلارتی** دانشجوی دوره کارشناسی ارشـد **رشته و گرایش تحصیلی : فیزیک – ذرات بنیادی** دانشکده **فیزیک** دانشگاه صنعتی شاهرود نویسنده پایان نامه **اثر وابستگی به زمینه در ایمنی توزیع کلیـد کوانتـومی** تحت راهنمائی دکتر حسین موحدیان‌متعهد می شوم .

- 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 ارائـه 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 .

امضای دانشجو

تاریخ

چکیده

امروزه ارسال اطلاعات میان فرستنده و گیرنده به روش مکانیک کوانتومی کانون توجه دانشمندان و محققان است. در این مسیر، تلاش برای امنیت هرچه بیشتر اطلاعات بسیار حائز اهمیت است. اولین پروتکل مشهور به **BB84** بر پایه‌ی اندازه‌گیری مشاهده‌پذیرهای کوانتومی پادجابه‌جاپذیر (از ویژگی-های بنیادی فیزیک کوانتومی) بنا شده است. در این پایان نامه، با بکارگیری یکی از ویژگی‌های جهان کوانتومی به نام وابستگی به زمینه که در متناقض نمای کوشن-اسپکر متبلور شده است، امنیت سیستم افزایش می‌یابد. حتی اگر دستگاههایی که تولید آمار می‌کنند مطمئن نباشند. این متناقض-نما، شامل توزیع‌های احتمال دوتایی است که به طور موضعی شرایط متناقض نمای کوشن-اسپکر را نشان می‌دهند و علاوه بر آن، همبستگی‌های کامل را هم معرفی می‌کند. در ادامه یک نامساوی بل جدید، شامل همبستگی‌هایی قوی‌تر از همبستگی‌های کوانتومی طراحی می‌شود و با نقض آن بازه‌ای برای بررسی حضور یا عدم حضور استراق سمع کننده تعیین می‌کنیم. به علاوه، پس از بررسی نویز آستانه، نرخ محرمانه بودن کلید را بدست می‌آوریم.

کلمات کلیدی: غیرموضعیت- اطلاعات کوانتومی-همبستگی کوانتومی- درهم‌تنیدگی کوانتومی- اندازه‌گیری کوانتومی- وابستگی به زمینه- توزیع کلید کوانتومی

مقالات مستخرج از این پایان‌نامه

۱. کنفرانس فیزیک سالانه ایران" مزیت‌های پروتکل توزیع کلید کوانتومی شش- حالته در مقایسه با پروتکل توزیع کلید کوانتومی چهار- حالته"

فهرست مطالب

فهرست شکل‌ها

فهرست جدول ها

فصل اول:

تاریخچه‌ی رمزنگاری

۱-۱ مقدمه

رمزنگاری[1](کریپتوگرافی) دانشی است که به بررسی و شناخت اصول و روش‌های انتقال یا ذخیره‌ی اطلاعات به صورت امن (حتی اگر مسیر انتقال اطلاعات و کانال‌های ارتباطی یا محل ذخیره اطلاعات ناامن باشند) می‌پردازد [۲]. کریپتوگرافی دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است، قادر به استخراج اطلاعات اصلی از اطلاعات رمزی شده می‌باشد و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد، نمی‌تواند به اطلاعات دسترسی پیدا کند. دانش رمزنگاری بر پایه‌ی مقدمات بسیاری، از قبیل تئوری اطلاعات، نظریه اعداد و آمار بنا شده است و امروزه به طور خاص در علم مخابرات مورد بررسی و استفاده قرار می‌گیرد. لغت کریپتوگرافی برگرفته از لغات یونانی کریپتوس[2] و گرافین[3] است.

رمزنگاری پیشینه‌ای طولانی و درخشان دارد که به هزاران سال قبل برمی گردد. متخصصین رمزنگاری بین رمز وکد تمایز قائل می‌شوند. رمز عبارتست از تبدیل کاراکتر به کاراکتر یا بیت به بیت، بدون آن که به محتویات زبان شناختی آن پیام توجه شود. در صورتی که، کد تبدیلی است که کلمه‌ای را با یک کلمه یا علامت دیگر جایگزین می‌کند. امروزه از کدها استفاده‌ی چندانی نمی‌شود، اگر چه استفاده از آن، پیشینه‌ی طولانی و پرسابقه‌ای دارد. موفق‌ترین کدهایی که تاکنون نوشته شده، توسط ارتش ایالات متحده ابداع شد و در خلال جنگ جهانی دوم بکار گرفته شد. فنون رمزنگاری موجود به دو دسته‌ی سنتی و نوین تقسیم می‌شوند [۱]. رمزنگاری سنتی که در زمان‌های گذشته مورد استفاده قرار می‌گرفت، شامل شیوه‌های دستی ساده‌ای مانند تغییر ترتیب حروف و یا عوض کردن یک سری از حروف با حروف دیگر بود. در مقابل، فنون جدید از کامپیوترهایی که توانایی به کارگیری الگوریتم‌های پیچیده را دارا هستند، استفاده می‌کنند. علاوه بر این، کامپیوترها می‌توانند هر

[1] Cryptography
[2] Kryptos
[3] Grapphien

نوع داده‌ای را که قابل نمایش دادن به صورت دودویی[1] باشند، رمزگذاری کنند. برخلاف روش‌های سنتی که تنها به متن‌های نوشتاری محدود می‌شدند.

با توجه به پیدایش شبکه‌های ارتباطی مانند اینترنت، ایمیل و تلفن‌های همراه که در آن‌ها از طریق یک کانال عمومی اطلاعات مهم سیاسی، تجاری، مالی و شخصی مبادله می‌شود، علمِ رمزنگاری از اهمیت روزافزونی برخوردار گردیده است.

دو نوع کلید رمزنگاری کلاسیک نوین به نام رمزنگاری کلید عمومی(PKC)[2] و سرّی یا خصوصی(SKC)[3] وجود دارد. رمزنگاری هنر ابداع کدها و الگوریتم‌هاست. در رمزنگاری اطلاعات توسط یک الگوریتم رمزگذاری و توسط یک الگوریتم دیگر رمزگشایی می‌گردد، که پنهان ماندن اطلاعات به امن بودن هر دو مرحله بستگی دارد. در روش رمزنگاری کلید سرّی این الگوریتم ها اعلام عمومی می‌شوند، بدون این که امنیت متن در معرض خطر قرار گیرد. به این ترتیب که در این روش یک کلید سرّی (یا دو کلید که به سادگی از روی هم قابل محاسبه باشند) بین دو استفاده‌کننده به اشتراک گذاشته می‌شود و به‌همراه الگوریتم‌ها برای تبدیل متن به رمز و بازگرداندن آن به حالت عادی مورد استفاده قرار می‌گیرد. یک کلید مجموعه‌ای از پارامترها است که سرّی ماندن آن مهم‌ترین مساله در سرّی ماندن پیام در این روش است. اما مساله‌ی اصلی در این روش مبادله‌ی یک کلید سرّی است، به این ترتیب که یا دو فرد باید با هم ملاقات کنند که بر سر یک کلید توافق کنند، که روش مناسبی در اغلب موارد نیست، یا باید از طریق یک کانال ارتباطی سرّی با هم تماس برقرار کنند، که با توجه به حجم بالای تعداد افرادی که تمایل به فرستادن اطلاعات دارند ایجاد کانال‌های سرّی به تعداد زیاد عملا غیرممکن است و اگر هم باشد به هر حال سختی ورود به این کانال به‌معنی غیرممکن بودن آن نیست. بنابراین تغییراتی در علم کامپیوتر بوجود آمد. نقطه شروع این دگرگونی در

[1] binary
[2] Public key chanel
[3] Secret key chanel

سال ۱۹۳۶ توسط آلن تورینگ[1] بود که به عنوان پدر علم محاسبه‌ی نوین و علم رایانه شناخته شده است و مهمترین جایزه‌ی علمی رایانه به افتخار وی، جایزه تورینگ نام گرفته است. وی مدلی برای محاسبات ارائه داد، این مدل به عنوان، ماشین تورینگ مشهور است. او به کمک ماشین تورینگ فرمولاسیون موثری برای روش الگوریتم و محاسبه تهیه کرد و با کمک آزمایش تورینگ، سهم مؤثر و محرکی در زمینه‌ی هوش مصنوعی ارائه داد. او با معرفی ماشین تورینگ، یک مدل ریاضی برای تحلیل توانایی‌های ذاتی الگوریتم‌ها بنیان گذاشت. به همین دلیل ماشین تورینگ یکی از عناصر اصلی در نظریه محاسبات و نظریه پیچیدگی است.

در سال ۱۹۴۶ سخت افزار کامپیوتر با کشف ترانزیستور توسط جان باردین[2] ، والتر براتین[3] و ویلیام شاکلی[4] جهش بزرگی کرد[۱]. پیشرفت و رشد سخت افزار همچنان با سرعت ادامه دارد، به طوری که گوردن مور[5] در مقاله ی مشهور خود در آوریل ۱۹۶۵، در ژورنال الکترونیک نوشت: "مدارهای مجتمع منجر به شگفتی‌هایی بزرگ همچون رایانه‌های خانگی یا حداقل ترمینال‌های متصل به یک رایانه‌ی مرکزی، کنترل‌های خودکار برای اتومبیل‌ها، و تجهیزات ارتباطی قابل حمل شخصی خواهند شد". او در این رابطه نظریه‌ای داد که به قانون مور مشهور گردید، پیش بینی او در سال ۱۹۶۵ میلادی در مورد دو برابر شدن شمار ترانزیستورهای به کار رفته در یک تراشه در هر سال و به بیان دیگر، دو برابر شدن قدرت تراشه ها، "قانون مور"، نام گرفته است. او ده سال پس از آن، با توجه به دگرگونی‌های پدید آمده در فناوری نیمه‌هادی‌ها، آن قانون را به روز کرد و به دو برابر شدن قدرت تراشه‌ها در هر دو سال نظر داد. این روند کما بیش در سال‌های پس از آن نیز ادامه داشت، تا آنجا که سنجه‌ای برای پیش بینی آینده‌ی صنعت میکروالکترونیک شد و کم کم نام قانون به خود گرفت. به

مرور زمان، آن عدد دو برابر برای هر سال، دستخوش دگرگونی گردید و به دو برابر برای هر هجده ماه رسید.

[1] Alien Turing
[2] John Bardin
[3] Walter Brattain
[4] William Shockley
[5] Gordon Moore

این دو برابر شدن شمار ترانزیستورها به معنای این است کـه ابعـاد ترانزیـستورها در حـال اتمـی شدن است و با شتاب به جایی خواهیم رسید که محدودیت‌های فیزیکی، اجازه‌ی این اتمی شدن ابعاد را نخواهند داد. این یعنی نزدیک شدن به پایان قانون مور، هر چند شاید این قانون تا حـدود ده سـال دیگر همچنان با ارزش بماند اما مردم به دنبال راه حل‌های دیگری هستند تا بـدون رسـیدن بـه ابعـاد اتمی، سرعت و توانایی کامپیوترهای کلاسیکی را بالا ببرند. یک راه حل این مـشکل کـشف الگـوریتم-های متفاوتی برای محاسبات است کـه توانـایی بـالاتری نـسبت بـه الگـوریتم‌هـای کلاسـیکی دارنـد. الگوریتم‌های با ایمنی بالا توسط محاسبات کوانتومی انجـام مـی‌شـود کـه بـر پایـه ایـده‌ی اسـتفاده از مکانیک کوانتومی در انجام محاسبات است .

وقتی اندازه ترانزیستورهایی که متخصصان می سازند به ابعاد اتمـی نزدیـک مـی شـود، دیگـر قـوانین حاکم بر فیزیک کلاسیک بر رفتار اتم‌ها حاکم نیست. به طور مثال کسی نمـی دانـد یـک الکتـرون در یک زمان مشخص دقیقا در کجا قرار دارد یا کسی نمی تواند به درستی تشخیص دهد که الکتـرون در یک سیم به کجا می رود. یعنی وقتی به ابعاد اتمی نزدیک می شویم، فیزیک کوانتومی رفتار اتم هـا را توضیح می‌دهد و دیگر قوانین کلاسیک کاربرد ندارد. در واقع کامپیوترهای نـسل آینـده بـا اسـتفاده از فناوری‌های میکروسکوپیک ذره‌ها کار می‌کنند، به طور مثال در مورد الکترون از خاصیت اسپین آنها و در تابش از خاصیت پولاریزاسیون و غیره استفاده می‌کنند. به همین دلیل است که سرعت و حجم این کامپیوترها با کامپیوترهای امروزی قابل قیاس نیست.

نخستین ایده‌ها در مورد کامپیوترهای کوانتومی به دهه ۱۹۸۰ برمـی‌گـردد. در آن زمـان دانـشمندانی همچون دیوید دویچ[1] و ریچارد فایمن[2] با ارائه مقاله‌هـایی از لحـاظ نظـری بـه توصـیف کامپیوترهـای کوانتومی پرداختند، ولی دستیابی متخصصان به جنبه‌های عملی آن امکان پذیر نشد.

[1] David Deutch
[2] Richard Fayman

تا آنکه در نهایت در نوامبر ۱۹۹۴، پیتر شور[1] با طراحی یک الگوریتم کوانتومی که بعدها بـه الگـوریتم شور معروف شد، تا حد زیادی جهان را در دستیابی به کامپیوترهای کوانتومی نزدیک‌تر کرد. براسـاس این روش می‌توان با استفاده از کامپیوترهای کوانتومی یک عدد را با سرعت فوق العـاده‌ای بـه مقـسوم علیه‌های اول آن تجزیه کرد. اگر برای انجام عمل ریاضی مشابهی از کامپیوترهای فعلی استفاده کنـیم، با افزودن هر رقم به عدد مورد نظر سرعت کامپیوتر برای حل مسئله به نصف کاهش می یابـد. قـدرت ریاضی الگوریتم شور دانشمندان زیادی را به فکر انداخت تا برای پیدا کردن الگـوریتم‌هـای کوانتـومی دیگر یا یافتن روش‌های عملی اجرای این الگوریتم‌ها فعالیت کنند[۱۳].

پی‌آمد این فعالیت‌ها در نهایت در سال ۱۹۷۶ به عنوان روشی درمقالـه‌ی وایـت فیلـد[2] و مـارتین هلمن[3] معرفی شد که برای رفع مشکل توزیع کلید رمزنگاری بود. در این روش از دو کلید متفاوت، اما از نظر ریاضی مرتبط استفاده می‌شود :کلید عمومی و خصوصی .

کلید عمومی که در مرحله‌ی رمزگذاری استفاده می‌شود، می‌تواند در اختیار عموم قرار گیرد، ولـی کلید خصوصی که برای رمزگشایی استفاده می‌شود، باید سری بماند. بـرای مثـال سیـستم RSA یـک نمونه از PKC است، کـه در آن فـردی کـه مـی‌خواهـد پیـامی دریافـت کنـد بایـد دارای یـک جعبـه پیام(جعبه میل[4]) با دو قفل باشد .صاحب جعبه پیام یک کلید برای انـداختن پیـام بـه داخـل جعبـه منتشر می‌کند، ولی تنها خود او کلید باز کردن جعبه و خواندن پیام‌ها را دارد. این روش از دو تبـدیل متقابلاً عکس هم استفاده می‌کند که در آن انجام عملیات ریاضی از یک سـو بـسیار سـاده‌تـر از سـوی دیگر است. به این ترتیب کلید عمومی به شکلی طراحی می‌شود که محاسبه‌ی کلید خـصوصی از روی آن عملا غیرممکن باشد. بنابراین در این روش استفاده‌کننده‌ها نیاز ندارند که بر سر یـک کلیـد سـری توافق کنند و ایمنی این روش به علت دشواری محاسبه‌ی کلید خصوصی است.

[1] Peater Shor
[2] Whitfield Diffe
[3] Martin Hellman
[4] Mail box

رمزنگاریِ کوانتومی اولین بار توسط استفان وینسنر[1] در اوایل دهه‌ی ۱۹۷۰ ارائه شد، که مقاله‌ی وی در این زمینه در سال۱۹۸۳ به چاپ رسید[۱] و در سال ۱۹۸۴ اولین پروتکل رمزنگاری کوانتومی توسط بنت[2] و براسارد[3] ارائه شد و آن به نام **BB84** مشهور شد،[۱۴][۶] پس از آن در سال ۱۹۹۱ یک دانشجوی دوره‌ی دکتری دانشگاه آکسفورد به نام آرتور ایکرت[4] روش دیگری برای رمزنگاری کوانتومی ارائه داد. و پس از او در سال ۱۹۹۲ بنت، براسارد و مرمین[5] پروتکلی پیشرفته‌تر نسبت به آنچه در سال ۱۹۸۴ ارائه شد، معرفی کردند. این طرح با نام **BBM** یا **B92** نام گرفت. بارت[6]، هاردی[7] و کنت[8] پس از مطالعه‌ی این طرح، توانستند پروتکل رمزنگاری با استفاده از اصول فرا کوانتومی طراحی کنند [۲]. این طرح یک پیشرفت در دنیای رمزنگاری کوانتومی بود به طور کلی پروتکل‌های تولید شده‌ی اخیر بسیار مورد توجه هستند و برای تکنولوژی مدرن بسیار مهم است.

با پدید آمدن رایانه‌ها و افزایش قدرت محاسباتی آنها، دانش رمزنگاری وارد حوزه‌ی علوم رایانه‌ای گردید و این پدیده، موجب بروز سه تغییر مهم در مسائل رمزنگاری شد:

وجود قدرت محاسباتی بالا این امکان را پدید آورد که روش‌های پیچیده‌تر و مؤثرتری برای رمزنگاری به وجود آید.

روش‌های رمزنگاری که تا قبل از آن اصولا برای رمزی کردن پیام به کار می‌رفتند، کاربردهای جدید و متعددی پیدا کردند.

تا قبل از آن، رمزنگاری عمدتا روی اطلاعات متنی و با استفاده از حروف الفبا انجام می‌گرفت، اما ورود رایانه باعث شد که رمزنگاری روی انواع اطلاعات و بر مبنای بیت انجام شود.

---

[1] Stephen Wiesner
[2] bennett
[3] brassard
[4] Artur Ekert
[5] Mermin
[6] Barrett
[7] Hrdy
[8] Kent

در فصل بعد مختصری راجع به مفاهیم مهم در جهان محاسبات کوانتومی می‌پردازیم که ما را بـر مطالب اصلی مشرف می‌سازد. در فصل سوم به بررسی چند پروتکل که از پیش ارائـه شـده اسـت و در اینجا به آنها اشاره شد، می‌پردازیم. در فصل آخر مطالب اصلی پایان‌نامه مطرح خواهد شد.

فصل دوم

تعاریف و مفاهیم

۲-۱ مقدمه

در این فصل به مفاهیم مهم کوانتومی که با علم کامپیوتر عجین شده است، می‌پردازیم. اساس این شاخه از علم، محاسبه‌ی اطلاعات در سیستم‌ها به روش کوانتومی است. پس از بررسی قانون دوم ترمودینامیک توسط ماکسول این دگرگونی‌ها در علم کامپیوتر پدید آمد. همانطور که می‌دانیم قانون دوم ترمودینامیک می‌گوید، اگر گاز را در جعبه‌ای دو قسمتی شامل قسمت‌های a و b محبوس کنیم، آنگاه مولکول‌های گاز با سرعت از قسمت a به b و کندتر از b به a می روند. پس a سرد و b گرم است. جریان گرم از یک محیط سرد به محیط گرم هزینه بردار است[۶]. به همین دلیل در ترمودینامیک آموختیم که در فضایی که گرما از دست می‌دهیم فرایند برگشت‌ناپذیر است. در گیت-های دو ورودی کامپیوترها که تک خروجی هستند، فرایند برگشت‌ناپذیر اتفاق می‌افتد چرا که در این گیت‌ها برای اینکه از دو ورودی یک خروجی داشته باشیم یک بیت از بین می‌رود و بدین ترتیب در فضای مربوطه دو درجه‌ی آزادی از دست می‌دهیم و به اندازه‌ی $-k\ln\Omega$ گرما از بین رفته و آنتروپی تغییر می‌کند. پس با توجه به گزارش ترمودینامیک و اطلاعات، ما به رابطه‌ای میان آنتروپی و ضبط اطلاعات میرسیم. به همین دلیل در ادامه به معرفی نظریه اطلاعات می‌پردازیم.

۲-۲ نظریه اطلاعات کوانتومی[1]

برای مطالعه‌ی نظریه اطلاعات کوانتومی ابتدا به دنبال این هستیم که چگونه اطلاعات را کمّی کنیم. کمّی‌سازی اطلاعات با مفهومی به نام آنتروپی انجام می‌پذیرد که به نوعی به اندازه‌گیری بی‌نظمی در سیستم‌ها می‌پردازد. اطلاعات در نقطه‌ی مقابل بی‌نظمی است. آنتروپی حجم اطلاعات را درون یک سیگنال مشخصه‌بندی می‌کند و تعداد بیت لازم برای انتقال یک سیگنال مطمئن را مشخص می‌کند. حال ما به دنبال یافتن ارتباط میان پردازش اطلاعات کوانتومی و آنتروپی هستیم. محاسبات کوانتومی یک راه جدید پردازش اطلاعات است به همین دلیل متدهای قدیمی و پردازش اطلاعات، به اطلاعات

[1] Quantum Information Theory

کلاسیکی شبیه هستند. برای این موضوعات جدید، ابتدا چگونگی دسته بندی اطلاعات را بررسی می‌کنیم. یکی از پایه‌های مهم در اطلاعات، بیت نام دارد که تنها می تواند مقدار ۰ و یا ۱ را بپذیرد. حال اگر در یک سیستم دوتایی، تعداد m حالت برای n بیت داشته باشیم، در این صورت می‌توان گفت:

$$m \le 2^n \qquad \Rightarrow \qquad n \ge \log_2 m \tag{۱-۲}$$

رابطه‌ی بالا توسط هارتلی[1] در سال ۱۹۲۷ ارائه شد و این اولین تلاش در تعیین مقدار یک کمیت برای میزان اطلاعات در یک پیام بود. مثلا می گوید که n بیت می تواند به m پیام متفاوت دسته‌بندی شود[۲].

روش هارتلی روشی اساسی در مشخصه‌بندی حجم اطلاعات درون یک سیگنال است. اما روش دیگری که شانون[2] نامیده می‌شود به ما کمک می‌کند که حجم اطلاعات درون یک سیگنال را با دقت بالاتری مشخصه‌بندی کنیم. آنچه این روش را بسیار متمایز می‌سازد این است که، این روش به محاسبه‌ی اطلاعات با بیانی احتمالی می‌پردازد. بدین ترتیب می توانیم به طور دقیق از یک سیگنال، اطلاعاتی را به دست آوریم. احتمالات با لگاریتمی در مبنای ۲ تعیین می‌شود. اگر I نماد حجم اطلاعات باشد و احتمال وقوع ρ باشد، آنگاه اطلاعات را به صورت زیر بدست می‌آوریم:

$$I = -\log_2 \rho \tag{۲-۲}$$

و علامت - نشان می‌دهد که اطلاعات مثبت است و از این فرمول چنین استنباط می‌شود که کمترین احتمال وقوع یک پیام، بیشترین اطلاعات را نتیجه می‌دهد. بنابراین به طور خلاصه، از لگاریتم در

[1] Hartly
[2] Shannon

مشخصه‌بندی اطلاعات در یک سیگنال استفاده می‌کنیم و این را نظریه اطلاعات شانون[1] می‌نامیم[۱,۲]. حال به بررسی کامل نظریه اطلاعات شانون می‌پردازیم:

مفهوم کلیدی نظریه اطلاعات کلاسیکی، آنتروپی شانون است. اگر ما مقدار x را ندانیم و آنتروپی شانون x، مقدار غیر قطعی اطلاعات را بدست می‌آورد.

ما معمولا آنتروپی را به عنوان یک تابع توزیع احتمال می‌نویسیم. آنتروپی شانون را با این توزیع احتمال که به صورت زیر تعریف شده ، می‌نویسیم:

$$H(x) \equiv H(p_1,...,p_n) \equiv -\sum_x p_x \log p_x \qquad (۳-۲)$$

به طور قراردادی آنتروپی را با تبدیل شدن به log در بیت‌ها اندازه می‌گیریم. اکنون چرا آنتروپی را تعریف کرده‌ایم؟ بهترین علت برای تعریف آنتروپی آن است که از آن در مشخص شدن ذخایری که برای ذخیره‌ی اطلاعات احتیاج داریم، استفاده می‌کنیم. مثلا فرض کنیم تعدادی منبع (مثل یک آنتن رادیویی) که اطلاعات را دسته‌بندی می‌کند، به صورت یک رشته بیت داشته باشیم، اگر به عنوان یک رشته $x_1, x_2, ...$ مستقل، متغیرهای تصادفی همسان توزیع شده است، با استفاده از آنتروپی شانون بهترین وسیله برای بدست آوردن کمترین منابع اطلاعاتی که برای دسته‌بندی اطلاعات تولید شده در منبع احتیاج داریم، آنتروپی است که به صورت بیت‌های لازم تقسیم بر نمونه‌ی منبع تعریف می‌شود،

$$H(x) \equiv H(x_1) = H(x_2) = ...$$

این مطلب به عنوان تئوری برنامه‌نویسی نویزی شانون شناخته شده است که برای هر دو نوع کلاسیکی و کوانتومی کاربرد دارد. به عنوان مثال فرض می‌کنیم که یک منبع اطلاعاتی ۴ نمونه دارد که عبارتند از ۱و ۲ و۳ و۴ و به ترتیب متناظر با چهار علامت با احتمالات زیر است یعنی ۱، احتمال $\frac{1}{2}$ و ۲ با احتمال $\frac{1}{4}$ و ۳ و ۴ با احتمال $\frac{1}{8}$. برای طرح متراکم‌سازی اطلاعات آن‌ها را به

[1] Shannon Information Theory

صورت رشته بیت‌ها معرفی می کنیم به این صورت که رشته بیت اول، ۰ و رشته بیت دوم، ۱۰ و رشته بیت سوم، ۱۱۰ و رشته بیت چهارم، ۱۱۱ است. برای فشرده سازی اطلاعات با استفاده از احتمال و طول رشته بیت‌ها خواهیم داشت:

$$\frac{1}{2}\times 1+\frac{1}{4}\times 2+\frac{1}{8}\times 3+\frac{1}{8}\times 3=\frac{7}{4}!$$

و پس از محاسبه‌ی آنتروپی شانون می توان دید:

$$-\frac{1}{2}\log(\frac{1}{2})-\frac{1}{4}\log(\frac{1}{4})-\frac{1}{8}\log(\frac{1}{8})-\frac{1}{8}\log(\frac{1}{8})=\frac{7}{4}!=H(x)$$

به طور شگفت‌انگیزی با هم برابر خواهند بود. به هر حال در فشرده‌سازی اطلاعات منبع نتیجه می‌شود که اطلاعات به طور شهودی گم می شوند و این انگیزه‌ای برای اندازه‌گیری اطلاعات با استفاده از آنتروپی هم به طور کلاسیکی و هم به طور کوانتومی است. در زیر به آنتروپی شرطی و اطلاعات متقابل که بسیار حائز اهمیت است، می‌پردازیم[۱] و [۳] و [۴].

۲-۳ آنتروپی شرطی و اطلاعات متقابل

فرض کنید X و Y دو متغیر تصادفی هستند. چگونه اطلاعات محتوی X با اطلاعات محتوی Y ارتباط دارند؟ در این بخش دو مفهوم را معرفی می‌کنیم، آنتروپی شرطی و اطلاعات متقابل که ما را در جواب به این سوال کمک می کند.

۲-۳-۱ آنتروپی شرطی

آنتروپی توامان[1] را برای یک جفت متغیر تصادفی X و Y به صورت زیر تعریف می‌کنیم:

$$H(X,Y) \equiv -\sum_{x,y} p(x,y) \log_2 p(x,y) \qquad (۴-۲)$$

که $p(x,y) = p(x)p(y|x)$ است. البته این تعریف برای هر متغیر تصادفی در فضای برداری قابل بسط است. آنتروپی توامان، مقادیر غیر قطعی را برای جفت X و Y تعریف می‌کند. فرض کنید ما مقدار Y را می دانیم. بنابراین، H(Y) بیت اطلاعاتی درباره‌ی جفت X و Y احتیاج داریم و اطلاعات باقیمانده‌ی غیر قطعی درباره‌ی X و Y با اطلاعات باقیمانده‌ی گم‌شده‌ی درباره‌ی X عجین شده است، حتی با توجه به آنکه Y را می‌دانیم، آنتروپی X به شرط دانستن Y نهایتا با استفاده از تعریف آنتروپی زنجیری به صورت زیر به دست می‌آید. متغیر تصادفی X را با مقدار x و Y را با مقدار y در نظر می‌گیریم. آنتروپی شرطی Y برای X به صورت زیر خواهد شد:

$$\begin{aligned}
H(Y|X) &\equiv \sum_{x \in X} p(x) H(Y|X=x) \\
&= -\sum_{x \in X} p(x) \sum_{y \in Y} p(y|x) \log p(y|x) \\
&= -\sum_{x,y} p(x,y) \log p(y|x) \\
&= -\sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)} \\
&= -\sum_{x,y} p(x,y) \log p(x,y) + \sum_{x} p(x) \log p(x) \\
&= H(X,Y) - H(X)
\end{aligned} \qquad (۵-۲)$$

[1] Joint entropy

آنتروپی شرطی $H(X|Y)$ آن دسته از اطلاعات است که می‌توان در صورت دانستن Y، درباره‌ی X بدست آوریم به عبارتی آنتروپی شرطی، اطلاعات باقیمانده را مشخص می‌کند.

۲-۳-۲ اطلاعات متقابل

کمیت دومی که به توصیف آن می‌پردازیم حجم اطلاعات متقابل X وY است که اطلاعات مشترک میان X و Y را اندازه می‌گیرد. فرض کنید ما حجم اطلاعات X را به حجم اطلاعات Y اضافه می‌کنیم. اطلاعاتی که میان X و Y مشترک هستند دوباره شمرده می‌شوند و آنها که مشترک نیستند به طور قطع یکبار شمرده می‌شوند. اطلاعات مشترک کاهیده شده میان X و Y را $H(X,Y)$ می‌نامیم، بنابراین اطلاعات متقابل یا مشترک میان X و Y را اینگونه تعریف می کنیم:

$$I(X:Y) \equiv H(X) + H(Y) - H(X,Y) \qquad (۶\text{-}۲)$$

که معادله‌ی بالا از جایگذاری معادله‌ی (۲-۵) در معادله‌ی $I(X:Y) = H(X) - H(X|Y)$ بدست آمده است و در ارتباط با آنتروپی شرطی و اطلاعات متقابل است. برای بررسی چگونگی رفتار آنتروپی، ما اکنون تعدادی از روابط ساده میان آنتروپی‌های مختلف را بررسی می‌کنیم[۱] و [۳] و [۴].

خصوصیات اصلی آنتروپی شانون عبارتند از:

۱) $I(X:Y) = I(Y:X)$ و $H(X,Y) = H(Y,X)$

۲) $H(Y|X) \geq 0$ و بنابراین $I(X:Y) \leq H(Y)$ و با تساوی اگر و فقط اگر Y یک تابع از X باشند، یعنی: $Y = f(X)$

۳) $H(X) \leq H(X,Y)$ ،با تساوی اگر و فقط اگر Y یک تابع از X باشد.

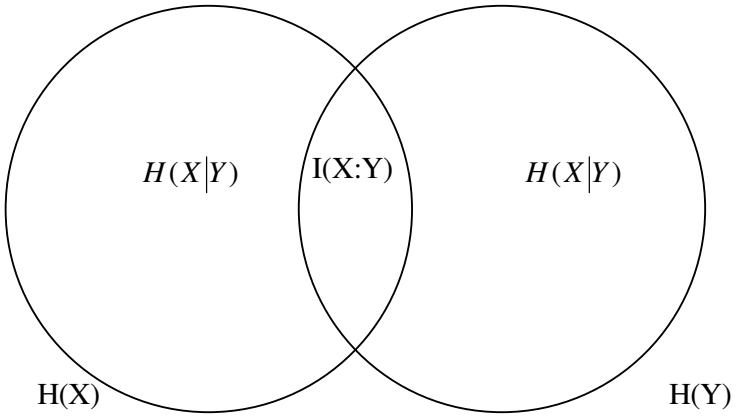
۴) $H(X,Y) \le H(X) + H(Y)$ برای تساوی اگر و فقط اگر X و Y متغیرهای تصادفی مستقل باشند.

۵) $H(X|Y) \le H(Y)$ و بنابراین $I(X:Y) \ge 0$، برای تساوی در هر کدام اگر و فقط اگر X و Y متغیرهای تصادفی مستقل باشند.

۶) $H(X,Y,Z) + H(Y) \le H(X,Y) + H(Y,Z)$ برای تساوی اگر و فقط اگر $Z \to Y \to X$ به شکل زنجیره‌ی ماکوف.

۷) $H(X|Y,Z) \le H(X|Y)$

شکل زیر نمودار آنتروپی Venn نام دارد که به طور کامل نمی‌تواند خصوصیات متفاوت آنتروپی را به ما آموزش دهد اما باعث به خاطر سپردن و یادآوری آسان آن‌ها می‌شود



شکل(۲-۱) ارتباط میان آنتروپی شرطی و اطلاعات متقابل

خصوصیات ابتدایی آنتروپی شرطی و اطلاعات متقابل شامل قانون مهم و مفید و ساده‌ی زنجیره‌ای می‌شود[۱] و [۲] و [۳].

اگر $Y, X_1, X_2, ..., X_n$ متغیرهایی تصادفی باشند، $H(X_1,...,X_n|Y) = \sum_{i=1}^{n} H(X_i|Y, X_1,...,X_{i-1})$

اثبات:

مابرای n=2 اثبات را انجام می‌دهیم. تنها با استفاده از تعاریف و جبر ساده خواهیم داشت:

$$\begin{aligned} H(X_1,X_2\big|Y) &\overset{?}{=} \sum_{i=1}^{2} H(X_i\big|Y,X_1,X_2) \\ H(X_1,X_2\big|Y) &= H(X_1,X_2,Y)-H(Y) \\ &= H(X_1,X_2,Y)+H(X_1,Y)-H(X_1,Y)-H(Y) \\ &= H(X_2\big|X_1,Y)+H(X_1,Y) \end{aligned} \qquad (۷\text{-}۲)$$

اکنون رابطه‌ی بالا را برای n حالت تعمیم می‌دهیم:

$$\begin{aligned} H(X_1,...,X_{n+1}\big|Y) &= \sum_{i=2}^{n+1} H(X_i\big|Y,X_1,...,X_{i+1})+H(X_1\big|Y) \\ &= \sum_{i=1}^{n+1} H(X_i\big|Y,X_1,...,X_{i-1}) \end{aligned} \qquad (۸\text{-}۲)$$

۲-۴ کیوبیت

از قبل گفتیم که، واحد پردازش اطلاعات در کامپیوترهای کلاسیکی بیت است و تابع قوانین کلاسیکی است، به شیوه‌ای مشابه می توان یک واحد اصلی پردازش اطلاعات کوانتومی در نظر گرفت که این واحد به محاسبات کوانتومی می‌پردازد و تابع قوانین فیزیک کوانتومی است و آن را کیوبیت[1] مخفف بیت کوانتومی می‌نامیم. بر خلاف این‌که بیت و کیوبیت در روشهایی با هم مشابه هستند اما اساس آنها با هم متفاوت است و به همین دلیل می‌توان برای محاسبات به روش‌های جدید از آن استفاده کرد. کیوبیت هم مثل بیت می‌تواند دو مقدار را بپذیرد. حالت یک کیوبیت به وسیله‌ی یک بردار یکه در فضای برداری دوبعدی روی میدان اعداد مختلط بیان می‌گردد. $|\psi\rangle=\begin{pmatrix} a \\ b \end{pmatrix}$ که پایه‌های ثابت این فضا با $\{|0\rangle,|1\rangle\}$ مشخص می‌شوند. این پایه‌های راست هنجار $|0\rangle$ و $|1\rangle$ ممکن است به ترتیب با

[1] qubit

قطبش‌های فوتون ۰ و ۹۰ درجه و یا ۴۵ و ۱۳۵ درجه متناظر باشند و یا حتی می‌توانند به حالت‌های اسپین بالا و پایین الکترون ذرات با اسپین $\frac{1}{2}$ مرتبط باشند و یا اینکه به صورت برهم‌نهشی از دو راستا باشد. تمام اندازه‌گیری‌ها با توجه به پایه‌های استاندارد برای محاسبات کوانتومی، یعنی $\{|0\rangle,|1\rangle\}$ انجام می‌شوند. حالت‌های پایه‌ی فضا را با $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$ و $|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$ نشان می‌دهیم. حالت سیستم کیوبیتی به صورت $|\psi\rangle=a|0\rangle+b|1\rangle$ است که a و b اعداد مختلطی هستند که در رابطه‌ی $|a|^2+|b|^2=1$ صدق می‌کنند که نتیجه‌ی اندازه‌گیری حالت سیستم با احتمال $|a|^2$، $|0\rangle$ و نتیجه‌ی اندازه‌گیری حالت سیستم با احتمال $|b|^2$، $|1\rangle$ است.

اساس رمزنگاری کوانتومی و اطلاعات و محاسبات کوانتومی[1] بر سه مفهوم است:

۲-۵ درهم‌تنیدگی

از مواردی که محاسبات کوانتومی را از محاسبات کلاسیکی به شدت متمایز می‌سازد، درهم‌تنیدگی کوانتومی است که یکی از ویژگی‌های دنیای کوانتومی است. همبستگی‌های کوانتومی حالت‌های درهم تنیده، هیچ مشابه کلاسیکی ندارد و می‌توان گفت درهم‌تنیدگی از بنیادی‌ترین مفاهیم است که باعث جدایی فیزیک کوانتومی از فیزیک کلاسیک می‌شود. حالاتی که درهم‌تنیده نیستند را می‌توان به صورت حاصلضرب حالاتی که یکی فقط به ویژگی‌های سیستم ۱ و یکی فقط به ویژگی‌های سیستم ۲ وابسته است، نوشت اما در حالت‌های دیگر که درهم‌تنیده[2] نامیده می‌شوند، نمی‌توان این‌گونه عمل کرد [۲]. با استفاده از حالت‌های درهم تنیده می‌توانیم کارهای جدیدی را در پردازش اطلاعات انجام دهیم که در فیزیک کلاسیک غیرممکن است. همچنین می‌توانیم بسیاری از روش‌هایی را که با استفاده از فیزیک کلاسیک برای پردازش اطلاعات به کار می‌بریم، بهبود بخشیم.

[1] Quantum Information and Computation
[2] Entangled

برای هر حالت خالص دوقسمتی[1] می‌توان یک عدد صحیح مثبت بـه نـام عـدد اشـمیت[2] نـسبت داد و برحسب این کمیت می‌توانیم بگوییم درهم تنیده بودن یک حالت خاص دوقسمتی به چه معنی است: اگر عدد اشمیت بزرگتر از یک باشد، $|\psi_{AB}\rangle$ درهم تنیده یا تفکیک‌ناپذیر است و در غیـر ایـن صـورت تفکیک‌پذیر بوده و غیر درهم‌تنیده است. در نتیجه یک حالت خالص دو قسمتی تفکیـک‌پـذیر، ضـرب مستقیمی از حالت‌های خالص در فضای H_A و H_B است. هر حالتی که نتوان آن را بـه صـورت یـک ضرب مستقیم بیان کرد درهم تنیده نامیده مـی‌شـود[۱][۶][۷]. حالـت‌هـای در هـم تنیـده بـه طـور طبیعی به عنوان نتیجه‌ای از برهم کنش بین ذرات ایجاد می‌شود مانند حالتی که یـک جفـت ذره بـه طور همزمان تحت پاره‌ای از ویژگی‌ها تولید می‌شوند[۸] و هرگاه اندازه‌گیری روی یکی از آن‌هـا انجـام می‌شود، حالت‌های هر دو ذره تعیین می‌شود و درهم‌تنیدگی از بین می‌رود[۶][۹]. این ویژگـی منجـر به ارائه‌ی مقاله‌ی EPR توسط انیشتین و پدولسکی و روزن شد. آن‌ها با انتشار مقاله‌ای[3] به عنوان (آیـا مکانیک کوانتومی می تواند به طور قطع حالت یک سیستم را بررسی کند؟) پرداختند [۵].

انیشتین معتقد بود که مکانیک کوانتومی کامل نیست و زمانی می تـوان مقـداری بـرای یـک سیـستم پیش‌بینی کرد که آن را مشاهده کنیم و یا مقادیر قطعی آن قبل از اندازه گیری وجـود داشـته باشـند. حال اگر یک کیوبیت با حالت $|0\rangle$ در نظر بگیریم، آنگاه برای بدست آوردن نتایج اندازه‌گیـری $|\psi\rangle$ در راستای x، داریم:

$$|\Psi\rangle = |0\rangle = \frac{|+\rangle + |-\rangle}{2}$$

[1] Bipartitr pure state
[2] Schmidt number
[3] EPR

$|\Psi\rangle$ در بالا بر حسب ویژه حالتهای x نوشته شده است. به طوریکه:

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

$$\Rightarrow \qquad |0\rangle = \frac{|+\rangle + |-\rangle}{2}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{2}$$

با توجه به شرایط اولیه‌ی آزمایش و شناخت محیط و قوانین فیزیک و مکانیک کوانتومی پیش‌بینی می‌کنیم که نتیجه‌ی اندازه‌گیری اسپین فوتون با احتمال $\frac{1}{2}$، $|+\rangle$ و با احتمال $\frac{1}{2}$، $|-\rangle$ است. همانطور که گفته شد در مکانیک کوانتومی تنها می‌توان نتیجه‌ی آزمایش را پیش‌بینی کرد و حالت سیستم زمانی معلوم می‌شود که اندازه می‌گیریم، اگر یک الکترون را دقیقا درحالت $|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha|\uparrow\rangle + \beta|\downarrow\rangle)$ قرار دهیم، تعداد زیادی ذره را اندازه می‌گیریم که در شرایط یکسان همه این‌ها برای اسپین، یا $\uparrow$ و یا $\downarrow$ بدست می آورند اما برای حالات کلاسیکی می‌توان قبل از اندازه-گیری نتیجه‌ی اندازه‌گیری را حدس زد و این یعنی احتمال اندازه‌گیری در مکانیک کلاسیکی و مکانیک کوانتومی متفاوت است و علت این تفاوت آن است که ماتریس چگالی احتمال مکانیک کلاسیکی $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ است ولی ماتریس چگالی[1] احتمال کوانتومی $\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ است. پس نتیجه‌ی اندازه-گیری برای حالات کلاسیکی همواره یکسان است اما در مکانیک کوانتومی نتیجه‌ی اندازه‌گیری متفاوت است. به همین دلیل EPR با توجه به تعاریف کلاسیکی اندازه‌گیری که بر مبنای موضعیت[2] و

[1] Density Matrix
[2] locality

واقع‌گرایی[1] است معتقد بودند که مکانیک کوانتومی ناقص است[۵] و [۴]. به طور خلاصه تعاریف اندازه‌گیری کلاسیکی به صورت زیر هستند:

موضعیت: اندازه‌گیری ذره‌ی A فقط به خودش وابسته است و به هیچ ذره‌ی دیگری ارتباط ندارد.

واقع‌گرایی: خصوصیات سیستم به راحتی و روشنی قابل درک است و اندازه‌گیری سیستم از قبل وجود داشته و در هر صورت همان مقدار بدست می‌آید.

دیوید بوهم نظریه‌ی EPR را به گونه‌ی دیگری ارائه داد و علت این موضوع را وجود متغیرهایی معرفی می‌کند که مشاهده نمی‌شوند و به همین علت آنها را متغیرهای مخفی[2] H نامید. وی گفت اگر حالت سیستم به صورت زیر باشد:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) + H$$

و اگر ما بتوانیم متغیرهای مخفی را بدانیم، به راحتی می توانیم حالت سیستم را قبل از اندازه‌گیری بدست آوریم. البته این تاکنون غیرممکن بوده است.

یکی دیگر از پیامدهای درهم‌تنیدگی مفهوم توزیع کلید کوانتومی[3] است که در ادامه به توضیح آن می‌پردازیم.

۲-۵-۱ توزیع کلید کوانتومی (QKD)

ارتباط ایمن میان دوطرف فرستنده و گیرنده‌ی پیام به طوری که هیچ شخص سومی از اطلاعات آن‌ها مطلع نگردد، می‌تواند از طریق توزیع کلید انجام شود که از آن کلید برای بازیابی و رمزگشایی استفاده می‌شود. در حال حاضر کلید رمزنگاری تولید شده با استفاده از الگوریتم‌های کوانتومی، روش توزیع کلیدی است که متکی به قوانین فیزیک است. البته نه ۱۰۰درصد امن اما بسیاری از مزایای آن در مقابل روش‌های قدیمی چشمگیر است[۱] و [۲].

[1] realism
[2] Hidden variable
[3] Quantum Key Distribution

در حال حاضر با کامپیوترهای ۸ بیتی کار می‌کنیم:

$$2^8 = 256 \quad characters$$

مثلا فرض می‌کنیم می‌خواهیم جمله ی I am here را از طریق کامپیوتر کوانتومی به صورت سری بفرستیم و اطلاعات برای هیچ شخص سومی افشا نشود، عبارت را به صورت *IbambhereI* می‌فرستیم. فرض می کنیم در *ASCII Code*[1] کار می‌کنیم، هر کاراکتر ۸ بیت دارد، هر کدام از این خانه‌ها می‌توانند دو مقدار ۰ و یا ۱ را بپذیرند، البته در کامپیوترهای کوانتومی از اسپین استفاده می‌کنند. اسپین‌های فوتون مدنظر است که که اسپین ↑ را ۰ و اسپین ↓ را ۱ می‌نامند.

این رشته‌ی ۸ کاراکتری که شامل ۰ و یا ۱ است را می‌فرستیم. اگر کسی در مسیر این رشته را دریافت کند می‌تواند آن را بخواند، پس برای رمزگذاری روی این رشته می‌توان رشته ای از ۰ و ۱ به طور اختیاری در نظر گرفت و از طریق گیت‌های کامپیوتری برای مثال *OR* یا *XOR* رشته‌ی اصلی را تغییر دهیم. در این صورت رشته‌ی سوم بدست می‌آید که کاملا عوض شده و سپس این رشته را به صورت عمومی برای باب می‌فرستیم. این رشته را باب تنها می تواند در صورت دانستن رشته‌ی کلی بخواند و این اساس رمزنگاری است. حال در رمزنگاری کوانتومی به دنبال توزیع کلید کوانتومی به صورت فوق محرمانه هستیم زیرا رشته‌های توزیع کلید کلاسیکی پس از نهایتا ۶ ماه شکسته می‌شود اما امکان شکستن رشته کلیدهای کوانتومی غیرممکن است.

مثلا اگر به دنبال ارسال حرف A باشیم، باید رشته بیت مقابل را بفرستیم:

۰	۱	۰	۰	۰	۰	۰	۱

برای جلوگیری از افشای پیام رشته بیت زیر را به عنوان رشته بیت کلید انتخاب می‌کنیم:

[1] این عبارت مربوط به یک جدول جهانی است که برای هر کاراکتر در کامپیوتر یک رشته بیت هشت تایی از ۰ و ۱ تعریف کرده است.

۰	۰	۰	۱	۱	۰	۱	۱

از طریق اثر کردن گیت کامپیوتری XOR روی رشته پیام اصلی به رشته پیام رمزی شده‌ی زیر می‌رسیم:

۰	۱	۰	۱	۰	۰	۱	۰

به فرایند ارسال رشته بیت کلید از طریق کانال عمومی و ارسال رشته پیام رمزی شده از طریق کانال کوانتومی، توزیع کلید کوانتومی می‌گوییم[۶].

در کانال کلاسیکی (عمومی) استراق سمع کننده نمی‌تواند به حضور فرستنده و گیرنده پی ببرد اما آنها می‌توانند به حضور استراق سمع کننده پی ببرند و این کانال ایمن است و به همین دلیل کلید از طریق این کانال ارسال می‌شود.

۲-۶ غیرموضعیت[1]

اگر A حالت سیستم خود را به صورت زیر داشته باشد:

$$|\Psi\rangle=\frac{1}{2}(|\uparrow\rangle_1^z|\downarrow\rangle_2^z-|\downarrow\rangle_1^z|\uparrow\rangle_2^z)=\frac{1}{2}(|\uparrow\rangle_1^x|\downarrow\rangle_2^x-|\downarrow\rangle_1^x|\uparrow\rangle_2^x)$$

معمولاً حالت سیستم را در پایه‌های z می‌نویسیم:

$$\text{قرارداد}: \quad |\uparrow\rangle^x=|+\rangle \qquad |\uparrow\rangle^z=|0\rangle \qquad |\downarrow\rangle^x=|-\rangle \qquad |\downarrow\rangle^z=|1\rangle \qquad (۹-۲)$$

[1] Nonlocality

حال اگر Alice و Bob حالت سیستم را مشترکاً اندازه بگیرند، هر کدام حالت سیستم را در راستای مورد نظر خودش اندازه می‌گیرد. چرا که هر کدام دو راستای اندازه‌گیری دارند:

۱)یا اسپین را در راستای z اندازه می‌گیرند.

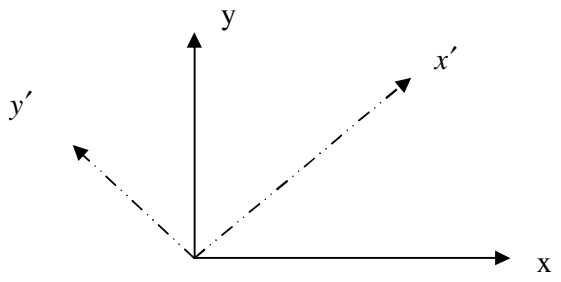
۲)یا اسپین را در راستای x اندازه می‌گیرند.

در حالت کلی هر کدامشان دو خروجی دارند یا به عبارتی ۲ نتیجه‌ی اندازه‌گیری خواهیم داشت که یکی $\uparrow$ و دیگری $\downarrow$ می باشد. در این‌جا چون فوتون مدنظر است و با توجه به ۱ بودن اسپین و ۰ بودن جرم سکونش تنها دو حالت $\uparrow,\downarrow$ برای اسپین آن داریم یعنی $m_s = \pm 1$ اما اگر جرم سکون صفر نباشد و اسپین ۱ باشد، در این‌صورت ۳ خروجی داریم. به همین دلیل به پروتکل‌هایی که تاکنون با فوتون طراحی شده‌اند، ۴ حالته می‌گوییم.

برای این پروتکل‌ها راستای اندازه‌گیری یا ۰ و ۹۰ درجه است و یا ۴۵ و ۱۳۵ درجه می‌باشد. در این صورت پایه‌های اندازه‌گیری قابل تبدیل به همدیگر هستند و می‌توان یکی را بر حسب دیگری نوشت. به عبارتی اگر مطابق شکل زیر پایه‌ها را بر حسب x و y به ترتیب برای ۰ و ۹۰ درجه و بر حسب x' و y' برای ۴۵ و ۱۳۵ درجه نوشت می‌توان گفت:

$$\hat{x} = \cos 45^\circ \hat{x}' - \sin 45^\circ \hat{y}' = \frac{1}{\sqrt{2}}(\hat{x}' - \hat{y}')$$

$$\hat{y} = \cos 45^\circ \hat{x}' + \sin 45^\circ \hat{y}' = \frac{1}{\sqrt{2}}(\hat{x}' + \hat{y}')$$



شکل(۲-۲) پایه‌های حالت یک سیستم کوانتومی که با زاویه‌ی ۴۵ درجه دوران یافته‌اند

اگرحالت سیستم $|\psi\rangle = \frac{1}{2}(|\uparrow\rangle_1^z|\downarrow\rangle_2^z - |\downarrow\rangle_1^z|\uparrow\rangle_2^z)$ باشد، در صورتی که آلیس پس از اندازه‌گیری S_z، $|\uparrow\rangle^z$ بدست آورد و اگر باب S_z را اندازه بگیرد. با احتمال ۱، $|\downarrow\rangle^z$ بدست می‌آورد، اما اگر باب S_x را اندازه بگیرد، با احتمال $\frac{1}{2}$، $|\downarrow\rangle^x$ و با احتمال $\frac{1}{2}$، $|\uparrow\rangle^x$ را به دست می‌آورد. خلاصه اینکه توزیع احتمال در طرف باب وابسته به این است که آلیس چه چیزی را اندازه می‌گیرد و این تعریف غیرموضعیت است.

در این رابطه در سال ۱۹۶۴ بل نظریه‌ای ارائه داد که به اندازه‌گیری اسپین در راستای محورهای متعامد به عنوان نظریه‌ای واقعی و موضعی می‌پرداخت. وی معادله‌ای را ارائه داد که می‌گفت در صورت موضعی بودن این سیستم یعنی این‌که معادله‌ی ارائه شده در بازه‌ی [۲،۲-] باشد، اما مکانیک کوانتومی که غیرموضعی بودن را پیشنهاد می‌کرد بیان کننده‌ی آن است که در صورت غیر موضعی بودن سیستم، باید معادله در بازه‌ی [$0,2\sqrt{2}$] باشد. پس از آزمایش آن به صورت تجربی مقدار $2\sqrt{2}$ بدست آمد و این باعث شد که نامساوی بل[1] نقض شود و ثابت شد که سیستم کوانتومی غیرموضع است. این کار توسط کلازر، هرن، شیمینی و هلتز[2] انجام شد و آن‌ها با نام CHSH مشهور شدند[۲][۸][۱۰].

۲-۷ تکثیرناپذیری[3]

همان‌طور که می‌دانیم قدرت یک کامپیوتر کوانتومی از این است که یک کیوبیت می‌تواند در یک حالت برهم‌نهشی باشد یعنی:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

[1] Bell inequality
[2] Crazern,Horn,Sheminey,Hortz
[3] No-Cloning

حال می‌خواهیم بدانیم که آیا کپی در این کامپیوترها اتفاق می‌افتد؟ جواب منفی است. عدم توانایی در کپی‌برداری حالت‌های کوانتومی، تئوری تکثیرناپذیری نام دارد که توسط ووتر[1] و زورک[2] در سال ۱۹۸۲ اثبات شد و علت برتری کامپیوترهای کوانتومی بر کلاسیکی معرفی شد[۲]. دو حالت خالص[3] را مورد بررسی قرار می دهیم که $|\Psi\rangle$ و $|\Phi\rangle$ هستند و ما فرض می‌کنیم که یک اپراتور U داریم و حالت هدف $|\chi\rangle$است:

$$U(|\Psi\rangle\otimes|\chi\rangle)=|\Psi\rangle\otimes|\Psi\rangle \qquad (I)$$
$$U(|\Phi\rangle\otimes|\chi\rangle)=|\Phi\rangle\otimes|\Phi\rangle \qquad (II) \qquad (۱۰\text{-}۲)$$

از طرف چپ رابطه‌ی I را با II ضرب داخلی می‌کنیم و با این نکته که $U^{\dagger}U=1$ داریم:

$$(\langle\Psi|\otimes\langle\chi|)\ U^{\dagger}U\ (|\Phi\rangle\otimes|\Psi\rangle)=\langle\Psi|\otimes\langle\Psi|\Phi\rangle\otimes|\Phi\rangle$$
$$\langle\Psi|\Phi\rangle\langle\chi|\chi\rangle=\langle\Psi|\Phi\rangle\langle\Psi|\Phi\rangle \qquad (۱۱\text{-}۲)$$
$$\Rightarrow\quad \langle\Psi|\Phi\rangle=|\langle\Psi|\Phi\rangle|^2$$

این معادله در صورتی می تواند درست باشد که یا $\langle\Psi|\Phi\rangle=1$ باشد که بدان معنی است که $|\Psi\rangle$ و $|\Phi\rangle$ با هم برابرند و یا $\langle\Psi|\Phi\rangle=0$ یعنی $|\Psi\rangle$ و $|\Phi\rangle$ متعامد می‌باشند و هیچ حالت یکانی نامتعامدی وجود ندارد که بتوان از آن برای کپی کردن استفاده کرد. البته برای حالت‌هایی که برهم-نهش ندارند کپی اتفاق می‌افتد اما حالت‌هایی که در حالات برهم‌نهشی هستند کپی اتفاق نمی‌افتد. از طرفی چون کامپیوترهای کوانتومی از حالات درهم‌تنیده و برهم‌نهشی استفاده می‌کنند، پس کپی کردن در کامپیوترهای کوانتومی امکان‌ناپذیر است[۲].

[1] Wooter
[2] Zurek
[3] Pure

۲-۸ عدم علامت‌دهی[1]

پس از آن مفهوم دیگری به معنی عدم علامت دهی را شرح می‌دهیم که این مفهوم، وسیله‌ای برای تولید پروتکل‌هایی است که دارای ایمنی قوی‌تری هستند.

عدم علامت‌دهی یعنی این‌که هرگز فرستنده قادر به ارسال سیگنال برای گیرنده نمی‌باشد. حال اگر فرض کنیم که A به عنوان فرستنده به B به عنوان گیرنده سیگنال بفرستد، آنگاه A نقطه‌ی x_A را در زمان t_A اندازه می‌گیرد و B نقطه‌ی x_B را در زمان t_B اندازه می‌گیرد، در این صورت با توجه به تعریف نسبیت خواهیم داشت:

$$\frac{x_B - x_A}{t_B - t_A} > C$$

و این حالت فضاگونه است. با توجه به این‌که فاصله بسیار زیاد است به عبارتی چون اطلاعات به طور آنی منتقل می شوند پس رابطه به صورت زیر خواهد بود:

$$\frac{x_B - x_A}{t_B - t_A}_{\Delta t \to 0} > C \qquad \Rightarrow \qquad v \to \infty$$

پس سرعت بسیار بزرگتر از سرعت نور خواهد شد و این اتفاق با نسبیت منافات دارد.

به عنوان مثال دیگر سیستمی را شامل مشاهده‌پذیرهای b', a', b, a که به ترتیب دارای نتایج اندازه-گیری j', i', j, i هستند را در نظر می‌گیریم. به علاوه همه‌ی مشاهده‌پذیرها دارای نتیجه‌ی اندازه-گیری ۰ یا ۱ هستند. بر خلاف آنچه غیرموضعیت بر آن دلالت دارد یعنی نتیجه‌ی اندازه‌گیری یا احتمال اندازه‌گیری باب وابسته به آن است که آلیس چه مشاهده‌پذیری را اندازه می‌گیرد، عدم علامت‌دهی بر این دلالت دارد که هیچ سیگنالی نمی‌تواند با سرعتی بیش از سرعت نور در یک لحظه از آلیس به باب منتقل شود. در این صورت می‌توان تعریف کرد که:

[1] Non-signaling

اگر آلیس، S_zرا اندازه بگیرد و $i=0$ باشد و دیگری هم S_z را اندازه بگیرد و $j=1$ باشد، پس احتمال توامان را به صورت زیر نشان می‌دهیم:

$$P^{0,1}_{s_z,s_z}$$

و وقتی آنها نمی‌توانند برای هم سیگنال بفرستند، پس احتمال مستقل از دیگری است. پس می‌تواند با حالتی که آلیس پس از اندازه‌گیری S_z ، i=0 و باب پس از اندازه‌گیری S_z، j=0 را بدست آورد، برابر است با:

$$P^{0,0}_{s_z,s_z}$$

بنابراین مجموع احتمالات برای حالتی که آلیس پس از اندازه‌گیری مقدار صفر را مستقل از باب بدست می‌آورد،به صورت رابطه‌ی زیر خواهد بود:

$$\Rightarrow \qquad \sum_j P^{0\,j}_{a\,b} = \sum_{j'} P^{0\,j'}_{a\,b'} \qquad (۱۲-۲)$$

خلاصه بحث آن است که احتمال اینکه آلیس پس از اندازه‌گیری S_z مقدار ۰ را بدست آورد، مستقل از آن است که باب چه چیزی را چه مقدار اندازه بگیرد:

$$P^{0,0}_{S_z,S_z} + P^{0,1}_{S_z,S_z} = P^{0,0}_{S_z,S_x} + P^{0,1}_{S_z,S_x} \qquad (۱۳-۲)$$

پس احتمال اینکه مقدار a هر چقدر باشد برای اولی کاملا از این که b چقدر باشد یا b' چقدر باشند، مستقل است[۱۱].

۲-۹ کره‌ی بلاخ

مفهوم دیگری که در شناخت پروتکل‌ها مهم است شناخت کره‌ی بلاخ[1] است. در ادامه مختصری راجع به آن می‌پردازیم:

[1] Bloch sphere

سیستمی را در نظر می‌گیریم که یک تک کیوبیت است. حالت کلی ماتریس چگالی را می‌توان به صورت هر ماتریس 2×2 یکانی بر حسب ماتریس‌های پائولی و ماتریس یکه بنویسیم $(I,\sigma_1,\sigma_2,\sigma_3)$ و بسط دهیم. . از آنجایی ماتریسهای σ_i (i=1,2,3) مجموع عناصر قطریشان صفر است $Tr(\sigma_i)=0$ و $Tr(\rho)=1$ است، ضریب ماتریس چگالی ρ باید $\frac{1}{2}$ باشد.

$$\Rightarrow \quad \rho = r_0 I + \beta\sigma_1 + \gamma\sigma_2 + \delta\sigma_3$$
$$\rho = r_0 I + \vec{n}\cdot\sigma_i \qquad (۱۴\text{-}۲)$$

در فرمول بالا β,γ,δ مولفه‌های بردار $\vec{n}$ هستند و خواهیم داشت:

$$\rho_n = \frac{1}{2}(I + \vec{n}\cdot\vec{\sigma}_i) = \frac{1}{2}\begin{pmatrix} r_0+z & x-iy \\ x+iy & r_0-z \end{pmatrix} \qquad (۱۵\text{-}۲)$$

حال در نظر داریم که:

۱- ρ هرمیتی است. بنابراین ضرایب r_0,β,γ,δ همگی حقیقی هستند.

۲- $Tr(\rho)=1$. بنابراین $r_0=1$

۳- $\rho\geq 0$، برای بررسی این شرط باید ویژه مقادیر را حساب کنیم. ویژه مقادیر به صورت زیر است:

$$\lambda_{1,2} = \frac{1}{2}(1\pm n) \qquad (۱۶\text{-}۲)$$

و n اندازه‌ی بردار $\vec{n}$ است.

چون می‌دانیم باید دارای ویژه مقادیر مثبت باشد به همین دلیل n باید کمتر از یک باشد. پس یک تناظر یک به یک بین ماتریس چگالی یک کیوبیت و نقاط روی کره‌ی سه بعدی داریم، که این کره کره‌ی بلاخ نام دارد. هر عملگر یکانی را می‌توان با نوعی چرخش این کره متناظر ساخت. در مکانیک

کوانتومی کره‌ی بلاخ نمایش هندسی فضای حالت خالص یک سیستم کوانتومی دو حالتی است. نقـاط روی کره‌ی بلاخ نقاطی هستند که در آن‌ها $n=1$ و بنابراین، ویـژه مقـادیر برابـر بـا ۰ و ۱ هـستند. در نتیجه این نقاط متناظر با حالت‌های خالص هستند و برای مرکز کره ویژه‌مقادیر برابر بـا $\frac{1}{2}$ اسـت کـه نشاندهنده‌ی حالت کاملاً آمیخته[1] است.

(رد یک ماتریس در تمام تبدیلات ثابت است به عبارتی دوران یک ماتریس هرگز رد آن را عوض نمی-کند) پس ρ را دوران می‌دهیم تا قطری شود، اکنون رد آن باید برابر با ۱ باشد، پس اگر ویژه مقـادیر منفی شود غلط است، در این صورت ماتریس چگالی متناظر با نقطه‌ای در داخل کره است و ایـن کـره شعاعش یک است. تمام ماتریس‌های چگالی را می‌توان برحسب رابطه‌ی (۲-۱۵) نوشت.

قبلا نشان دادیم که هر اسپین را می‌توان بر حسب θ و φ نوشت، حال اگر به اندازه‌ی θ و φ دوران دهیم، اسپین دیگری بدست می‌آوریم. از ریاضی فیزیک می‌دانیم که $(\vec{n}.\vec{\sigma}_i)^2 = I$ است. اگر $\vec{n}$ یـک بردار یکه باشد، می‌توان حاصلضرب داخلی را بدست آورد پس در این صورت می‌تـوان گفـت $\vec{n}$ بـردار یکه‌ای است که نقاط روی سطح را جاروب می‌کند و جهت اسپین را نشان می‌دهد. پس بـرای حـالتی که نقاط روی کره مدنظر است می‌توان گفت:

$$\rho_n = \frac{1}{2}(I + \vec{n}\cdot\vec{\sigma}_i)$$

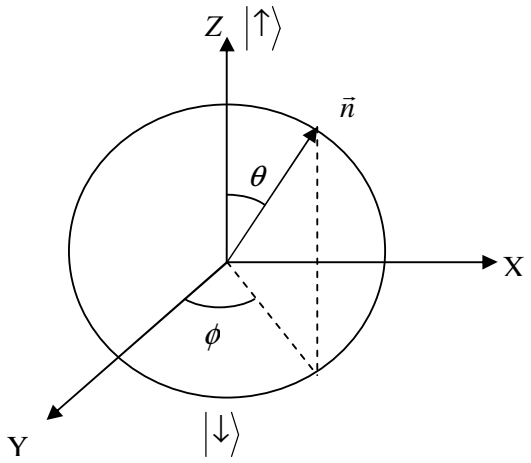
$$\rho_n = \frac{1}{2}((\vec{n}\cdot\vec{\sigma}_i)^2 + \vec{n}\cdot\vec{\sigma}_i) = \frac{1}{2}(\vec{n}\cdot\vec{\sigma}_i)((\vec{n}\cdot\vec{\sigma}_i)+1) = \rho_n(\vec{n}\cdot\vec{\sigma}_i) \qquad (۲\text{-}۱۷)$$

$$\rightarrow\ (\vec{n}\cdot\vec{\sigma}_i) = \rho_n \qquad \Rightarrow \qquad \rho_n^2 = \rho_n$$

حال با توجه به این مشخصه می‌فهمیم که ρ عملگر تصویر است پـس $\rho_n = |\psi_n\rangle\langle\psi_n|$. $|\psi\rangle$ بـه $\vec{n}$ وابسته است. مولفه‌های بردار یکه‌ی $\vec{n}$ در مختصات کروی به صورت زیر است:

$$\vec{n} = \sin\theta\cos\varphi\,\vec{i} + \sin\theta\sin\varphi\,\vec{j} + \cos\theta\,\vec{k} \qquad (۲\text{-}۱۸)$$

[1] Mixed state



شکل(۲-۳) $\vec{n}$ بردار کروی در کره‌ی بلاخ

پس هر حالت اسپین به یک نقطه روی کره بلاخ مربوط است که می‌توانـد روی آن توسـط بـردار یکـه معلوم شود. در آنسامبل خالص، همگی در یک حالت قرار گرفته‌اند و همه‌ی الکترون‌ها در یـک حالـت هستند

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$

اما آنسامبل مخلوط، به صورتی است که N_1 تای آن در حالت $|\psi_1\rangle$ و N_2 تای آن در حالت $|\psi_2\rangle$ و ... است و ماتریس چگالی آن‌ها متفاوت است.

$$P_1 \Rightarrow |\psi_1\rangle = \alpha_1|\uparrow\rangle + \beta_1|\downarrow\rangle \quad , \quad P_1 = \frac{N_1}{N}$$

$$P_2 \Rightarrow |\psi_2\rangle = \alpha_2|\uparrow\rangle + \beta_2|\downarrow\rangle \quad , \quad P_2 = \frac{N_2}{N}$$

$$P_3 \Rightarrow |\psi_3\rangle = \alpha_3|\uparrow\rangle + \beta_3|\downarrow\rangle \quad , \quad P_3 = \frac{N_3}{N}$$

و نهایتا می‌شود:

$$P_n \;\Rightarrow\; |\psi_n\rangle = \alpha_n |\uparrow\rangle + \beta_n |\downarrow\rangle \qquad , \qquad P_n = \frac{N_n}{N}$$

و $P_1 + P_2 + ... + P_n = 1$

حالت‌های آمیخته مربوط به نقاط داخل کره بلاخ می‌شود و در ماتریس چگالی آنها، عناصر غیرقطری صفر است اما حالت‌های خالص[1] مربوط به نقاط روی کره می‌شود و در ماتریس چگالی آنها همه‌ی عناصر غیر صفر هستند.

[1] Pure state

فصل سوم

معرفی چند پروتکل مهم

۳-۱ مقدمه

در این فصل به معرفی چند پروتکل مهم که نقش عمده‌ای در روند پیشرفت رمزنگاری کوانتومی داشتند، می‌پردازیم. در هر پروتکل هدف اصلی بدست آوردن کلید است که برای دقیق بودن هر چه بیشتر آن مراحل زیر روی آن اعمال می‌گردد:

۱. استخراج کلید خام: با استفاده از کانال کوانتومی یک رشته بیت بین فرستنده و گیرنده به اشتراک گذاشته می شود. پس از بررسی همبستگی‌ها، آن دسته که به علت وجود استراق سمع کننده با هم همبستگی ندارند حذف می‌شوند به گونه‌ای که تنها بخشی از رشته‌ی فرستنده و رشته‌ی گیرنده که برابر هستند، باقی می‌مانند. طول این بخش برابر به عوامل مختلفی از جمله نوع پروتکل، ویژگی‌های کانال و اینکه آیا استراق سمع کننده ارتباط را شنود می کند یا نه، بر می‌گردد.

۲. تصفیه: حذف بسیاری از بیت‌های رشته که در نزد گیرنده و فرستنده همبستگی ندارند. این کار برای حذف بیت‌های مخدوش به کار می رود بدون آنکه هیچ اطلاعاتی در مورد خود بیت‌ها بر روی کانال منتقل شود. پس از انجام این کار، طول این رشته‌ی تصفیه شده‌ای که در اختیار فرستنده و گیرنده قرار دارد، کوچکتر شده است که میزان کوچکتر شدن به ویژگی های کانال و اعمال شنود بستگی دارد.

۳. تصحیح خطا یا بازیابی کلید: بر اساس نوع پروتکل به کار گرفته شده، با استفاده از بیت‌های حذف شده در مرحله‌ی قبل، عملیات تصحیح خطا انجام می شود و با تخمین نرخ خطای بیت، مشخص می-کنند که آیا استراق سمع کننده وجود دارد یا نه. اگر نرخ خطای بیت از یک حد از پیش تعیین شده فراتر رود، فرستنده و گیرنده حدس می زنند که شنود صورت گرفته و پروتکل قطع شده و مراحل باید از سر گرفته شوند.

۴. تقویت محرمانه بودن: اگر نرخ خطای بیت کمتر از یک حد مشخص باشد، باز هم احتمال این وجود دارد که استراق سمع کننده بخشی از ارتباط را شنود کرده باشد و بنابراین، فرستنده و گیرنده

با حذف کردن بخشی دیگر از رشته بیت، سعی می کنند دانسته‌های استراق سمع کننده را باز هم کاهش دهند و این‌گونه نرخ محرمانه بودن کلید افزایش می‌یابد.

۳-۲ پروتکل BB84

رمزنگاری متعارف کلاسیکی مثل RSA کلید ایمنی لازم را ندارد مگر آنکه برای هر کاراکتر یک کلید رمز در نظر گرفته شود. در رمزنگاری کوانتومی از مفهوم دیگری به نام اصل عدم قطعیت در مکانیک کوانتومی استفاده شده است. در این روش فرستنده و گیرنده حتی در حضور استراق سمع کننده هم می‌توانند توزیع کلید کوانتومی را از طریق کانال‌های ارتباطی به صورت ایمن انجام دهند.

اولین پروتکل رمزنگاری توسط بنت[1] و براسارد[2] در سال ۱۹۸۴ ارائه شد که مبنای اصلی آن بر اساس درهم‌تنیدگی کوانتومی بنا شده است[۱۴] و همان‌طور که در شکل زیر آمده است، آلیس برای اندازه-گیری حالت تکتایی داده شده در سیستم، می‌تواند دو مشاهده پذیر σ_z و σ_x را انتخاب کند. اگر آلیس σ_z را اندازه بگیرد و $\left|\uparrow\right\rangle^z$ بدست آورد، باب در صورت انتخاب کردن σ_z برای اندازه‌گیری با توجه به حالت سیستم با احتمال ۱، $\left|\downarrow\right\rangle^z$ بدست می‌آورد ولی اگر σ_x را انتخاب کند با احتمال $\frac{1}{2}$، $\left|\uparrow\right\rangle^x$ و یا $\left|\downarrow\right\rangle^x$ بدست می‌آورد.

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

Alice	Bob
$\sigma_x \rightarrow \left\|\uparrow\right\rangle_x, \left\|\downarrow\right\rangle_x$	$\sigma_x \rightarrow \left\|\uparrow\right\rangle_x, \left\|\downarrow\right\rangle_x$
$\sigma_z \rightarrow \left\|\uparrow\right\rangle_z, \left\|\downarrow\right\rangle_z$	$\sigma_z \rightarrow \left\|\uparrow\right\rangle_z, \left\|\downarrow\right\rangle_z$

شکل (۳-۱) مشاهده پذیرهای فرستنده و گیرنده در پروتکل BB84

[1] Bennett
[2] Brassard

پس در این پروتکل دو راستای اندازه‌گیری داریم که یکی در راستای قائم (+)، برای فوتون‌های با پولاریزاسیون ۰درجه ($\rightarrow$) و ۹۰ درجه ($\uparrow$) هستند و دیگری راستای مورب (×)، برای فوتون‌های ۴۵ درجه ($\nearrow$) و ۱۳۵ درجه ($\searrow$) هستند و مراحل پروتکل به صورت زیر می‌باشد:

۱- ابتدا آلیس به طور تصادفی پایه‌های اندازه‌گیری خود را انتخاب می‌کند و فوتون‌ها را اندازه می‌گیرد و نتایج را بدون اعلام پایه‌ها از طریق کانال‌های عمومی برای باب ارسال می‌کند و این نکته مهم است که آلیس و باب پایه‌های همدیگر را نمی‌شناسند. اما نهایتا هر چه جواب بدست می‌آید باید با رابطه‌ی $|\psi\rangle$ سازگار باشد یعنی جواب $|\uparrow\rangle^z$، $|\downarrow\rangle^z$ و یا جواب $|\downarrow\rangle^x$ و $|\uparrow\rangle^x$ است.

۲- باب فوتون‌های ارسالی را دریافت کرده و خود با انتخاب پایه به طور تصادفی به اندازه‌گیری فوتون‌ها می‌پردازد.

۳- آلیس به صورت تصادفی تعدادی از پایه‌های انتخابی خود را برای باب اعلام می‌کند.

۴- پس از بررسی نتایج اگر نتایج مشترک بین آنها بیش از نصف انتخاب‌ها بود، آنها کلید را استخراج می‌کنند و در غیر این صورت به این معناست که احتمال وجود استراق سمع کننده بیش از نصف بوده و پروتکل قطع می‌گردد و اندازه‌گیری دوباره شروع می‌شود.

بیت‌های انتخابی آلیس	۰	۱	۱	۰	۰	۱	۱	۱
پایه‌های تصادفی آلیس	+	×	×	+	×	+	×	+
قطبش ارسال شده از طرف آلیس	$\rightarrow$	$\searrow$	$\searrow$	$\uparrow$	$\nearrow$	$\rightarrow$	$\searrow$	$\uparrow$
پایه‌ی تصادفی باب	+	×	+	×	×	×	+	+
قطبش اندازه‌گیری شده‌ی باب	$\rightarrow$	$\searrow$	$\uparrow$	$\searrow$	$\nearrow$	$\searrow$	$\uparrow$	$\uparrow$
کلید محرمانه‌ی توافق شده	۰	۱			۰			۱

جدول(۳-۱) نحوه‌ی محاسبه‌ی کلید در پروتکل BB84

حضور استراق سمع کننده در سیستم به صورت زیر برای آنها آشکار می‌شود. اگر استراق سمع کننده در میان آنها باشد و بخواهد اندازه‌گیری انجام دهد و پایه‌ی $|\uparrow\rangle^z$ را انتخاب کند، ممکن است پایه درست و یا اشتباه باشد، حال اگر درست باشد، در این صورت متوجه وجود استراق سمع کننده نمی-شوند اما اگر اشتباه باشد، با احتمال $\frac{1}{2}$ مثلا $|\uparrow\rangle^x$ را اشتباه می‌فرستد و باب با احتمال $\frac{1}{2}$، $|\uparrow\rangle^z$ و با احتمال $\frac{1}{2}$، $|\downarrow\rangle^z$ بدست می‌آورد. در این صورت پس از بررسی نتایج متوجه حضور استراق‌سمع‌کننده می‌شوند.

در محاسبه‌ی ایمنی پروتکل معتقدیم احتمال این‌که استراق سمع کننده پایه‌ی غلط را انتخاب کند $\frac{1}{2}$ است و احتمال این که باب پایه‌ای مشابه با آلیس انتخاب نماید، $\frac{1}{2}$است. بنابراین احتمال اینکه یک فوتون آشکار شده جوابی غلط در کلید ایجاد کند $\frac{1}{4}$ است. یعنی با احتمال $\frac{3}{4}$ جواب درست است. آلیس و باب n تا از بیت‌های کلیدشان را به طور عمومی با هم مقایسه می‌کنند تا از محرمانه بودن کلید اطمینان حاصل نمایند. احتمال اینکه هیچ خطایی پیدا نکنند $\left(\frac{3}{4}\right)^n$ است پس احتمال این که خطایی پیدا شود برابر است با:

$$p = 1 - \left(\frac{3}{4}\right)^n$$

خلاصه آنکه با احتمال خیلی خوبی می‌توان تشخیص داد که استراق سمع کننده وجود دارد یا نه. از طریق زیاد کردن تعداد کیوبیت‌ها و یا اعلام نتایج مشترک، می‌توان خطاها را کم و کمتر کرد. این پروتکل آن‌قدر تکرار می‌شود تا از عدم حضور استراق سمع کننده اطمینان حاصل شود. البته این را می‌دانیم که استراق سمع کننده به دلیل خاصیت تکثیرناپذیری در کامپیوترهای کوانتومی، نمی‌تواند پس از گرفتن اطلاعات از آن کپی بگیرد و برای باب بفرستد و علت آن، این است که کیوبیت پس از اندازه‌گیری فروریزش می‌کند چون حالت کوانتومی پس از فروریزش حالت قابل بازیافت نیست، زیرا

مثلا حالت $\alpha|\uparrow\rangle_z + \beta|\downarrow\rangle_z$ پس از اندازه‌گیری متلاشی شده و قابل بازسازی نیست. چون نمی دانیم α و β چه مقدار بوده، فقط می‌توانیم کیوبیت را اندازه بگیریم و متلاشی می‌شود. در صورتی می-توان آن‌ها را اندازه گرفت که بینهایت α و β داشته باشیم و ببینیم چند درصد $|\uparrow\rangle_z$ و چند درصد $|\downarrow\rangle_z$ می‌شود. پس در این حالت می‌توان مقدار آن‌ها را به دست آورد. حال پس از متوجه شدن عدم حضور استراق سمع کننده، می توان رشته را فرستاد. چون ایمنی سیستم تضمین شده است. این رشته ارسال شده همان رشته بیت کلید است و باب پس از گرفتن این رشته، رشته‌ی رمزی شده‌ای که قبل از آن از طریق کانال کوانتومی فرستاده شده بود، رمزگشایی می‌کند و پیام را می‌فهمد. این روش دارای این حسن است که حضور استراق سمع کننده را می‌توان تشخیص داد و این رشته را هرگز کسی به جز باب و آلیس نمی‌داند، اما در کامپیوترهای کلاسیکی این اتفاق نمی‌افتد و این به واسطه‌ی این دو موضوع است که عبارتند از:

۱- اینکه کیوبیت‌های کوانتومی قابل کپی کردن نیستند.

۲-هر کیوبیت پس از اندازه‌گیری فروریزش می‌کند و یا به عبارتی پس از مختل شدن کیوبیت‌ها، دیگر بازسازی نمی‌شود. البته مشکل دیگری هم ممکن است پیش آید و آن اینکه سیگنال ارسالی در کانال-های کوانتومی باعث ایجاد چرخش در سیگنال ارسالی می‌شود به عبارتی اگر $|\uparrow\rangle$ را بفرستد، ممکن است با کمی انحراف منتقل شود پس در این صورت خطایی ایجاد می‌شود که البته این قابل اندازه-گیری است. پس خطای ناشی از این محیط به راحتی قابل کنترل است، به عبارتی خطای ناشی از استراق سمع کننده قابل تشخیص است.

چند سال بعد ایکرت[1] ایده‌ی جدیدی برای رمزنگاری ارائه داد که بر مبنای همبستگی‌های میان ذرات درهم‌تنیده‌ای که باهم به اشتراک گذاشته شده‌اند، می‌باشد[۱۵] و شرح پروتکل ایکرت به طور مختصر در زیر آمده است و امنیت این پروتکل از طریق غیرموضعیت قابل بررسی است.

[1] Ekert

۳-۳ پروتکل ایکرت

این پروتکل از طریق آنالیزورهایی که در کره‌ی بلاخ، زوایای مشخصی دارند کار می‌کنند. به این صورت که طبق شکل زیر آلیس زوایای $\phi = 0, \frac{\pi}{4}, \frac{\pi}{2}$ و باب $\phi = \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}$ انتخاب می‌کنند.

Alice	Bob
$a_1 \rightarrow \varphi_1^a = 0$	$b_1 \rightarrow \varphi_1^b = \frac{\pi}{4}$
$a_2 \rightarrow \varphi_2^a = \frac{\pi}{4}$	$b_2 \rightarrow \varphi_2^b = \frac{\pi}{2}$
$a_3 \rightarrow \varphi_3^a = \frac{\pi}{2}$	$b_3 \rightarrow \varphi_3^b = \frac{3\pi}{4}$

شکل(۳-۲) مشاهده‌پذیرهای پروتکل ایکرت

هر دو، سه انتخاب برای اندازه‌گیری حالت سیستم یگانه دارند. پس از اینکه پیام‌ها ارسال شد، آلیس و باب آنالیزورهای انتخابی خود را برای هم اعلام می‌کنند. انتخاب‌های آنها به دو دسته تقسیم می‌شود: گروه اول آنالیزورهایی که دارای زوایای سمتی مشابه هستند، می‌باشد که از آنها برای بررسی همبستگی میان نتایج استفاده می‌کنیم. به طوری که پس از اعلام اندازه‌گیری ها تمام آنهایی که دارای همبستگی نیستند، حذف می‌کنیم و از بقیه کلید را استخراج می‌کنیم.

گروه دوم آنهایی هستند که آنالیزورهای‌شان با هم زوایای سمتی نامشابه دارند. نتیجه‌ی آنالیزورها بر حسب $\frac{\hbar}{2}$ است و نتایج اندازه‌گیری ± 1 می‌باشد که معرف اسپین بالا یا پایین هستند و از طریق یک کیوبیت اطلاعاتی آشکارسازی می‌شوند:

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j) \qquad (۱-۳)$$

نتایج اندازه‌گیری $P_{\pm\pm}(a_i,b_j)$، همواره ± 1 است. به عبارتی نتیجه‌ی اندازه‌گیری a_i، ± 1 و نتیجه‌ی اندازه‌گیری b_j، ± 1 خواهد بود. پس طبق قوانین کوانتومی خواهیم داشت:

$$E(a_i,b_j) = -a_i.b_j = -\cos\theta \qquad (۲-۳)$$

که θ زاویه‌ی میان دو آنالیزور است و طبق روابط بالا با توجه به آن‌که $a_1 = 0$, $a_3 = \frac{\pi}{2}$, $b_1 = \frac{\pi}{4}$, $b_3 = \frac{3\pi}{4}$ خواهیم داشت:

$$\begin{aligned} E(a_1,b_1) &= -\cos(\frac{\pi}{4}) = -\frac{\sqrt{2}}{2} \\ E(a_1,b_3) &= -\cos(\frac{3\pi}{4}) = \frac{\sqrt{2}}{2} \\ E(a_3,b_1) &= -\cos(\frac{\pi}{4}) = -\frac{\sqrt{2}}{2} \\ E(a_3,b_3) &= -\cos(\frac{\pi}{4}) = -\frac{\sqrt{2}}{2} \end{aligned} \qquad (۳-۳)$$

در این صورت رابطه بل به صورت زیر بدست می‌آید:

$$\left|E(a_1,b_1) - E(a_1,b_3) + E(a_3,b_1) + E(a_3,b_3)\right| \le 2\sqrt{2} \qquad (۴-۳)$$

حال در زیر نحوه ی سنجیدن سیستم برای حضور یا عدم حضور استراق سمع کننده با استفاده از نامساوی بل را شرح می دهیم. مثالی از نامساوی بل:

Alice	Bob
1) σ_z 0,1	1) σ_z 0,1
2) σ_x 0,1	2) σ_x 0,1

شکل(۳-۳) مشاهده‌پذیرهای انتخابی در نامساوی بل

فرض می‌کنیم آلیس در دوحالت می‌تواند اندازه‌گیری را انجام دهد، که اینجا σ_z را اندازه می‌گیرد و شماره‌ی ۱ می‌گذاریم و برای σ_x شماره‌ی ۰ را می‌گذاریم. برای باب هم به همین ترتیب. اگر ورودی-های سیستم را σ_z و σ_x و خروجی‌های a و b هر کدام برابر با ۰ و ۱ قرار دهیم (برای سیستم دوحالتی) احتمالات سیستم را این‌گونه تعریف می‌کنیم $P(a,b|x,y) \equiv P_{x,y}^{a,b}$، نامساوی بل اینگونه بدست می‌آید:

احتمال اینکه آلیس ۱ را داشته باشد یعنی σ_z را اندازه بگیرد و مقدار ۱ را بدست آورد و باب هم ۱ را بگیرد و یعنی σ_z را اندازه بگیرد و مقدار ۰ را بدست آورد به این صورت نمایش می‌دهیم، $P_{1,1}^{1,0}$ و احتمال اینکه آلیس ۱ را داشته باشد یعنی σ_z را اندازه بگیرد و مقدار ۰ را بدست آورد و باب هم ۲ را بگیرد و یعنی σ_x را اندازه بگیرد و مقدار ۰ را بدست آورد به صورت $P_{1,2}^{0,0}$ نمایش می‌دهیم، و احتمال اینکه آلیس ۲ را داشته باشد یعنی σ_x را اندازه بگیرد و مقدار ۰ را بدست آورد و باب هم ۱ را بگیرد و یعنی σ_z را اندازه بگیرد و مقدار ۱ را بدست آورد به صورت $P_{2,1}^{0,1}$ نمایش می‌دهیم، و احتمال اینکه آلیس ۲ را داشته باشد یعنی σ_x را اندازه بگیرد و مقدار ۰ را بدست آورد و باب هم ۲ را بگیرد و یعنی σ_x را اندازه بگیرد و مقدار ۰ را بدست آورد به این صورت نمایش می‌دهیم، $P_{2,2}^{0,0}$ می‌توان گفت:

$$0 \le P_{11}^{10} + P_{12}^{00} + P_{21}^{01} - P_{22}^{00} \le 1 \qquad (۵-۳)$$

که در حالت کلاسیکی این حدود برقرار است ولی اگر حالت سیستم درهم‌تنیده باشد، مثلا $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. در این صورت به جای آنکه این نامساوی کوچکتر و مساوی ۱باشد، کوچکتر و مساوی $\sqrt{2}$ است، در این صورت نامساوی بل نقض می‌شود، پس اگر درهم‌تنیده باشد، نامساوی بل نقض می‌شود و با نقض این نامساوی غیرموضعیت هم پدیدار می‌شود. حال چگونه آلیس و باب متوجه حضور استراق سمع کننده می‌شوند؟ اگر کسی در این میان جاسوسی کند این حالت که درهم‌تنیده است به حالت حاصل‌ضرب تبدیل می‌شود (یعنی استراق سمع کننده این میان سیستم را مغشوش

می‌کند و به $|01\rangle$ و یا $|10\rangle$ تبدیل می‌شود که در آن صورت دیگر درهم‌تنیده نیست و احتمال بین ۱و۰ می‌شود و نمی‌توان در رابطه با حضور استراق سمع کننده حرفی زد ولی اگر رابطه میان 0 و $\sqrt{2}$ بود این دلیل بر عدم حضور استراق سمع کننده است.

ایده بعدی توسط بنت و براسارد و مرمین[1] ارائه شد که نقطه‌ی قوتی در رمزنگاری کوانتومی شد[۱۶] و این پروتکل در زیر آمده است:

۳-۴ پروتکل BBM

بر خلاف $BB84$ که برحسب پایه‌های متعامد $|\pm\rangle$ و یا $|\uparrow\rangle,|\downarrow\rangle$ هستند، $B92$ برحسب پایه‌های نامتعامد، $|\uparrow\rangle$ و $|\rightarrow\rangle$ که به ترتیب روی کره‌ی بلاخ در راستای محور x و z می‌باشند و اپراتورهای تصویر آن به صورت زیر نوشته می‌شوند:

$$P_0 = 1-|\uparrow\rangle\langle\uparrow| \qquad (۶-۳)$$
$$P_1 = 1-|\rightarrow\rangle\langle\rightarrow|$$

و $\alpha = \left|\langle\uparrow|\rightarrow\rangle\right|^2$ خواهیم داشت و α مقداری مثبت است.

Alice	Bob
$a_1 \rightarrow \|\uparrow\rangle$	$b_1 \rightarrow \|\uparrow\rangle$
$a_2 \rightarrow \|\rightarrow\rangle$	$b_2 \rightarrow \|\rightarrow\rangle$

شکل(۳-۴) مشاهده‌پذیرهای انتخابی در پروتکل B92

احتمال اینکه در P_0، $|\uparrow\rangle$ داشته باشیم، ۰ است. پس مقدار چشم داشتی آن هم صفر است. در این راستا هیچ تصویری ندارد، حال اگر P_0 روی $|\uparrow\rangle$ اثر کند، داریم:

$$(۷-۳)$$

[1] Mermin

$$\langle\uparrow|P_0|\uparrow\rangle = \langle\uparrow|(1-|\uparrow\rangle\langle\uparrow|)|\uparrow\rangle = \langle\uparrow|\uparrow\rangle - \langle\uparrow|\uparrow\rangle\langle\uparrow|\uparrow\rangle = 0$$
$$\Rightarrow \qquad \langle\uparrow|P_0|\uparrow\rangle = 0$$

و اگر P_1 روی $|\uparrow\rangle$ اثر کند، خواهیم داشت:

$$\langle\uparrow|P_1|\uparrow\rangle = \langle\uparrow|(1-|\rightarrow\rangle\langle\rightarrow|)|\uparrow\rangle = \langle\uparrow|\uparrow\rangle - \langle\uparrow|\rightarrow\rangle\langle\rightarrow|\uparrow\rangle$$
$$= 1-|\langle\uparrow|\rightarrow\rangle|^2 = 1-\alpha \qquad (۸\text{-}۳)$$
$$\Rightarrow \qquad \langle\uparrow|P_1|\uparrow\rangle = 1-\alpha \geq 0$$

و به همین ترتیب:

$$\langle\rightarrow|P_0|\rightarrow\rangle = \langle\rightarrow|(1-|\uparrow\rangle\langle\uparrow|)|\rightarrow\rangle = \langle\rightarrow|\rightarrow\rangle - \langle\rightarrow|\uparrow\rangle\langle\uparrow|\rightarrow\rangle$$
$$= 1-|\langle\rightarrow|\uparrow\rangle|^2 = 1-\alpha \qquad (۹\text{-}۳)$$
$$\Rightarrow \qquad \langle\rightarrow|P_0|\rightarrow\rangle = 1-\alpha \geq 0$$

و

$$\langle\rightarrow|P_1|\rightarrow\rangle = \langle\rightarrow|(1-|\rightarrow\rangle\langle\rightarrow|)|\rightarrow\rangle = \langle\rightarrow|\rightarrow\rangle - \langle\rightarrow|\rightarrow\rangle\langle\rightarrow|\rightarrow\rangle = 0 \qquad (۱۰\text{-}۳)$$
$$\Rightarrow \qquad \langle\rightarrow|P_1|\rightarrow\rangle = 0$$

حال اگر آلیس رشته بیتی برای باب بفرستد، طبق معادلات بالا پیش می‌رویم. به طوری که آلیس یک سری حالت‌ها شامل $|\uparrow\rangle$ و $|\rightarrow\rangle$ به صورت تصادفی برای باب می‌فرستد، ضمنا در این پروتکل $|\uparrow\rangle$ معرف ۰ و $|\rightarrow\rangle$ معرف ۱ است. حال فرض می‌کنیم آلیس رشته‌ی زیر را برای باب بفرستد،

10011001 $\qquad |\rightarrow\rangle|\uparrow\rangle|\uparrow\rangle|\rightarrow\rangle|\rightarrow\rangle|\uparrow\rangle|\uparrow\rangle|\rightarrow\rangle$

آنگاه باب اپراتورهای تصویر را اندازه می‌گیرد و به صورت تصادفی P_0 و P_1 را روی آنها اثر می‌دهد، آنهایی که نتیجه‌ی مثبت می‌گیرد، درست محاسبه شده‌اند و آنهایی که نتیجه‌ی ۰ می‌دهند رد می‌شوند:

P_1	P_0	P_1	P_1	P_0	P_0	P_1	P_0
$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$
0	0	+	0	+	0	+	+

جدول(۳-۲) نحوه‌ی محاسبه‌ی کلید در پروتکل B92

باب نتایج را به آلیس گزارش می‌دهد و مثلا می‌گوید شماره‌های ۳ و ۵ و ۷ و ۸، + هستند و آلیس می‌داند که شماره‌های ارائه شده چه هستند. پس می‌فهمد که باب چه کار کرده، پس کلید رمز را تا این‌جا 0101 در نظر می‌گیرند. حالا برای سنجش حضور یا عدم حضور استراق سمع کننده باید قبل از ارسال کل پیام به صورت تصادفی چند اندازه‌گیری را برای هم ارسال کنند، مثلا شماره ۵ را می‌گوید P_1 اعمال کردیم و + بدست آمده است. اگر مغشوش شده باشد این‌گونه آلیس می‌فهمد که استراق-سمع کننده حضور دارد و در این صورت پروتکل را متوقف کرده و دوباره از اول شروع می‌کنند.

پس از آنها بارت و هاردی و کنت[۲۱] پروتکلی برای رمزنگاری ارائه کردند که در آن پروتکل فقط به غیر موضعیت توجه داشتند و این بسیار حائز اهمیت است چرا که منجر به پروتکل‌های مستقل از دستگاه شد یعنی عملکرد این پروتکل‌ها به گونه‌ای است که حتی اگر استراق سمع کننده حالت سیستم را توزیع کرده باشد، باز هم ایمنی حفظ می‌شود و اطلاعات به صورت ایمن منتقل می‌گردد.

فصل چهارم

پروتکل مستقل از دستگاه

۴-۱ مقدمه

در پروتکل BB84 آلیس حالات سیستم را اندازه می‌گیرد و این‌گونه آلیس تعیین می‌کند که باب باید چه حالتی را برای سیستم بدست آورد. به همین دلیل می‌گوییم که در این پروتکل، آلیس حالت سیستم را توزیع می‌کند و پروتکل کاملا وابسته به دستگاه است[۱۴]. ما برای امنیت بیشتر سیستم به دنبال رفع این مشکل هستیم[۳۲]، چرا که اگر به جای آلیس استراق سمع کننده[1] حالت را توزیع کند، در این صورت خطا زیاد شده و اطلاعات ارسالی به خطر می‌افتد. در این پایان نامه به بررسی چگونگی رفع این مشکل می‌پردازیم یعنی به دنبال پروتکلی هستیم که مستقل از دستگاه[2] باشد. منبع اصلی که در این راه ما را یاری می کند یکی از خصوصیات مهم جهان کوانتومی، وابستگی به زمینه[3] است که در متناقض نمای کوشن- اسپکر[4][۱۹] متبلور شده است. نهایتاً ما به دنبال پروتکلی شبیه به BBM هستیم[۱۶] به طوری که به دستگاه وابسته نباشد.

۴-۲ پروتکل مستقل از دستگاه

این پروتکل براساس یک جفت سیستم است که یکی نزد آلیس باقی می ماند ودیگری به سمت باب ارسال می شود، این‌گونه اطلاعات به دست استراق سمع کننده نمی‌رسد. در این پروتکل علاوه بر وابستگی به زمینه به طور ضمنی غیرموضعیت هم شرکت دارد، در ادامه خواهیم دید که در حقیقت ارتباط عمیقی میان متناقض‌نمای کوشن-اسپکر و نامساوی بل[۱۰] برقرار است [۲۷]. پس برای بررسی امنیت سیستم یا اثبات عدم حضور استراق سمع کننده، به دنبال نقض یک نامساوی بل براساس همبستگی‌ها، هستیم. نقض این نامساوی از طریق اصل مهمی به نام اصل علیت اطلاعات انجام می‌شود [۲۴]. این اصل یک مفهوم مهم در فیزیک کوانتومی است که در نتیجه‌ی اصل عدم

[1] Eve(Evesdropper)
[2] Divise-indeendent
[3] contextuality
[4] Kochen-Speker paradox

علامت‌دهی به وجود می‌آید و بر این دلالت دارد که بـرای مـا همبـستگی‌هـای قـوی‌تـر از قـوی‌تـرین همبستگی‌های کوانتومی ایجاد می‌کند.

این اصل به عنوان نتیجه باعث بروز خـصوصیاتی مثـل تکثیرناپـذیری و تـصادفی ذاتـی[1] در مبادلـه‌ی اطلاعات در سیستم می‌شود. در این‌جا از مفهوم جعبه‌ای که شامل مجموعه‌ای از توزیـع‌هـای احتمـال است، استفاده خواهیم کرد، منظور از جعبه این است که تعداد مشخصی ورودی و خروجـی دارد و هـر خروجی متناظر با یک ورودی مخصوص به خود است. ورودی‌ها، مشاهده‌پذیرهـای سـاده‌ای هـستند و جعبه، مکانیک کوانتومی را ارضا می کند یعنی از طریق فیزیکی قابل فهم است، بـه بیـان دیگـر چـون تعداد توزیع‌های احتمال، مشخص و متناهی است، آنها به صورت آماری بدون هیچ اطلاعاتی راجـع بـه چگونگی ساخته شدن سیستم قابل آزمایش هستند و خروجی‌ها نتیجه‌ی اندازه‌گیری مـشاهده‌پـذیرها هستند. در این پروتکل، این جعبه‌ها از طریق متناض‌نمای‌کوشن- اسپکر کار می‌کنند یعنی یک جعبـه دو طرفه کوشن- اسپکر خواهد بود که ویژگی‌های آن عبارتند از:

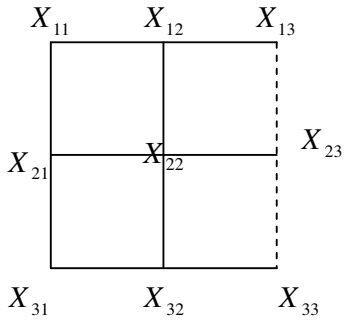
این جعبه نتایج موضعی شرایط کوشن-اسپکر(KS)[۱۹] که بعداً توضیح داده خواهد شد، را ارضا مـی-کند که آن‌ها باید از مشاهده‌پذیرهایی که نمی‌توانند به طور همزمان اندازه گیری شوند (یعنی بـا هـم جا به جا نمی‌شوند) استفاده کنند و از طرف دیگر اگر مشاهده‌پذیرهای انتخابی آلـیس و بـاب بـا هـم یکسان باشند، با هم همبستگی کامل خواهند داشت، البته در ادامه اثبات خواهیم کرد کـه در شـرایط ایده‌آل، در این چنین حالتی تقریباً نصف ایمنی سیستم تضمین می‌شود.

۴-۳ جعبه‌های پرس-مرمین

برای به اشتراک گذاشتن یک پیام کوانتومی با توجه به همبستگی‌های کوانتومی، می‌تـوان اطلاعـات را با استفاده از جعبه‌های پرس-مرمین [۲۵] و [۲۶] که از شرط عـدم علامـت‌دهـی تبعیـت مـی‌کننـد،

[1] Intrinsic randomness

فرستاد. در این جعبه‌ها از روش پرس- مرمین[1] که بیانی واضح‌تر از متناقض‌نمای کوشن- اسپکر است را مدنظر قرار می‌دهیم. همانطور که در شکل ۱ مشاهده می‌شود، جعبهٔ پرس- مرمین که به اختصار آن را جعبهٔ PM می‌نامیم، مجموعه‌ای از توزیع‌های احتمال توأمان است که هر توزیع احتمال از ۳ مشاهده پذیر تشکیل شده است. این جعبه دارای ۹ مشاهده پذیر به عنوان ورودی است که آرایه‌های یک ماتریس ۳×۳ را می‌سازد و در هر سطر یا ستون مشاهده‌پذیری‌های دوطرفه می‌توانند به طور همزمان اندازه‌گیری شوند، ولی نمی‌توان همه‌ی ۹ مشاهده پذیر را همزمان اندازه گرفت و ما انتظار داریم که این جعبه شرایط زیر را ارضا کند، یعنی اینکه حاصل ضرب نتایج اندازه‌گیری توزیع‌های احتمال توأمان[2] در سطرها برابر با مقدار ۱+ و حاصل ضرب نتایج اندازه‌گیری توزیع‌های احتمال توأمان در ستون‌ها برابر با مقدار ۱- است و این شرایط KS است.



شکل(۴-۱) ماتریس 3×3 که هر X_{ii} ، یک مشاهده‌پذیر است.

اگر برای ماتریس بالا مشاهده‌پذیرها را شبیه به جدول (۴-۱) انتخاب کنیم و یک سیستم دودویی را مدنظر قرار دهیم، σ^i ماتریس های پائولی سیستم i ام است که برای هر سطر یا ستون، می‌توان مشاهده‌پذیرها را به طور همزمان اندازه گرفت. نظریه‌ای که توسط انیشتین و بوهر روی آن بحث شد، این بود که آن‌ها معتقد بودند مقادیر کوانتومی از قبل وجود داشته و ما آن‌ها را طی شرایطی آشکار

[1] Peres-Mermin version
[2] Joint probability

می‌کنیم. مکانیک کوانتومی با آن‌ها مخالف است و معتقد است که حالات کوانتومی مقادیر مشخص ندارند، چرا که اگر این‌گونه بود، باید طی هر شرایطی یک مقدار بدست می‌آمد اما با توجه به متناقض-نمای‌کوشن- اسپکر اثبات شد که بسته به زمینه‌ی اندازه گیری، حاصل‌ضرب مقادیر آن‌ها یا ۱+ و یا ۱- می‌باشد و این یعنی وابستگی به زمینه. در این شرایط مشاهده‌پذیرهای هر سطر و هر ستون با هم جا به جا می‌شوند و به عبارتی به طور همزمان قابل اندازه‌گیری هستند اما یک مشاهده‌پذیر از سطر و یکی از ستون را نمی‌توان همزمان اندازه گرفت، پس به همین دلیل نمی‌توان همه‌ی ۹ مشاهده‌پذیر را همزمان اندازه گرفت. نهایتاً متناقض‌نمای‌کوشن-اسپکر برحسب نامساوی‌هایی معرفی شد که وابستگی به زمینه را بررسی می‌کردند.

σ_z^1	σ_z^2	$\sigma_z^1\sigma_z^2$
σ_x^2	σ_x^1	$\sigma_x^2\sigma_x^1$
$\sigma_z^1\sigma_x^2$	$\sigma_z^2\sigma_x^1$	$\sigma_y^1\sigma_y^2$

جدول (۴-۱) جدول ماتریس‌های پائولی که مشاهده می‌شود به عنوان مشاهده‌پذیرهای سیستم در نظر می‌گیریم.

در زیر ابتدا طبق جدول بالا، اثبات خواهیم کرد که گفته‌های بالا درست است یعنی مشاهده‌پذیرهای هر سطر یا ستون (هر توزیع احتمال) همزمان قابل اندازه‌گیری است و سپس وابستگی به زمینه را اثبات خواهیم کرد. اگر مثلاً سطر اول را در نظر بگیریم، خواهیم داشت:

$$[\sigma_z^1,\sigma_z^2]=0$$
$$[\sigma_z^1,\sigma_z^1\sigma_z^2]=\sigma_z^1[\sigma_z^1,\sigma_z^2]+[\sigma_z^1,\sigma_z^1]\sigma_z^2=0 \qquad (۱-۴)$$
$$[\sigma_z^2,\sigma_z^1\sigma_z^2]=\sigma_z^1[\sigma_z^2,\sigma_z^2]+[\sigma_z^2,\sigma_z^1]\sigma_z^2=0$$

اما مثلاً برای مشاهده‌پذیری از سطر اول و سطر دوم این شرط وجود ندارد.

$$[\sigma_z^1, \sigma_x^1] \neq 0 \qquad (۲-۴)$$

حال به اثبات وابستگی به زمینه می‌پردازیم، اگر سطر سوم و ستون سوم را مدنظر قرار دهیم، با توجه به شرایط مقابل خواهیم داشت:

$$\begin{aligned} &\left[\sigma_i^1, \sigma_j^2\right] = 0 \\ &\sigma_i^1 \sigma_j^1 = i\varepsilon_{ijk}\sigma_k^1 \end{aligned} \qquad (۳-۴)$$

$$\begin{aligned} &row: \sigma_z^1\sigma_x^2\sigma_z^2\sigma_x^1\sigma_y^1\sigma_y^2 = \sigma_z^1\sigma_x^2\sigma_x^1\sigma_z^2\sigma_y^1\sigma_y^2 \\ &= \sigma_z^1\sigma_x^1\sigma_x^2\sigma_z^2\sigma_y^1\sigma_y^2 = i\sigma_y^1(-i)\sigma_y^2\sigma_y^1\sigma_y^2 = +1 \\ &column: \sigma_z^1\sigma_z^2\sigma_x^2\sigma_x^1\sigma_y^1\sigma_y^2 = \sigma_z^1 i\sigma_y^2\sigma_x^1\sigma_y^1\sigma_y^2 \\ &= i\sigma_z^1\sigma_x^1\sigma_y^2\sigma_y^1\sigma_y^2 = i\sigma_y^1 i\sigma_y^2\sigma_y^1\sigma_y^2 = -1 \end{aligned} \qquad (۴-۴)$$

همانطور که مشاهده شد، ترتیب قرار گرفتن مشاهده‌پذیرها در جواب آن‌ها تأثیر می‌گذارد و این همان وابستگی به زمینه است. حال جعبه‌ی PM توزیع شده در جدول (۴-۱) را مدنظر قرار داده و تصادفی ذاتی را روی آن بررسی می کنیم:

جعبه‌ای که تعریف کردیم ما بین آلیس و باب به طور مشترک اندازه‌گیری می‌شود که مشاهده-پذیرهای آن به صورت موضعی شرایط اشاره شده را به صورت زیر ارضا می‌کنند (شرایط KS و همبستگی های AB). وقتی آلیس در ستون اول σ_z^1 را اندازه می‌گیرد، در کل جعبه σ_z^1 را نداریم و این یعنی زمینهٔ آزمایش یکی است و آلیس در ۹ زمینه می‌تواند سیستم را اندازه بگیرد و برای باب هم وضع به همین ترتیب است. به علاوه ما همبستگی‌های AB هم در نظر می‌گیریم یعنی که همبستگی‌های کاملی میان نتایج مشاهده‌پذیرهای مشابه در طرف آلیس و باب وجود دارد. به این گونه که اگر آلیس، σ_z^1 را اندازه بگیرد و باب هم σ_z^1 را اندازه بگیرد و با توجه به حالت در هم‌تنیده‌ی

اصلی سیستم، آن‌ها باید با هم همبستگی داشته باشند. همچنین در این جعبه شرط دیگری به نام عدم علامت‌دهی را مورد بررسی قرار می‌دهیم و همانطور که قبلا اشاره شد، بر این معناست که هر چه آلیس اندازه می‌گیرد نمی‌تواند با سرعت بیشتر از سرعت نور به باب منتقل شود یا به عبارت دیگر، مجموع احتمال‌های طرف آلیس برای یک سیستم باید مستقل از مجموع احتمالات طرف باب باشد.

حال تأکید می‌کنیم که جعبه‌ی PM بصورت ضروری بر غیرموضعیت دلالت دارد. در واقع عدم وابستگی به زمینه به غیرموضعیت تبدیل می‌شود. به طور کلی جعبه‌ی تعریف شده از ۹ توزیع شرطی $p(\vec{ab}|\vec{x},\vec{y})$ که در اینجا $A=1,2,3$ و $B=1,2,3$ که شماره‌ی درآیه‌ی سطر یا ستون است و $a=a_1\,a_2\,a_3$ که نتایج اندازه گیری آلیس هستند و $b=b_1\,b_2\,b_3$ که نتایج اندازه گیری باب در سطرهاست و شرایط زیر به طور کلی حاکم است.

۱) شرایط KS : برای $A=1,2$ و $B=1,2,3$ نتایج اندازه گیری توزیع‌های احتمال ۱+ است یعنی سطرها و ستون ما قبل آخر، $a\in\{+++,+--,-+-,--+\}$ و برای $A=3$ و $B=1,2,3$ نتایج اندازه‌گیری توزیع‌های احتمال توأمان ۱- یعنی ستون سوم که شامل، $a\in\{---,-++,+-+,++-\}$ است.

۲) شرایط همبستگی AB : برای $A=i$ و $B=j$ نتایج اندازه‌گیری $a_i=b_j$ است به عبارت دیگر به ازای انتخاب مشاهده‌پذیرهای مشابه برای دو طرف باید ویژه مقادیر یکسان در دو طرف بدست آید.

۳) شرط عدم علامت دهی : مجموع احتمال اندازه گیری روی سیستم A مستقل از مجموع احتمالات اندازه گیری روی سیستم B است.

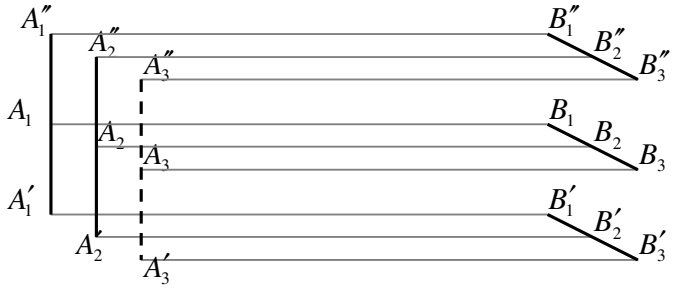
۴-۴ تصادفی ذاتی از جعبه PM توزیع شده ایده‌آل

ما اکنون فرض خواهیم کرد که یک جعبهٔ PM توزیع شده، مکانیک کوانتومی را ارضا می کند و در این صورت ما در یک الگوی امنیت مستقل از دستگاه هستیم[۲۳] که فرض می شود، مکانیک کوانتومی معتبر است.

حال به دنبال این هستیم نشان دهیم که در سطر اول طرف باب، طبق گفته‌ی مکانیک کوانتومی همه مشاهده‌پذیرها نمی‌توانند مقادیر قطعی ۰ و ۱ را داشته باشند ولی باید حاصلضرب آن‌ها مقدار ۱+ باشد. پس می‌تواند چهار حالت $(+++,+--,-+-,--+)$ را داشته باشد. با فرض اینکه مقادیر در سطر اول همگی ۱+ باشند و با استفاده از شرایط KS و همبستگی‌های AB، یک سیستم همبسته را تعیین خواهیم کرد. باتوجه به شرایط KS داریم، $B_3 = B_1 B_2$ و $B_3' = B_1' B_2'$. (این شرایط را برای طرف A نمی‌توان در نظر گرفت، چون آن‌ها سطرها را محاسبه نکرده‌اند.)

فرض می‌کنیم که سطر بالایی باب با قطعیت نتایج $+++$ را بدهد، این بدان معنی است که با توجه به همبستگی‌های AB مشاهده‌پذیرهای سطر بالایی از هر سطر آلیس، مقدار ۱+ را بدهد، به عبارت دیگر با توجه به شکل(۴-۲) با قطعیت خواهیم داشت:

$$A_1'' = +1 \quad , \quad A_2'' = +1 \quad , \quad A_3'' = +1 \qquad (۵\text{-}۴)$$



شکل(۴-۲) ارتباط میان آلیس و باب در پروتکل مستقل از دستگاه، به طوری که هر کدام ۹ مشاهده‌پذیر دارند که با هم همبستگی دارند.

بنابراین به علت شرایط KS خواهیم داشت:

$$A_1 = A_1' \quad , \quad A_2 = A_2' \quad , \quad A_3 = -A_3' \tag{۴-۶}$$

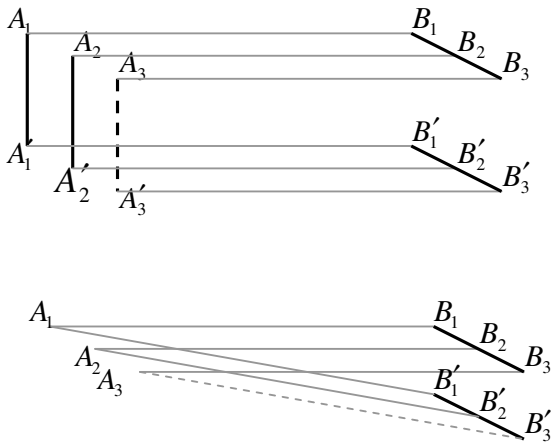
از طرف دیگر، با توجه به همبستگی‌های AB می‌دانیم که همه مشاهده‌پذیرها همبستگی کامل با مشاهده پذیرهای متناظرشان دارند (یعنی $A_i' = B_i'$, $A_i'' = B_i''$, $A_i = B_i$ برای همه‌ی i ها). پس در این صورت، ما همبستگی‌های زیر را در کل سیستم تعیین می کنیم:

$$\begin{aligned} A_1 = B_1 \qquad & A_1 = B_1' \\ A_2 = B_2 \qquad & A_2 = B_2' \\ A_3 = B_3 \qquad & A_3 = -B_3' \end{aligned} \tag{۴-۷}$$

پس علاوه بر همبستگی‌های کامل برای جفت‌های (A_i, B_i) با مقدار $i = 1,2,3$ ، همبستگی‌های کاملی برای جفت‌های (A_1, B_1') ، (A_2, B_2') و ناهمبستگی‌های کاملی برای (A_3, B_3') خواهیم داشت که در شکل (۴-۳) به وضوح نمایش داده شده است.

سه مشاهده‌پذیر آلیس و ۶ مشاهده‌پذیر برای باب داریم. اکنون همبستگی‌های (۴-۷) را با توجه به فرمولبندی نامساوی‌های بل به صورت زیر فرمولبندی می‌کنیم:

$$\gamma(A:B) \equiv \langle A_1 B_1 \rangle + \langle A_2 B_2 \rangle + \langle A_3 B_3 \rangle + \langle A_1 B_1' \rangle + \langle A_2 B_2' \rangle - \langle A_3 B_3' \rangle \leq 4 \tag{۴-۸}$$



شکل (۴-۳) نحوه طراحی نامساوی بل. در شکل بالا همانطور که گفته شد مقادیر سطر اول باب و آلیس را ۱+ در نظر گرفته‌ایم، پس شکل (۴-۲) به این صورت در آمده و با توجه به همبستگی‌ها خلاصه می‌شود و از آن نامساوی بل طراحی می‌شود.

همبستگی‌های رابطه (۴-۷) به این معنی است که مقدار نامساوی $\gamma(A:B)=6$ است و چون این مقدار برای حالت خاصی از سیستم بدست آمده نمی‌توان گفت در حالت کلی، γ لزوما ۶ است. حال به دنبال محدودیتی برای توزیع احتمالات سطر اول باب به صورت کلی‌تر هستیم و سپس ارتباطی میان درجه‌ی نقض نامساوی بل و محدودیت روی توزیع احتمال سطر اول باب بدست می‌آوریم. از طرفی برای بررسی ایمنی سیستم به دنبال نقض هرچه قوی‌تر نامساوی (۴-۸) هستیم. بنابراین از روشی آماری که اصل علیت اطلاعات نام دارد، برای نقض این نامساوی بل استفاده خواهیم کرد.

برای این هدف از نامساوی معادل برحسب همبستگی‌ها استفاده می‌کنیم.

$$\beta(A:B) \equiv P(A_1 = B_1) + P(A_2 = B_2) + P(A_3 = B_3) + P(A_1 = B'_1) + P(A_2 = B'_2) + P(A_3 \neq B'_3) \leq 5 \qquad (۴-۹)$$

با توجه به این دو می توان نتیجه گرفت:

$$\beta(A:B) = \frac{1}{2}[\gamma(A:B) + 6] \qquad (۴-۱۰)$$

در حالت ایده‌آل برای همبستگی‌های AB خواهیم داشت:

$$p(A_1 = B_1) = p(A_2 = B_2) = p(A_3 = B_3) = 1 \qquad (۱۱-۴)$$

حالا ما میان احتمالات دیگر با توزیع سطر اول باب ارتباط برقرار خواهیم کرد، اگر توزیع سطر اول باب را با q_i و $i=0,1,2,3$ نشان دهیم، خواهیم داشت:

$$\begin{aligned} q_0 &= \Pr(+,+,+) \\ q_1 &= \Pr(+,-,-) \\ q_2 &= \Pr(-,+,-) \\ q_3 &= \Pr(-,-,+) \end{aligned} \qquad (۱۲-۴)$$

و q_iها را توزیع‌های احتمال توأمان می نامیم و Pr توزیع احتمال است و داریم:

$$q_0 + q_1 + q_2 + q_3 = 1$$

حال توزیع‌های حاشیه‌ای[1] هر مشاهده‌پذیر از سطر را بررسی می‌کنیم. منظور از توزیع‌های احتمال حاشیه‌ای زیرمجموعه‌ای از مجموعه‌ی متغیرهای تصادفی است که اصطلاحاً آن‌ها را متغیرهای حاشیه‌ای می‌نامیم و آن‌ها به محاسبه‌ی مجموع مقادیر روی هر سطر یا هر ستون می‌پردازند به طوری که اگر p_i احتمال آن باشد که ما برای مشاهده‌پذیر i ام، مقدار ۱+ را تعیین کنیم، آن‌را با $p_i = \Pr(B_i'' = +1)$ نشان می‌دهیم. به طور کلی این‌گونه نشان می‌دهیم که $p_i(k) = \Pr(B_i'' = k)$ و برای $k = \pm 1$. حال ما رابطه‌ی میان p_iها و q_i ها را بدست می‌آوریم. برای p_1، از چهار توزیع احتمال هرکدام که دارای مقدار $B_1'' = +1$ است را در نظر می‌گیریم، پس:

$$p_1 = q_0 + q_1$$

[1] marginal

و به همین ترتیب:

$$p_2 = q_0 + q_2$$
$$p_3 = q_0 + q_3 \qquad (۱۳-۴)$$

مجموع p_i ها ۱ نمی‌شود، چرا که آن‌ها از سه توزیع احتمال متفاوت از هم $(p_i, 1-p_i)$ ساخته شده‌اند و مجموع آن‌ها به صورت زیر می‌باشد:

$$p_1 + p_2 + p_3 = q_0 + q_1 + q_0 + q_2 + q_0 + q_3 = 1 + 2q_0$$

و با استفاده از آن ارتباط میان q_iها و p_i ها را بدست می‌آوریم:

$$p_1 + p_2 + p_3 - 1 = 2q_0$$
$$\Rightarrow \qquad q_0 = \frac{1}{2}[-1 + p_1 + p_2 + p_3]$$

$$p_1 - p_2 - p_3 = q_0 + q_1 - q_0 - q_2 - q_0 - q_3 + q_1 - q_1 = 2q_1 - 1$$
$$\Rightarrow \qquad q_1 = \frac{1}{2}[1 + p_1 - p_2 - p_3]$$

$$-p_1 + p_2 - p_3 = -q_0 - q_1 + q_0 + q_2 - q_0 - q_3 - q_2 + q_2 = -1 + q_2 \qquad (۱۴-۴)$$
$$\Rightarrow \qquad q_2 = \frac{1}{2}[1 - p_1 + p_2 - p_3]$$

$$-p_1 - p_2 + p_3 = -q_0 - q_1 - q_0 - q_2 + q_0 + q_3 + q_3 - q_3 = 2q_3 - 1$$
$$\Rightarrow \qquad q_3 = \frac{1}{2}[1 - p_1 - p_2 + p_3]$$

در نگاه اول، ممکن است به نظر برسد که q_i ها در روابط بالا باید منفی باشد، اما یادآوری می‌کنیم که p_i ها به علت تبعیت از شرایط KS مانع از این موضوع خواهند شد. حال در این مرحله محدودیت-هایی روی p_i ها بدست می‌آوریم و سپس آن‌ها را بر حسب q_i ها می‌نویسیم.

همانطور که در شرایط KS آمده است حاصل ضرب نتایج اندازه‌گیری ستون اول باید ۱+ باشد و با توجه به شرطی که برای سطر اول باب در نظر گرفتیم و شرایط همبستگی AB باید $A'' = +1_1$ باشد از طرفی برای ارضا شدن شرایط KS باید $A_1' = A_1$ باشند. بنابراین برای توزیع احتمال در طرف آلیس رابطه‌ی زیر را خواهیم داشت:

$$\Pr(A_1 = A_1') = \Pr(A_1'' = +1) = p_1 \qquad (۱۵-۴)$$

به طور مشابه:

$$\begin{aligned} &\Pr(A_2 = A_2') = p_2 \\ &\Pr(A_3 = A_3') = p_3 \end{aligned} \qquad (۱۶-۴)$$

حالا با بررسی سه رویداد زیر:

$$X = \{A_1 = A_1'\} \;; Y = \{A_1' = B_1'\} \;; Z = \{A_1 = B_1'\} \qquad (۱۷-۴)$$

واضح است که $X \cap Y \subset Z$ و با استفاده از نامساوی که از قبل می شناختیم برای هر رویداد خواهیم داشت:

$$\Pr(Z) = \Pr(X \cap Y) \geq P(X) + P(Y) - 1 \qquad (۱۸-۴)$$

در این صورت پس از جایگذاری سه رویداد در نامساوی بالا نامساوی زیر را بدست خواهیم آورد:

$$\Pr(A_1 = B_1') \geq \Pr(A_1 = A_1') + \Pr(A_1' = B_1') - 1 \qquad (۱۹-۴)$$

$\Pr(A_1 = A_1') = p_1$ که در فرمول (۴-۱۵) ارائه شد و با توجه به شرایط همبستگی های AB خواهیم داشت:

$$\Pr(A_1 = B_1') \geq p_1 + 1 - 1 = p_1 \qquad (۴-۲۰)$$

و به طور مشابه برای بقیه هم خواهیم گفت:

$$\begin{aligned} &\Pr(A_2 = B_2') \geq p_2 \\ &\Pr(A_3 \neq B_3') \geq p_3 \end{aligned} \qquad (۴-۲۱)$$

بنابراین با جایگذاری روابط (۴-۲۰) و (۴-۲۱) و اعمال همبستگی‌های AB در نامساوی (۴-۹) به صورت زیر بدست خواهیم آورد:

$$\begin{aligned} &\beta(A:B) \equiv \Pr(A_1 = B_1) + \Pr(A_2 = B_2) + \Pr(A_3 = B_3) + \Pr(A_1 = B_1') + \\ &\Pr(A_2 = B_2') + \Pr(A_3 \neq B_3') \geq 3 + p_1 + p_2 + p_3 \end{aligned} \qquad (۴-۲۲)$$

بنابراین ارتباط میان p_i ها و β به صورت زیر خواهد بود:

$$\beta(A:B) \equiv 3 + p_1 + p_2 + p_3 \qquad (۴-۲۳)$$

که با استفاده از لم زیر خواهیم داشت:

لم ۱: اگر β نامساوی بل (۴-۹) را نشان دهد و p_i ها احتمال بدست آوردن مقدار ۱+ را در طول اندازه گیری مشاهده پذیر iام سطر اول باب باشد، سپس

$$p_1 + p_2 + p_3 \leq \beta - 3 \qquad (۴-۲۴)$$

لم با تجزیه و تحلیل یک موقعیت برای باب هنگامی که خروجی + + + هستند در سطر اول با تعـدادی احتمال، که ضرورتاً برابر با ۱ نیست، تعیین شده ست. در یک راه مشابه می توان برای سه حالت دیگر ، - - +، - + - و + - - محاسبه کرد. می‌توان دوبـاره همبـستگی هـا و ناهمبـستگی هـای کامـل بـرای مشاهده پذیرهای (۴-۷) تعریف کرد. مثلا برای حالت - - +، A_2 و B_2' ناهمبـستگی دارنـد و بـرای - + = A_1 و B_1' ناهمبستگی دارنـد و نهایتـاً بـرای + - - ، A_i و B_i' ناهمبـستگی دارنـد، بـه ازای $i = 1,2,3$. حالات ذکر شده به ترتیب $\beta_1, \beta_2, \beta_3$ کمیت های بل هستند که همگی آنها با کمیت β، معادل می-باشند. بنابراین مقادیر بیشینه مکانیک کوانتومی همهٔ این کمیات یکسان است و ما این بیشینه مقـدار را β_0 می‌نامیم و با این تعریف برای ارائهٔ حـدود نقـض نامـساوی مکانیـک کوانتـومی (۴-۹)، خـواهیم داشت:

$$\beta(A:B) \le \beta_0 < 6 \qquad (۴-۲۵)$$

و از طرفی داریم:

$$\beta \ge p_1 + p_2 + p_3 + 3 \qquad \Rightarrow \qquad \beta_0 - 3 \ge p_1 + p_2 + p_3 \qquad (۴-۲۶)$$

با تجزیه و تحلیل سه حالت نمایش داده شده مثلاً بـرای حالـت (- - +)بـه روش مـشابه بـالا، بـا ایـن تعریف که p_i احتمال+ بودن و $(1-p_i)$ احتمال - بودن است ، خواهیم داشت،

$$p_1 + (1-p_2) + (1-p_3) \le \beta - 3 \qquad (۴-۲۷)$$

و برای حالت های (- +-) و (+--) به ترتیب به صورت زیر است:

$$\begin{aligned} &(1-p_1) + p_2 + (1-p_3) \le \beta - 3 \\ &(1-p_1) + (1-p_2) + p_3 \le \beta - 3 \end{aligned} \qquad (۴-۲۸)$$

حال با استفاده از روابط (۴-۱۵) و توزیع های احتمال (۴-۲۷) و (۴-۲۹)، توزیع های احتمال توأمـان را برای سطر اول باب به صورت زیر بدست می‌آوریم:

$$p_1 + 1 - p_2 + 1 - p_3 \le \beta - 3$$
$$\frac{1}{2}(1 + p_1 - p_2 - p_3) \le \frac{1}{2}(\beta_0 - 4)$$

و با توجه به $q_1 = \frac{1}{2}(1 + p_1 - p_2 - p_3)$ خواهیم گفت:

$$q_1 \le \frac{1}{2}(\beta_0 - 4) \qquad (۴-۲۹)$$

پس برای حالت‌های دیگر داریم:

$$\begin{aligned} &1 - p_1 + p_2 + 1 - p_3 \le \beta_0 - 3 \\ &\frac{1}{2}(1 - p_1 + p_2 - p_3) \le \frac{1}{2}(\beta_0 - 4) \end{aligned} \quad \Rightarrow \quad 1 - p_1 + p_2 - p_3 \le \beta_0 - 4$$
$$q_2 \le \frac{1}{2}(\beta_0 - 4) \qquad (۴-۳۰)$$

$$\begin{aligned} &1 - p_1 + 1 - p_2 + p_3 \le \beta_0 - 3 \\ &\frac{1}{2}(1 - p_1 - p_2 + p_3) \le \frac{1}{2}(\beta_0 - 4) \end{aligned} \quad \Rightarrow \quad 1 - p_1 - p_2 + p_3 \le \beta_0 - 4$$
$$q_3 \le \frac{1}{2}(\beta_0 - 4)$$

برای حالت اول $(+\ +\ +)$ هم داریم:

$$\begin{aligned} &p_1 + p_2 + p_3 \le \beta_0 - 3 \\ &\frac{1}{2}(-1 + p_1 + p_2 + p_3) \le \frac{1}{2}(\beta_0 - 4) \Rightarrow \end{aligned} \qquad -1 + p_1 + p_2 + p_3 \le \beta_0 - 4$$
$$q_0 \le \frac{1}{2}(\beta_0 - 4) \qquad (۴-۳۱)$$

پس به طور کلی خواهیم داشت:

$$q_i \le \frac{1}{2}(\beta_0 - 4) \ , \ i = 0,1,2,3 \qquad (۳۲-۴)$$

لم ۲: همبستگی های AB و شرایط KS و ارتباط میان دو نامساوی (۴-۱۰) را به کار خواهیم برد و این حدود را برحسب γ_0 که یک مقدار بیشینه مکانیک کوانتومی است، به صورت زیر می‌نویسیم:

$$\begin{aligned} & q_i \le \frac{1}{2}(\frac{1}{2}[\gamma_0 + 6] - 4) = \frac{1}{2}(\frac{\gamma_0}{2} - \frac{1}{2}) = \frac{1}{4}(\gamma_0 - 2) \\ & \Rightarrow \qquad q_0 \le \frac{1}{4}(\gamma_0 - 2) \end{aligned} \qquad (۳۳-۴)$$

و $\{q_i\}$توزیع های احتمال توأمان نتایج سطر اول باب است.

همانطور که در روابط (۴-۳۳) آمده، برای محاسبه‌ی $\{q_i\}$ها باید مقدار γ_0را بدست آوریم. با توجه به آن‌چه در [۲۰]، آمده می‌توان آن را به صورت عددی محاسبه کرد. با استفاده از روابط مکانیک کوانتومی رابطه‌ی (۴-۸) را به صورت زیر بازنویسی می‌کنیم:

$$\begin{aligned} & \gamma = \langle\psi|A_1 \otimes B_1|\psi\rangle + \langle\psi|A_2 \otimes B_2|\psi\rangle + \langle\psi|A_3 \otimes B_3|\psi\rangle \\ & + \langle\psi|A_1 \otimes B_1'|\psi\rangle + \langle\psi|A_2 \otimes B_2'|\psi\rangle - \langle\psi|A_3 \otimes B_3'|\psi\rangle \\ & = A_1 \cdot B_1 + A_2 \cdot B_2 + A_3 \cdot B_3 + A_1 \cdot B_1' + A_2 \cdot B_2' - A_3 \cdot B_3' \end{aligned} \qquad (۳۴-۴)$$

اگر $A_1, A_2, A_3, B_1, B_2, B_3, B_1', B_2', B_3'$ مشاهده‌پذیرهایی با ویژه مقادیر ± 1 برای آلیس و باب باشند و در نظر می‌گیریم که:

$$\|A_1\| = \|A_2\| = \|A_3\| = \|B_1\| = \|B_2\| = \|B_3\| = \|B_1'\| = \|B_2'\| = \|B_3'\| = 1 \qquad (۳۵-۴)$$

حال اگر $\Gamma = [\gamma_{ij}]$ برای مشاهده‌پذیرهای $\{I, A_1, A_2, A_3, B_1, B_2, B_3, B_1', B_2', B_3'\}$ خواهیم داشت:

$$\Gamma = \begin{pmatrix} I\cdot I & I\cdot A_1 & I\cdot A_2 & I\cdot A_3 & I\cdot B_1 & I\cdot B_2 & I\cdot B_3 & I\cdot B_1' & I\cdot B_2' & I\cdot B_3' \\ A_1\cdot I & A_1\cdot A_1 & A_1\cdot A_2 & A_1\cdot A_3 & A_1\cdot B_1 & A_1\cdot B_2 & A_1\cdot B_3 & A_1\cdot B_1' & A_1\cdot B_2' & A_1\cdot B_3' \\ A_2\cdot I & A_2\cdot A_1 & A_2\cdot A_2 & A_2\cdot A_3 & A_2\cdot B_1 & A_2\cdot B_2 & A_2\cdot B_3 & A_2\cdot B_1' & A_2\cdot B_2' & A_2\cdot B_3' \\ A_3\cdot I & A_3\cdot A_1 & A_3\cdot A_2 & A_3\cdot A_3 & A_3\cdot B_1 & A_3\cdot B_2 & A_3\cdot B_3 & A_3\cdot B_1' & A_3\cdot B_2' & A_3\cdot B_3' \\ B_1\cdot I & B_1\cdot A_1 & B_1\cdot A_2 & B_1\cdot A_3 & B_1\cdot B_1 & B_1\cdot B_2 & B_1\cdot B_3 & B_1\cdot B_1' & B_1\cdot B_2' & B_1\cdot B_3' \\ B_2\cdot I & B_2\cdot A_1 & B_2\cdot A_2 & B_2\cdot A_3 & B_2\cdot B_1 & B_2\cdot B_2 & B_2\cdot B_3 & B_2\cdot B_1' & B_2\cdot B_2' & B_2\cdot B_3' \\ B_3\cdot I & B_3\cdot A_1 & B_3\cdot A_2 & B_3\cdot A_3 & B_3\cdot B_1 & B_3\cdot B_2 & B_3\cdot B_3 & B_3\cdot B_1' & B_3\cdot B_2' & B_3\cdot B_3' \\ B_1'\cdot I & B_1'\cdot A_1 & B_1'\cdot A_2 & B_1'\cdot A_3 & B_1'\cdot B_1 & B_1'\cdot B_2 & B_1'\cdot B_3 & B_1'\cdot B_1' & B_1'\cdot B_2' & B_1'\cdot B_3' \\ B_2'\cdot I & B_2'\cdot A_1 & B_2'\cdot A_2 & B_2'\cdot A_3 & B_2'\cdot B_1 & B_2'\cdot B_2 & B_2'\cdot B_3 & B_2'\cdot B_2' & B_2'\cdot B_2' & B_2'\cdot B_3' \\ B_3'\cdot I & B_3'\cdot A_1 & B_3'\cdot A_2 & B_3'\cdot A_3 & B_3'\cdot B_1 & B_3'\cdot B_2 & B_3'\cdot B_3 & B_3'\cdot B_2' & B_3'\cdot B_2' & B_3'\cdot B_3' \end{pmatrix} \quad (۳۶-۴)$$

با توجه به آن که $X = \{I, A_1, A_2, A_3, B_1, B_2, B_3, B_1', B_2', B_3'\}$ و $\Gamma = X^{\dagger}X$. در این صورت $\Gamma \geq 0$ است.حال ماتریس W با استفاده از نامساوی به صورت زیر می‌نویسیم:

$$W = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (۳۷-۴)$$

اکنون اگر مسئله را از طریق برنامه‌نویسی به روش SDP که مخفف SemiDefinite Programing است به معنی برنامه‌نویسی به روش نیمه معین است[۳۱] و برای ماتریس‌های بزرگتر و مساوی صفر استفاده می‌شود، بازنویسی کنیم، خواهیم داشت که:

$$\begin{aligned} &\max && \gamma \\ &\textit{subject to} && \frac{1}{2}Tr(\Gamma W),\Gamma \geq 0,\forall \gamma_{ij}=1 \end{aligned} \qquad (۳۸-۴)$$

حال اگر با توجه به شرایط در نظر گرفته شده، معادله‌ی زیر را محاسبه کنیم:

$$\frac{1}{2}Tr[\Gamma=\begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&1&0&0&1&0&0\\ 0&0&1&0&0&1&0&0&1&0\\ 0&0&0&1&0&0&1&0&0&-1\\ 0&1&0&0&1&0&0&1&0&0\\ 0&0&1&0&0&1&0&0&1&0\\ 0&0&0&1&0&0&1&0&0&-1\\ 0&1&0&0&1&0&0&1&0&0\\ 0&0&1&0&0&1&0&0&1&0\\ 0&0&0&-1&0&0&-1&0&0&1 \end{pmatrix}\cdot W=\begin{pmatrix} 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&1&0\\ 0&0&0&0&0&0&1&0&0&-1\\ 0&1&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0\\ 0&0&0&-1&0&0&0&0&0&0 \end{pmatrix}]$$

با استفاده از کدنویسی آن در SDP به آسانی می‌توان مشاهده کرد که مقدار بیشینه‌ی آن برابر با ۶ می‌شود و این محاسبات با اصل علیت اطلاعات سازگار است. پس از بهینه سازی این محاسبات از طریق نرم‌افزاری به نام SDPT3 که یک مجموعه‌ی کدنویسی در برنامه‌ی مطلب است[۲۲]، به مقداری برابر با $\gamma_0 = 5.6364$ می‌رسیم که ما این مقدار را برای حد بالای نامساوی بل برمی‌گزینیم و اگر رابطه (۴-۳۳) را به صورت زیر اصلاح کنیم:

$$q_i \leq x \qquad (۳۹-۴)$$

پس نهایتاً محدودیتی برای هر چهار حالت ذکر شده در سطر اول باب بدست آوردیم، حال مقدار x چگونه خواهد بود:

$$x=\frac{1}{4}(\gamma_0-2)=\frac{1}{4}(5.6364-2)=0.9091 \qquad (۴۰-۴)$$

و برای حالت کلاسیک $\gamma(A:B)\le 4$ بود، پس برای حالت کوانتومی باید $\gamma(A:B)$ از این مقدار بیشتر باشد، در این صورت x خواهد بود:

$$x=\frac{1}{4}(\gamma_0-2)=\frac{1}{4}(4-2)=\frac{1}{2} \qquad \Rightarrow \qquad x\ge\frac{1}{2} \qquad (۴۱-۴)$$

پس دراین صورت برای بررسی عدم وجود Eve به این نتیجه خواهیم رسید که γ_0 باید دارای بازه‌ای به صورت زیر باشد، که گواه آن است که Eve در سیستم دخالت ندارد و سیستم ایمن است.

$$4\le\gamma_0\le 5.6364 \qquad (۴۲-۴)$$

به همین ترتیب محدودیت روی سطر اول باب برای چهار حالت اینگونه خواهد بود:

$$\frac{1}{2}\le x\le 0.9091 \qquad (۴۳-۴)$$

۴-۵ ایمنی کلید در جعبهٔ ایده آل

فرض کنید آلیس و باب یک جعبه R_{AB} را مشترکاً اندازه گیری کنند، استراق‌سمع‌کننده می‌تواند این جعبه را به صورت زیر تجزیه کند، که هر جعبه خود یک جعبه‌ی PM است یعنی اگر مثلا برای جعبه‌های کوچک شرایط جعبه‌ی PM را بررسی کنیم به این می‌رسیم که جعبه‌های کوچک تجزیه شده هم PM هستند و شرایط KS و همبستگی‌های AB و شرط عدم علامت‌دهی را ارضا می‌کنند:

$$R_{AB} = \sum_e r_e R_{AB}^e \qquad (۴۴-۴)$$

(که ما به طور عمدی با جعبه های e برچسب زده ایم، زیرا تنها Eve است که جعبـه‌ی R_{AB} را قطعاً می شناسد یعنی اگر فرض کنیم آنها جعبهٔ A و B را با آزمون بررسـی کننـد و نـوع جعبـه را بدسـت آورند. پس با آزمون های نمونه های مختلف جعبه ها رامشخص می کنند یعنی ورودی‌ها و خروجی‌هـا را شناسایی می کنند و با آزمون نمونه های مختلف A و B می توانند بدانند جعبـه هـا چـه هـستند، تجزیهٔ (۴۴-۴) به صورت زیر بدست می آید:

Eve یک جعبهٔ مشترک R_{ABE} می سازد و R_{AB} را به آلیس و باب می فرستد ، پس مـی تـوان گفـت، این جعبه یک سیستم سه ذره ای است که دو تا را برای آلیس و باب مـی فرسـتد و یکـی مربـوط بـه خودش است ، وقتی آلیس و باب انتخاب های اندازه گیری شده‌ی خود را به هم می‌گوینـد، Eve هـم قسمت خودش را اندازه می گیرد. مثلا اگر حالت اصلی سیستم به صورت زیر باشد:

$$\left|\uparrow\uparrow\downarrow\right\rangle^z + \left|\downarrow\uparrow\uparrow\right\rangle^z + \left|\uparrow\downarrow\uparrow\right\rangle^z$$

اگر Eve حالت سیستم را در پایه‌ی z اندازه بگیرد و $\left|\downarrow\right\rangle^z$ بدست آورد، حالت توزیع شده برای آلـیس و بـاب، $\left|\uparrow\uparrow\right\rangle^z$ خواهـد بـود و اگـر $\left|\uparrow\right\rangle^z$ بدسـت آورد، حالـت آنهـا $\left|\downarrow\uparrow\right\rangle^z + \left|\uparrow\downarrow\right\rangle^z$ خواهـد شـد. حال اگر روی پایه های x اندازه بگیرد، آنگاه باید پایـه هـا بـه x تبـدیل شـوند و بعـد از آن ، روی آن اعمال می شود پس Eve می تواند، جعبه‌ی R_{AB} را هرگونه که بخواهد بـسازد. اکنـون اسـتراق‌سـمع-کننده هر کدام را برای یک جعبه‌ی کوچک ارسال می‌کند و این‌گونه برای جعبه‌هـای کوچـک تجزیـه شده حالت سیستم را متفاوت توزیع می‌کند. این یک نوع حمله از حملات استراق‌سمع‌کننده است که

آن را حمله‌ی منفرد[1] می‌نامیم. در این پایان‌نامه به دنبال بررسی ایمنی پروتکل با جعبه‌های ایده‌آل و نویزی در مقابل این حمله هستیم.

تا اینجا می‌دانیم که Eve می‌تواند جعبه های R_{AB} مربوط به آلیس و باب را در آنسامبل اختیاری $\{q_e, R^e_{AB}\}$ که به صورت $R_{AB} = \sum_e r_e R^e_{AB}$ مشخص می شود، دو نیم کند. این توانایی، مشابه با موقعیتی در مکانیک کوانتومی است که Eve با خالص سازی[2] حالت های آلیس و باب همهٔ جهان پیرامون آن‌ها به جز خودشان را کنترل کند و این تنها کاری است که Eve می تواند انجام دهد. در این حالت ارسال سیگنال از Eve به آلیس و باب غیر ممکن است. پس Eve فقط می‌تواند نوع جعبه را بررسی کند، اما آنچه که آلیس و باب برای اندازه گیری انتخاب می‌کنند را نمی‌تواند تعیین کند. حال اگر جعبهٔ R_{AB} یک جعبه دو طرفه PM باشد، R_{AB} باید به جعبه های PM تبدیل شود و این به خاطر شرایط جعبه های PM دو طرفه یعنی همان شرایط KS و همبستگی های AB است که بر مبنای عدم علامت دهی که یک اصل است فرمول بندی شده اند یعنی احتمال ارسال سیگنال از Eve به آلیس و باب به طور قطع ۰ است. بنابراین Eve فقط می تواند جعبه‌ی R_{AB} را دوباره به جعبه های دوطرفه‌ی PM تجزیه کند.

فرض کنید که آلیس و باب n جعبه را مشترکاً اندازه گیری کنند. آنها یک نمونه از n جعبه را برای بررسی اینکه آیا جعبه ای که به اشتراک گذاشته اند، PM است یا نه، انتخاب می کنند. در فرایند اثبات آن، آلیس ستون ها را به طور تصادفی اندازه می گیرد. در این زمان باب سطرها را به طور تصادفی اندازه می گیرد و اینگونه بررسی می کنند که آیا جعبه PM است یا خیر. از بقیه جعبه ها برای استخراج کلید استفاده می کنند.

ما گفتیم که Eve نمی تواند به طور قطع سطر اول را در طول زمانی که آلیس و باب همبستگی کامل دارند، بداند یا به عبارتی با توجه به حدود تعیین شده برای γ_0، استراق‌سمع‌کننده در سیستم وجود

[1] Individual attack
[2] Purification

ندارد. پس آلیس و باب باید هر دو سطر اول را اندازه بگیرند و با استفاده از همبستگی AB، کلید را تعیین کنند. البته آلیس اگر سطر را اندازه می گیرد، باید از یک دستگاه با تنظیم متفاوت از آنکه ستون‌ها را محاسبه کرده است، استفاده کند، چون پروتکل ما مستقل از دستگاه است، ما باید فرض کنیم که وسیله می تواند مخرب باشد. در این خصوص هنگامی که آلیس می خواهد سطرها را اندازه بگیرد، او ممکن است در حقیقت تعدادی مشاهده پذیر کاملاً متفاوت نسبت به هنگامی که سطرها را اندازه می گیرد، اندازه بگیرد و در غیر این‌صورت Eve می تواند نتایج اندازه‌گیری را به طور کامل بداند.

به هرحال، چون ما از قبل می دانیم که نتایج سطراول باب تا اندازه ای ایمن است، این کافی است که نتایج سطر اول آلیس با سطر اول باب همبستگی داشته باشند. پروتکل اینگونه پیشنهاد می شود:

آلیس و باب n جفت ذره را به اشتراک گذاشته اند. آن‌ها دو نمونه از n جفت ذره را انتخاب می کنند. روی نمونه اول، آنها ستون ها و سطرها را به ترتیب اندازه می گیرند و اینگونه بررسی می کنند که جعبه PM به اشتراک گذاشته اند. در نمونه دوم آلیس و باب فقط سطر اول را اندازه می‌گیرند و بررسی می‌کنند که آیا نتایج، همبستگی دارد یا نه. روی بقیه جفت‌ها آلیس و باب سطر اول را همچنین اندازه می گیرند و نتایج، کلید خام را تشکیل می دهد. سپس آنها روش‌های استاندارد تصحیح خطا و تقویت محرمانه را برای کوتاه کردن و ایمن کردن آن به کار می برند. در حالت جعبهٔ ایده‌آل تصحیح خطا احتیاج نداریم چرا که نتایج آلیس و باب کاملاً با هم همبستگی دارند و تنها تقویت محرمانه انجام خواهد شد. تصحیح خطا برای حالت نویزی است که در ادامه توضیح خواهیم داد.

در ارزیابی ایمنی کلید تعیین شده ما اکنون به تجزیه و تحلیل متغیرهای تصادفی سه‌تایی (A, B, E) خواهیم پرداخت. A و B مشاهده پذیرهایی هستند که به ترتیب سطر اول آلیس و باب را توصیف می کنند و E متغیر Eve است، که آنسامبل تصادفی (۴-۴۴) را توصیف می کند یعنی $E = e$ با احتمال q_e .

حال ما می توانیم با استفاده از فرمول معروف کسازر-کرنر[1] حد پایینی برای نرخ امنیت کلید(K) بدست آوریم[۲۸,۲۹] که در آن I(A:B) اطلاعات متقابل شانون از توزیع های احتمالی توأمان سطر اول آلیس و باب است و I(A:B) نشان دهنده اطلاعات متقابل شانون از توزیع های احتمال توأمان سطراول آلیس و نتایج اندازه گیری Eve است و البته بررسی سطر اول مدنظر است ولی در اینجا به علت وجود همبستگی‌های کامل می توان سطر اول آلیس هم بررسی کرد، ولی برای حالت نویزی تنها باید به بررسی سطر اول باب بپردازیم:

$$K \geq I(A:B) - I(A:E) \qquad (۴۵-۴)$$

این فرمول را می توان با بیان آنتروپی شرطی دوباره نویسی کرد:

$$K \geq H(A|E) - H(A|B) \qquad (۴۶-۴)$$

$H(A|B)$ به علت همبستگی‌های کامل برابربا ۰ است گرچه Eve جعبه را در یک آنسامبل تجزیه خواهد کرد، هر جز آنسامبل جعبه PM است که شرایط (۴-۴۴) را ارضا خواهد کرد. با توجه به حدودی که برای سطر اول باب قائل شدیم، پس کمترین توزیع آنتروپی را اینگونه تعریف می کنیم:

$$(x,1-x,0,0) \qquad (۴۷-۴)$$

و $x = 0.9091$ پس میزان آنتروپی شرطی به صورت زیر است:

$$H(A|E) = -\sum p(A|E)\log_2 p(A|E) \qquad (۴۸-۴)$$

[1] Csiszar-Korner

پس داریم:

$$H(A|E) = -[(0.9091)\log_2(0.9091) + (1-0.9091)\log_2(1-0.9091)] = 0.439$$

و از آن می توان نرخ امنیت کلید را بدست آورد که برابر با ۰/۴۳۹ است.

جعبه ایده آل PM بررسی شده متناظر با موقعیتی است که هیچ اختلالی (یعنی همبستگی کامل میان آلیس و باب) در سیستم وجود ندارد. ما می بینیم که در این حالت، Eve می تواند تنها قسمتی از اطلاعات را بدست آورد. بنابراین اکنون ما یک نسخهٔ استخراج اطلاعات در حضور اختلال را مشاهده می‌کنیم.

۴-۶ حالت نویزی[1]

در این قسمت به بررسی سیستمی می پردازیم که ذرات آن با محیط بر هم‌کنش کرده و باعث اغتشاشاتی در حالت سیستم می‌شوند، مثلاً حالت را دچار چرخش می کند. در چنین حالاتی حتی در حالت همبستگی کامل هم کل اطلاعات سیستم قابل حصول نیست. در ادامه این جعبه را بررسی می کنیم.

اول از همه توجه می کنیم که این جعبه شرایط KS را کاملا ارضا می‌کند به عبارتی آلیس و باب جعبه را وادار می کنند که شرایط KS را داشته باشند، به این طریق که دو مشاهده پذیر از سه‌تای سطر اول اندازه می گیرند و سومی را با توجه به آنها می سازند. بنابراین نویز تنها همبستگی‌های میان آلیس و باب را تحت تأثیر قرار می دهد. ما فرض خواهیم کرد که برای مشاهده‌پذیرهای پرس-مرمین، آلیس و باب همبستگی‌هایی با احتمال $\varepsilon - 1$ تعیین می‌شود یعنی ε میزان خطای حاصل از نویز است. به طور واضح خواهیم دید که افزایش خطای سیستم باعث کم شدن محدودیت‌های سطر اول باب می شود. در زیر به دنبال بررسی محدودیت روی سطر اول باب در حالت نویزی هستیم:

[1] Noisy case

با استفاده از نامساوی که از قبل می دانستیم و با $p_i \equiv p(B_i'' = +1)$ شروع خواهیم کرد و با اسـتفاده از اینکه می دانیم همبستگی میان A_i'' و B_i'' با احتمال $1-\varepsilon$ است ، خواهیم داشت:

$$p(A_i'' = +1) \geq p(A_i'' = B_i'') + p(B_i'' = +1) - 1$$
$$p(A_i'' = +1) \geq p_i + (1-\varepsilon) - 1 = p_i - \varepsilon \qquad (۴۹\text{-}۴)$$

و با استفاده از شرایط KS خواهیم داشت:

$$p(A_1 = A_1') = p(A_1'' = +1)$$
$$p(A_2 = A_2') = p(A_2'' = +1)$$
$$p(A_3 = A_3') = p(A_3'' = +1) \qquad (۵۰\text{-}۴)$$
$$\Rightarrow \quad p(A_i = A_i') = p_i - \varepsilon$$

چون A_i' و B_i' با احتمال $1-\varepsilon$همبستگی دارند، پس با استفاده دوباره از نامساوی (۴-۱۸)، داریم:

$$p(A_1 = B_1') \geq p(A_1 = A_1') + p(A_1' = B_1') - 1 = p_1 - \varepsilon + 1 - \varepsilon - 1 = p_1 - 2\varepsilon$$
$$\Rightarrow \quad p(A_1 = B_1') \geq p_1 - 2\varepsilon$$

$$p(A_2 = B_2') \geq p(A_2 = A_2') + p(A_2' = B_2') - 1 = p_2 - \varepsilon + 1 - \varepsilon - 1 = p_2 - 2\varepsilon \qquad (۵۱\text{-}۴)$$
$$\Rightarrow \quad p(A_2 = B_2') \geq p_2 - 2\varepsilon$$

$$p(A_3 \neq B_3') \geq p(A_3 = A_3') + p(A_3' = B_3') - 1 = p_3 - \varepsilon + 1 - \varepsilon - 1 = p_3 - 2\varepsilon$$
$$\Rightarrow \quad p(A_3 \neq B_3') \geq p_3 - 2\varepsilon$$

و از طرفی هم داریم:

$$p(A_i = B_i) \geq 1 - \varepsilon \qquad (۵۲-۴)$$

پس با جایگذاری آنها در رابطه نامساوی (۴-۹) حدود را برای سطر اول باب در جعبه نویزی به صورت زیر بدست خواهیم آورد:

$$\begin{aligned} &\beta(A:B) \geq p_1 + p_2 + p_3 + 3 - 9\varepsilon \\ &p_1 + p_2 + p_3 \leq \beta' - 3 \end{aligned} \qquad (۵۳-۴)$$

همانطور که مشاهده شد، برای حالت نویزی هم حدودی مشابه با حالت بدون نویز بدست آوردیم، با این تفاوت که به جای β از $\beta' = \beta + 9\varepsilon$ استفاده کرده‌ایم. به همین طریق می توانیم برای حالات دیگر در سطر اول باب ($--+$ و $-+-$ و $+--$) این کار را انجام دهیم و حدود زیر را برای احتمالات توأمان q_i مربوط به نتایج سطر اول بدست آوریم:

$$q_i \leq \frac{1}{2}(\beta_0 + 9\varepsilon - 4) \qquad (۵۴-۴)$$

که نهایتاً می توان گفت:

$$q_i \leq \frac{1}{2}(\beta_0 - 4) + 4.5\varepsilon \qquad (۵۵-۴)$$

و با توجه به مقدار بدست آمده برای نامساوی (۴-۸)، $\gamma_0 \leq 5.6364$ خواهیم داشت:

$$q_i \leq \frac{1}{4}(\gamma_0 - 4) + 4.5\varepsilon \qquad \Rightarrow \quad q_i \leq 0.9091 + 4.5\varepsilon \qquad (۵۶-۴)$$

برای $i = 0,1,2,3$

حال به بررسی نرخ ایمنی کلید که نتیجتاً به ارزیابی نویز آستانه منجر می شود، می پردازیم. ما یک جعبه *PM* نویزی را بررسی می کنیم، شرایط KS هنوز کامل هستند و تنها همبستگی های AB کامل نیستند. ارزیابی خطای پروتکل به دو بخش تقسیم می‌شود. ابتدا آلیس ستون ها را به طور تصادفی اندازه می گیرد و سپس باب سطرها را به طور تصادفی اندازه می گیرد. ۹ ترکیب متفاوت از سطر و ستون وجود دارد و در هر ترکیب، یک مشاهده پذیر مشترک وجود دارد.برای مثال می‌توان گفت، اگر آلیس ستون اول و باب سطر اول را انتخاب کنند، آنگاه مشاهده‌پذیر مشترک طبق جدول (۴-۱) σ_z^1 می‌باشد. ما فرض خواهیم کرد که در هر ترکیب، احتمالات با خطای مشابه ε هستند. سپس همانطور که مشاهده شد، حدودی روی سطر اول باب تعیین می شود که این مقدار برابر با $q_i \le 0.9091+4.5\varepsilon$ شد و در نتیجه با استفاده از آن حدودی روی $H(B|E)$ بدست می‌آوریم. حال آنتروپی سطر اول باب در حضور نویز ε را این‌گونه تعریف می‌کنیم:

$$H(B;\varepsilon)\ge h(x)\equiv f(\varepsilon) \qquad (۵۷-۴)$$

$f(\varepsilon)$ یک تابع نزولی است و مثبت است که این تابع بر حسب ε می‌باشد. معادل با آنتروپی باب هنگامی که در سیستم ناهمبستگی داریم و آن را با h(x) به معنای آنتروپی دوتایی می نامیم و به صورت زیر محاسبه می شود:

$$h(x)\equiv f(\varepsilon)=(x\log_2 x+(1-x)\log_2(1-x)) \qquad (۵۸-۴)$$
$$x=\min(0.9091+4.5\varepsilon,1)$$

با توجه به x می‌توان گفت h(x) از نظر ریاضی یک تابع نزولی است که در مقابل کمترین ε یعنی کمترین دامنه، بیشترین برد خود یعنی ۱ را دارد.

پس از اینکه استراق‌سمع‌کننده روی سیستم خودش، یک اندازه‌گیری انجام دهد، جعبه‌ی آلیس و باب را به آنسامبل زیر به دو نیم می کند. برای حالت نویزی برای اندیس آنسامبل به جای e از i استفاده می‌کنیم:

$$R_{AB} = \sum_e r_e R^e_{AB} = \sum_i r_i R^i_{AB}$$

$$H(B|E) = \inf \sum_i r_i H(B)_i \qquad (۵۹-۴)$$

$H(B)_i$ آنتروپی سطر اول باب از جعبه R^i_{AB}، r_i احتمال تجزیه شدن جعبه است و inf[1] به معنی بیشترین حد پایین مجموعه است و روی تمام تجزیه ها اثرمی کند. به عبارتی رابطه بالا به این معنی است که $H(B:E)$ برابر با کمترین آنتروپی متوسط سطر اول باب برای جعبه‌ها است. چون ما به دنبال کمترین توزیع آنتروپی هستیم و از طرفی می‌دانیم که در حضور Eve جعبه ها به دو نیم تقسیم می‌شوند، پس باید آنتروپی شرطی میان B و E را به صورت بالا محاسبه کنیم. با توجه به اینکه جعبه‌های R_{AB} که به آنسامبل $\sum_i r_i R^i_{AB}$ ، پس می توان گفت، آن‌ها شرایط زیر را ارضا می‌کند:

$$\varepsilon = \sum_i r_i \varepsilon_i \qquad (۶۰-۴)$$

$$\Rightarrow \ f(\varepsilon) = \sum_i r_i f(\varepsilon_i) \qquad (۶۱-۴)$$

پس رابطه آنتروپی $H(B|E)$ می‌شود:

$$H(B|E) \geq \inf_{\{q_i, \varepsilon_i\}} \sum_i r_i f(\varepsilon_i) \qquad (۶۲-۴)$$

که در آن $\sum_i r_i = 1$ و $\sum_i r_i \varepsilon_i = \varepsilon$ است.

[1] infimum

برای ارزیابی رابطه‌ی (۴-۶۲) با استفاده از نامساوی مارکوف[1] که حد پایینی برای احتمال اینکه مقدار چشم‌داشتی کمیتی کمتر از مقدار مثبتی بیان می‌کند، خواهیم داشت:

$$\Pr(\varepsilon < \delta) \geq 1 - \frac{\varepsilon}{\delta} \quad , \delta > 0 \qquad (۴-۶۳)$$

همانطور که گفته شد r_iها احتمال تجزیه‌ی جعبه‌هاست، پس می توان نامساوی مارکوف را به صورت زیر بازنویسی کرد:

$$\sum_{i;\varepsilon_i < \delta} r_i \geq 1 - \frac{\varepsilon}{\delta} \qquad (۴-۶۴)$$

چون در رابطه (۴-۶۲) به دنبال inf روی r_i و ε_iهستیم و $\varepsilon_i < \delta$ است پس یعنی بیشینه حد پایین ε_i مدنظر است، به همین دلیل به جای ε از δ در محدویت سطراول باب استفاده می کنیم.
حال چون می‌خواهیم کمترین حد بالای $\sum_i r_i$ را مدنظر قرار دهیم، پس از مفهوم sup[2] که کمترین حد بالا را برای مجموعه تعیین می‌کند، استفاده می‌کنیم و آن را روی δ اعمال می‌کنیم. پس در نهایت رابطه مربوط به آنتروپی $H(B|E)$ به صورت زیر می شود:

$$H(B|E) \geq \sup_{\delta}(1 - \frac{\varepsilon}{\delta}) h(0.9091 + 4.5\delta) \qquad (۴-۶۵)$$

در بخش دوم ارزیابی خطا، آلیس سطر اول را اندازه می گیرد و باب هم سطر اول را اندازه می‌گیرد، احتمال آنکه نتایجشان متفاوت باشد $\tilde{\varepsilon}$ می باشد. به منظور داشتن یک پارامتر تک نویز در سطر،

[1] Markov's inequality
[2] supremum

(یعنی همهٔ آرایه ها فقط یک مقدار نویز داشته باشد) که برای سادگی فرض می‌کنیم ε باشد، از شرایط KS داریم:

$$\varepsilon = \frac{2}{3}\tilde{\varepsilon} \qquad (۶۶-۴)$$

که می توان آن را به صورت زیر تعریف کرد:

خطای مربوط به هر گره(ε)، با توجه به شرایط KS شامل $\frac{2}{3}$ خطای اشتباه اندازه گرفتن($\tilde{\varepsilon}$) است. با استفاده از نامساوی فانو[1] که به دنبال بدست آوردن اطلاعات غلط میان دو متغیر تصادفی X و Y است به این معنی که حد بالایی برای آنتروپی شرطی میان X و Y با توجه به محاسبه‌ی نتایج غلط میان آن دو بدست می‌آورد. این نامساوی به صورت زیر تعریف می‌شود:

$$H(p_e) + p_e \log_2(|x|-1) \geq H(X|Y) \qquad (۶۷-۴)$$

که $|x|$ تعداد نتایج ممکن و p_e احتمال اشتباه بودن نتایج اندازه‌گیری و H(.) آنتروپی دوتایی است. پس می‌توان گفت:

$$p_e = \tilde{\varepsilon}$$

و اگر به جای X و Y به ترتیب A (آلیس) و B (باب) در نظر بگیریم:

$$H(\tilde{\varepsilon}) + \tilde{\varepsilon} \log_2(|B|-1) \geq H(B|A) \qquad (۶۸-۴)$$

که $H(\tilde{\varepsilon})$ آنتروپی دوتایی است یعنی:

$$H(\tilde{\varepsilon}) = \tilde{\varepsilon} \log_2 \tilde{\varepsilon} + (1-\tilde{\varepsilon}) \log_2 (1-\tilde{\varepsilon}) \qquad (۶۹-۴)$$

[1] Fano's inequality

پس نهایتاً خواهیم داشت:

$$H(\frac{3}{2}\varepsilon)+(\frac{3}{2}\varepsilon)\log_2(4-1)\geq H(B|A) \qquad (۷۰-۴)$$

آنتروپی دوتایی را بهتر است با $h(.)$ نشان دهیم:

$$h(\frac{3}{2}\varepsilon)+(\frac{3}{2}\varepsilon)\log_2 3\geq H(B|A) \qquad (۷۱-۴)$$

و بدین طریق با استفاده از رابطه Csiszar-korner خواهیم داشت:

$$K\geq H(B|E)-H(B|A)\geq \sup_{\delta}(1-\frac{\varepsilon}{\delta})h(0.9091+4.5\delta)-\{h(\frac{3}{2}\varepsilon)+(\frac{3}{2}\varepsilon)\log_2 3\} \qquad (۷۲-۴)$$

برای محاسبه‌ی بیشترین حد آنتروپی که منجر به بیشترین نرخ کلید می شود، گفته بودیم که $x=(0.9091+4.5\varepsilon,1)$ و این یعنی $h(0.9091+4.5\varepsilon)=1$ است، پس در این صورت برای $Max\,H(B|E)$ خواهیم داشت:

$$H(B:E)=(1-\frac{\varepsilon}{\delta})h(0.9091+4.5\varepsilon)\cong 0.44 \qquad (۷۳-۴)$$

$$1-\frac{\varepsilon}{\delta}=0.44 \qquad \Rightarrow \qquad \frac{\varepsilon}{\delta}=0.56$$

$$\Rightarrow\ \delta=1.8\varepsilon \qquad (۷۴-۴)$$

پس از قرار دادن $\delta = 1.8\varepsilon$ در (۴-۴۵) به فرمول زیر که همه برحسب ε است، می‌رسیم:

$$K \geq 0.44h(0.9091+8.1\varepsilon) - h(\frac{3}{2}\varepsilon) - (\frac{3}{2}\varepsilon)\log_2 3 \qquad (۷۵-۴)$$

کم ترین نرخ کلید ۰ است. پس می توان نویز آستانه را بدست آورد.

$$0.44(0.9091+8.1\varepsilon)\log_2(0.9091+8.1\varepsilon) - 0.44(1-0.9091-8.1\varepsilon)\log_2(1-0.9091-8.1\varepsilon)$$
$$+(\frac{3}{2}\varepsilon)\log_2(\frac{3}{2}\varepsilon) + (1-\frac{3}{2}\varepsilon)\log_2(1-\frac{3}{2}\varepsilon) - \frac{3}{2}\varepsilon\log_2 3 = 0$$

با استفاده از حل عددی این معادله در مطلب، مقدار نویز آستانهٔ سیستم برابر بـا مقـدار $\varepsilon_0 \leq 0.0068$ بدست آمد یعنی اگر نویز سیستم از این مقدار بیشتر باشد کلید دیگر معتبر نیست.

حال اگر بیشترین حالت کلید که مقدار 0.439 است مدنظر باشد، میزان خطای سیستم به صورت زیر خواهد بود:

$$0.439 = -0.44(0.9091+8.1\varepsilon)\log_2(0.9091+8.1\varepsilon) - 0.44(0.09091-8.1\varepsilon)\log_2(0.09091-8.1\varepsilon)$$

$$+(\frac{3}{2}\varepsilon)\log_2(\frac{3}{2}\varepsilon) + (1-\frac{3}{2}\varepsilon)\log_2(1-\frac{3}{2}\varepsilon) - \frac{3}{2}\varepsilon\log_2 3 \qquad \Rightarrow \qquad \varepsilon \cong 0$$

پس نویز سیستم در بازه‌ی $0 < \varepsilon < 0.0068$ قرار دارد و همانطور که می‌دانیم نرخ محرمانه بودن کلید در این بازه به صورت زیر خواهد بود:

$$0 \leq K \leq 0.439$$

۷-۴ بررسی ایمنی بدست آمده با به کارگیری مکانیک کوانتومی

تا اینجا ما یک جعبه‌ی آرمانی و خیالی را مورد بررسی قرار دادیم، با استفاده از نتایج خود، لازم می-دانیم که این جعبه در آزمایشگاه قابل بررسی باشد یعنی از طریق مکانیک کوانتومی تأیید شود. در واقع جعبه توسط اندازه گیری مشاهده پذیری های پرس – مرمین توسط آلیس و باب تعیین می-شود، که نهایتاً منجر به استخراج غیر موضعیت از وابستگی به زمینه می شود[۳۰].

حال اگر ما یک جعبه سه تایی داشته باشیم، می توان نشان دادکه ایمنی بیت با سه قسمت تعیین می شود و به علاوه ایمنی تنها با فرض عدم علامت دهی برقرار است. به هر حال گر چه چنین جعبه ای وجود دارد اما متاسفانه نمی توان آن را با وسایل مکانیک کوانتومی به وجود آورد یعنی آن در طبیعت وجود ندارد (این قطعا با نتایج ما سازگار است).

دلایل ما اثبات می کند که کلید تعیین شده تحت حمله منفرد ایمن است (یعنی Eve با هر جعبه به طور مستقل جفت می شود و قبل از آلیس و باب اندازه می گیرد، به این حمله ،حمله منفرد می-گوییم)

نتیجه‌گیری و پیشنهادات

در این پایان نامه با پروتکل مستقل از دستگاه که شبیه به BB84 بود آشنا شدیم. این پروتکل با بهره‌گیری از متناقض نمای کوشن-اسپکر به اندازه‌گیری کمیات ناسازگار می‌پردازد و تبادل میان اطلاعات بدست آمده و اختلالات سیستم انجام می‌شود.

اگر این پروتکل را با پروتکل‌هایی که بطور مستقیم از غیرموضعیت استفاده می‌کنند مقایسه کنیم، به طور واضح باید جعبه‌های دو طرفه‌ی ما غیرموضع باشند. در غیر این صورت طبق گفته‌ی ایکرت، استراق سمع کننده می‌تواند تمام نتایج اندازه‌گیری‌های آلیس و باب را بدست آورد. پس ارتباط مستقیمی میان این پروتکل‌ها و پروتکل‌های غیر موضع وجود دارد. به علاوه مشاهده کردیم که پس از بررسی سیستم با استفاده از نقض نامساوی بل و بهینه سازی آن به یک غیرموضعیت قوی رسیدیم. بعد از استخراج کلید و بررسی نرخ محرمانه بودن کلید با استفاده از مفاهیم آماری به ایمنی بسیار بالاتری نسبت به بقیه‌ی پروتکل‌های غیر موضعیت رسیدیم چرا که برای ایمن‌ترین پروتکل تا به اکنون نویز آستانه‌ی سیستم ۲٪ بدست آمده است و ارسال اطلاعات از طریق این پروتکل با مقدار ۰/۶۸٪ بسیار ایمن‌تر است.

در ادامه پیشنهاد می‌شود که:

۱- ضمن بررسی و اعمال بقیه‌ی متناقض‌نماهای کوشن-اسپکر، می‌توان ایمنی پروتکل‌های مستقل از دستگاه را بالا برد.

۲- به علاوه می‌توان ایمنی این پروتکل را در مقابل بقیه‌ی حملات استراق‌سمع‌کننده بررسی کرده و آن‌ها را با پروتکل‌های غیرموضعیت دیگر مقایسه کرد

منابع:

[1] M. A. Nielson and I. L. Chuang, **(2000)** "**Quantum computation and quantum information**", Cambrige, United Kingdom

[2] D. McMahon ,"**Quantum computation explained**", A John Wiley & Sons, Inc., Publication

[3] J. Cirasella, (2008) "**Historicalbibliography of quantum computing**", Brooklyn College Library

[4] وحید کریم پور، مقاله‌ی پانزدهم، نظریه اطلاعات کلاسیکی **(http://sina.sharif.edu/~vahid/teachingQI.html)**

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

[6] J. Preskill, **(1998)** "**Lecture Notes for Physics 229: Quantum information and computation**", California Institude of Technology,September

[7] M. Oskin, "**Quantum computing-Lecture Notes**", Department of Computer Science and Engineering University of Vashington

[8] M. L. Bellac, **(2006)** "**An introduction to quantum information and quantum computation**", translated by Patricia de forcrand –millard, Cambrige

[9] P. Kaye, Raymond Laflamme Michel Mosca, "**An Introduction to quantum computing**", Oxford

[10] J. F. Clauser, M. A. Horne, A.Shimony, and R. A. Holt **(1969)**, **Phys. Rev. Lett.23,880**

[11] H. Movahhedian, **(2008)** "Stonger Violation of Local Theories whit Equalities", **arxiv.org:quant-ph/0611124v5**

[12] P. Shor, **(1995)** "Scheme for reducing decoherence in quantum computer memory", **Phys. Rev. A 52,R2493**

[13] G. P. Berman, G. D. Doolen, R. Mainiery, V. I. Tsifrenovich, **(1998)** "**Introduction to quantum computers**", British Library Cataloguing-in-Publication Data

[14] C. H. Bennett and G. Brassard, **(1984)** in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing **(IEEE Computer Society Press, New York, Bangalore, India, December 1984), pp. 175–179**.

[15] A. K. Ekert, **(1991) Phys. Rev. Lett. 67, 661**

[16] C. H. Bennett, G. Brassard, and N. D. Mermin, **(1992) Phys. Rev. Lett. 68, 557**

[17] H. Bechmann-Pasquinucci and A. Peres **(2000) Phys. Rev. Lett. 85, 3313 arXiv:quant-ph/0001083.**

[18] K. Nagata, **(2005) Phys. Rev. A 72, 012325), arXiv.org:quant-ph/0503158**

[19] S. Kochen and E. P. Specker **(1967)**, **J. Math. Mech. 17, 59**

[20] S.Wehner, **(2006) Phys. Rev. A 73, 022110 arXiv:quantph/0510076**

[21] J. Barrett, L. Hardy, and A. Kent, **(2005)**, **Phys. Rev. Lett. 95,010503**

[22] R. H. Tutuncu, K. C. Toh and M. J. Todd, **March.(2001)** " Solving semide_nite-quadratic-linear programs using SDPT3",

[23] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani , **(2007) Phys. Rev. Lett. 98, 230501. arXiv.org:quant-ph/0702152.**

[24] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski **(2009)**, **Nature 461, 1101, arXiv.org:quant-ph/0905.2292**.

[25] A. Peres**, (1990). Phys. Lett. A 151, 107**

[26] N. D. Mermin**, (1990). Phys. Rev. Lett. 65, 3373**

[27] A. Stairs, Philos. **(1983).Sci 50, 578**

[28] I. Csisz´ar and J. Körner, **(1978). IEEE 24, 339**

[29] U. M. Maurer**, (1993).IEEE 39, 773**

[30] A. Cabello, A bell inequality with local violation **(2009). arXiv.org:quant-ph/0910.5507**.

[31] E. J. Sullivan, **(2008).** A thesis submitted to the Graduate Faculty of **North Carolina State University** in partial fullfillment of the requirements for the Degree of Master of Science

[32] K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki3,2, Marcin Pawłowski, and M. Bourennane, **(2010). ArXiv.org:quant-ph/1006.468.**

Abstract

Nowadays, transmission information between Alice and Bob, by method of quantum mechanics is focus of attention of scientists and researchers. In this way, trying for the most of security is very important.

The first protocol, so called BB84, based on the fundamental quantum feature: incompatibility of measurements of quantum non-computing observables. So, following security of transmission information in systems that they have many eavesdroppers, we receive to below results.

In this thesis, we use another feature of quantum world- contextuality that manifested in famous Kochen-Specker paradox, and we increasing security of system, even if they do not trust devices.

This paradox includes families of bipartite probability distributions which locally exhibit the Kochen-Specker paradox conditions and, in addition, exhibit a new Bell's inequality by using of principle information causality, that it has correlations stranger than quantum correlations. After all by using violation it, we gain an interval for considering about existing or not existing eavesdropper. In addition, after computing threshold noise, we obtain the rate of secure key.

Keywords: Non locality - quantum information - quantum entanglement - quantum measurement - contextuality - quantum key distribution

Shahrood University of Technology

Faculty of physics

The effect of contextuality on the security of quantum key distribution

Fatemeh Mohammadi Pelarti

Supervisor:
Dr. Hossein Movahhedian

September 2011