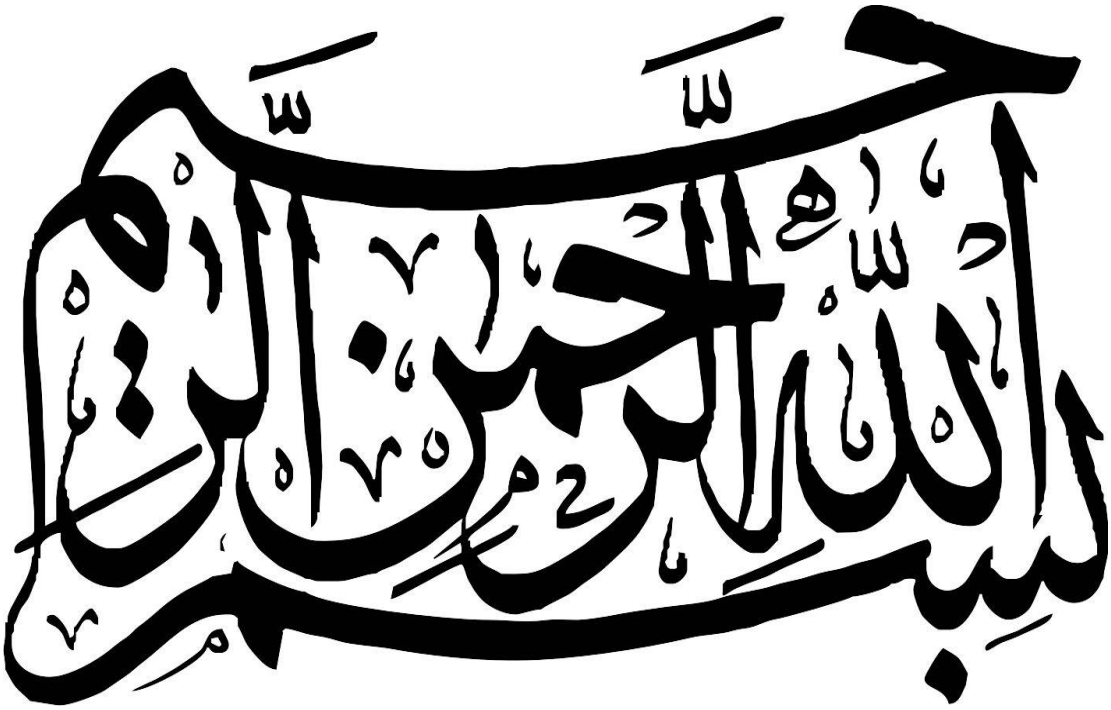

بسم الله الرحمن الرحيم

دانشکده فیزیک

پایان نامه کارشناسی ارشد

فیزیک ذرات بنیادی

عنوان:

ایمنی در پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه

ارائه دهنده : تکتم کاشانی

استاد راهنما :

دکتر حسین موحدیان

زمستان ۹۰

تقدیم به:

خواهرزاده‌های نازنینم پارسانا و پارمیدا،خواهر مهربانم مونا، مادر و پدرعزیزم

وبهترین مشوق زندگی‌ام دکتر فرحی

با سپاس و قدردانی فراوان از:

به نام او آغاز کرده بودیم و مدد از او طلبیدیم ولی در انتخاب موضوع چند شاخه بودیم و در جستن منابع یک تنه در جهت هم سویی به لطفی دل بستیم و راهنمائیش را خواستار شدیم و اینجا جناب آقای **دکترحسین موحدیان** استاد گرامی مرا را به ((نور)) هدایت کرد و در آن مسیر مرا پا به پا برد. لذا لذا جا دارد از ایشان که با راهنمایی‌ها و صبر و بردباری‌شان به بنده کمک زیادی کردند کمال تشکر را بنمایم.

همچنین از تمامی اساتید محترم دانشگاه صنعتی شاهرود و هیأت محترم داوران به خاطر قبولی داوری و نقد و بررسی رساله کمال تشکر و قدردانی را انجام دهم. در نهایت از خانم شیردل و دوستان عزیزم: فاطمه خطیب، منا عزیزی، جواد محمدیان، زهرا شیخ الاسلام، بصیرا کبیری و مریم برزگر که در طول مدت تحصیلم کمک‌های شایانی به من کردند صمیمانه قدردانی و تشکر می‌کنم. باشد که آنان نیز ما را یاد کنند و بر ایمان ادامه‌ی این تحقیق و جستن را تا رسیدن آرزو کنند.

چکیده:

یکی از مهمترین مسائلی که در اطلاعات کوانتومی با آن مواجه هستیم، انتقال اطلاعات بصورت ایمن می‌باشد. این عمل در رمزنگاری کلاسیکی امکان پذیر نمی‌باشد. از اینرو ما پروتکلی را معرفی می‌کنیم که همانند همه پروتکل‌های توزیع کلید کوانتومی(QKD)، امنیت آن مبتنی بر قوانین فیزیک کوانتومی است و دیگر اینکه هیچ اطلاعاتی از آزمایشگاه دو کاربر مجاز فاش نمی‌شود. این طرح پروتکل توزیع کلید کوانتومی مستقل از دستگاه(DIQKD) نام دارد. اثبات ایمنی این پروتکل بر فرضیات کمتری استوار است، بدین معنی که دو کاربر نه تنها از ساختار دستگاه‌هایشان بطور دقیق خبر ندارند بلکه به دستگاه‌هایشان هم اعتماد نخواهند کرد و یا اینکه ما فرض نمی‌کنیم که دستگاه های آلیس و باب مشخصه‌ی از قبل تعیین شده داشته باشند، چون ممکن است که دستگاه‌های اندازه‌گیری آلیس و باب توسط استراق سمع کنند(Eve) دستکاری شوند. ما نشان خواهیم داد که ایمنی این نوع پروتکل‌ها از بهم آمیختن دو واقعیت تبعیت می‌کند بطوریکه اگر از نقض نامساوی بل استفاده شود، در آنصورت هر پروتکل توزیع کلید کوانتومی مستقل از دستگاه در مقایسه با پروتکل استاندارد توزیع کلید کوانتومی ایمنی به مراتب قوی‌تری خواهد داشت و علاوه بر این، اینکه ایو محدود به حملات دسته جمعی است-در حملات دسته جمعی فرض شده‌است که ایو به هر دستگاه مورد استفاده در پروتکل بطور یکسان و مستقل حمله می‌کند. هدف پروتکل‌های مستقل از دستگاهی که ما دراینجا تحلیل و بررسی می‌کنیم؛ توزیع کلید سّری‌ای است که امنیت آن بر اساس قوانین فیزیک کوانتومی است، بنابراین در این طرح فرض می‌کنیم که بیتهای رشته کلید مستقل از هم باشند و با هم بر هم کنش نداشته باشند، همچنین با یکدیگر فاصله فضا گونه داشته باشند و در نتیجه از آن برای تولید نرخ ایمنی کلیداستفاده می‌کنیم.

واژگان کلیدی: توزیع کلید کوانتومی، توزیع کلید کوانتومی مستقل از دستگاه، اطلاعات کوانتومی، BB۸۴، آنتروپی، نرخ کلید محرمانه، حملات دسته جمعی.

فهرست مطالب صفحه

۱سیر تکامل محاسبه و اطلاعات کوانتومی

۲ توزیع کلید کوانتومی

۳ آنتروپی و اطلاعات

لیست تصاویر **صفحه**

لیست جداول **صفحه**

۱

سیر تکامل محاسبه و اطلاعات کوانتومی

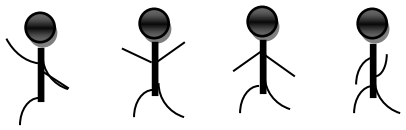
۱-۱ پیشگفتار

هدف محاسبات کوانتومی و اطلاعات کوانتومی مطالعه پردازش اطلاعات و انتقال اطلاعات بصورت ایمن است که با استفاده از سیستم‌های مکانیک کوانتومی می‌تواند انجام پذیر باشد. این ایده عمیق قبل از پردازش اطلاعات با استفاده از مکانیک کوانتومی از زمانهای باستان ذهن بشر را به خود جلب کرده بود. در این حین رمزنگاری اهمیت بسزایی پیدا کرده‌بود.

در زمانهای قدیم برای‌اینکه اطلاعات را به صورت محرمانه انتقال دهند، سعی داشتند که این پیام را بطور ایمن بفرستند. اوائل از روش‌های خیلی ابتدایی استفاده می‌کردند، مثلاً با استفاده از مرکب‌های نامرئی متن را می‌نوشتند، سپس در مقصد متن را نزدیک شعله آتش می‌گذاشتند و متن مورد نظر ظاهر می‌شد. بعدها برای ایمنی بیشتر رمز را بدین صورت انتقال می‌دادند که موهای‌سر شخصی را از ته کوتاه می‌کردند و پیام را روی سر این فرد می‌نوشتند و مدتی صبر می‌کردند تا موهای سر فرد بلند شود و وی را به مقصد می‌فرستادند، سپس در مقصد متن را بازگشایی می‌کردند.

زمانی تاریخ اروپا از ارتباطات بصورت رمزی غنی بود که باعث پیشرفت آن شده بود و این رمزنگاری و رمزگشایی در طول تاریخ پیشرفت بسیاری کرد و به یک علم مهم و خیلی جدی تبدیل شد و چه خون‌ها بر سر این رمزنگاریها ریخته نشده است!

نوع دیگر رمزنگاری رشته‌ای از آدمک‌ها است که بصورت گوناگون کشیده شده‌است و هرکدام از این آدمک‌ها نشان دهنده یک حرفی است.

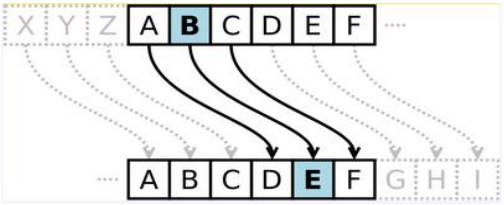


تصویر ۱-۱

در مورد اینگونه رمزنگاری یک داستان غم‌انگیز در قرن شانزدهم وجود دارد، ماری ملکه اسکاتلند

در تبعید و رقیب دختر عمویش ملکه الیزابت، پادشاه انگلیس بود. عده‌ای از ماری برای به سلطنت رساندن وی پشتیبانی می‌کردند و در زندان برعلیه الیزابت اول ملکه انگلیس با وی مکاتبه می‌کردند که بتوانند آزادش کنند و پادشاهی را در دست بگیرد. ملکه الیزابت در دربار صدراعظمی بسیار هوشمند داشت بنام سِر فرانسیس واشینگام[۱] که به این مکاتبات شک کرد و آنرا به متخصصان نشان داد و آنها رمز را باز کردند و به متن واقعی پی بردند و این امر باعث گردن زدن ملکه ماری به جرم خیانت شد[۱].

یکی از ساده‌ترین و شناخته شده‌ترین تکنیک‌های رمزنگاری که در آینده ابداع شد کد سزار بود که این روش رمزنگاری، هر حرف با حرف مشخصی جایگذاری می‌شود. در این روش همانطور که در تصویر۱-۲ نشان داده شده‌است، حروف الفبا را به اندازهٔ سه تا جابه‌جا می‌کردند و در نتیجه متنی که رمزینه شده‌بود تبدیل به یک متن ناخوانا می‌شد و کسی در این وسط نمی‌توانست به آن دسترسی پیدا کند و متوجه چیزی نمی‌شد مگر اینکه این شخص بفهمد که این متن جابه‌جا شده و به آن متن آگاهی پیدا کند و یااینکه اگر در زمان رم باستان باشیم، همه میفهمند که کد سزار وجود دارد و سه بار آنرا جابه‌جا می‌کند، و همچنین ممکن است در رمزگذاری سزار، افراد مختلف از کلیدهای مختلف استفاده کنند و متن را می‌توانند چندین بار شیفت دهند و سپس پیام واقعی را پیدا کنند[۲]. مثلاً اگر مقدار انتقال ۳ باشد، حرف A به حرف D منتقل خواهد شد و B به E و C به F و به همین ترتیب بقیه‌ی حروف مشخص می‌گردد. این روش به‌نام ژولیوس سزار نامگذاری شده که برای ارتباط با ژنرال-ها خود از آن بهره می‌جست.



تصویر ۱-۲

۱. Sir Francis Walsingham

حال به گذشته‌ای نه چندان دور برمیگردیم و به ایده بنیادی در محاسبات کوانتومی و اطلاعات کوانتومی، علوم‌کامپوتر و تئوری‌اطلاعات که در زمینه رمزنگاری نقش بسزایی داشت، نگاهی می-اندازیم. همچنین می‌خواهیم نگاه کوتاهی به تاریخچه‌ی بررسی تحول علوم‌کامپیوتر بیاندازیم.

روند این تحولات در قرن بیستم شروع شد، یک تحول غیرقابل انتظار در مسیر علم ویک بحران جدی در فیزیک به وقوع پیوست. گسترش رمزنگاری مدرن تا حد زیادی مدیون تحقیقاتی است که زیر فشار جنگ جهانی دوم برای شکستن کدهای رمزنگاری توسط ریاضی‌دان بزرگ آلن تورینگ[۱] در سال ۱۹۳۶ انجام شد که مدلی برای محاسبات به عنوان ماشین تورینگ ارائه داد[۳]، تورینگ نقش مهمی در خاتمه پیدا کردن جنگ جهانی و شکست آلمان‌ها داشت. در زمان جنگ جهانی دوم آلمان-ها رمزی را درست کرده‌بودند بنام دستگاه انیگما[۲]، این ماشین دارای چندین چرخ دنده است که حروف الفبا را به حروف دیگری نگاشت می کند، برای مثال حرف A به حرف P نگاشت می شود و الی آخر. برای این کار لازم است اپراتور یک سری تنظیمات اولیه را بر روی دستگاه انجام دهد که در طرف دیگر دریافت کننده پیغام نیز دقیقاً همان تنظیمات را انجام داده است. برای جلوگیری از کشف سریع نگاشت ها در هر بار تکرار یک حرف، چرخ دنده یک بار می چرخد و این بار مثلاً حرف A به جای اینکه به P نگاشت شود به X نگاشت می شود. این کار طبق همان تنظیمات اولیه صورت می پذیرد. در طرف دریافت کننده نیز جهت رمزگشایی پیغام نیاز به یک ماشین انیگما دقیقاً مطابق با طرف فرستنده و همچنین نیاز به دانستن تنظیمات اولیه چرخ دنده است . با این وجود در زمان جنگ به رهبری تورینگ و یک عده متخصص و ریاضیدانان یک کامپیوتر عملی را ساختند که وقتی آلمانها صبح شروع به مخابره می‌کردند، این ریاضیدانان در مدت زمانی معقول رمز را باز می‌کردند، با وجود اینکه رمز خیلی پیچیده بود اما این رمزگشایی یکی از دلایل مهم شکست آلمان‌ها بود. در دهه‌های پس از جنگ جهانی دوم استفاده از کامپیوترها در شکستن کدهای رمزنگاری شده انقلابی را در

---

۱. Alan Turing

۲. Enigma

رمزنگاری ایجاد کرد و باعث انتشار گسترده رمزنگاری در سازمانهای نظامی و اطلاعاتی شد و دامنه استفاده از آن تا سیستم های کامپیوتری معمولی نیز گسترش پیدا کرده است.

توانایی ماشین تورینگ برای حل مسائلی که ماشین‌های دیگر از آن عاجز هستند، بسیار زیاد است. تورینگ ادعا کرد، یک ماشین تورینگ جهانی وجود دارد که از آن می‌توان برای شبیه سازی دیگر ماشین‌های تورینگ استفاده کرد. بعد از مقاله تورینگ سازنده اولین کامپیوتر شامل اجزاء الکترونی جان ون نیومن [۱] بود که مدل تئوری ساده‌ای را ارائه داد که چطور در مدل عملی می‌توان اجزاء یک کامپیوتر را کنار هم قرار داد تا توانایی‌های ماشین تورینگ جهانی را داشته باشد.

سخت افزار در سال ۱۹۵۴ توسعه پیدا کرد، وقتی که جان باردین[۲] ، والتر براتین[۳] ، و ویل شاکلی[۴] ترانزیستور را کشف کردند. پیشرفت رشد سخت افزار با سرعت ادامه پیدا کرد تا اینکه در سال ۱۹۶۵توسط گوردون مور[۵] قانونی تجربی وضع شد که به عنوان "قانون مور" شناخته شده‌است که می‌گوید: " توان کامپیوترها در هر سال دو برابر می‌شود." البته قانون مور تا حدودی برقرار است و تا قرن بیست‌ویکم به ابعاد اتمی خواهدرسید و اثرات کوانتومی ظاهر خواهد شد. این امر باعث تفکر بشر برای پیدایش کامپیوترهای کوانتومی شد که شاید بتوان با استفاده از دنیای ذرات میکروسکوپی و قوانین کوانتومی، ضعف ایجاد کلید در رمزنگاری را از بین برد.

چون کنترل سیستم‌های کوانتومی در ابعاد اتمی بسیار مشکل است، مردم به دنبال راه‌حل‌های دیگری هستند تا بدون رسیدن به ابعاد اتمی سرعت و توانایی‌های کامپیوتر کلاسیک را بالا ببرد.

یک راه ممکن برای حل این مشکل کشف الگوریتم‌های متفاوتی برای به اجرا در آوردن محاسبات است که براساس ایده استفاده از مکانیک کوانتومی به جای فیزیک کلاسیک است که توانایی بالاتری نسبت به الگوریتم‌های فعلی دارند و نشان دهنده توان بالای کامپیوترهای کوانتومی بود.

---

۱ . John Von Neuman

2 . John Bardin

3 .Waiter Brattain

4 . Will Shockley

5 .Gordon Moore

اولین چالش اصلی برای تئوری قویِ ماشین تورینگ در اواسط سال ۱۹۷۰ برخاسته شد، وقتی که رابرت سولوی[۱] و والکر استراسن[۲] نشان دادند که با استفاده از الگوریتم تصادفی می‌توان امتحان کرد که یک عدد معین اول است یا مرکب [۴]. الگوریتم با قاطعیت مشخص نمی‌کرد که آیا عدد اول است یا مرکب. به‌جای آن، الگوریتم می‌توانست احتمال اول بودن را مشخص‌کند. با تکرار آزمایش سولوی– استراسن با احتمال نزدیک به یقین می‌توان گفت که آیا عدد اول است یا مرکب.

الگوریتم‌های تصادفی چالشی را برای تئوری ماشین تورینگ قطعی مطرح کرد، بطوریکه یک مسئله مؤثر غیرقابل حل وجود داشت که می‌توانست بطور مؤثر روی ماشین تورینگ قطعی حل شود. این چالش بطوری ظاهر می‌شود که بتواند تغییرات ساده تئوری ماشین تورینگ را برطرف کند.

هر فرایند الگوریتمی را می‌توان بطور مؤثر با استفاده از ماشین تورینگ احتمالی شبیه سازی کرد.

در سال ۱۹۸۵ دیوید دوویچ[۳] فهمید که می‌توان از قوانین فیزیک برای ارائه نوع قویترِ تئوری تورینگ استفاده‌کرد[۶،۵]، همچنین دوویچ تلاش کرد که دستگاه محاسباتی را تعریف کند که قادر به شبیه سازی یک سیستم فیزیک دلخواه باشد. چون قوانین فیزیک کاملاً براساس مکانیک کوانتومی هستند، دوویچ دستگاه‌های محاسباتی‌ای را درنظر گرفت که براساس اصل مکانیک کوانتومی باشد. وی به دنبال این بود که بداند آیا توسط کامپیوترهای کوانتومی امکان حل مسائلی که هیچ حلی در ماشین تورینگ کلاسیک ندارد وجود دارد؟ مدلی ارائه داد که نشان‌دهنده قدرت محاسباتی کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیکی بود.

اوج این پیشرفت در سال ۱۹۹۴توسط پیترشور[۴] بود که به دو مسئله خیلی مهم اشاره کرد[۷] که یک کامپیوتر کوانتومی می‌تواند بطور مؤثری یک عدد بزرگ را به عامل‌های اول تجزیه کرد و آنرا "

---

۱. Robert Solovay

۲ .Volker Strassen

3.David Deutsch

4 . Peter Shor

الگوریتم گسسته" نامید و توانست در کامپیوتر کوانتومی بسیار کارآمدتر از کامپیوترهای کلاسیک باشد.

در حالت کلی اگر p و q اعداد اول بزرگی باشند حاصلضرب آنها n = pq می‌تواند به سرعت محاسبه شود، اما اگر عدد n داده شود پیداکردن p و q مشکل خواهد بود. زمان مورد نیاز برای پیدا کردن عاملهای اول هنگامی‌که n افزایش می‌یابد سریعتر از هر توانی از Ln n رشد می‌کند. با استفاده از این الگوریتم مثلاً می‌توان ۶۵ عامل اول از یک عدد ۱۳۰ رقمی را در مدت زمان حدود یک ماه حساب کرد و انجام این عمل توسط کامپیوتر کلاسیکی برای یک عدد ۴۰۰ رقمی حدود $۱۰^{۱۰}$ سال طول خواهدکشید ولی محاسبه با استفاده از الگوریتم شور کمتر از سه سال انجام می‌شود و یا تجزیه یک عدد ۶۰۰ یا۷۰۰ رقمی به اندازه عمرکیهان طول خواهدکشید. نتیجه شور دلالت بر این داشت که کامپیوترهای کوانتومی بسیار قویتر از ماشین‌های تورینگ است.

در همین زمان که الگوریتم شور کشف شده‌بود، بسیاری از مردم در حال توسعه ایده ریچارد فاینمن[1] بودند که در سال ۱۹۸۲مطرح شده بود. فاینمن مشاهده کرد که اثرات مکانیک کوانتومی خاص نمی‌تواند بطور مؤثری بر یک کامپیوتر کلاسیکی شبیه سازی شود[۸]. این مشاهده منجر به درک این مسئله شد که شاید با استفاده از این اثرات کوانتومی بتوان محاسباتی با بازده بالاتر انجام داد. مسئله دیگری که کامپیوترهای کوانتومی بسیار سریعتر از کامپیوترهای کلاسیکی حل کردند این بود که:

طراحی الگوریتم برای کامپیوترهای کوانتومی دشوار به نظر می‌رسید زیرا طراحان با دو مشکل مواجه می‌شوند که در ساختار الگوریتم ها برای کامپیوترهای کلاسیکی با این مسئله رو به رو نشده‌اند. اولین مسئله این است که بینش بشر بر پایه جهان کلاسیک است. بنابراین اگر بخواهیم الگوریتمی را طراحی کنیم که از هر الگوریتم کلاسیکی در آن زمینه کارآمدتر و مؤثرتر باشد پس باید کلاسیک را

[1] . Richard Feynman

کنار بگذاریم و دید کوانتومی پیدا کنیم. دومین مسئله این است که نباید الگوریتمی طراحی کنیم که فقط جنبه مکانیک کوانتومی داشته باشد. الگوریتم باید بهتر از هر الگوریتم‌های کلاسیکی موجود در حال‌حاضر باشد، بنابراین امکان‌پذیر است که الگوریتمی پیدا کنیم که در مقابل نویز[۱] ایمنی بیشتری داشته باشد.

در همین زمان که علم کامپیوتر در سال ۱۹۴۰ در حال پیشرفت بود، تحول دیگری در درک ارتباطات در حال وقوع بود که در سال ۱۹۴۸ کلود شانون[۲] مقاله چشم‌گیری را که پایه واساس تئوری اطلاعات و ارتباطات مدرن بود را منتشر کرد و ثابت کرد که روش One Time Pad حتی با داشتن کامپیوتری با توان محاسباتی بی‌پایان غیرقابل رمزگشایی است، شاید اولین مرحله برای تعریف ریاضی مفهوم اطلاعات توسط شانون بود.

شانون به دو مسئله کلیدی مربوط به انتقال اطلاعات روی کانال ارتباطی علاقمند بود.

۱) یکی اینکه چه ابزاری برای فرستادن اطلاعات روی کانال ارتباطی مورد نیاز است؟ مثلاً شرکت های مخابره‌ی اطلاعات نیاز دارند به اینکه چطور بتوانند اطلاعات را بطور امن روی کابل تلفن مخابره کنند.

۲) دوم اینکه آیا می‌توان اطلاعات را منتقل کرد به طریقی که در مقابل نویز در یک کانال ارتباطی ایمن باشد؟

شانون با اثبات دو قضیه بنیادی تئوری اطلاعات به این دو سؤال پاسخ داد:

۱) قضیه کدگذاری کانال بدون نویز شانون، با معین‌کردن وسیله‌های فیزیکی مورد نیاز برای ذخیره کردن خروجی از یک منبع اطلاعاتی، به سوال اول خود پاسخ داد.

۲) دومین قضیه بنیادی شانون، تئوری کدگذاری کانال نویزدار است که معین می‌کند ایمنی اطلاعاتی که از درون کانال ارتباطی نویزدار ارسال می‌شود چقدر است؟ شانون نشان داد که از کدهای

---

۱. Noise

۲. Claude Shannon

تصحیح-خطا برای محافظت اطلاعات فرستاده شده استفاده می‌شود. متأسفانه قضیه شانون بطور واضح و آشکار کدهای تصحیح–خطای مفیدی برای دستیابی به این اطلاعات را به ما نداد. بعد از مقاله‌ی شانون تا به امروز، تحقیقات بیشتر و بهتری از این کدهای تصحیح و خطای کوانتومی ارائه شد که از حالت‌های کوانتومی در مقابل نویز محافظت می‌کند.

حال چطور می‌توان اطلاعات کلاسیکی رایج را با استفاده از کانال کوانتومی منتقل کرد؟ در سال ۱۹۹۲ چارلز بنت[1] و استفان ویزنر[2] بیان کردند که می‌توان دو بیت حاوی اطلاعات کلاسیکی را ارسال کرد، بطوریکه فقط یک بیت کوانتومی از فرستنده به گیرنده ارسال می‌شود. این نتیجه به نام کد کردن فوق چگال نامگذاری می‌شودکه در این فصل اشارهٔ مختصری به آن خواهیم کرد.

تصور کنید که می‌خواهیم اطلاعات کوانتومی را از سوی آلیس در درون یک کانال کوانتومی نویز-دار به باب بفرستیم، سپس غیرممکن است که اطلاعات بدون هیچ اختلالی از آلیس به باب برسد. از اینرو لازم است تا این اطلاعات بطور رمزنگاری شده از آلیس به باب ارسال شود که در مبحث آینده به آن می‌پردازیم. البته مسائل دیگری نیز مطرح شد که یکی از آن مسئله شبیه سازی[3] سیستم کوانتومی است و اینکه آیا امکان پذیراست که از اثرات مکانیک کوانتومی استفاده کرد که اطلاعات بیشتر از سرعت نور انتقال پیدا کند– بر پایه تئوری نسبیت اینشتین– این مسئله در صورتی به نتیجه مطلوب می‌رسد که شبیه سازی یک حالت کوانتومی نامشخص امکان‌پذیر باشد یعنی یک کپی از حالت کوانتومی ساخته شود. اگر شبیه سازی امکان‌پذیر باشد آنگاه می‌توان با استفاده از اثرات کوانتوم اطلاعات را بیشتر از سرعت نور ارسال کنیم. برای درک بیشتر این مسئله قضیه نوکلونینگ را مورد بحث و بررسی قرار دهیم.

[1] . Charles Bennett
[2]. Stephen Wiesner
[3] .Cloning

۱-۲ قضیه نوکلونینگ یا عدم شبیه سازی[1]

این نظریه توسط ووترز[2] و زورگ[3] ارائه شده‌است[۹]. آنها ثابت کردند که نظریه کوانتومی یک نظریه خطی است، یعنی اینکه تبدیلات در آن خطی‌اند.

استدلال خطی بودن کوانتوم مکانیک:

$$U(|0\rangle|b\rangle) = |0\rangle|0\rangle \quad (۱-۱)$$

$$U(|1\rangle|b\rangle) = |1\rangle|1\rangle \quad (۱-۲)$$

$$U((|0\rangle + |1\rangle)|b\rangle) = (|0\rangle + |1\rangle)(|0\rangle + |1\rangle) = |0\rangle|0\rangle + |1\rangle|1\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle \quad (۱-۳)$$

علاوه برآن، عمل شبیه سازی یا کپی‌کردن اطلاعات کوانتومی درصورت وجود در بسیاری از کاربردهای نظریه کوانتومی و محاسبات کوانتومی کار آمد خواهد بود[۱۰]. اما خواهیم دید که خطی بودن مکانیک کوانتومی باعث می‌شود که نتوانیم تبدیل جهانی[4] داشته باشیم که از هر حالت دلخواه کوانتومی مدل یکسانی خلق کند، آنرا بصورت زیر ملاحظه می‌کنیم.

فرض می‌کنیم که تبدیل یکانی جهانی داریم که از حالت دلخواه $|\psi_1\rangle$ مدل یکسان دیگری بسازد، و حالت سیستم کوانتومی که حالت جدید آن $|\varphi_1\rangle$ است، درضمن بقیه عالم که شامل دستگاه کپی کننده باشد را در حالت $|x\rangle$ قرار می‌دهیم. اثر این تبدیل یکانی شبیه سازی روی این سیستم‌ها اینگونه است:

$$U(|\psi_1\rangle|\varphi\rangle|x\rangle) = |\psi_1\rangle|\psi_1\rangle|X'_{\psi_1}\rangle \quad (۱-۴)$$

که در آن $|X'_{\psi 1}\rangle$ حالت بقیه سیستم‌ها پس از شبیه سازی است که به ψ_1 هم وابسته است. حال فرض می‌کنیم که این تبدیل جهانی، حالت $|\psi_1\rangle$ را شبیه سازی کند. پس داریم:

[1] . Nocloning theorem
[2] .Wooters
[3] .Zurek
[4] .Universal

$$U(|\psi_2\rangle|\varphi\rangle x\rangle) = |\psi_2\rangle|\psi_2\rangle|x'_{\psi_2}\rangle \quad (۵-۱)$$

حال اگر حالت $|\psi\rangle = a_1|\psi_2\rangle + a_2|\psi_2\rangle$ را به تبدیل جهانی نسبت دهیم، طبق معادله (۱) داریم:

$$U(|\psi\rangle|\varphi\rangle|x\rangle) = U([a_1|\psi_1\rangle + a_2|\psi_2\rangle]|\varphi\rangle|x\rangle) = a_1U(|\psi_1\rangle|\varphi\rangle|x\rangle) +$$
$$a_2U(|\psi_2\rangle|\varphi\rangle|x\rangle) = a_1|\psi_1\rangle|\psi_1\rangle|x_{\psi_1}\rangle + a_2|\psi_2\rangle|\psi_2\rangle|x_{\psi_2}\rangle \neq |\psi\rangle|\psi\rangle|x'_{\psi}\rangle \quad (۶-۱)$$

بنابراین در حالت کلی خطی‌بودن مکانیک کوانتومی مانع از شبیه سازی عام حالت‌های دلخواه می‌شود. این موضوع به قضیه نوکلونینگ معروف است [۱۰, ۱۱].

این نکته قابل توجه است که از معادله‌های ۱ و۲ با ضرب داخلی دو طرف و استفاده از یکانی بودن U به این نتیجه می‌رسیم :

$$\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle\langle\psi_1|\psi_2\rangle\langle x_{\psi_1}|x_{\psi_2}\rangle \quad (۷-۱)$$

پس دیده می شود به جز حالت بدیهی که در آن $|\psi_1\rangle = |\psi_2\rangle$ است، شبیه سازی غیر ممکن است، مگر در حالت $\langle\psi_1|\psi_2\rangle = 0$. بنابراین کپی شدن برای حالت‌های غیریکسان (نامتعامد) امکان پذیر است نه برای هرحالت کوانتومی دلخواه که گاهی به آن "قضیه نوکلونینگ حالت‌های نامتعامد" هم می‌گویند. پس حالت‌های کوانتومی را نمی‌توان برای مدارهای پیچیده‌تر کپی کرد. با توجه به نامساوی عدم قطعیت در مکانیک کوانتومی این مسئله صحیح است، به این دلیل که:

در مکانیک کوانتومی، وقتی می‌خواهیم بطور همزمان دو کمیت جابجا نشدنی را اندازه‌گیری کنیم، نامساوی عدم قطعیت قیدی را روی حاصل این اندازه‌گیری می‌گذارد، بدین‌گونه که دقت هرکدام را نمی‌توان از یک حدی بیشتر کرد، اندازه‌گیری یکی روی اندازه‌گیری دیگری تأثیر می‌گذارد، درحقیقت این‌دو کاملاً به‌هم وابسته‌اند.

حال اگر شبیه سازی دقیق امکان پذیر بود، در آنصورت می‌توانستیم روی یکی از مدل‌ها (حالت ها)، یکی از این دو کمیت‌ها را با دقت اندازه‌گیری کنیم و بعد روی مدل دیگر هم کمیت دیگر را اندازه‌گیری نماییم ، بدون اینکه نتیجه آزمایش روی همدیگر اثر کند.

پس در حالت کلی هیچ عمل فیزیکی نمی‌تواند تبدیل $|\psi_i\rangle \rightarrow |\psi_i\rangle|\psi_i\rangle$ را انجام دهند. بطور کلی پدیده نوکلونینگ در مکانیک کوانتومی ممکن نیست. تئوری نوکلونینگ در اوایل سال ۱۹۸۰ کشف شد، که این یکی از نتایج اخیر ارتباطات کوانتومی و اطلاعات کوانتومی است.

مسئله اصلی در رمزنگاری تبادل اطلاعات بین دو کاربر بطورسرّی می‌باشد. فرض کنید که شما می‌خواهید برای مبادله کالا شماره کارت اعتباری خود را به همکار خود بدهید، بدون اینکه نفر سومی به رمز کارت شما دسترسی پیداکند. روشی که می‌توان ازآن استفاده‌کرد پروتکل رمزنگاری[۱] است که از موفقیت‌های بزرگ ارتباطات کوانتومی و اطلاعات کوانتومی است، به‌این‌دلیل که در مقابل جاسوس(استراق سمع کننده) با توان محاسباتی نامحدود کاملاً ایمن است. این امر در مکانیک کلاسیک امکان پذیر نیست چون رمزنگاری به روش کلاسیک راحتتر شکسته می‌شود، (شکستن قویترین رمز در کلاسیک حداکثر شش ماه طول می‌کشد و یک کامپیوتر کوانتومی می‌تواند رمزِ یک کامپیوتر کلاسیکی را در زمان حدود چند دقیقه رمز بشکند و جاسوس به آسانی به محتوای پیام دسترسی پیدا کند ولی اگر یک کامپیوتر کوانتومی داشته‌باشیم، هیچ کامپیوتر کوانتومی دیگری-به جز خودش- نمی‌تواند رمز آنرا بشکند) علاوه براین درهم‌تنیدگی در رمزنگاری کوانتومی باعث شده-است که پروتکل رمزنگاری بسیار قویتر و مؤثرتری داشته باشیم که در کلاسیک غیر ممکن است. در بخش بعدی به توضیح مختصری از حالت‌های درهم تنیدگی که فقط مختص به فیزیک کوانتوم می-باشد، می‌پردازیم.

---

۱. Cryptography Protocol.

۱-۳ درهم‌تنیدگی کوانتومی

آنچه که درانتقال اطلاعات کوانتومی نقش اساسی دارد وجود حالت‌های درهم‌تنیده است. همچنین از اطلاعات کوانتومی که شامل درهم‌تنیدگی، برهم‌نهی، عدم شبیه سازی و انجام عملیات دیگری که از لحاظ کلاسیک امکان‌پذیر نیست، برای مخابره‌ی اطلاعات استفاده می‌کنند.

به هر حالت خالص[۱] دو قسمتی می‌توان یک عدد مثبت نسبت داد، بنام عدد اشمیت که برابر با تعداد ویژه مقادیر غیر صفر ρ_A یا ρ_B است. بنابراین اگر عدد اشمیت بزرگتر از یک باشد $|\psi\rangle_{AB}$ درهم‌تنیده[۲] است، درغیر اینصورت جدائی‌پذیر است[۱۲, ۱۳].

فرض می‌کنیم که سیستم M از دو زیر سیستم A و B تشکیل شده است و $|\psi\rangle_{AB}$ حالت سیستم است و $|i\rangle_A$, $|\mu\rangle_B$ حالت‌های هرکدام از این زیر سیستم‌ها هستند. ψ را جداپذیر می‌گوییم اگر بتوان ماتریس چگالی آنرا بصورت زیر نوشت :

$$\rho_{AB}=\sum a_{i\mu} \quad \rho_A^{i} \otimes \rho_B^{i} \qquad (۸-۱)$$

که $a_{i\mu}$ احتمال حضور در حالت iام است.

حالت‌های $|\psi\rangle_{AB}$ ای که ماتریس چگالی آنها را نمی‌توان بصورت حاصلضرب ماتریس چگالی هر کدام از زیر سیستم‌ها نوشت را حالت درهم‌تنیده گویند. خصوصیت درهم‌تنیدگی این است که چون ماتریس چگالی‌های ρ_A , ρ_B خالص نیستند و آنرا نمی‌توان بصورت حاصلضرب حالت‌های مجزا نوشت، بنابراین فضای هیلبرت یک حالت درهم تنیده $H_A \otimes H_B$ است که نمی‌توان آنرا به صورت $|i\rangle_A\ |\mu\rangle_B$ نوشت. لذا در حالت‌های درهم‌تنیده اندازه‌گیری روی قسمتی از سیستم بر کل سیستم اثر خواهد گذاشت. این ایده به ذهن می‌رسد که به دلیل‌اینکه اندازه‌گیری باعث تقلیل سیستم می‌شود، از اینرو به وجود استراق سمع کننده پی‌برده می‌شود. بنابراین بین این زیرسیستم‌ها همبستگی‌ای وجود دارد.

---

۱. pure

۲. Entanglement

اما همبستگی در حالت‌های درهم‌تنیده کاملاً متفاوت است. مثلاً در حالت $\frac{1}{\sqrt{2}}$ ($|\uparrow\downarrow\rangle$ - $|\downarrow\uparrow\rangle$) اگر آلیس روی ذره A اندازه‌گیری کند و نتیجه ↑ را بدست آورد، ذره دوم حتماً باید در حالت ↓ قرار بگیرد. بنابراین اندازه‌گیری بر روی یکی از زیرسیستم‌ها بر روی حالت دیگر اثر می‌گذارد.

ولی در حالت‌های جداپذیر مثل حالت $|\uparrow\rangle_A |\uparrow\rangle_B$ که هر دو ذره در حالت ↑ هستند، هیچگونه همبستگی‌ای میان زیر سیستم‌ها وجود ندارد. بدین‌صورت که اندازه‌گیری روی ذره A تأثیری بر روی حالت ذره دوم نخواهد داشت و در آن تغییری بوجود نمی‌آورد.

از حالت‌های درهم‌تنیده برای ارسال اطلاعات استفاده می‌کنند. از مهمترین حالت‌های درهم‌تنیده جفت حالت EPR یا حالت‌های چهارگانه در پایه‌های بل است.

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

اگر آلیس روی دوکیوبیتی که دراختیار دارد در این پایه‌ها اندازه‌گیری انجام‌دهد، چهار نتیجه ممکن است حاصل شود که به ازای هر یک از نتایج ممکن، حالتی که دردسترس باب است دچار تغییر می‌شود.

در سالهای اخیر تلاش برای درک بهتر خواص درهم‌تنیده‌گی صورت‌گرفته، اما تاکنون تئوری کاملی ارائه نشده است. البته می‌دانیم که حالت‌های درهم‌تنیده در انجام الگوریتم‌ها و پروتکل‌های کوانتومی نقش بسزایی دارد.

این حالت‌ها را می‌توان به شکل فشردهٔ زیر نوشت :

$$|\varphi_{mn}\rangle = Z^m \otimes X^n \ |\varphi_{00}\rangle = \sum_{k=0}^{1} (-1)^{km} \ |k, k+n\rangle \qquad (۹-۱)$$

این حالت‌ها یک پایه متعامد برای فضای دوکیوبیت را تشکیل می‌دهند، بدین شکل :

$$\langle \varphi_{mn} | \varphi_{kl} \rangle = \delta_{mk}\, \delta_{nl} \qquad (۱۰-۱)$$

$$\sum_{mn} |\varphi_{mn}\rangle \langle \varphi_{mn}| = \mathrm{I} \qquad (۱۱-۱)$$

منظور از اندازه‌گیری در پایه بل، یعنی اندازه‌گیری با عملگرهای تصویری $P_{mn} = |\varphi\rangle_{mn}\langle\varphi|$.

۱-۴ کدگذاری فوق چگال[۱]

این نوع کدگذاری مثالی از کاربرد درهم‌تنیدگی در انتقال اطلاعات است. آلیس پیغامی را از طریق کانال کوانتومی به باب می‌فرستد. بطور مثال آلیس می‌تواند فوتون‌هایش را در راستای z $|\uparrow\rangle_z$ | یا z $|\downarrow\rangle_z$ | کد کند و این فوتون‌ها را برای باب بفرستد. باب با اندازه‌گیری در راستای z به جهت پلاریزیشن ارسالی پی می‌برد که این یکی از مزیت‌های کیوبیت‌ها در مقایسه با بیت‌های کلاسیکی است. البته این بهترین کار نیست.

حال وضعیتی را درنظر بگیرید که فوتون‌ها درهم‌تنیده باشند، مثلاً یکی از چهار حالت بل $|\varphi^+\rangle_{AB}= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$ که بینشان مشترک است را بکار می‌گیرند. سپس آلیس با مبادله یک کیوبیت، اطلاعات را بصورت دو بیت کلاسیکی به باب می‌فرستد[۱۰]، او یکی از چهار تبدیل یکانی زیر را روی کیوبیت خود اعمال می‌کند:

۱. I او هیچ عملی را انجام ندهد
۲. σ_1 دوران به اندازه ۱۸۰ حول محور x
۳. σ_2 دوران به اندازه ۱۸۰ حول محور y
۴. σ_3 دوران به اندازه ۱۸۰ حول محور z

۱ .Super-dense coding

جدول۱- ۱: کد گذاری فوق چگال

حالت نهایی	عملگری که آلیس اثر می‌دهد	زوج بیتی که مخابره می‌شود
$\|\varphi^+\rangle$	I	00
$\|\psi^+\rangle$	δ_x	01
$\|\varphi^-\rangle$	δ_z	10
$\|\psi^-\rangle$	δ_y	11

بطور مثال آلیس و باب با هم قرارداد کرده‌اند که حالت $|\varphi^+\rangle_{AB}$ را بیانگر کد ۰۰ و حالت $|\varphi^-\rangle_{AB}$ را بیانگر کد ۱۰ باشد و الی آخر. بدین ترتیب با انتقال یک کیوبیت تنها دو بیت کلاسیکی منتقل شده‌است.

با اعمال این حالت‌ها، $|\varphi^+\rangle_{AB}$ به ترتیب به حالت‌های $|\varphi^+\rangle_{AB}$, $|\psi^+\rangle_{AB}$, $|\psi^-\rangle_{AB}$ و $|\varphi^-\rangle_{AB}$ تبدیل می‌شود (طبق معادله (۱-۹) و (۱-۱۰)). سپس وی کیوبیتش را برای باب ارسال می‌کند و باب بعد از دریافت کیوبیت، یک اندازه‌گیری از حالت‌های بل انجام می‌دهد. بنابراین چهار حالت ممکن برای اندازه گیری باب بوجود می‌آید که بستگی به عمل آلیس دارد.

در مبحث بعد، سعی می‌کنیم تا بعد از آشنایی مختصر با نامساوی بل و حالت‌های کوانتومی EPR، اول نگاهی به رمزنگاری کلاسیکی و سپس رمز نگاری کوانتومی که ایمنی قویتری نسبت به کلاسیکی دارد، می‌اندازیم. در آخر ایمنی پروتکل‌های مختلف را ارائه‌خواهیم داد.

۲

توزیع کلید کوانتومی

۲- ۱ مقدمه

در فیزیک کلاسیک شناختی که از علم بدست آورده‌ایم این‌است که اشیاء در جهان خارج از ذهن (جهان واقعی) خصلت‌هایی دارند که توسط آزمایش و اندازه‌گیری، وجود این خصلت‌ها را کشف می-کنیم. مثلاً درخت سبز است، خصلت سبز بودن رنگ درخت بواسطه دیدن یا آزمایش مشاهده می-شود.

در مکانیک کوانتومی این تفسیر و تعبیر را می‌پذیریم که اشیای کوانتومی خصلت‌های ذاتی ندارند، این خصلت‌ها نتیجهٔ عمل مشاهده است. به عنوان مثال اگر ذره‌ای بواسطه آزمایش اشترن‌گرلاخ حالت اسپین ↑ یا ↓ بدست بیآورد، به این نتیجه می‌رسیم که در آزمایش خلق شده، نه اینکه حالت اسپین از قبل ↑ یا ↓ بوده‌باشد و ما آنرا کشف کرده باشیم. این ایده برای مردم که ترجیح می‌دادند جهان واقعی را آنطور که هست بشناسند یک مسئله ناخوشایند است، به دلیل اینکه ما علاقمندیم که جهان را آنطور که هست بشناسیم.

دیدگاه جذاب کلاسیکی اینگونه است که قوانین فیزیک را کشف می‌کنیم تا دنیای واقعی را بشناسیم. درصورتی‌که درکوانتوم مکانیک یاد می‌گیریم که به اسپین ذره قبل از مشاهده نمی‌توان وضعیت خاصی را اطلاق کنیم. در نتیجه در مقایسه‌ی فیزیک کلاسیک با فیزیک کوانتومی با تناقض مواجه می‌شویم. البته این ایده ناشی از خطای آزمایشگاه نیست، بلکه ناشی از محدودیتی است که برای فهم آن داریم.

انیشتین و همکارانش به این بحث‌های فلسفی که بصورت کلامی و بر مبنای واقعیت و حقیقت بود، خاتمه دادند و آنرا بصورت ریاضی دقیق بیان کردند.

۲-۲ تناقض EPR و نامساوی بل[۱]:

این ایده شگفت انگیز در تئوری مکانیک کوانتومی اولین بار در سال ۱۹۳۵ توسط اینشتین و پودولسکی و روزن[۲] مطرح شد که تلاش کردند تا نتایج اندازه‌گیری بر روی زوج‌های درهم‌تنیده را بصورت کلاسیکی و با در نظرگرفتن متغیرهای پنهانی توجیه کنند[۱۵].

تا آنکه در سال ۱۹۶۰ بل نامساوی‌ای را ارائه داد که بیان کننده اعتبار آمار کلاسیکی بود[۱۳, ۱۶]، با یک آزمایش ساده روی زوج‌های درهم‌تنیده مشاهده شد که آمار بدست آمده نامساوی را نقض کرد.

آنها معتقد بودند که خواص فیزیکی جسم مستقل از مشاهده است و اندازه‌گیری تأثیری روی آن نمی‌گذارد(چون خواص فیزیکی جسم عنصری از واقعیت است). در صورتی‌که در مکانیک کوانتومی از نتیجه اندازه‌گیری اطلاعی نداریم، (چون نتیجه اندازه‌گیری احتمالی است، با احتمال $|\alpha|^2$ ذره اول بدست می‌آید وبا احتمال $|\beta|^2$ ذره دوم) بلکه خواص فیزیکی ذره منوط بر آزمایش است.« مثال معروف انیشتین این است که آیا وقتی من به ماه نگاه نمی‌کنم، آنرا می‌بینم؟ کوانتوم مکانیک می‌گوید که وقتی من ماه را نگاه نمی‌کنم، آنرا نمی‌بینم. یعنی وجود چیزی نتیجه‌ی آزمایش است» اینشتین و پودولسکی و روزن، این تصویر ناخوشایند را قبول نداشتند. آنها می‌خواستند جهان را آنطور که هست،بنگرند. در واقع تمام تلاش اینشتین و همکارانش این بود که از خود کوانتوم مکانیک استفاده کنند و ثابت کنند که کوانتوم مکانیک یک نظریه‌ی کامل نیست. بنابراین آنها حالتی را درنظر گرفتند و فرض کردند که ذره‌ی آلیس و باب در حالت یکتایی[۳] $|\psi\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)$ است، سپس آنها را بطور فضا گونه از هم دور می‌کنیم. اگر آلیس ذره خود را اندازه بگیرد و $(+)$ بدست بیاورد، از آنجایی که اسپین کل سیستم صفر است در نتیجه ذره‌ی باب در حالت $(-)$ قرار خواهد

---

۱. Bell Inequality

۲. Einstein, Podolsky, N.Rosen

۳. Singlet

داشت و چون سیگنال را با سرعت بیشتر از سرعت نور به باب می‌فرستد، بنابراین نتیجه گرفتند که کوانتوم مکانیک ناکامل است. این پیش‌بینی هچ تناقضی با نسبیت خاص و اصل موضعیت[1] ندارد. " اصل موضعیت می‌گوید سیستم‌هایی که فاصله فضا گونه دارند نمی‌توانند هیچگونه ارتباطی با هم داشته باشند. " چون آلیس می‌تواند فقط نتیجه باب را پیش‌بینی کند ولی نمی‌تواند هیچ سیگنالی را به او مخابره کند. در مثال فوق کوانتوم مکانیک می‌گوید که آلیس وقتی ذره‌ی خودش را اندازه‌گیری می کند و (+) بدست می‌آورد، لذا تمام احتمالات (+) بودن برای باب از بین می‌رود و هیچگونه سیگنالی در فاصله‌ی اندازه‌گیری آلیس و اندازه‌گیری باب فرستاده نمی‌شود، یعنی آزمایش آلیس هیچ تأثیری بر ماتریس چگالی ذره باب نمی‌گذارد. فقط آلیس می‌تواند نتیجه‌ی باب را پیشگویی کند که این مسئله ربطی به سرعت نور ندارد. وجود این همبستگی ابهاماتی در نظریه کوانتومی رخ داد.

نظریه EPR تناقضی را در زمینه مکانیک کوانتومی بدین صورت مطرح کرد که یک سیستم فیزیکی را که از دو ذره آلیس و باب تشکیل شده‌است را در نظربگیرید. آلیس در راستای Z روی ذره خودش اندازه‌گیری می‌کند و ۱+ بدست می‌آورد، در اینصورت ذره باب در همان راستای Z را با قطعیت پیش‌بینی می‌کند. در اینصورت دستگاه باید خاصیتی از ذره آلیس داشته باشد تا بدون مختل کردن حالت آن‌را اندازه‌گیری کند که مربوط به متغیرهای پنهانی است که نتیجه آزمایش را آشکار می‌کند، نه اینکه آن‌را خلق کند.

به این ترتیب آلیس می‌تواند در هر راستای دیگری ذره‌اش را اندازه‌گیری کند و اسپین ذره باب را پیش‌بینی نماید. پس می‌توان گفت که دو انتخاب در پیش داریم، یا اینکه در این اندازه‌گیری کوانتومی نتیجه آزمایش اولی بلافاصله روی ذره دوم که با آن فاصله فضاگونه دارد اثر می‌گذارد که در صورت وقوع این اتفاق سرعتش باید از سرعت نور بیشتر باشد که با نظریه نسبیت انیشتین سازگار

[1] . Locality منظور از موضعیت این‌است که قطبیدگی یک فوتون با اندازه‌گیری روی فوتون دیگری که در فاصله دور ازهم هستند، اثر نمی‌گذارند.

نبود، به همین دلیل بود که مکانیک کوانتومی را قبول نکرد و یا اینکه پذیرفت در باطن فیزیک کوانتومی یک متغیر پنهان λ وجود دارد.

نتیجه می‌گیریم که EPR می‌گوید خواص سیستم فیزیکی معین است، به این مضمون که، چه سیستم را اندازه‌گیری کنیم و چه اندازه‌گیری نکنیم مقدار آن‌را قبل از اندازه‌گیری می‌دانیم، چون واقعی بودن نباید تحت تأثیر آزمایش باشد. ولی مکانیک کوانتومی می‌گوید که قبل از اندازه‌گیری نمی‌توانیم خواص سیستم را بگوییم و از نظر کوانتوم هیچ عنصری از واقعیت وجود ندارد. در نهایت هدف EPR این بود که نشان دهد کوانتوم مکانیک ناکامل است.

تحلیل دقیقتر آزمایش EPR نتایج جالبی را به دنبال داشت که در سال ۱۹۶۹ توسط جان بل [1] ارائه شد. بل فرضیاتی را مطرح کرد: هیچ متغیر پنهانی وجود ندارد، موضعیت را قبول کرد و با وجود در هم‌تنیدگی در سیستم، نامساوی‌ای را ارائه داد که کوانتوم مکانیک را نقض می‌کند [۱۷]. برای اثبات آلیس دو ذرهٔ R و Q را از منبع عمومی دریافت می‌کند و روی هر کدام از این ذرات در پایه‌های انتخاب شده اندازه‌گیری انجام می‌دهد و همچنین باب روی دو ذره خودش که از منبع دریافت کرده، اندازه‌گیری می‌کند. فرض می‌کنیم که آلیس و باب دستگاه‌های متفاوتی برای اندازه‌گیری دارند، این دستگاه‌های اندازه‌گیری خواص فیزیکی‌ای دارند که برای آلیس P_R, P_Q است و برای باب با P_T, P_S نمایش می‌دهیم. و همچنین فرض می‌کنیم که خروجی‌های اندازه‌گیری تنها دو مقدار ۱- و ۱+ را دارند. نتایج این اندازه‌گیری‌ها را به ترتیب با t,s,r,q نشان می‌دهیم. همچنین آلیس و باب در یک زمان اندازه‌گیری انجام می‌دهند و چون فرض کرده‌ایم که این خواص عنصری از واقعیت هستند و اینکه اثرات فیزیکی نمی‌توانند سریعتر از سرعت نور حرکت کنند بنابراین نتایج آلیس نمی‌تواند نتایج باب را خراب کند و برعکس.

پس از پایان آزمایشات مقدار متوسط کمیت $QS + RS + RT - QT = (Q + R)S + (R - Q)T$ را محاسبه می‌کنیم و چون $R, Q = \pm 1$ است پس باید یکی از دو جمله (Q+R)S و یا $(R - Q)T$ صفر

[1]. John Bell

شود پس این رابطه‌ی $QS + RS + RT - QT \leq ۲$ برقرار است. حال اگر P (Q,R,S,T) احتمال قبل از انجام آزمایش باشد، و درضمن درنظر بگیریم که سیستم در حالت $T = t, S = s, R = r, Q = q$ باشد، E مقدار متوسط کمیت بدین صورت درمی‌آید:

$$E(QS + RS + RT - QT) =$$

$$\sum_{q,r,s,t} P(Q,R,S,T)(qs + rs + rt - qt) \leq \sum_{q,r,s,t} 2P(q,r,s,t) = 2$$

$$E(QS + RS + RT - QT) = \sum_{q,r,s,t} P(Q,R,S,T)[(q + r)s + (r - q)t] =$$

$$\sum_{q,r,s,t} P(q,r,s,t)qs + \sum_{q,r,s,t} P(q,r,s,t)rs + \sum_{q,r,s,t} P(q,r,s,t)rt - \sum_{q,r,s,t} P(q,r,s,t)qt =$$

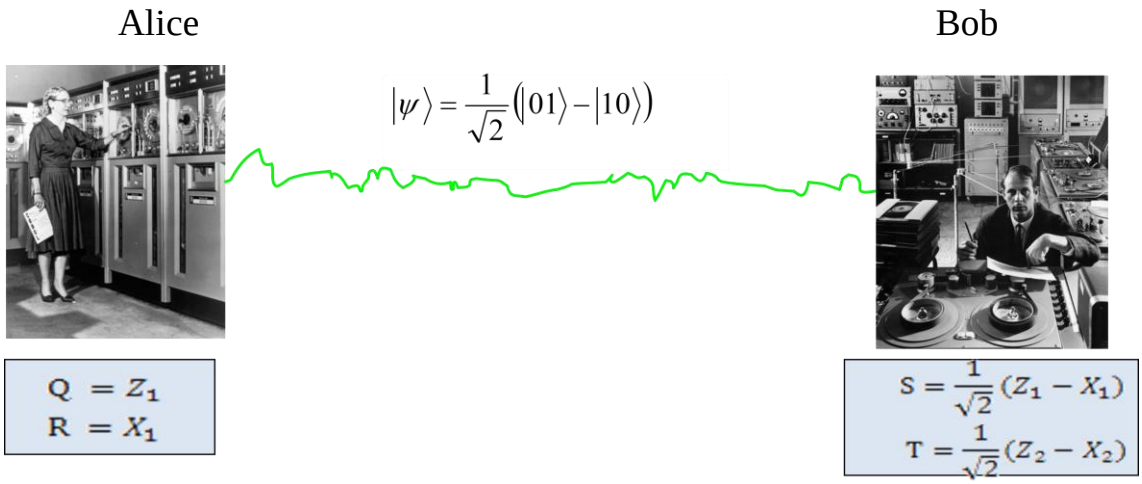
$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle \leq 2 \qquad (۱-۲)$$

نامساوی بالا را نامساوی بل می‌گوییم، این نتیجه به عنوان نامساوی CHSH نیز شناخته شده است. حال می‌خواهیم آزمایشی معرفی کنیم که در آن نامساوی بل نقض می‌شود. فرض می‌کنیم:

اگر حالت اولیه توزیع شده بین آلیس و باب را یک حالت یکتایی به فرم زیر در نظر بگیریم:

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

سپس آلیس و باب روی ذره‌هایشان اندازه‌گیری انجام می‌دهند و مشاهده پذیرهای T, S, R, Q به شکل زیرخواهد بود:



تصویر ۲-۱: تناقض EPR و نامساوی بل

حال مقدار متوسط کمیت $(Q+R)S+(R-Q)T$ را در مکانیک کوانتومی و با حالت اولیه $|\psi\rangle$ داده شده محاسبه می‌کنیم:

$$\langle\psi|(Q+R)S+(R-Q)T|\psi\rangle = \langle\psi|QS+RS+RT-QT|\psi\rangle = \langle\psi|QS|\psi\rangle + \langle\psi|RS|\psi\rangle + \langle\psi|RT|\psi\rangle - \langle\psi|QT|\psi\rangle \quad (۴-۲)$$

که داریم:

$$\langle QS\rangle = \frac{1}{\sqrt{2}}, \langle RS\rangle = \frac{1}{\sqrt{2}}, \langle RT\rangle = \frac{1}{\sqrt{2}}, \langle QT\rangle = \frac{1}{\sqrt{2}} \quad (۵-۲)$$

و در نهایت معادله (۱) تبدیل می‌شود به:

$$\langle(Q+R)S+(R-Q)T\rangle = \langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} \quad (۶-۲)$$

نتیجه گرفتیم که بیشینه مقدار متوسط $۲\sqrt{۲}$ است که نامساوی بل را نقض می‌کند و با نتایج مکانیک کوانتومی سازگار نیست. پس قبول این مسئله مشخص است که یا فیزیک کوانتومی نتایج اندازه‌گیری-ها را بطور صحیح پیش بینی نمی‌کند و یا اینکه یکی از فرضیاتی که بر اساس قضیه‌ی بل می‌باشد، نادرست است. طبیعت رابطه (۲-۶) را تأیید می‌کند، یعنی مکانیک کوانتومی با طبیعت سازگار است.

این واقعیت که نامساوی بل نقض می‌شود به این معنا است که نظریه‌ای که موضعیت را حفظ کند با آزمایش سازگار نیست.

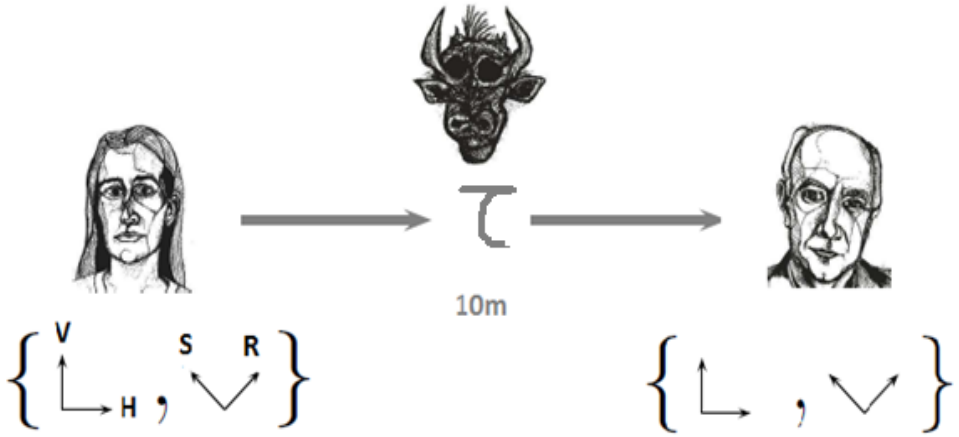
البته به این نکته توجه کنید که از دستگاه EPR نمی‌توان برای انتقال اطلاعات استفاده‌کرد، چون در اینصورت باید اطلاعات بیشتر از سرعت نور انتقال یابد که این گفته با نظریه نسبیت انیشتین تناقض دارد. نکته دوم اینکه از حالت‌های درهم‌تنیده برای ارتباطات کوانتومی و اطلاعات کوانتومی استفاده می‌شود و نظریه باید ناموضعیت[۱] را حفظ کند که با طبیعت و مکانیک کوانتومی سازگار باشد.

۲-۲-۱ آزمون تجربی نامساوی بل

در سال ۱۹۸۱ آلن اسپکت[۲] و همکارانش برای اثبات نقض نامساوی بل در آزمایشگاه، آزمایشی را بدین صورت مطرح کردند[۱۸]: منبع(می‌تواند دستگاه اشترن‌گرلاخ باشد) جفت فوتون‌های درهم-تنیده را تولید می‌کنند و بعد این فوتون‌ها را برای آلیس و باب می‌فرستند، آلیس فوتون‌هایش را با پلاریزیشن در راستای V و H اندازه‌گیری می‌کند و باب با پلاریزیشن در راستای 45° چرخیده(مثلاً راستای R وS)را اندازه‌گیری می‌کند. البته فاصله این دو نفر در آزمایشگاه محدود است (مثلاًدر بهترین حالت ۱۰ متر).

۱. Nonlocality

۲ .Alen Aspect



تصویر۲-۲ : آزمون تجربی نامساوی بل

در ضمن ایندو نفر هیچ رابطهٔ علی‌ای با یکدیگر ندارند. اگر فاصله‌ی ایندو نفر را در مدت زمان τ درنظربگیریم، سپس می‌دانیم که $\tau \leq ۱۰ \times$ سرعت نور باید باشد:

$$\tau \leq \frac{10}{3\times10^{8}} = 3 \times 10^{-8} \simeq 30\mathrm{n}s$$

بنابراین کلیدی که این پلاریزاسیون‌ها را تنظیم می‌کند باید در فاصله زمانی $۳۰\ ns$ تغییر کند که این آزمایش باید دقت بالایی داشته باشد که این اندازه‌گیری را انجام دهد. در این آزمایش مقدار $۲\sqrt{۲}$ بدست می‌آید که به وضوح نامساوی بل نقض می‌شود. نشان خواهیم‌داد که نتایج مکانیک کوانتومی با آزمایش فوق سازگار است.

یک زوج درهم‌تنیده را درنظر می‌گیریم:

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

آلیس و باب فوتون‌هایشان را در راستای S_x و S_z اندازه‌گیری می‌کنند.

تصویر ۲-۳ : آزمون تجربی نامساوی بل

$A = S_n$ $\qquad$ $C = \alpha S_x + \beta S_z$

$B = S_z$ $\qquad\qquad$ $D = -\beta S_x + \alpha S_z$

جهت‌های اندازه‌گیری A و B برهم عمود هستند ولی فعلاً جهت‌های C و D اختیاری هستند و سپس رابطه‌ای که بین جهت‌های فوتون‌های ذرهٔ باب و فوتون‌های ذرهٔ آلیس با توجه به نقض نا-مساوی بل وجود دارد را پیدا خواهیم کرد.

حال می‌خواهیم متوسط این کمیت را محاسبه کنیم:

$$\langle (A+B)C + (A-B)D \rangle = \langle \psi | (S_x + S_z) \otimes (\alpha S_x + \beta S_z) + (S_x - S_z) \otimes (-\beta S_x + \alpha S_z) | \psi \rangle$$

$$= \frac{1}{2} (0\ 1\ 1\ 0) \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} \beta & \alpha \\ \alpha & -\beta \end{bmatrix} + \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} \alpha & -\beta \\ \beta & -\alpha \end{bmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

حال α و β را طوری انتخاب می‌کنیم که این متوسط بیشترین مقدار که $2\sqrt{2}$ است را داشته باشد. بنابراین:

$$\begin{cases} \alpha^2 + \beta^2 = 1 \\ \alpha - \beta = \sqrt{2} \end{cases} \longrightarrow \alpha = \frac{3\sqrt{2}+1}{2} \text{ و } \beta = \frac{\sqrt{2}+1}{2}$$

۲-۳ رمزنگاری

اساس رمزنگاری یک شیوه باستانی حفاظت از اطلاعات است که سابقه آن به حدود ۴۰۰۰ سال پیش از میلاد باز می گردد و تاکنون مورد توجه بشر بوده‌است و از آن برای پیام‌هایی استفاده می‌کردند که کسی بجز دو کاربر نمی‌توانست به محتوی اطلاعات دسترسی داشته باشد و همچنان ایمنی آن در حال پیشرفت است. امروزه رمزنگاری در دنیای مدرن از اهمیت ویژه ای برخوردار است، به طوری که رمزنگاری به عنوان یک روش مؤثر برای حفاظت از اطلاعات حساس به کار می رود. اطلاعاتی مانند اطلاعات طبقه بندی شده نظامی، اطلاعات حساس مؤسسات مالی، کلمات عبور که بر

روی سیستم های کامپیوتری ذخیره شده اند و داده هایی که بر روی اینترنت و یا از طریق امواج رادیویی انتشار می یابند. رمزنگاری، ارسال اطلاعات بطور سّری است که هیچ حجمی از اطلاعات به سرقت نرود. رمزنگاری از دو بخش کدگذاری[۱] و کدگشایی[۲] تشکیل شده است. به عنوان مثال فرض کنید پلیس در تعقیب مجرمی از گروه مافیا است و عکس و اطلاعات این شخص را می‌خواهد به ایستگاه‌های پلیس در جاهای مختلف کشور مخابره کند و در تلاش است که بجز گروه پلیس کسی نتواند به اطلاعات مجرم دستیابی داشته باشد که این اطلاعات را با استفاده از کلید خصوصی (کلید خصوصی کلیدی است که تنها برای خود شخص فرستنده مشخص است) کدگذاری می‌کند، سپس آن‌را به پلیس‌های سراسر کشور می‌فرستد، پلیس گیرنده نیز باید اطلاعات اصلی را با در دست داشتن کلید خصوصی که فقط در دسترس پلیس است، کدگشایی کند ولی مجرم و همکارانش فقط به کلید عمومی[۳] دسترسی دارند. با داشتن کلید عمومی نباید به کلید خصوصی دستیابی داشت. در اصل بین این دو کلید عمومی و کلید خصوصی همبستگی‌ای وجود ندارد.

اولین ایده رمزنگاری کوانتومی توسط استفان ویزنر در اواخر سال ۱۹۶۰ پیشنهاد شد اما برای انتشار مورد استقبال قرار نگرفت. ویزنر به این نتیجه رسید که کانال کوانتومی می‌تواند به عنوان منبعی برای رمزنگاری‌های مختلف بکار رود، چون کانال کوانتومی از اصل عدم قطعیت پیروی می‌کند بدین گونه که حالت‌هایی که خواص مشخصی دارند نمی‌توانند همزمان آشکار شوند و اندازه‌گیری یکی از آن حالت‌ها، حالت دیگری را از بین می‌برد، پس نسبت به کانال کلاسیک مزیت دارد.

ویزنر طرحی را برای ارسال دو پیغام پیشنهاد کرد، یکی از این‌دو پیغام مخابره شود که به لحاظ فیزیکی جعل آن امکان پذیر نیست. در سال ۱۹۸۴ بنت[۴] و براسارد[۱]روی مقاله ویزنر کار کردند[۲۰]، و

---

۱. Enciphering

۲. Deciphering

۳. یک حالت کوانتومی را درهم‌تنیده گوییم اگر همبستگی بین کیوبیت‌های آن کلاسیکی نباشد مثلاً $|11\rangle+|00\rangle$ یک حالت در-هم‌تنیده است اگر روی کیوبیت اول اندازه‌گیری شود و بدست بیاورد، اندازه‌گیری روی کیوبیت دوم ۱ خواهدبود.

۴.Charles Bennet

و یک پروتکلی را -که در آن بر مبنای فیزیک کوانتومی استوار است- پیشنهاد کردند تحت عنوان پروتکل BB۸۴ و بالاخره به طرح توزیع کلید بین آلیس و باب تبدیل شد.

ما جزئیات اینکه این پروتکل چگونه کار می‌کند و راه استفاده از اینکه این اطلاعات ایمن‌تر باشد را در مبحث بعدی توضیح خواهیم داد.

۲-۳-۱ توزیع کلید کوانتومی

جدیدترین اکتشافات در زمینه ارتباطات کوانتومی و اطلاعات کوانتومی ماشین کوانتومی است و یک ایده بنیادی اصل مکانیک کوانتومی است. این پروسه به عنوان رمزنگاری کوانتومی یا توزیع کلید کوانتومی مشهور است (QKD) که در مقابل استراق سمع کننده با توان محاسباتی نامحدود کاملاً ایمن است[۱۹].

اساس رمزنگاری، توزیع کلید محرمانه بین دو کاربر قانونی است که فاصله زیادی از یکدیگر دارند، این عمل در کلاسیک امکان‌پذیر نیست، علت این است که ایمنی در رمزنگاری کلاسیکی براساس سختی مسائل ریاضی است، بدین صورت که اگر یک عدد خیلی بزرگ داشته باشیم، تجزیه آن به عوامل اول سخت است ولی اگر یک کامپیوتر قوی داشته باشیم، خیلی سریع تجزیه به عوامل اول می‌کنیم و در آنصورت رمز را می‌توانیم به آسانی بشکنیم (مشکل‌ترین رمزهای کلاسیکی نهایتاً در شش ماه شکسته می‌شود). ممکن است سال‌ها طول بکشد تا یک کامپیوتر کوانتومی ساخته شود که بتوان روی آن یک الگوریتم کوانتومی برای تجزیه یک عدد بزرگ را پیاده‌سازی کرد. به این نتیجه می‌رسیم که در رمزنگاری به روش کوانتومی وقتی یک سیگنال رمزی شده را می‌فرستیم به جز دو کاربر قانونی هیچ کس دیگری نمی‌تواند رمز را بشکند. از طرف دیگر اگر استراق سمع کننده (ایو) قدرتش نامحدود باشد یعنی مسلط به کامپیوترهای کوانتومی باشد، به راحتی رمز کلاسیکی را

---

۱. Cillen Brassard

می‌تواند بشکند. بنابراین توزیع کلید کوانتومی ایمنی را در مقابل استراق سمع کننده با قدرت محاسباتی نامحدود را ارائه می‌دهد.

به گونه‌ای دیگر می‌توانیم بیان کنیم که امنیت رمزنگاری کلاسیکی براساس خواص ریاضی کلید است – که چطور کلید در عمل خلق شده است، در اصل مستقل از ایمنی است – در حالی‌که در توزیع کلید کوانتومی این ایمنی بصورت خیلی حساس وابسته به خواص فیزیکی فرایند خلق کلید است.

سوال این است که چطور می‌توانیم سطح ایمنی توسط اجراسازی QKD در زندگی واقعی را تشخیص دهیم که بطور بدیهی متفاوت با راه‌های جزئی حالت ایده‌آل در توصیف تئوری است؟[۲۱]

مثلاً وقتی‌که سیگنالی را می‌خواهیم کدگذاری کنیم یا اینکه سیگنال باب را بازگشایی کنیم و یا ویژگی‌های آشکارسازها که در تحلیل تئوری در نظر گرفته نمی‌شوند، باعث ایجاد خطاهایی می‌شود که ایمنی طرح‌های QKD در زندگی واقعی را از بین می‌برد. فیزیکدانان می‌خواهند این خطاها را به حداقل مقدار برسانند و ایمنی این پروتکل‌ها را افزایش دهند. حال پروتکل‌هایی را بررسی می‌کنیم که ایمنی را تضمین می‌کنند.

۲-۳-۲ پروتکل BB۸۴

چون هیچ پروتکل کلاسیکی‌ای مصون نیست، لذا به دنبال پروتکلی هستیم که با مکانیک کوانتومی و خصلت‌های کوانتومی بتوان توزیع کلید انجام داد. خوشبختانه در سال ۱۹۸۴ بنت و براسارد پروتکلی را طراحی کردند که با استفاده از کامپیوترهای کوانتومی توزیع کلید انجام دهد و چون در سال ۸۴ این پروتکل را کشف کردند، آن‌را بنام BB۸۴ نامگذاری کردند. این پروتکل بر اساس توابع پیچیده ریاضی نیست که توابع یکطرفه در آن دخالت کند، بلکه بر اساس خصلت‌های کوانتومی است[۱۹].

این مدل، طرحی از توزیع کلید کوانتومی است که در این روش هرگونه استراق سمع‌کننده قابل شناسایی است. آلیس و باب توسط یک کانال کوانتومی (می‌تواند منبع باشد) و یک کانال کلاسیکی با هم ارتباط برقرار می‌کنند. بدین صورت که آلیس پیام را از طریق کانال کوانتومی به باب می‌فرستد و ایو می‌تواند از طریق این کانال کوانتومی به پیام دسترسی داشته‌باشد، ولی نمی‌تواند مستقیماً پیام اصلی را برای باب بفرستد- بنابراین کانال کوانتومی یک کانال ناامن خواهد بود- سپس وقتی باب تمام کیوبیت‌هایش را دریافت کرد، از طریق کانال کلاسیکی نتایج را بطور عموم اعلام می‌کند. لازم به یادآوری است که کانال کوانتومی یک کانال ارتباط عمومی و کانال کلاسیکی یک کانال خصوصی و یک کانال معتبراست که هر کسی نمی‌تواند به اطلاعات درون آن دستیابی داشته باشد. بنابراین از نتایج به عنوان کلید سّری استفاده می‌کنند.

در ضمن ایو توان محاسباتی نامحدودی دارد و به هر دو کانال دسترسی دارد ولی نمی‌تواند پیغامی را که از طریق کانال کوانتومی- طبق قضیه‌ی عدم شبیه سازی که قبلاً بیان کردیم که در مکانیک کوانتومی امکان پذیر نمی‌باشد- می‌گذرد را تغییر بدهد.

این پروتکل اینگونه کار می‌کند که آلیس و باب دو پایه‌ی x و یا z که عملگرهای ماتریس پائولی هستند و در ضمن مکمل نیز هستند را بطور تصادفی[1] انتخاب می‌کنند و بعد از انتخاب، کدگذاری‌های زیررا انجام می‌دهند:

$$\begin{cases} 0 \to |z+\rangle \\ 1 \to |z-\rangle \end{cases} \qquad \begin{cases} 0 \to |x+\rangle \\ 1 \to |x-\rangle \end{cases} \qquad (۷-۲)$$

آلیس و باب بصورت عمومی یک قراردادی با هم می‌گذارند که ۰ را بصورت اسپین مثبت در راستای z یا در راستای x انتخاب می‌کنند، یعنی ۰ و ۱ را در حالت‌های کوانتومی کد می‌کنند.

---

۱. Randomness می‌تواند یک دستگاه اشترن‌گرلاخ باشد و ذرات را از آن عبور دهند.

حال اگر آلیس قصد داشته باشد یک رشته ۰ و ۱ را برای باب بفرستد، باید این رشته صفر و یک را بصورت رندوم در پایه‌ی x و یا z انتخاب کند و بعد این ذره را از کانال کوانتومی به باب ارسال‌کند، باب بعد از اینکه این رشته که رمزگذاری‌شده را دریافت کرد، اسپین‌های ارسالی را در پایه‌های تصادفی خودش(x و یا z) اندازه‌گیری می‌کند.

باب این فرایند را چندین بار تکرار می‌کند و از پایه‌ها و بیت‌های کد شده و یا نتایج اندازه‌گیری یادداشت برمی‌دارد. سپس آلیس از طریق کانال کلاسیکی، پایه‌هایی را که از آن برای کدگذاری استفاده کرده به باب می‌گوید. اگر باب در پایه اشتباه اندازه‌گیری کند، (یعنی پایه تصادفی انتخابی دیگر) در نتیجه باب یک بیت غیرهمبسته با آنچه که آلیس فرستاده بدست می‌آورد و پایه‌های متفاوت را حذف می‌کند و پایه‌ای را که همانند پایه آلیس است را نگه می‌دارد، این در حالی است که هنوز نتایجش را اعلام نکرده باشد[1]. وقتی که اندازه‌گیری به اتمام رسید، پایه‌ها بطور عمومی اعلام می‌شوند. آلیس و باب بعضی از بیت‌ها را بطور رندومی انتخاب می‌کنند و آنرا چک می‌کنند، اگر باب بیت‌های صحیحی را دریافت کند از آن به عنوان کلید استفاده می‌کنند.

فرض کنیم در غیاب ایو و اینکه کیوبیت‌ها با محیط بر هم کنشی نکنند (یعنی محیط هیچ اثری روی ذرات ندارد)، آنگاه تمام نتایج باید با هم سازگار باشند ولی در حضور ایو و اینکه نویز هم وجود داشته باشد، با احتمال $\frac{1}{2}$ باب خطا بدست می‌آورد که دراینصورت آلیس و باب می‌فهمند که یک نفر مشغول استراق سمع است. سپس پروتکل را قطع می‌کنند و دوباره از اول شروع می‌کنند، این عمل را مکرراً تکرار می‌کنند تا مطمئن شوند ایو دیگر این وسط حضور ندارد.

[1]. پایه‌های باب را فقط خودش می‌داند ولی پایه‌های آلیس را همه می‌دانند.

پیام	پایه های انتخابی			
0	x	$\|x_+\rangle$	z	0
0	x	$\|x_-\rangle$	z	0
0	z	$\|z_+\rangle$	x	$\|x_+\rangle$ / $\|x_-\rangle$
0	z	$\|z_+\rangle$	z	0
1	x	$\|x_-\rangle$	x	1
1	x	$\|x_-\rangle$	z	0
0	x	$\|x_+\rangle$	x	0
1	z	$\|z_-\rangle$	x	1

تصویر۲-۴: پروتکل BB۸۴

با توجه به شکل بالا، نتیجه می‌گیریم که با احتمال خوبی می‌توانیم حضور ایو را تشخیص دهیم، در نهایت این احتمال را می‌توانیم کمتر کنیم، یعنی تعداد کیوبیت‌ها را افزایش دهیم، نتایجی را هم که اعلام می‌کنیم بیشتر باشد سپس حضور ایو را به خوبی می‌توانیم تشخیص دهیم. هدف BB۸۴ طراحی کلیدی است که وجود استراق سمع کننده در این پروتکل قابل تشخیص است و همچنین چنین کلیدی بین آلیس و باب برای رمزگذاری و رمزگشایی قرار داده شود.

۲-۳-۳ ایمنی پروتکل BB۸۴ در برابر ایو

فرض کنید که ایو بتواند کانال کوانتومی بین آلیس و باب را استراق سمع کند و فوتون را اندازه‌گیری کند، وقتی پایه‌هایی را که در آن پایه‌ها بیت‌ها کد[۱] شده‌اند را نمی‌داند سپس با احتمال $\frac{۱}{۲}$ پایه‌های اشتباه را اندازه‌گیری می‌کند (می‌دانیم که بیت‌های باب هم بطور کاتوره‌ای انتخاب شده‌اند)، حتی وقتی که باب در همان پایه‌هایی که آلیس برای کد کردن استفاده کرده باشد، اندازه‌گیری کند، به این دلیل که ایو نمی‌تواند حالت ارسالی آلیس را دریافت کرده و آنرا استراق سمع کند و مستقیماً برای باب بفرستد(علت این است که براساس قضیه نوکونینگ هیچ فرایندی نمی‌تواند حالتهای نامتعامد را کپی کند)، همچنان این خطاها حضور ایو را برای آلیس و باب آشکار می‌کنند و در نتیجه پروتکل متوقف می‌شود.

مسئله دیگر این است که ایو نیازی ندارد که فوتونی را که از درون کانال کوانتومی عبور می‌کند را اندازه بگیرد، اما می‌تواند حملات پیچیده‌تری انجام دهد، مثلاً ایو می‌تواند سیستم را با فوتون درهم-تنیده کند و آنرا ذخیره کند و اندازه‌گیری که می‌خواهد انجام دهد را به تأخیر بیندازد و بعد از اینکه آلیس و باب پایه‌هایشان را برای کدگذاری آشکار کردند، اندازه‌گیری‌خود را انجام دهد. اما مشکلاتی هم در این حین بوجود می‌آید و آن اینکه اجراسازی فیزیکی پروتکل کامل نخواهد بود، چون همیشه ناخالصی شامل محیط و آشکارسازهای نامطمئن وجود دارد که با وجود این ناخالصی‌ها برای کانال یک کلید محرمانه تولید خواهد شد.

چند سال بعد از قرارداد BB۸۴ توسط بنت و براسارد، شخصی به نام ایکرت[۲] یک پروتکل توزیع کلید کوانتومی[۱] پیشنهاد کرد که براساس خواص فیزیکی کوانتومی است. در حقیقت دو تا سیستم

---

۱. Encode

۲. Ekert

کوانتومی قویاً درهم‌تنیده و همبسته[۲] هستند که می‌توانند با سیستم سوم در هم تنیدگی ضعیفی داشته باشد[۲۳] و تا به امروز پروتکل‌های مختلفی برای امنیت بیشتر طراحی شده است.

در اصل هدف ما محدودکردن توانایی‌های محاسباتی و دسترسی شخص سوم(که همان ایو یا استراق‌سمع‌کننده است) که می‌خواهد بطور غیرقانونی به اطلاعات ما دسترسی داشته باشد، می‌باشد.

از اینرو برای رمزگذاری کلیدهای مختلفی طراحی شد که در آینده به آن اشاره خواهیم کرد.

۲- ۴ رمزنگاری کوانتومی

هدف رمزنگاری تدوین پروتکل‌هایی است که برای مبادله اطلاعات ایمن از یک مکان به مکان دیگر صورت می‌گیرد. رمزنگاری را می‌توان به شیوه زیر تعریف کرد:

پیام اصلی را M می‌نامیم، وقتی این پیغام رمزینه می‌شود تبدیل به $E_k(\mathrm{M})$ خواهد شد، k کلید مشترک بین فرستنده و گیرنده است.

$$\mathrm{M} \rightarrow E_k(\mathrm{M})$$

این سیستم باید دوتا شرط اساسی داشته باشد:

شرط ۱) از $E_k(\mathrm{M})$ نباید به رمز دسترسی پیدا کنیم

$$\mathrm{M} \not\rightarrow E_k(\mathrm{M})$$

شرط ۲) وقتی شخصی مشغول استراق سمع کردن است، باید بدون اینکه طرف‌های قانونی اطلاع پیدا کنند که وی روی خط است، مرتب پیام‌های $E_k(\mathrm{M}_1)$, $E_k(\mathrm{M}_2)$, ... دریافت کند ولی همچنان از M آگاهی ندارد. لذا با در اختیار داشتن مجموعه E_{k} ها، نباید k را پیدا کند، چون در اینصورت کانال ناامن خواهد شد. وقتی پیام به دست شخص مورد نظر می‌رسد، این شخص با استفاده از نگاشت D_{k} رمز را باز می‌کند که دارای دو خاصیت زیر هستند:

---

۱. Quantum key distribution

۲. Correlated

$$D_k \circ E_k = I \qquad (۸-۲)$$

$$D_k\big(E_k(M)\big) = M \qquad (۹-۲)$$

M را رمزینه می‌کنند و آن‌را بصورت $E_k(M)$ در می‌آورند و بعد یک تابع معکوس روی آن اعمال می‌کنند و به رمز پی می‌برند که این اصل رمزنگاری است. برای وضوح این نوع رمزنگاری یک مثالی می‌زنیم:

پیغام را بصورت رشته‌ای از اعداد ۰و۱ در می‌آوریم → پیغام M =10001

رشته رندوم ۰و۱ که بین آلیس و باب مشترک است → K= 0 011

$$E_k(M) = M \oplus K \qquad (۱۰-۲)$$

$$D_k(M) = K \oplus E_k(M) \rightarrow K \oplus K \oplus M = M \qquad (۱۱-۲)$$

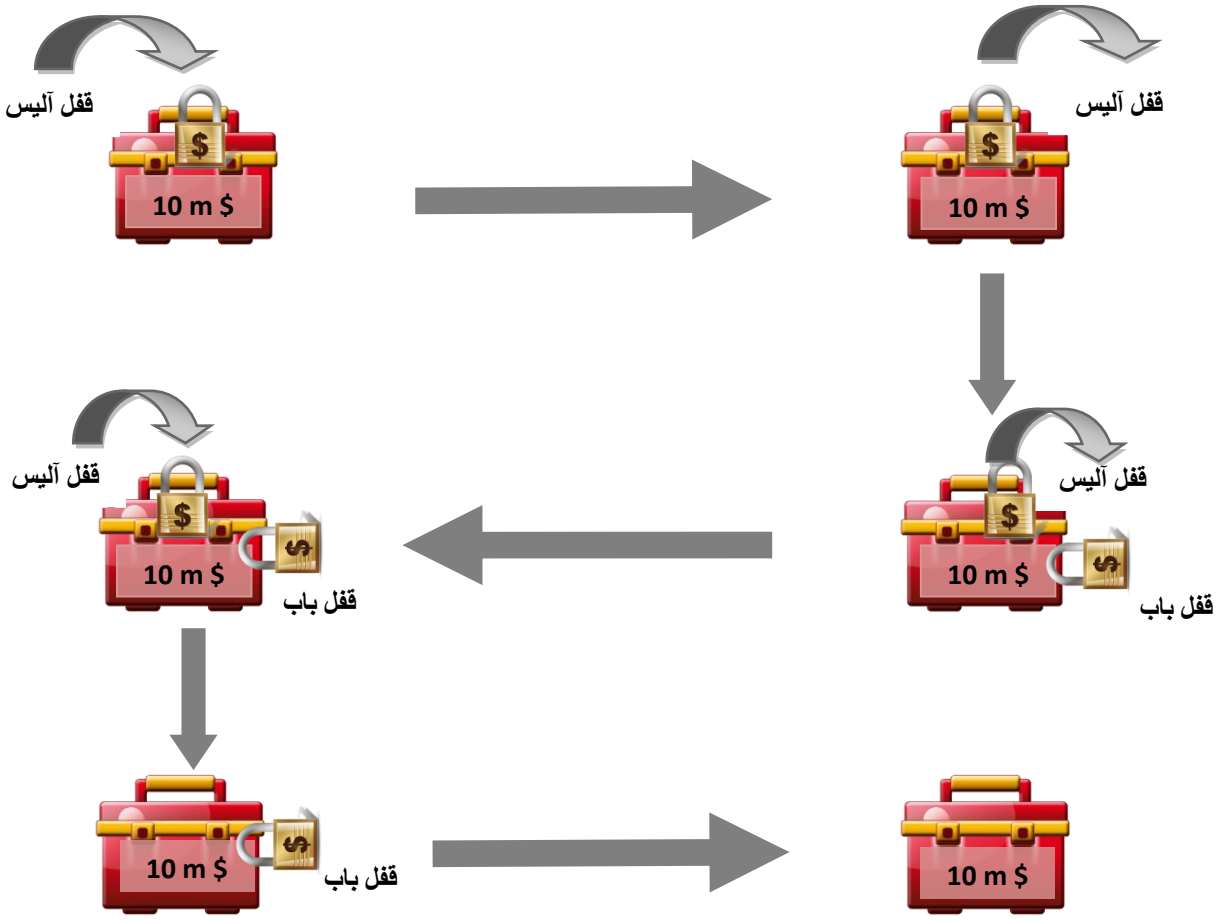
همچنین می‌دانیم: $a \oplus a = 0$

سوال اینجاست که آلیس و باب چطور یک رشته رندوم k بین خودشان به اشتراک می‌گذارند؟ مثلاً یک راهش این است که با هم قرار می‌گذارند که k یک صفحه از کتاب مشخص‌شده بین خودشان باشد و آن‌را بصورت ۰ و ۱ در بیاورند که این رمز بین آن‌ها باشد، البته این نوع اشتراک رمز خطراتی هم دارد! بدین‌گونه که اگر از این کد زیاد استفاده کنیم، عبارت‌ها و کلمه‌هایی تکرار می‌شود و ایو می‌تواند از همبستگی‌هایی که درآن وجود دارد استفاده کند و بنابراین آلیس و باب مجبورند مرتباً همدیگر را ملاقات کنند، چون نمی‌توانند از یک کلید به مدت طولانی استفاده کنند. در نتیجه در دهه ۷۰ میلادی منجر به یک مسئله اساسی بنام مسئله توزیع کلید شد[۱۹].

قضیه one time pad: حجم رشته بیت‌های ارسالی به طول کلید وابسته است. هر کلیدی که طول آن محدود باشد ایمن نیست و قابل باز شدن است که بطور عام ثابت شده است. بنابراین تنها کلیدی ایمن است که طولش بی‌نهایت باشد.

۲- ۴-۱ نمونه‌ای از رمزنگاری کوانتومی

آلیس می‌خواهد ۱۰ میلیون دلار را برای باب بفرستد، بنابراین با کلید خصوصی مربوط به خودش آن‌را قفل می‌کند و برای باب می‌فرستد. همچنین باب آن‌را با کلید خصوصی خودش قفل می‌کند و برای آلیس برمی‌گرداند. حال این جعبه دوتا قفل دارد، بعد آلیس قفل خودش را که زده بود باز می-کند و دوباره برای باب می‌فرستد. در نهایت باب قفل خودش را باز می‌کند. این مثال از رمزگشایی به وضوح در تصویر ۲-۵ نشان داده شده‌است.



تصویر ۲-۵ : رمزنگاری کوانتومی

مسئله این است که کلید k را چگونه از طریق یک راه ایمن بفرستد! این کار در سال ۱۹۷۴انجام شد که این مسئله تبدیل به توسعه ریاضی شد که موسوم به کلید عمومی است. در این نوع رمزنگاری هر شخصی دو تا کلید دارد، یک کلید عمومی و یک کلید خصوصی که به ترتیب P_{A} و S_A می‌نامیم(از کلید عمومی همه اطلاع دارند ولی کلید خصوصی را فقط خود شخص می‌داند و محرمانه است).

کلیدها دارای این خاصیت هستند که :

$$S_A \circ P_{\mathrm{A}} = \mathrm{I} \qquad (۱۲-۲)$$

$$S_B \circ P_{\mathrm{B}} = \mathrm{I} \qquad (۱۳-۲)$$

وهمچنین با داشتن کلید خصوصی می‌توان به کلید عمومی دست پیدا کرد ولی عکس آن امکان-پذیر نیست.

$$S_A \rightarrow P_{\mathrm{A}} \qquad (۱۴-۲)$$

$$P_{\mathrm{A}} \nrightarrow S_A \qquad (۱۵-۲)$$

به عنوان مثال فرض می‌کنیم که از روی p و q به راحتی می‌توانیم حاصل‌ضربش $n = pq$ را پیدا کنیم ولی بر عکس این مسئله امکان پذیر نیست، چون این یک تابع یک‌طرفه است.

فرض کنید که دولت یک پیام M را برای سفارتخانه می‌فرستد که فقط سفارتخانه آنرا باز کند، باید عملی انجام دهیم که سفارتخانه بفهمد که این پیام از طرف دولت است، چون ممکن است کسی که دشمن ایندو است آنرا جعل کرده باشد و پیام جعلی را مخابره کند و چیزی که به سفارتخانه می‌رسد کاملاً مخالف مصالح دولت است. بنابراین برای‌اینکه سفارتخانه بفهمد که آنرا دولت فرستاده، باید با

کلید خصوصی خودش که فقط در دسترس خودش است آنرا رمزینه کند و بعد P_{B} را استفاده می‌کند و آن‌را دو بار قفل می‌کند، حال این متن رمزشده فرستاده می‌شود و درنهایت سفارتخانه کلید S_B را که در دست خودش است باز می‌کند. بنابراین M بدست می‌آید و سپس می‌فهمد که واقعاً پیام از طرف دولت رسیده‌است. البته باید بدانیم که چیزی که با P_{B} رمزی شده فقط با S_B باز می‌شود[۲۲].

۳

آنتروپی و اطلاعات

۳-۱ مقدمه

علم تئوری اطلاعات مربوط به مشاهداتی است که بطور بنیادی احتمالات و ارتباطات را به یکدیگر مربوط می‌کند. در اواسط قرن هجدهم، بایاس[۱] تشخیص داد که احتمالات بستگی به میزان اطلاعات ما دارد، بدین گونه که اگر به اطلاعاتِ یک پیشامد دست یابیم سپس احتمالات مربوط به این پیشامد تغییر داده می‌شود. مثلاً احتمال اینکه وقتی خانه را ترک می‌کنیم و باران ببارد، در حدود۰,۲ است اما اگر۱۰ دقیقه قبل از ترک کردن منزل به بیرون از خانه بنگریم و مشاهده کنیم که باران می‌بارد، در آنصورت اطلاعات افزوده مطابق با احتمال بیشتر از ۰,۹ است. بطور کلی نتیجه می‌گیریم که اطلاعات تابعی از احتمالات است؛ از دیدگاه فیزیک، آنتروپی وابسته به توزیع احتمالات است. این نتیجهٔ تحقیقی از طبیعتِ فیزیکِ آنتروپی توسط بالتزمن[۲] و دستیارانش بود.

آنتروپی مفهوم کلیدی تئوری کوانتومی است که اطلاعات موجود در حالت فیزیکی را اندازه‌گیری می کند و می‌توان این اطلاعات را فشرده کرد، بدون اینکه به محتوی آن لطمه‌ای وارد کرد. همچنین اینکه نویز یک کانال کوانتومی، مقداری از اطلاعات کوانتومی فرستاده شده را از بین می‌برد که ما می-توانیم مقادیر این اطلاعات را تخمین بزنیم.

در این فصل به علت اینکه می‌خواهیم نظریه اطلاعات کوانتومی را مطالعه کنیم، ابتدا تعریف بنیادی و خواص آنتروپی را در تئوری کلاسیکی بیان می‌کنیم، سپس مرتبط با ماتریس چگالی، آنتروپی در تئوری اطلاعات کوانتومی مورد بررسی قرار می‌دهیم.

---

۱. Bayes

۲. Baltzmann

۳-۲ احتمالات شرطی

منظور از کانال کلاسیک عملگری است که یک آنسامبل تصادفی A را به آنسامبل تصادفی B تبدیل می‌کند، کانال مخابراتی کلاسیکی طبق تعریف گفته‌شده رفتار می‌کند[۲۵]. در این حالت A را ورودی کانال و B را خروجی آن می‌نامیم. یک کانال بدون نویز کانالی است که خروجی آن دقیقاً با ورودی‌اش برابر است. یک رویداد یا آزمایش A را در نظر بگیرید، مثلاً اندازه‌گیری یا نتیجه شانس یک بازی می‌تواند تعدادی از نتایج یا پیشامدهای ممکن $\{a_i\}$را داشته باشد. احتمال اینکه a_i رخ بدهد =A (a_i)، برابر $P(a_i)$ است و می‌دانیم که $P(a_i)$ در این بازه‌ی $0 \leq P(a_i) \leq 1$ قرار دارد. اگر مجموعه $\{a_i\}$ شامل تمام نتایج ممکن باشد، پس جمع احتمالات به صورت زیر است:

$$\sum_i P(a_i) = I \qquad (۱-۳)$$

رویداد دوم را B و نتایج آن‌را $\{b_j\}$ معرفی می‌کنیم، سپس تنها احتمالاتِ $P(a_i)$ و $P(b_j)$، تمام اطلاعات مورد نیاز را در اختیار ما نمی‌گذارند. توصیف کاملتر با احتمالات الحاقی $\{P(a_i,b_j)\}$ بدست می‌آید.

در حالتی‌که A و B مستقل باشند در آن‌صورت رویدادها غیر همبسته خواهند بود، پس

$$P(a_i,b_j) = P(a_i)\, P(b_j) \qquad (۲-۳)$$

اگر تابع دو متغیر تصادفی A و B را با $P(a_i, b_j)$ نشان دهیم، حال می‌توان احتمالات رویدادهای مجزا را بر حسب احتمالات الحاقی با جمع روی همه خروجی‌ها اینگونه تعریف کرد:

$$p(a_i) = \sum_j P(a_i, b_j)$$

$$p(b_j) = \sum_i P(a_i, b_j) \qquad (۳-۳)$$

واضح است که اطلاعات بدست‌آمده با دانستن مقدار A، می‌تواند احتمال هر کدام از متغیرهای تصادفی B را تغییر دهد. هر کانال کلاسیک با تعیین مقادیر $P(a_i|b_j)$ به ازای تمام i وj ها مشخص می شود. فرض می‌کنیم با دانستن متغیر تصادفی $A=a_0$، احتمال شرطی اینگونه است: $P(b_j|a_0)$ یعنی احتمال اینکه $B=b_j$ باشد، به شرطی‌که $A=a_0$ معلوم شده‌باشد(این احتمال شرطی مربوط به رویدادی برای $A=a_0$ و $B=b_j$ است)، بنابراین واضح است که این کمیت وابسته به احتمال الحاقی است:

$$P(b_j|a_0) = K(a_0)P(a_0,b_j) \qquad (۴-۳)$$

$K(a_0)$ ثابت است و آنرا می‌توان با جمع معادله بالا روی مجموعه‌ای از خروجی‌های $\{b_j\}$ بدست آورد. همچنین جمع روی $P(b_j|a_0)$ باید یکتا و بصورت مجموعه کامل احتمالات برای خروجی B باشد.

$$\sum_j P(b_j|a_0) = \sum_j K(a_0)P(a_0,b_j) \longrightarrow 1 = K(a_0)\sum_j P(a_i,b_j) \longrightarrow$$
$$1 = K(a_0)P(a_0) \rightarrow K(a_0) = [P(a_0)]^{-1} \qquad (۵-۳)$$

بنابراین می‌توان احتمالات شرطی و الحاقی را با روابط (۴-۳) و (۵-۳) به یکدیگر ربط دهیم.

$$P(a_0,b_j) = P(b_j|a_0)P(a_0) \qquad (۶-۳)$$

حال با تکرار تحلیل قبل، بادانستن احتمال $A=a_i$، مقدار متغیر تصادفی $B=b_j$ را بدست می‌آید. بنابراین برای توزیع احتمال $P(a_i|b_j)$ داریم:

$$P(a_i,b_j) = P(a_i|b_j)P(b_j) \qquad (۷-۳)$$

می‌خواهیم از رابطه‌ی (۳-۷) نتیجه‌ی دیگری را بدست بیاوریم. یعنی اینکه تئوری بایاس نتیجه‌ی ترکیب دو معادله (۳-۶) و (۳-۷) با یکدیگر می‌باشد و رابطه‌ای را با احتمالات شرطی بدست می‌آورد:

$$P(a_i|b_j) = \frac{P(b_j|a_i)P(a_i)}{P(b_j)} \qquad (۳-۸)$$

تئوری بایاس بصورت تناظر به این فرم نوشته می‌شود:

$$P(a_i|b_j) \propto P(b_j|a_i)\,\mathrm{P(a_i)} \qquad (۳-۹)$$

همچنین برای استفاده از شکل کلی تئوری بایاس می‌توانیم رابطه (۳-۹) را با بکار بردن شرط نرمالیزاسیون $\sum_{ij} P(a_i|b_j) = 1$ بگونه‌ی دیگری بنویسیم و در این حالت، هرگاه در خروجی سیگنال b_j دریافت گردد، می‌توان احتمال شرطی این که چه سیگنال a_i ای منجر به این خروجی شده است را بصورت زیر محاسبه کرد:

$$P(a_i|b_j) = \frac{P(b_j|a_i)P(a_i)}{\sum_i P(b_j|a_i)P(a_i)} \qquad (۳-۱۰)$$

در عبارت فوق $\mathrm{P}(a_\mathrm{i})$ مشخصه‌ی منبع A و $\mathrm{P}(a_\mathrm{i}, \mathrm{b_j})$ مشخصه کانال است که برای ما معلوم می‌باشد. لذا به راحتی می‌توان $P(b_j|a_i)$ را محاسبه کرد. در ضمن توجه می‌کنیم که احتمالات شرطی فقط محدود به دو رویداد نیستند، بلکه می‌توانیم آنرا بسط داده و برای چند رویداد بنویسیم. یعنی دو رویداد A و B را با رویداد سوم C با نتایج ممکن $\{\mathrm{C_k}\}$ کامل‌کنیم:

$$\mathrm{P}(a_i, b_j, c_k) = P(a_i|b_j, c_k)P(b_j, c_k) = P(a_i|b_j, c_k)P(b_j|c_k)P(c_k) \qquad (۳-۱۱)$$

و دیگر اینکه

$$P(a_i, b_j, c_k) = P(a_i, b_j|c_k)P(c_k) \qquad (۳-۱۲)$$

در نهایت تئوری بایاس برای سه رویداد اینگونه بسط داده می‌شود:

$$P(a_i|b_j,c_k)=\frac{P(b_j,c_k|a_i)P(a_i)}{P(b_j,c_k)} \qquad (۱۳-۳)$$

۳-۳ آنتروپی و اطلاعات کلاسیکی

۳-۳-۱ آنتروپی شانون[۱]

در مبحث قبل دیدیم که چطور اطلاعات از رویدادها بدست می‌آیند که منجر به تغییر احتمالات برای تعیین قطعیت رویدادها می‌شوند. از لحاظ شهودی هرچقدر پیشامدی محتمل‌تر باشد، اطلاعاتی که کسب کرده‌ایم کمتر خواهدبود و بر عکس. هرگاه احتمال رویداد a_i را با $P(a_i)$ و احتمال رویداد b_j را با $P(b_j)$ نشان دهیم، میزان اطلاعاتی که از وقوع دو پیشامد کسب می‌کنیم برابر خواهد بود با $h[P(a_i,b_j)]$ و با توجه به اینکه دو رویداد مستقل ازهم هستند یعنی $P(a_i,b_j)=P(a_i)P(b_j)$، بنابراین انتظار داریم:

$$h[P(a_i,b_j)]=h[P(a_i)P(b_j)]=h[P(a_i)]+h[P(b_j)] \qquad (۱۴-۳)$$

مسلم است که تنها تابعی که بطور دقیق این تفسیر را برآورده می‌کند، تابع لگاریتم است[۲۶,۲۵]:

$$h[P(a_i)]=-K\log P(a_i) \qquad (۱۵-۳)$$

اطلاعات وابسته به رویداد A و زیرمجموعه‌های کامل A آنرا با میانگین معادله قبلی روی تمام مجموعه خروجی‌های ممکن بدست می‌آوریم:

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

۱. Shannon

(۱۶-۳)

که این تابع، تابع آنتروپی یا آنتروپی شانون است که در گذشته در مکانیک آماری با آن آشنا شده-ایم. منظور از log تابع لگاریتم در پایه‌ی ۲ است.

آنتروپی شانون نقش اساسی‌ای را در نظریه اطلاعات ایفا می‌کند و یک تابع مثبت است. آنتروپی شانون مربوط به متغیر تصادفی a_i، بیانگر میزان اطلاعاتی است که ما با آگاه شدن از متغیر تصادفی a_i کسب می‌کنیم، به عبارت دیگر آنتروپی شانون نشان دهنده میزان ناآگاهی ما از متغیر a_i، قبل از دانستن مقدار آن است که این a_i می‌تواند مقادیر مختلفی را کسب کند. این دو دیدگاه مکمل هم هستند، یعنی می‌توان آنتروپی را به عنوان ناآگاهی قبل از اندازه‌گیری متغیر a_i، یا اطلاعات بدست آمده بعد از اندازه‌گیری آن تعبیر و تفسیر کرد. به عنوان مثال متغیر تصادفی A که مقادیر «شیر یا خط» را با احتمالات p و 1-p می‌پذیرد و متغیر تصادفی B که مقادیر«۰ یا ۱» را با احتمالات p و 1-p می‌پذیرد، حاوی اطلاعات یکسانی بوده و آنتروپی یکسانی خواهند داشت. رابطه (۳-۱۶) تعریف تابع اطلاعات است که H(A) بیانگر میزان حافظه‌ای است که برای ذخیره کردن متغیر A مورد نیاز است[۲۴]. اطلاعات در واقع در آنتروپی توزیع احتمال مهم است، نه برچسب‌ها[۱]. در حقیقت یک منبع را درنظر بگیرید که رشته تصادفی $X_1X_2 \dots X_N$ را که هر کدام توزیع احتمالات یکسانی دارند را تولید و ارسال می‌کند. کمترین میزان حافظه‌ای برای ذخیره کردن اطلاعات مورد نیاز این منبع به آنتروپی شانون مربوط می‌شود. نتایج مهم از خواص آنتروپی استنباط می‌شود.

۳-۳-۲ اطلاعات الحاقی[۲]

[۱] .Lable

[۲] .Joint Probability

اگر دو رویداد A و B با نتایج مربوطه $\{a_i\}$و $\{b_j\}$ را داشته باشیم، سپس مشابه با رابطه (۳-۱۶)، می‌توانیم اطلاعات مربوط به دو رویداد A و B را بر حسب توزیع احتمال الحاقی$P(a_i, b_j)$ این‌گونه بنویسیم:

$$\mathrm{H(A,B)} = -\sum_{ij} P(a_i, b_j) \log P(a_i, b_j)$$

(۳-۱۷)

H(A, B) بیانگر میزان کل ناآگاهی ما از متغیر تصادفی A و B است. البته می‌توانیم اطلاعات را برای رویدادهای مجزای A و B بر حسب توزیع احتمالات الحاقی اینگونه می‌نویسیم:

$$\mathrm{H(A)} = -\sum_{ij} P(a_i, b_j) \log \sum_{k} P(a_0, b_k)$$

$$\mathrm{H(B)} = -\sum_{ij} P(a_i, b_j) \log \sum_{l} P(a_0, b_l)$$

(۳-۱۸)

مقادیر H(A)، H(B) و H(A,B) با نامساوی زیر مشخص می‌شوند:

$$\mathrm{H(A) + H(B) \geq H(A,B)}$$

(۳-۱۹)

که H(A) + H(B) - H(A,B) می‌تواند بصورت آنتروپی نسبی برای دو توزیع احتمالِ الحاقی $\{P(a_i)P(b_j)\}$ و $\{P(a_0, b_j)\}$ نوشته شود:

$$\mathrm{H(A,B)} = \sum_{ij} P(a_i, b_j) \log\left(\frac{P(a_i, b_j)}{P(a_i)P(b_j)}\right) = \mathrm{H}(\{P(a_i, b_j)||P(a_i)P(b_j)\})$$

$$- \mathrm{H(A)} + \mathrm{H(B)}$$

(۳-۲۰)

تعریف آنتروپی نسبی: $P(a_i)$ و $P(b_j)$ احتمالات ذاتی برای رویداد A که مربوط به a_i هستند. آنتروپی نسبی برای دو توزیع احتمال بدین صورت تعریف می‌شود:

$$\mathrm{H}(P||\mathrm{Q}) = \sum_{i} P(a_i)[\log P(a_i) - \log Q(a_i)] = \mathrm{H(P)} - \sum_{x} p(a_i) \log q(a_i)$$

(۲۱-۳)

توجه کنید که آنتروپی نسبی تابع متقارن نیست $\mathrm{H}(\mathrm{Q}||P) \neq \mathrm{H}(P||\mathrm{Q})$

۳-۳-۳ آنتروپی و اطلاعات شرطی

لازم است بدانیم که میزان اطلاعات A و B به یکدیگر مربوط می‌باشند. دو متغیر تصادفی A و B که توزیع آنها با تابع $P(a_i, b_j)$ مشخص می‌شود (با توجه به رابطه (۳-۷)) را درنظر می‌گیریم. فرض می‌کنیم که مقدار یکی از متغیرهای تصادفی مثل A با a_i مشخص باشد، در اینصورت توزیع متغیر تصادفی B عوض خواهد شد و تبدیل به $\mathrm{P}(\mathrm{B}|a_\mathrm{i})$ می‌شود.

در نتیجه اطلاعات باقیمانده در متغیر تصادفی B برابر است با:

$$\mathrm{H}(\mathrm{B}|a_\mathrm{i}) = -\sum_j \mathrm{P}(\mathrm{b_j}|a_\mathrm{i}) \log_2 \mathrm{P}(\mathrm{b_j}|a_i)$$

(۲۲-۳)

این اطلاعات مربوط به B می‌باشد که می‌دانیم $\mathrm{A}= a_i$ است. اگر بخواهیم بدانیم که بطور متوسط دانستن یک مقدار از A چه مقدار در B باقی می‌گذارد، باید روی $\mathrm{H}(\mathrm{B}|a_\mathrm{i})$ متوسط بگیریم. بنابراین:

$$\mathrm{H}(\mathrm{B}|\mathrm{A}) = \sum_{i,j} P(a_i)\mathrm{H}(\mathrm{B}|a_\mathrm{i}) = -\sum_{i,j} P(a_i)\mathrm{P}(\mathrm{b_j}|a_\mathrm{i}) \log_2 \mathrm{P}(\mathrm{b_j}|a_\mathrm{i})$$

$$= -\sum_{\mathrm{i,j}} P(a_i, b_j) \log_2 \mathrm{P}(\mathrm{b_j}|a_\mathrm{i}) = -\sum_{\mathrm{i,j}} P(a_i, b_j) \log_2 \frac{P(a_i, b_j)}{P(a_i)} \quad \mathrm{H}(\mathrm{A}, \mathrm{B}) - \mathrm{H}(\mathrm{A})$$

(۲۳-۳)

$\mathrm{H}(\mathrm{B}|\mathrm{A})$ بیان‌کننده میزان اطلاعات B، مشروط بر اینکه مقادیر A را بدانیم، می‌باشد. بنابراین می توانیم معادله (۳-۲۳) را بصورت زیر بازنویسی کنیم:

$$\mathrm{H}(\mathrm{A}, \mathrm{B}) = \mathrm{H}(\mathrm{A}) + \mathrm{H}(\mathrm{B}|\mathrm{A})$$

(۲۴-۳)

$H(A,B)$ معیار مناسبی برای میزان اطلاعاتی است که باب می‌تواند با دانستن B راجع به A کسب کند.

آنتروپی شرطی بیانگر ناآگاهی ما از مقدار B است، وقتی که مقدار A را می‌دانیم.

قاعده زنجیره‌ای برای آنتروپی شرطی:

$$H(b_1, \dots, b_n|a) = \sum_{i=1}^{n} H(b_i|a, b_1, \dots, b_{i-1}) \quad (۲۵-۳)$$

همچنین اگر دو متغیر تصادفی A و B مستقل باشند، یعنی دانستن A هیچ تأثیری در اطلاعات باقیمانده در B نخواهد داشت. در نتیجه:

$$H(A,B) = H(A) + H(B) \quad (۲۶-۳)$$

۳-۳-۴ اطلاعات متقابل

اطلاعات متقابل دو متغیر تصادفی A و B، اطلاعات مشترک این دو متغیر تصادفی را بیان می‌کند. فرض می‌کنیم که اطلاعات A را به اطلاعات B افزوده‌ایم. اطلاعات مشترک بین A و B دوبار و اطلاعاتی که غیر مشترک هستند، یک‌بار شمرده می‌شوند. بنابراین اطلاعات مشترک کاهیده شده به این شکل تعریف می‌شود:

$$I(A:B) := H(A) + H(B) - H(A, B) \rightarrow I(A:B) = H(A) - H(A|B) \quad (۲۷-۳)$$

محتویات اطلاعات A که مربوط به محتویات اطلاعات B است با آنتروپی شرطی و آنتروپی متقابل معرفی می‌شود.

۳-۳-۵ خواص آنتروپی کلاسیکی

به تعدادی از خواص آنتروپی و اطلاعات کلاسیکی اشاره می‌کنیم:

۱) $H(A:B) \geq 0$ و تساوی وقتی اتفاق می‌افتد که A و B مستقل باشند

۲) اطلاعات تابع محدبی از توزیع احتمال است یعنی اگر P_1 و P_2 دو تابع توزیع احتمال و همچنین $P_0(x) = \lambda P_1(x) + (1-\lambda) P_2(x)$ باشند، آنگاه $H_0(x) \geq \lambda H_1(x) + (1-\lambda) H_2(x)$ خواهد بود.

۳) اعمال شرط آنتروپی را کاهش می‌دهد، یعنی $H(A|B,C) \leq H(A,B)$

۳-۴ آنتروپی و اطلاعات کوانتومی

۳-۴-۱ آنتروپی فون نویمان[۱]

آنتروپی شانون بیانگر عدم قطعیت(میزان اطلاعاتی که از آن آگاه نیستیم) مربوط به توزیع احتمال کلاسیکی است. در آنتروپی فون نویمان اپراتورهای چگالی یک حالت کوانتومی، جایگزین توزیع احتمال کلاسیکی یک متغیر تصادفی شده‌اند. آنتروپی فون – نویمان برای حالت کوانتومی ρ است و با رابطه زیر توصیف می‌شود:

$$S(\rho) := -\mathrm{tr}(\rho \log \rho) \qquad (۲۸-۳)$$

همچنین فرض می‌کنیم که اگر ویژه مقادیر اپراتور چگالی ρ با λ_i مشخص شود، آنتروپی فون-نویمان برحسب ویژه مقادیر بدین صورت نوشته می‌شود:

$$S(\rho) = -\sum_{i=0}^{n} \lambda_i \log_2 \lambda_i \qquad (۲۹-۳)$$

۱. Von Neumann entropy

مثلاً برای یک حالت کوانتومی کاملاً آمیخته‌ای که در فضای n بعدی واقع است که تمام خروجی-های آن یکسان هستند(یعنی $P_i=\frac{1}{n}$)، آنتروپی در نتیجه $S(\rho) = \log_2 n$ خواهد بود.

از الان به بعد وقتی صحبت از آنتروپی می‌کنیم، واضح است که معمولاً منظور آنتروپی شانون یا فون – نویمان است. همچنین می‌دانیم که آنتروپی فون-نویمان تحت تغییرات پایه ناوردا است.

۳-۴-۲ آنتروپی نسبی کوانتومی

همانند آنتروپی شانون، می‌توانیم مدل کوانتومی آنتروپی نسبی را تعریف کنیم، علت این است که می‌خواهیم ویژگی‌های آنتروپی فون نویمان را بشناسیم.

فرض کنید ρ و σ اپراتورهای چگالی هستند. آنتروپی نسبی از ρ به σ اینگونه تعریف می‌شود

$$S(\rho \parallel \sigma) = tr(\rho \log \rho) - tr(\rho \log \sigma) \qquad (۳۰-۳)$$

آنتروپی نسبی کوانتومی نامنفی است، اغلب این نتیجه به‌نام نامساوی کلاین[۱] مشهور است.

$$S(\rho \parallel \sigma) \geq 0 \qquad (۳۱-۳)$$

و تساوی فقط زمانی رخ می‌دهد که $\rho = \sigma$ باشد.

اثبات : فرض می‌کنیم $\rho = \sum_i p_i|i\rangle\langle i|$ و $\sigma = \sum_j q_j|j\rangle\langle j|$ باشند، توجه شود که $|i\rangle$ها و $|j\rangle$ها ویژه‌حالت‌های ماتریس‌های ρ و σ هستند، بنابراین با استفاده از تعریف آنتروپی نسبی داریم:

$$S(\rho \parallel \sigma) = \mathrm{tr}(\rho \log \rho) - \mathrm{tr}(\rho \log \sigma) = \sum_i p_i \log p_i - \sum_i \langle i|\rho \log \sigma|i\rangle$$

و با توجه به رابطه جابجایی $\langle i|\rho = p_i \langle i|$ رابطه فوق بصورت زیر درمی‌آید:

$$S(\rho \parallel \sigma) = \sum_i p_i \log p_i - \sum_i \langle i|(\sum_j \log(q_j)|j\rangle\langle j|)|i\rangle =$$

[۱] .Klein’s inequality

$$\sum_{i} p_i(\log p_i - \sum_{j} \log q_j)$$

(۳۲-۳)

که در آن $p_{ij} = \langle i|j\rangle\langle j|i\rangle$ است و همچنین رابطه $\sum_j p_{ij} = 1$ صادق است. با توجه به خاصیت تحدّب تابع لگاریتم داریم:

$$\sum_{j} p_{ij} \log(q_j) \leq \log r_i$$

(۳۳-۳)

همچنین $r_i = \sum_j p_{ij} q_j$ و تساوی به ازاء همه مقادیر j که $p_{ij} = 1$ باشد، برقرار است. حال با توجه به روابط (۳-۳۲) و (۳-۳۳) خواهیم داشت:

$$S(\rho \parallel \sigma) \geq \sum_{i} \log(\frac{p_i}{r_i})$$

طبق رابطه تحدب، سمت راست معادله فوق مثبت است. لذا نتیجه می‌گیریم که

$$S(\rho \parallel \sigma) \geq 0$$

۳-۴-۳ خواص مهم آنتروپی کوانتومی

۱) آنتروپی یک کمیت نامنفی است که این ویژگی از نتیجه تعریف آنتروپی فون نویمان نتیجه شده است. ولی فقط برای حالت خالص برابر صفر خواهد بود.

۲) در فضای d بعدی، برای حالت‌های آمیخته $\rho = \frac{I}{d}$ بیشترین مقدار آنتروپی $\log d$ خواهد بود. این نتیجه با توجه به تعریف مثبت بودن آنتروپی نسبی بدست می‌آید:

$$0 \leq S(\rho \parallel \frac{I}{d}) = -S(\rho) + \log d \rightarrow S(\rho) \leq \log d \qquad (۳۴-۳)$$

۳) فرض می‌کنیم که یک سیستم دو بخشی A و B یک حالت خالص می‌باشند، سپس آنتروپی زیر سیستم‌های آن با هم برابر است. یعنی $S(A) = S(B)$.

اثبات: با توجه به تجزیه اشمیت، می‌دانیم که اگرتجزیه اشمیتِ حالت خالص $|\Psi\rangle_{AB}$ بصورت زیر باشد:

$$|\Psi\rangle_{AB} = \sum_i \lambda_i |i\rangle|i\rangle$$

در نهایت ویژه مقادیر اپراتورهای چگالی سیستم‌های A وB یکسان خواهند بود.

$$\rho_A = \sum_i |\lambda_i|^2 |i\rangle\langle i|$$

$$\rho_B = \sum_i |\lambda_i|^2 |i\rangle\langle i|$$

و از آنجا که ویژه مقادیر این دو ماتریس با هم برابر است، طبق رابطه (۳-۲۹) آنتروپی این دو حالت با هم برابر است، یعنی S(A)= S(B).

۴) اگر P_i یک توزیع احتمال و ماتریس‌های چگالی ρ_i با پایه‌های متعامد در زیرفضایی از این فضای برداری باشد، آنگاه:

$$S(\sum_i p_i\rho_i) = H(p_i) + \sum_i p_i S(\rho_i) \qquad (۳-۳۵)$$

اثبات: دقت می‌کنیم که چون λ_i و $|e_i\rangle$ به ترتیب ویژه‌مقادیر و ویژه‌بردارهای ماتریس چگالی ρ هستند، بنابراین $P_i\lambda_i$ و $|e_i\rangle$ ویژه‌مقادیر و ویژه‌بردارهای ماتریس قطری $\sum_i p_i\rho_i$ هستند. در اینصورت:

$$S(\sum_i p_i\rho_i) = -tr[(\sum_i p_i\rho_i \log(\sum_i p_i\rho_i)] = -\ tr \sum_i p_i\rho_i \log p_i\rho_i =$$

$$-\sum_i tr(p_i\rho_i \log p_i) + tr((p_i\rho_i \log \rho_i) = \sum_i p_i \log p_i - \sum_i p_i\rho_i \log \rho_i$$

$$= H(p_i) + \sum_i p_i S(\rho_i)$$

۵) تئوری آنتروپی الحاقی: فرض می‌کنیم که P_i یک توزیع احتمال و $|i\rangle$ها حالت‌های متعامد برای سیستم A باشند و همینطور ρ_i ها ماتریس چگالی برای سیستم B باشند، در نتیجه داریم:

$$S(\sum_i p_i|i\rangle\langle i|\otimes \rho_i) \;=\; H(Pi) + \sum_i p_i S(\rho_i)$$

(۳۶-۳)

۶) اگر روی سیستم اندازه‌گیری انجام دهیم، در نتیجه آنتروپی بعد از اندازه‌گیری بزرگتر از آنتروپی اولیه(قبل از اندازه‌گیری) می‌باشد.یعنی $S(\rho')\geq S(\rho)$

اثبات: فرض می‌کنیم که P_iها اپراتورهای تصویرگری هستند که تشکیل پایه‌های کامل می‌دهند. اگر سیستم قبل از اندازه‌گیری در حالت ρ باشد، سپس سیستم بعد از اندازه‌گیری در حالت $\rho' := \sum_i p_i \rho p_i$ قرار خواهد گرفت. بنابراین برای اثبات از نامساوی کلاینِ ρ به ρ' استفاده می‌کنیم:

$$0 \leq\; S(\rho' \parallel \rho) = -S(\rho) - tr(\rho \log \rho')$$

رابطه کامل بودن $\sum_i p_i = 1$ و رابطه ${p_i}^2 = p_i$ را بکار می‌بریم:

$$-tr(\rho \log \rho') = -tr(\sum_i p_i \rho \log \rho') = -\,tr(\sum_i p_i \log \rho' p_i)$$

توجه می‌کنیم که p_i و ρ' با یکدیگر جابجا می‌شوند، چون این رابطه برقرار است:

$$\rho' p_i := p_i \rho p_i = p_i \rho'$$

لذا داریم:

$$-tr(\rho \log \rho') = \; -tr(\sum_i p_i \rho p_i \log \rho') = -tr(\rho \log \rho') = \; S(\rho') \longrightarrow S(\rho' \parallel \rho)$$

$$= -S(\rho) + \; S(\rho') \;\geq 0 \;\longrightarrow S(\rho') \geq \; S(\rho)$$

۳-۵ نرخ کلید

فرض می‌کنیم که در حین عبور پیام از درون کانال، کانال بدون نویز باشد و وقتی که می‌خواهیم بیت ۰و۱ را ارسال کنیم، با احتمال p تبدیل به ۰ یا ۱شده و با احتمال 1-p بیت سالم عبور کند(چون ممکن است که بیت در حین عبور از کانال، با محیط اطراف برهم‌کنش کند) به این کانال، کانال

دودویی[1] می‌گویند. می‌خواهیم کاری بکنیم که باب بتواند پیام‌های صحیح را از پیام‌های دریافت شده استخراج کند[۲۴].

هدف مخابره رشته‌های ۰و۱ از درون کانال است و در انتهای این کانال رشته‌های ۰و۱ دریافت شده برای تعیین و تصحیح خطاها بررسی می‌شود و بعد در این کانال تصحیح شده، درآخر سر کد-گشایی می‌شود.

یک راه برای تعیین و تصحیح خطا آن است که عنصر تکراری را به نوعی وارد پیام‌های خود کنیم. مثلاً بجای مخابره یک ۰ سه تا ۰ و بجای ۱ سه تا ۱ مخابره کنیم و به باب بگوییم که از قانون اکثریت استفاده کند، یعنی یک رشته سه تایی دریافت کند. در واقع احتمال خطا که قبلاً p بود کمتر خواهد شد، حال احتمال در کد سه تایی برابر خواهد بود با $3p^2(1-p)$ و p^3 . در نتیجه احتمال وقوع احتمال خطا برابر است با $3p^2(1-p)+p^3$ که برای p های کوچک از مرتبه p^2 است. البته در این حالت نرخ مخابره اطلاعات پایین آورده شده است و به جای یک بیت از سه بیت برای مخابره استفاده کرده‌ایم.

در این حالت نرخ مخابره اطلاعات یعنی R برابر است با $\frac{1}{3}$. در حالت کلی اگر از n بیت برای مخابره 2^k پیام استفاده کنیم، می‌گوییم که نرخ مخابره اطلاعات برابر است با

$$R := \frac{k}{n} \qquad (۳۷-۳)$$

واضح است که با استفاده از کد تکرار می‌توان برای مخابره هر بیت تعداد بیشتری بیت بکار برد و وقوع خطا را کاهش داد که در این‌صورت نرخ مخابره اطلاعات هم به صفر میل خواهد کرد. در نتیجه برای جلوگیری از خطا، نرخ مبادله اطلاعات R حتماً باید از حد کلید K کمتر باشد.

فزض می‌کنیم که منبع حروف ۰ و ۱ را با آنتروپی H(X) تولید می‌کند.

[1] .Binary

$$R = \frac{k}{n} \leq H(X) - H(P) \qquad (۳۸-۳)$$

می‌دانیم که آنتروپی یک منبع بیانگر محتوای اطلاعاتی آن منبع است، وقتی که هیچ خروجی‌ای از کانال دریافت نشده و رشته حاوی اطلاعات از درون این کانال عبور نکرده باشد، میزان ناآگاهی از منبع با $H(X)$ مشخص می‌شود. زمانی‌که این رشته از منبع عبور کرد، در طول مسیر دستخوش خطا می‌گردد و احتمال برگشتن هر بیت(بوجود آمدن خطا) P خواهد بود که $H(P)$ اطلاعات عبور کرده از این کانال همراه با خطا است. سوال این است که آیا می‌توان نرخ بیشینه‌ای بوجود آورد که هر نوع مخابره اطلاعات را از درون یک کانال نویزدار عبور داد، بطوریکه احتمال خطا به صفر میل کند. این مسئله ایمنی نرخ کلید را بررسی می‌کند، یعنی اینکه نسبت اندازه ایمنی کلید به تعداد سیگنال‌ها داخل این کانال فرستاده‌می‌شود.

اگر پیام X از منبع عبور کرد، در اثر خطا یک رشته $Y=(y_1,y_2,\ldots,y_N)$ را دریافت می‌کنیم. بدین معنی است که میزان ناآگاهی از منبع به $H(X|y)$ تبدیل می‌شود و اطلاعاتی که از منبع داریم بصورت $H(X|Y)$ خواهد بود. لذا:

$$R \leq H(X)-H(X|Y) \qquad (۳۹-۳)$$

که R ظرفیت نرخ بیشینه اطلاعات است که اطلاعات کوانتومی را با این نرخ محاسبه می‌کنند.

$$K= \max(H(X)-H(X|Y)) = \max I(X:Y) \qquad (۴۰-۳)$$

بنابراین انتقال اطلاعات با نرخ کمتر از حد کلید امکان پذیر است. بطوریکه خطا در حد nهای بزرگ به صفر میل می‌کند.

حال اگر استراق سمع کننده به سیستم آلیس و باب دسترسی داشته باشد در نتیجه باب این اطلاعات را با این نرخ دریافت می‌کند[۳۰,۲۸]:

$$K= \max I(A:B|E) \rightarrow$$

$$K= \max\{I(A:B)-I(A:E), I(A:B)-I(B:E)\} \quad (۴۱-۳)$$

همانطور که در تعریف آنتروپی متقابل در رابطه (۳-۲۷)، داریم:

$$K= \max\{H(A|E)- H(A|B), H(A|B)- H(B|E)\}$$

بطور کلی در این بخش دیدیم که می‌توان از یک کانال نویزدار برای انتقال اطلاعات بطور ایمن استفاده کرد.

کلید خام[۱]: وقتی که یک رشته بیت از درون کانال کوانتومی (کانالی است که بین آلیس و باب به اشتراک گذاشته شده است) به باب ارسال می‌شود، به دلیل وجود عوامل مختلفی از قبیل نویز درون کانال که در اثر حضور ایو بوجود آمده‌است یا ویژگی‌های کانال و یا نوع پروتکل، ممکن است رشته‌ی بیت آلیس و رشته‌ی بیت باب با یکدیگر یکسان نباشند و تنها بخشی از رشته بیت آن‌دونفر برابر باشند که از آن رشته کلید یکسان به عنوان کلید خام استفاده خواهد شد.

۱. raw key

۴

توزیع کلید کوانتومی مستقل از دستگاه

۴-۱ مقدمه

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

فرض اول- استراق سمع کننده که معمولاً آن‌را (ایو) می‌نامند صرف‌نظر از قدرت او، باید از قوانین فیزیک کوانتومی تبعیت کند.

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

فرض سوم- آلیس و باب اعداد تصادفی را بصورت کاملاً ایمن تولید می‌کنند و از نتایج خروجی-شان به عنوان کلید استفاده می‌کنند، بطوریکه می‌توانند پایه‌های اندازه‌گیری خود را بصورت اتفاقی و مستقل از ایو انتخاب کنند. واضح است که اگر ایو پیشاپیش پایه‌های اندازه‌گیری را بداند، احتمال یک حمله موفقیت آمیز امکان‌پذیر است.

فرض چهارم- که ضروری‌ترین نیاز برای تحلیل ایمنی توزیع کلید کوانتومی است، این است که آلیس و باب کنترل کامل و دقیقی روی دستگاه‌های کوانتومی خود که از آن برای توزیع همبستگی استفاده می‌شود را دارند، و دقت و ویژگی کامل دستگاه را به خوبی می‌دانند در صورتیکه تنها کانال کوانتومی نقص دارد[۳۱,۲۹]. به عنوان مثال فرض می‌کنیم که دستگاه یک فوتونی را که با یک بیت کد شده باشد، منتشر کند و در مکانی‌که این بیت کد شده منتشر می‌شود، هیچ فوتون کدشده دیگری نتواند عبور کند. نقص این فرض منجر به حملات ممکن روی طرح توزیع کلید کوانتومی می‌شود. البته این فرض اغلب مورد نقض قرار می گیرد، مثلا اگر آلیس و باب بجای کیوبیت‌هایشان، سیستم-

های چهار بعدی را به اشتراک بگذارند، در این صورت امنیت پروتکل BB۸۴ بطور کامل دچارخطر کشف رمز قرار می‌گیرد. اگر اجرای توزیع کوانتومی کلید این شرایط را برآورده نکند، مثلاً در پروتکل توزیع کوانتومی کلید BB۸۴ ، اگر منبع بجای یک فوتون چندین فوتون را منتشر کند و یا دستگاه‌ها بجای اندازه‌گیری کردن در دو پایه مختلف، از یک پایه استفاده کنند، امنیت این پروتکل بطور کامل ناامن خواهد شد[۱۹].

در توزیع کلید کوانتومی، آلیس و باب ذرات درهم‌تنیده‌ای که از منبع عمومی منتشر می‌شود، دریافت می‌کنند و هر کدام از این ذرات منتشر شده را در پایه‌های تصادفی اندازه‌گیری می‌کنند. اندازه‌گیری‌های خروجی بطور سّری و محرمانه نگه‌داشته می‌شود و کلید خام را بوجود می‌آورد. حال منبع ذرات را بصورت مراکزی در نظر می‌گیریم که ذرات در هم‌تنیده را توزیع می‌کنند و بین دستگاه‌های ایمن آلیس و باب قرار گرفته اند. بنابراین این منابع ممکن است تحت کنترل ایو که همان استراق سمع کننده است، باشد که تحت این شرط دیگر ایمن نمی‌باشد. مثلاً ایو می‌تواند این منبع اصلی را دستکاری کند، یعنی اطلاعاتی که آلیس و باب در مورد نتایج اندازه‌گیری خود بدست-آورده‌اند، مستقیما به دست ایو برسد، سپس ایو این اطلاعات را برای باب بفرستد. در نهایت آلیس و باب با مقایسه نتایجشان، حالت کوانتومی‌ای را که از ایو دریافت کرده‌اند را به عنوان کلید سّری بکار ببرند و به این موضوع پی نبرند که این حالت‌ها را ایو برای آلیس و باب توزیع کرده‌است. بنابراین این کلید سّری دارای ایمنی مورد دلخواه ما نخواهد بود.

لذا به علت اینکه ایمنی این نوع پروتکل‌هایQKD استاندارد تضمین نمی‌شود، پس انگیزه‌ای برای معرفی پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاهی(DIQKD) را داریم که شکل ایمنی قویتری را ارائه می‌دهند[۲۹]. ایمنی این نوع پروتکل‌ها مبتنی بر فرضیات کمتری است یعنی بر خلاف QKD استاندارد که فرض شده بود حالت فرستاده شده برای آلیس و باب از قبل درهم-تنیده‌ی کامل است، ولی در این نوع پروتکل‌های مستقل از دستگاه حالت فرستاده شده ممکن است

درهم تنیده کامل نباشد و آن حالت کوانتومی توسط ایو به آلیس و باب فرستاده شود، بدین گونه که منبع همان استراق سمع کننده باشد. همانطور که فرض می شود، همانند طرح توزیع کلید کوانتومی که براساس قوانین فیزیک کوانتومی می‌باشد، پروتکل توزیع کلید کوانتومی مستقل از دستگاه نیز باید از قوانین فیزیک کوانتومی تبعیت کند.

مشکل این است که اجراسازی QKD در زندگی واقعی متفاوت با طرح ایده‌آل است. مثلاً دستگاه-های کوانتومی ممکن است در اثر برهم‌کنش با محیط دچار نویز شوند[۳۲]. پس انگیزه‌ای برای معرفی DIQKD داریم.

پروتکل مستقل از دستگاه با طرح استاندارد QKD متفاوت و ایمنی قوی‌تری نسبت به QKD استاندارد دارد، مشروط بر آنکه از نقض نامساوی بل استفاده شود.

۴-۲ ضرورت استفاده از پروتکل‌های مستقل از دستگاه

همانطور که قبلاً اشاره کردیم، پروتکل‌های توزیع کلید کوانتومی به خاطر وجود نقص‌هایی که توسط ایو بوجود می‌آید، قابل حمله هستند، به طریقی که ایو به آسانی می‌تواند دستگاه را به‌گونه‌ای دستکاری کند که این طرح توزیع کلید بطور کامل ناامن شود. این حملات نه تنها دارای ساختارهای تئوری هستند، بلکه در عمل نیز می‌توانند به گونه‌ای اجرا شوند که ایمنی طرح توزیع کلید کوانتومی را از بین ببرند. احتمالات حمله به این پروتکل بدین گونه است که:

۱- فرض کنید در پروتکل BB۸۴ ، چندین فوتون از آلیس به باب فرستاده می‌شود، ایو به راحتی می‌تواند با ذخیره کردن بعضی از این فوتون‌ها در حافظه‌اش به سیستم آلیس حمله کند و سپس ذرات را در پایه‌هایی که توسط آلیس اعلام شده اندازه‌گیری می‌کند و با قطعیت بیت کدشده را رمزگشایی کرد. بنابراین این طرح بطور دقیق بر منبعی استوار است که فوتون‌های تنها را از یک راه ایمن منتشر کند.

۲- در روش دوم حمله به سیستم، فرض می‌شود که دستگاه‌هایی[۱] که بیت‌ها را کدگذاری کرده‌اند و فوتون‌های اندازه‌گیری، نقص دارند.

وقتی دستگاه‌ها نقص دارند یعنی اینکه دستگاه فیزیکی تمام اطلاعات خام را به استراق سمع-کننده انتقال می‌دهد. بنابراین آلیس و باب باید از آزمایشگاه‌هایشان بطور کامل محافظت کنند و آن‌را پوشش دهند.

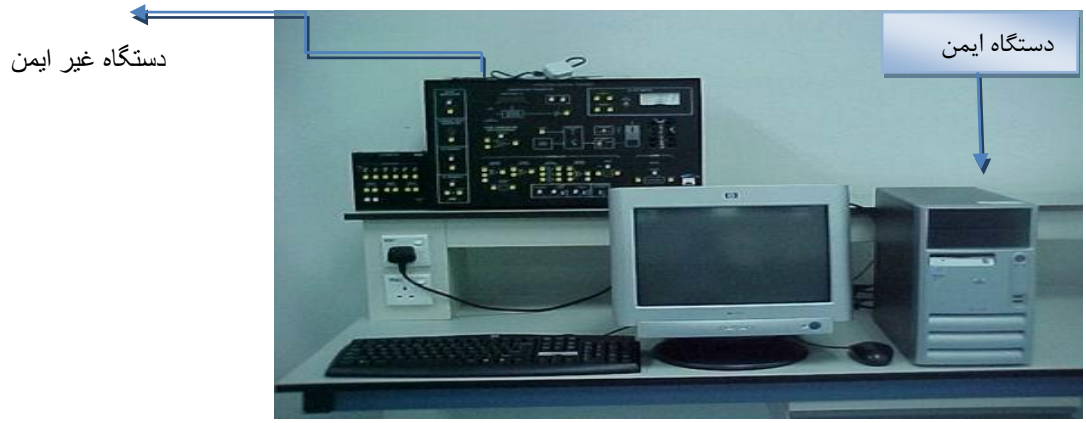
وقتی فوتون‌ها ایراد دارند، یعنی اینکه به جای کد کردن و اندازه‌گیری کردن در دو تا پایه‌های تصادفی، آلیس و باب همیشه از پایه‌های یکسان استفاده می‌کنند. سپس ایو چون این پایه‌ها را می‌داند، بدون اینکه سیستم را خراب کند، می‌تواند فوتون را در این پایه‌ها اندازه‌گیری کند و اطلاعات در مورد بیت را بطور کامل کشف کند، اما همچنان آلیس و باب از اینکه ایو به اطلاعات سّری آن‌ها دست پیدا کرده، بی‌اطلاع می‌مانند.

در پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه، آلیس و باب نه تنها به منبع ذرات مطمئن نیستند، بلکه به دستگاه‌های اندازه‌گیری‌شان هم اطمینان ندارند. مثلاً جهت‌های اندازه‌گیری به علت نقص در دستگاه‌ها ممکن است که با گذشت زمان دستخوش تغییر و انحراف گردد و یا اینکه دستگاه-هایی که قبل از اندازه‌گیری بدون عیب و نقص بود، ممکن است نامطمئن گردد. از این پس آلیس و باب تضمین نمی‌کنند که پایه‌های اندازه‌گیری واقعی متناسب با آن چیزی باشد که مورد انتظار ما خواهد بود.

نمونه‌ای از دستگاه اندازه‌گیری را در تصویر۴-۱ مشاهده می‌کنیم، مثلاً سیستم آلیس را درنظر می‌گیریم که شامل دستگاه غیر ایمن و یک دستگاه ایمن می‌باشد. دستگاه غیر ایمن همان دستگاه اندازه‌گیری آلیس است، علت نامطمئن بودن آن اینست که از بعد فضای هیلبرت و اپراتورها چشم-پوشی می‌کنیم. دستگاه ایمن یک کامپیوتر کلاسیک می‌باشد که اعداد تصادفی تولید می‌کند.

---

۱. Devices



تصویر۴-۱: ضرورت استفاده از پروتکل‌های مستقل از دستگاه

در حقیقت در تحلیل ایمنی توزیع کلید کوانتومی یکی از پارامترهای مهم مربوط به ایمنی، ابعاد سیستم یعنی فضای هیلبرت[۱] است که هم در محاسبه آنتروپی که جاسوس در مورد کلید خام دارد[۳۵] و هم در کاهش حالت‌های همدوسی[۲] که در نتیجه‌ی حملات دسته‌جمعی بوجود آمده‌است، نقش دارد و همیشه وارد محاسبات می‌شوند. بنابراین ایمنی پروتکل توزیع کلید کوانتومی زمانی معتبر است که ابعاد فضای هیلبرت مشخص باشد، اگرچه اغلب ادعا می‌شود که توزیع کلید کوانتومی خودبخود امن است و بر فرضیات محکمی استوار است(یعنی اینکه بر طبق سختی محاسباتی قرار نگرفته است).

در پروتکل‌های معمولی و استاندارد QKD فرض شده‌بود که آلیس و باب از اندازه‌گیری‌هایی که انجام می‌دهند و همچنین از بعد فضای هیلبرتِ حالت کوانتومی که اندازه‌گیری می‌کنند، اطلاعات

---

۱. سیستمی که بکار می‌گیریم مثلاً دو تا فوتون $\frac{۱}{۲}$ باشد،سیستم ۴ بعدی است، به جای دو ذره، سه ذره را داشته باشیم که ۳ تا ذره $\frac{۱}{۲}$ دارای ۸ بعد است و یا اگر سه ذره با اسپین ۱ داشته باشیم دارای ۹=۳×۳ بعد است.

۲. مثلاً حالت همدوس Coherent: $\frac{1}{\sqrt{2}}\left(|\uparrow> + |\downarrow>\right)$ است. به خاطر فاز نسبی وقتی ایو استراق سمع می‌کند این Coherent از بین می‌رود.

کاملی دارند. سپس آنها از این اطلاعات برای محدود کردن اطلاعات ایو استفاده می‌کنند. در صورتیکه در پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه، آلیس و باب نمی‌توانند هیچ فرضی را در مورد بعد فضای هیلبرت بگذارند. یعنی پروتکل DIQKD، این فرضیات بکار برده شده در پروتکل‌های QKD را به مینیمم کاهش می‌دهد. به علت اینکه این فرضیات اغلب بحرانی هستند، با این وجود ایمنی به مراتب قویتری نسبت به پروتکلهای معمولی QKD دارد.

هدف پروتکل‌های مستقل از دستگاه این است که فرضیات بالا را به مینیمم کاهش دهد و همچنین طراحی یک سری پروتکل‌های رمزنگاری است که در مقابل ایو بسیار قدرتمند ایمن است و ایمنی آنها نیازی به جزئیات مشخصه‌ی دستگاه‌ها ندارد، کار این دستگاه‌ها این است که برای ما کلید کوانتومی را بصورت محرمانه از طریق یک راه ایمن بوجود آورند. این شکل قویتر رمزنگاری به شرطی امکان‌پذیر است که رمزنگاری مبتنی بر مشاهده نقض نامساوی بل باشد. نقض نامساوی بل تضمین می‌کند که اطلاعات تولید شده توسط دستگاه‌های کوانتومی دارای مقداری ایمنی هستند، صرفنظر از اینکه این اطلاعات دقیقاً چگونه تولید شده‌اند.

یکی از مزیت‌های برجسته پروتکل‌های مستقل از دستگاه این است که برخی از اشکالات توزیع کلید کوانتومی معمولی را برطرف می‌کنند. در مدل DIQKD، همانطور که در تصویر (۴-۲) مشاهده می‌شود، دستگاه‌های کوانتومی به عنوان جعبه‌های سیاه[۱] در نظر گرفته می‌شوند. خصلت این جعبه-های سیاه این است: یک تابعی را برای ما محاسبه می‌کنند که فقط به ورودی و خروجی آن دسترسی داریم و همچنین از درون این جعبه‌های سیاه اطلاعی نداریم. بنابراین دستگاه‌های کوانتومی خروجی-های کلاسیکی را بوجود می‌آورند و این خروجی‌ها ممکن است به مقدار بعضی ازورودی‌های کلاسیکی بستگی داشته باشند. فرض می‌شود که این دستگاه‌ها یک فرایند کوانتومی را اعمال می‌کنند اما هیچ فرضی از قبیل ابعاد فضای هیلبرت، اپراتورها یا حالت‌ها درمورد فرایند کوانتومی واقعی (که در آن

[۱] در اصطلاح کامپیوتر Black box or Oracle.

خروجی‌ها بر اساس ورودی‌ها تولید می‌شوند) روی آن گذارده نمی‌شود. مثلاً از حالت درهم‌تنیده اطلاعاتی نداریم. بطور دقیق می‌توان گفت که هیچ شرطی روی عملکرد داخلی دستگاه‌های کوانتومی مورد استفاده در پروتکل نمی‌گذاریم.

تصویر ۴-۲ : ضرورت استفاده از پروتکل‌های مستقل از دستگاه

انگیزه‌ی عملی برای معرفی پروتکل‌های مستقل از دستگاه DIQKD وجود دستگاه‌های نامطمئن می‌باشد که همچنان می‌خواهیم ایمنی را به مراتب افزایش دهیم. در ضمن ایمنی فقط وابسته به همبستگی بین ورودی و خروجی‌های آلیس و باب است. بطور مثال کسی که به دستگاه‌های کوانتومی دسترسی دارد، گاهی اوقات ممکن است که این دستگاه‌ها را هک کند و یا اینکه آنها را جعل کند.

مسئله مهم دیگر چگونگی حمله ایو به سیستم آلیس و باب است که ما فرض را بر حملات دسته جمعی می‌گذاریم[۳۰]. حملات دسته جمعی یعنی اینکه ایو بطور یکسان و مستقل در هر دور پروتکل به سیستم‌های کوانتومی آلیس و باب حمله می‌کند، اما هیچ محدودیت دیگری بر ایو اعمال نمی‌شود. هر چند که ایو می‌تواند سیستم‌هایش را در حافظه کوانتومی قرار دهد و در هر زمان که بخواهد بطور همدوس به آنها حمله کند.

۳-۴ دلیل ایمن نبودن QKD درمقایسه با پروتکل مستقل از دستگاه DIQKD

علت اینکه مدل کلی‌تر مستقل از دستگاه را مطرح می‌کنیم اینست که پروتکل‌های قدیمی QKD ممکن است خیلی زیاد ایمن نباشند. به عنوان مثال نوع درهم‌تنیده BB۸۴ را درنظر بگیرید[۱۹]، آلیس و باب یک کانال کوانتومی را مشترکاً بکار می‌گیرند که این کانال کوانتومی حالت درهم‌تنیده توزیع می‌کنند. آلیس یک دستگاه اندازه‌گیری نیز دارد که بیت‌های۰ و۱ را در پایه کاتوره‌ای σ_z و σ_x اندازه‌گیری می‌کند و آنها را به‌عنوان ورودی کلاسیکی در نظرمی‌گیرد: $x \in \{۰,۱\}$ و یک خروجی $a \in \{۰,۱\}$ را تولید می‌کند و از آن به عنوان نتیجه اندازه‌گیری استفاده می‌کند، و بطور مشابه دستگاه باب ذرات ۰ و۱ را در پایه تصادفی σ_z و σ_x اندازه‌گیری می‌کند که ورودی $y \in \{۰,۱\}$ را می‌پذیرد و خروجی $b \in \{۰,۱\}$ را تولید می‌کند. بنابراین رشته‌بیت‌ها در پایه‌های تصادفی کوانتومی به شکل زیر کد می‌شوند:

$0 \rightarrow \sigma_x$

$1 \rightarrow \sigma_z$

همچنین خروجی‌های هر دو دستگاه آلیس و باب مقادیر محدودی خواهند داشت.

❖ بطور ایده آل فرض ما بر اینست که از ناخالصی (نویز) کانال صرفنظر کنیم و بین آلیس و باب یک همبستگی برقرار است. وقتی فرض می‌کنیم که کانال نویز ندارد یعنی اینکه پیام بدون هیچ تغییری به دست باب خواهد رسید. در اینصورت دو حالت رخ می‌دهد:

- حالت اول، اینگونه است که آلیس و باب هر دو در پایه‌های یکسان σ_z یا σ_x اندازه‌گیری کرده باشند. مثلاً بدین صورت:

Alice	Bob
σ_x	σ_x
0	0
1	1

فرض می‌کنیم که حالت درهم‌تنیده‌ی دو ذره $|\Psi\rangle$ باشد که برحسب پایه‌های x بسط داده‌شده است:

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

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

$$|--\rangle) = \frac{1}{2\sqrt{2}}(2|++\rangle + 2|--\rangle) \rightarrow |\Psi\rangle_x = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) \qquad (۱-۴)$$

در نتیجه‌ی اندازه‌گیری، احتمال الحاقی برای بدست آوردن خروجی ab اینگونه مشخص می‌شود:

$$\mathrm{P}(ab|00) = \mathrm{P}(ab|11) = \frac{1}{2} \qquad (۲-۴)$$

که $\mathrm{P}(ab|\mathrm{xy})$ احتمال مشاهدهٔ جفت خروجی‌های a,b است، وقتی که اندازه‌گیری x , y انجام می‌شود[۳۰].

بنابراین اگر آلیس و باب در پایه‌های یکسان اندازه‌گیری انجام‌دهند، آنها همیشه خروجی‌های کاملاً همبسته بدست می‌آورندکه آنرا بطریق زیر اثبات می‌کنیم.

$$\langle\Psi|\,\sigma_x \otimes \sigma_x\,|\Psi\rangle = \langle\Psi|\,\sigma_z \otimes \sigma_z\,|\Psi\rangle = 1 \qquad (۳-۴)$$

اثبات: اگر اپراتورهای اندازه‌گیری برحسب σ_z و σ_x باشند. تنها سیستم دو حالته‌ای که متناسب با این زمینه‌های اندازه‌گیری منتخب می‌باشد، حالت ماکزیمم درهم‌تنیدگی بدین صورت است:

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

که منجر به همبستگی به طریق زیر می‌شود:

$$\frac{1}{2}[\langle 00| + \langle 11|(\,\sigma_x \otimes \sigma_x)|00\rangle + |11\rangle] =$$

$$\frac{1}{2}(\langle 00|\sigma_x \otimes \sigma_x|00\rangle + \langle 00|\sigma_x \otimes \sigma_x|11\rangle + \langle 11|\sigma_x \otimes \sigma_x|00\rangle + \langle 11|\sigma_x \otimes$$

$$\sigma_x|11\rangle) = \frac{1}{2}(\langle 00|00\rangle + \langle 00|11\rangle + \langle 11|11\rangle + \langle 11|11\rangle) = 1$$

- حالت دوم، اگر پایه‌های اندازه‌گیری آلیس و باب متفاوت باشند، یعنی اگر آلیس σ_x را به عنوان پایه اندازه گیری انتخاب کند و باب σ_z را پایه اندازه‌گیری در نظر بگیرد و برعکس:

Alice	Bob
1	1
1	0
0	0
0	1

با توجه به $|\Psi\rangle$ در پایه‌های متفاوت که به قرار زیر است:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}[(\frac{|+\rangle + |-\rangle}{\sqrt{2}})_A|0\rangle_B + (\frac{|+\rangle - |-\rangle}{\sqrt{2}})_A|1\rangle_B]$$

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

در حالت فوق احتمال الحاقی در پایه‌های متفاوت به فرم زیر است:

$$P(ab|xy) = tr[\,\rho_{AB}\, A(a|x) \otimes B(b|y)] \qquad (۴-۴)$$

بنابراین: $P(ab|01) = tr[\,\rho_{AB}\, A(a|0)\, B(b|1)] = \frac{1}{4}$

پس باب با احتمال $\frac{۱}{٤}$ در حالت ۰ یا ۱ بدست می‌آورد. در نتیجه اگر آلیس و باب در پایه‌های مختلف اندازه‌گیری کنند، نتیجه اندازه‌گیری کاملاً غیرهمبسته است.

همچنین حالت ناهمبسته برای این حالت به فرم زیر ثابت می‌شود:

$$\langle\Psi\,|\,\sigma_x \otimes \sigma_z\,|\,\Psi\rangle = \langle\Psi\,|\,\sigma_z \otimes \sigma_x|\,\Psi\rangle = 0 \qquad (۵-۴)$$

چون فرض کرده‌ایم: $\sigma_z|0\rangle = +1|0\rangle\,, \sigma_z|1\rangle = -1|1\rangle$

$\sigma_x|0\rangle = +1|1\rangle\,, \sigma_x|1\rangle = +1|0\rangle$

$$\langle 00|\,\sigma_x \otimes \sigma_z|00\rangle + \langle 00|\,\sigma_x \otimes \sigma_z|11\rangle + \langle 11|\sigma_x \otimes \sigma_z\,|00\rangle +$$
$$\langle 11|\,\sigma_x \otimes \sigma_z\,|11\rangle$$
$$= ¼\,(-1)(-1) + ¼\,(-1)(-1) + ¼\,(1)(-1) + ¼\,(1)(1) = 0$$

در حالت کلی نتیجه می‌گیریم که اگر حالت بدون نویز را درنظر بگیریم، با توجه به ذرات ورودی همواره خروجی‌های همبسته و نا همبسته با احتمالات زیر بدست خواهند آورد:

$$\begin{cases} P(ab|00) = P(ab|11) = \frac{1}{2} & \text{اگر a=b} \\ P(ab|01) = P(ab|10) = \frac{1}{4} & \text{برای بقیهb و aها} \end{cases} \qquad (۶-۴)$$

بنابراین آلیس و باب نتیجه می‌گیرند که با این حالت ماکزیمم بالا و این پایه‌های اندازه‌گیری آنها می‌توانند از این اطلاعات استفاده کنند و یک کلید سّری را خلق کنند[۲۸].

در طرح پروتکل مستقل از دستگاه، همانطور که از قبل گفتیم؛ آلیس و باب هیچ فرضی نه روی پایه های اندازه‌گیری و نه هیچ فرضی هم روی حالت‌ها و بعد فضای هیلبرت می‌گذارند. حال برای اینکار یک حالت جدایی پذیر را انتخاب می‌کنیم و ادعا می‌کنیم که همین نتایج را ایجاد می‌کنند، در اینصورت موضوع را برای حالتی که پایه‌های یکسان دارند و ذرات در فضای $\mathbb{C}^۴\otimes\mathbb{C}^۴$ قرار داشته باشند را بررسی خواهیم کرد، پس حالت سیستم اینگونه است:

$$\rho_{AB} = ¼ \sum_{z_0, z_1=0}^{1} (\,|z_0\, z_1\rangle\langle z_0\, z_1|\,)_A \otimes (\,|z_0\, z_1\rangle\,\langle z_0\, z_1|\,)_B \rightarrow$$

$$\rho_{AB} = ¼(|00\rangle\langle 00|_A \otimes |00\rangle\langle 00|_B) + (|01\rangle\langle 01|_A \otimes |01\rangle\langle 01|_B) + (|10\rangle\langle 10|_B) +$$
$$(|11\rangle\langle 11|_A \otimes |11\rangle\langle 11|_B) \qquad (۷-۴)$$

همچنان روابط (۴-۵) برای این حالت صادق خواهد بود، در صورتیکه فرض کنیم که آلیس اندازه-گیری انجام دهد، یعنی $\sigma_z \otimes I$ برای زمینه‌ی[۱] ۰ و باب اندازه‌گیری انجام دهد یعنی $I \otimes \sigma_z$ برای زمینه‌ی ۱، بدین صورت:

$$\begin{cases} 0 \to \sigma_z \otimes I \\ 1 \to I \otimes \sigma_z \end{cases}$$

همچنین با انتخاب ذرات ورودی و حالت جدایی پذیر ۴ حالته‌ی (۴-۶)، سیستم کاملاً همبسته را بازنویسی می‌کنیم:

$$\langle \Psi | \sigma_z \otimes \sigma_z | \Psi \rangle = tr[\rho_{AB}(\sigma_z \otimes I) \otimes (\sigma_z \otimes I)] =$$

$$\tfrac{1}{4}\, \mathrm{tr}\Big[\sum_{z_0, z_1=0}^{1} (|z_0 z_1\rangle\langle z_0 z_1|)_A \otimes (|z_0 z_1\rangle\langle z_0 z_1|)_B (\sigma_z \otimes I) \otimes (\sigma_z \otimes I)\Big]$$

$$= \tfrac{1}{4} \sum_{z_0, z_1=0}^{1} tr[|z_0 z_1\rangle\langle z_0 z_1|_A \otimes (|z_0 z_1\rangle\langle z_0 z_1|_B (\sigma_z \otimes I) \otimes (\sigma_z \otimes I)]$$

$$= \tfrac{1}{4} \sum_{z_0, z_1=0}^{1} tr[|z_0 z_1\rangle\langle z_0 z_1| (\sigma_z \otimes I) \otimes |z_0 z_1\rangle\langle z_0 z_1| (\sigma_z \otimes I)]$$

$$= \tfrac{1}{4} \sum_{z_0, z_1=0}^{1} \mathrm{tr}[|z_0 z_1\rangle\langle z_0 z_1| (\sigma_z \otimes I)]\, \mathrm{tr}[|z_0 z_1\rangle\langle z_0 z_1| (\sigma_z \otimes I)]$$

$$= \tfrac{1}{4} \sum_{z_0, z_1=0}^{1} \langle z_0 z_1| \sigma_z \otimes I |z_0 z_1\rangle\langle z_0 z_1| \sigma_z \otimes I |z_0 z_1\rangle$$

$$= \tfrac{1}{4} \sum_{z_0, z_1=0}^{1} \langle z_0 |\sigma_z| z_0 \rangle^2 \langle z_1 |\sigma_z| z_1 \rangle^2 = 1$$

و برای سیستم کاملاً غیر همبسته و با توجه به محاسبات پیشین:

$$\langle \Psi | \sigma_z \otimes \sigma_x | \Psi \rangle = 0 \qquad (۴-۸)$$

[۱] .setting

همین عملیات را برای اندازه‌گیری باب نیز انجام می‌دهیم که دقیقاً همان نتایج پیشین حاصل می-شود. لذا ما از این حالت جدایی پذیر و از پایه‌های اندازه‌گیری یکسان در فضای متفاوت استفاده کردیم برای اینکه نشان دهیم سیستم همچنان بطور کاملاً همبسته می‌باشد که این نقطه ضعف پروتکل‌های توزیع کلید کوانتومی معمولی است. یعنی در این حالت اگر ایو سیستم را دستکاری کند، حضور ایو برای آلیس و باب غیر قابل تشخیص است.

❖ قبلاً در غیاب ناخالصی این حالت را ایجاد کردیم ولی حال می‌خواهیم درحضور ایو که اطلاع کاملی از حالت‌های موضعی آلیس و باب دارد، تمام این نتایج را بدست آوریم:

مثلاً، آلیس و باب این حالت سه تایی را باهم به اشتراک بگذارند:

$$\rho_{ABE} = ¼ \sum_{x,z=0}^{1} (|z_0\ z_1\rangle\langle z_0\ z_1|)_A \otimes (|z_0\ z_1\rangle\langle z_0\ z_1|)_B \otimes (|z_0\ z_1\rangle\langle z_0\ z_1|)_E$$

(۹-۴)

در نتیجه ایمنی کلید از روابط زیر حاصل می‌شود:

$$\sum_e \mathrm{P}(a\mathrm{be}|\mathrm{xyE}) \coloneqq \mathrm{P}(a\mathrm{b}|\mathrm{xy})\mathrm{P}((e|\mathrm{E})$$

$$\mathrm{P}(a\mathrm{b}|\mathrm{xy}) = \sum_e P_e\, P(a\mathrm{b}|\mathrm{xy})$$

(۱۰-۴)

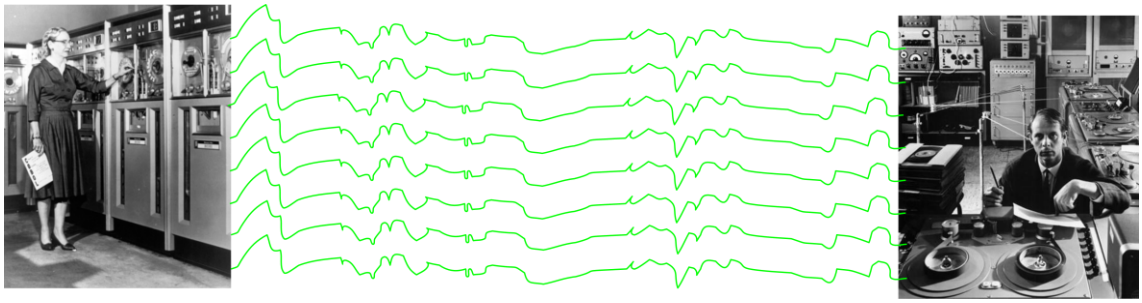
با توجه به رابطه‌ی (۴-۱۰) خروجی‌های(نتایج) دستگاه‌های آلیس و باب که از طریق ناموضعیت همبسته هستند، با ایو به اشتراک گذاشته می‌شوند. با وجود این همبستگی، آلیس و باب نامساوی CHSH که مثالی از نامساوی بل است را نقض می‌کنند. بنابراین می‌توان کلید ایمن را بوجود آورد.

نقض نامساوی بل یک نیاز ضروری برای پروتکل مستقل از دستگاه QKD است که این شرط نقض نامساوی بل توسط BB۸۴ ارضاء نخواهد شد.

نتیجه می‌گیریم که ناموضعیت – بنا به اصل فیزیک - شرط لازم برای اثبات ایمنی بیشتر تمام پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه می‌باشد که امنیت براساس آن پایه‌گذاری شده است.

۴-۴ ساختار کلی پروتکل مستقل از دستگاه

در این قسمت خلاصه‌ی نتایج ساختار کلی پروتکل مستقل از دستگاه را بیان می‌کنیم[۳۵]. در مدل کلی پروتکل توزیع کلید کوانتومی مستقل از دستگاه DIQKD، همانطور که در شکل زیر نمایان است، N جفت سیستم بین آلیس و باب توزیع می‌شود



تصویر ۴-۳ : ساختار کلی پروتکل مستقل از دستگاه

و همچنین دستگاه‌های کوانتومی باید حافظه کوانتومی داشته باشند. بطوریکه وقتی حالت iام سیستم را اندازه‌گیری می‌کنیم، حالت سیستم بعد از اندازه‌گیری شامل اطلاعات کلاسیکی در مورد اندازه‌گیری ورودی‌ها و خروجی‌ها در این مرحله i ام، به دور بعدی i+1 ام منتقل می‌شود.

اگر ρ_{AB}^{i} بیان کننده حالت سیستم قبل از اندازه‌گیری مرحله i باشد، حالت غیر نرمالیزه‌ای که به دور i+1 منتقل می‌شود اینگونه خواهد بود:

$$\tilde{A}_i^{\dagger}(a_i|x_i)\,\tilde{B}_i^{\dagger}(b_i|y_i)\,\rho_{AB}^{i}\;\tilde{A}_i(a_i|x_i)\,\tilde{B}_i(b_i|y_i) \qquad (۱۱-۴)$$

$\widetilde{A}_i(a\,|x\,)$ و $\widetilde{B}_i(b\,|y\,)$ اپراتورهای تعمیم یافته هستند که اندازه‌گیری‌های آلیس و باب را توصیف می‌کنند، اپراتورهای فوق بیانگر این است که وقتی در مرحله‌ی iام اندازه‌گیری سیستم هستیم، آلیس مقدار x را اندازه‌گیری کرده و نتیجه‌ی a را بدست می‌آورد و باب مقدار y را اندازه‌گیری کرده و نتیجه‌ی b را بدست می‌آورد، هچنین این اپراتورهای تعمیم یافته شرط زیر را برآورده می‌کنند:

$$\sum_a \widetilde{A}_i(a\,|x\,)\ \widetilde{A}_i^{\dagger}(a\,|x\,) = \sum_b \widetilde{B}_i(b\,|y\,)\ \widetilde{B}_i^{\dagger}(b\,|y\,) = I$$

(۱۲-۴)

ل احتمال $P(ab|xy)$ اینگونه بیان می‌شود:

$$P(ab|xy) = tr\,[\prod_{i=1}^{N} \widetilde{A}_i^{\dagger}(a_i|x_i)\ \widetilde{B}_i^{\dagger}(b_i|y_i)\ \rho_{AB}^{i} \prod_{i=1}^{N} \widetilde{A}_i(a_i|x_i)\ \widetilde{B}_i(b_i|y_i)]$$

(۱۳-۴)

همچنان می‌دانیم که ρ_{AB} حالت اولیه را در شروع پروتکل بیان می‌کند.

اگر از اثر حافظه منتقل شده به دورهای مختلف چشم پوشی کنیم، یعنی اینکه دستگاه‌ها بستگی به هیچ حالت کوانتومی ذخیره شده در حافظه داخلی نداشته باشند و نتایج اندازه‌گیری بدست آمده در دور قبلی ربطی به نتایج اندازه‌گیری بدست آمده در دور بعدی نداشته باشند:

$$A_i(a|x) = \widetilde{A}_i(a\,|x\,)\ \widetilde{A}_i^{\dagger}(a\,|x\,)$$
$$B_i(b|y) = \widetilde{B}_i(b\,|y\,)\ \widetilde{B}_i^{\dagger}(b\,|y\,) \qquad (۱۴-۴)$$

در تئوری کوانتومی اپراتورهای اندازه‌گیری با همدیگربرهم‌کنشی ندارند و بطور مستقل از هم عمل می‌کنند. در ضمن این اپراتورهای اندازه‌گیری در رابطه جابجایی زیر را صدق می‌کنند :

$$[A_i(a|x)\,, B_j(b|y)] = 0 \qquad (۱۵-۴)$$

رابطه (۴-۱۵)، رابطه جابجایی بین اپراتورهای دستگاه اندازه‌گیری آلیس $A_i(a|x)$ و اپراتورهای دستگاه اندازه‌گیری باب $B_i(b|y)$ را توصیف می‌کند. این رابطه الزاماً بخشی از هر مدل DIQKD است که ایمنی بدون آنها تضمین نمی‌شود.

همچنین این پروتکل باید رابطه جابجا پذیر زیر را ارضاء کند:

$$[\mathrm{A_i}(a|\mathrm{x})\ ,\ \mathrm{A_j}(a'|\mathrm{x}')] = [\mathrm{B_i}(\mathrm{b}|\mathrm{y})\ ,\ \mathrm{B_j}(\mathrm{b}'|\mathrm{y}')] = 0 \qquad (۱۶\text{-}۴)$$

رابطه (۴-۱۶)، معرف جابجایی بین اپراتورهای $\mathrm{A_i}(a_i|\mathrm{x_i})$ که درون دستگاه آلیس می‌باشد و رابطه جابجایی بین اپراتورهای $B_i(b_i|y_i)$ که درون دستگاه باب می‌باشد، خواهد بود.

که $\mathrm{A_i}(a_i|\mathrm{x_i})$ اپراتوری است که اندازه‌گیری آلیس روی سیستم iام خودش را توصیف می‌کند، این در صورتی است که ورودی x_i باشد و بطور مشابه $B_i(b_i|y_i)$ اپراتوری است که اندازه‌گیری باب را توصیف می‌کند. در ضمن $\mathrm{A_i}$ها این شرط را برآورده می‌کنند:

$$\sum_{a_i} \mathrm{A_i}(a_i|\mathrm{x_i}) = 1\ ,\ \mathrm{A_i}(a_i|\mathrm{x_i}) \geq 0 \qquad (۱۷\text{-}۴)$$

با تمام توضیحات فوق داریم:

$$\mathrm{P}(a\mathrm{b}|\mathrm{xy}) = \mathrm{tr}[\rho_{AB} \prod_{i=1}^{N} A_i(a_i|x_i)\ B_i(b_i|y_i)] \qquad (۱۸\text{-}۴)$$

۴-۵ ایمنی پروتکل مستقل از دستگاه با استفاده از نقض نامساوی CHSH

در پروتکلی که ما در اینجا تحلیل می‌کنیم، پروتکل مستقل از دستگاه با طرح استانداردQKD متفاوت و ایمنی قوی‌تری نسبت به QKD استاندارد دارد، مشروط بر آنکه از نقض نامساوی بل استفاده شود. دراین تحلیل برای بررسی اثرنقض نامساوی بل از نامساویCHSH[۱] استفاده می‌کنیم، چونکه اطلاعات ایو را از طریق نقض این نامساوی محدود می‌شود [۳۳]. قابل ذکر است که نامساوی فوق نمونه‌ای از نامساوی بل است. طرز کار این نامساوی اینطور است که:

[۱] . Clauser, Horne, Shimony, Holt

آلیس و باب یک کانال کوانتومی (کانال کوانتومی شامل منبعی است که جفت ذرات را در حالت درهم تنیده ρ_{AB} منتشر می‌کند) را با هم به اشتراک می‌گذارند. آلیس اپراتورهای A_0,A_1,A_2 را از زیرمجموعه‌ی ذراتش انتخاب کرده و همینطور باب اپراتورهای B_1, B_2 را انتخاب می‌کند و بعد آن‌ها را در پایه‌های دلخواه اندازه‌گیری می‌کنند. تمام اندازه‌گیری‌ها خروجی‌های دوتایی دارند یعنی $a_i, b_j \in \{+1, -1\}$.

کلید خام از جفت ذرات $\{A_0،B_1\}$ بدست می‌آیند. نرخ خطای بیت کوانتومی (QBER) اینگونه تعریف می‌شود Q=P($a\neq b$|01). پارامتری که مقدار همبستگی بین سیستم‌های آلیس و باب را مشخص می‌کند به مقدار تصحیح و خطای کلاسیکی نیاز دارد[۳۰].

همچنین ما فرض کرده‌ایم که اندازه‌گیری‌ها بطور تصادفی هستند، یعنی $\langle a_i \rangle = \langle b_j \rangle = 0$ که برای همه i و j ها برقرار می‌باشد.

به عنوان مثال، آلیس و باب ذراتشان را در پایه‌های تصادفی زیر اندازه‌گیری می‌کنند:

Alice	Bob
$A_0 = \sigma_z$	$B_1 = \sigma_z$
$A_1 = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x)$	$B_2 = \sigma_x$
$A_2 = \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x)$	

A_1،A_2،B_1،B_2 زیر مجموعه‌هایی از ذراتی هستند که از آنها برای تخمین نامساوی CHSH استفاده می‌شوند.

$$S = \langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle \qquad (۱۹-۴)$$

البته توجه می‌کنیم که $\langle a_i, b_j \rangle$ اینگونه تعریف می‌شود:

$$\langle a_i, b_j \rangle = P(a = b|ij) - P(a \neq b|ij) \qquad (۲۰-۴)$$

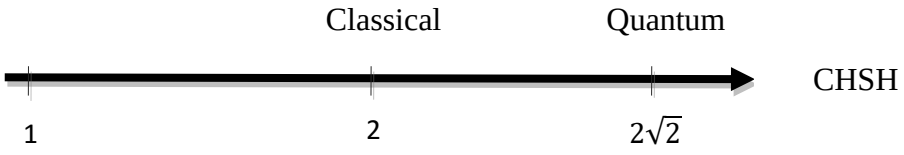
لذا داریم:

$$\langle a_1, \mathrm{b}_1 \rangle = P(a = b|11) - P(a \neq b|11)$$
$$\langle a_1, \mathrm{b}_2 \rangle = P(a = b|12) - P(a \neq b|12)$$
$$\langle a_2, \mathrm{b}_1 \rangle = P(a = b|21) - P(a \neq b|21)$$
$$\langle a_2, \mathrm{b}_2 \rangle = P(a = b|22) - P(a \neq b|22) \qquad (۲۱-۴)$$

اگر این نامساوی را برای حالت درهم‌تنیده ماکزیمم بکار ببریم:

$$|\varphi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \qquad (۲۲-۴)$$

بدست آمدن مقدار $S = ۲\sqrt{۲}$، منجر به نقض نامساوی می‌شود. با توجه به شکل زیر، در حالت کلاسیکی مقدار S، $۲ \leq S \leq -۲$ است، یعنی در حالت خالص[۱] نامساوی CHSH همواره برقرار است. ولی اگر مقدار S از این مقدار ۲ بیشتر باشد، در اینصورت نامساوی نقض خواهد شد و حالت سیستم کوانتومی می‌شود. یعنی ایمنی در فیزیک کوانتومی بیشتر از کلاسیک تضمین خواهد شد.



تصویر ۴-۴: ایمنی پروتکل مستقل از دستگاه با استفاده از نقض CHSH

[۱] . pure حالت خالص حالتی است که ذرات با یکدیگر درهم‌تنیدگی ندارند.

همانطور که قبلاً عنوان شد، در این حالت به بررسی سیستمی می‌پردازیم که این پروتکل نویز دارد. بنابراین اثر نویز، حالت کوانتومی (۴-۲۲) تبدیل به حالت زیر خواهد شد که به حالت ورنر[۱] مشهور است. حال داریم:

$$\rho_{AB} = p|\varphi^+\rangle\langle\varphi^+| + (1-p)\frac{I}{4} \rightarrow \qquad (۴-۲۳)$$

$$\rho_{AB} = \frac{p}{2}(\,|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\,) + \frac{1-p}{4}(\,|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|\,)$$

حال برای سادگی کار، رابطه (۴-۲۱) و (۴-۲۳) را بصورت ضرب ماتریسی اثبات می‌کنیم:

$$\rho_{AB} = \frac{p}{2}\left(\binom{0}{1}\binom{0}{1}\otimes(0 \quad 1)(0 \quad 1) + \binom{0}{1}\binom{0}{1}\otimes(1 \quad 0)(1 \quad 0) + \binom{1}{0}\binom{1}{0}\otimes(0 \quad 1)(0 \quad 1) + \binom{1}{0}\binom{1}{0}\otimes(1 \quad 0)(1 \quad 0)\right) + (1-p)\frac{I}{4}$$

$$= \frac{p}{2}\left[\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\otimes\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\otimes\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} + \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\otimes\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\right] + (1-p)\frac{I}{4}$$

$$= \frac{p}{2}\left[\begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} + \begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix} + \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}\right] + \frac{1-p}{4}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} = \frac{p}{2}\begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0\end{pmatrix} + \frac{1-p}{4}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$$

$$\langle a_1 b_1\rangle = tr(\rho A_1 B_1)$$

$$A_1 = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x) \rightarrow A_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

[۱]. Wernner

$$A_1B_1 = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & -1 & 0 & -1\\ 1 & 0 & -1 & 0\\ 0 & -1 & 0 & 1\end{pmatrix}\right.$$

$$tr(\rho A1\ B1) = \mathrm{tr}\left[\frac{p}{2\sqrt{2}}\begin{pmatrix}1 & -1 & 1 & 1\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0\\ 1 & -1 & 1 & 1\end{pmatrix} + \frac{1-p}{4\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & -1 & 0 & -1\\ 1 & 0 & -1 & 0\\ 0 & -1 & 0 & 1\end{pmatrix}\right] = \frac{p\sqrt{2}}{2}$$

$$\langle a_2, b_2\rangle = tr(\rho A_2\, B_2)$$

$$A_2\, B_2 = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1 & -1\\ -1 & -1\end{pmatrix}\otimes\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\\ 0 & -1 & 0 & -1\\ -1 & 0 & -1 & 0\end{pmatrix}\right.$$

$$tr(\rho A_2\, B_2) = \mathrm{tr}\left[\frac{p}{2\sqrt{2}}\begin{pmatrix}-1 & 1 & -1 & -1\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ -1 & 1 & -1 & -1\end{pmatrix} + \frac{1-p}{4\sqrt{2}}\begin{pmatrix}0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\\ 0 & -1 & 0 & -1\\ -1 & 0 & -1 & 0\end{pmatrix}\right] = \frac{-p\sqrt{2}}{2}$$

بنابراین بدست می‌آید:

$$\langle a_1 b_1\rangle = \langle a_1 b_2\rangle = \langle a_2 b_1\rangle = -\langle a_2 b_2\rangle = \frac{p\sqrt{2}}{4} \qquad (۲۴-۴)$$

$$\rightarrow S = 2\sqrt{2}P \qquad (۲۵-۴)$$

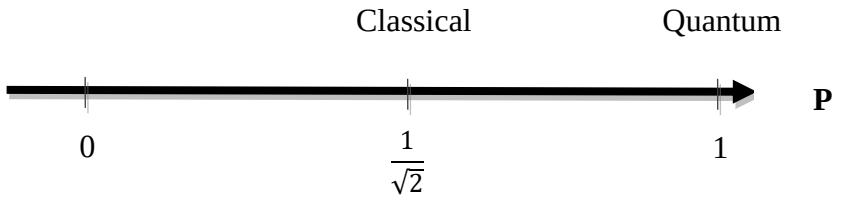
$$Q = P(a \neq b|01) \rightarrow Q = \frac{1-p}{2} \qquad (۲۶-۴)$$

رابطه بین P و Q اینگونه بدست می‌آید:

$$Q - \frac{1}{2} = -\frac{P}{2} \rightarrow -2Q + 1 = P \rightarrow S = 2\sqrt{2}(1-2Q) \qquad (۲۷-۴)$$

باید بدانیم Q,S دو پارامتری هستند که اطلاعات ایو را محدود می‌کنند، البته از قبل هیچ ارتباطی بین S و مقدار Q وجود نداشت.

همبستگی فقط با این نتایج توصیف شده تضمین می‌شود. در دیدگاه کلاسیکی، در صورتیکه اطلاعات همبسته باشند، $p \leq \frac{1}{\sqrt{2}}$ خواهد بود و نامساوی CHSH با بیشترین مقدار ۲ نقض می‌شود، یعنی $S \leq 2$ خواهد بود. اگر مقدار S از این مقدار کلاسیکی کمتر باشد، در اینصورت ایمنی DIQKD برقرار نخواهد بود. همانند شکل زیر:



تصویر ۴-۵ : ایمنی پروتکل مستقل از دستگاه با استفاده از نقض CHSH

در دیدگاه کوانتومی ماکزیمم مقدار نقض ، وقتی که p=1 باشد، $S = 2\sqrt{2}$ خواهد بود، که در صورت ظاهر شدن این مقدار ذکر شده، نامساوی نقض خواهد شد. یعنی‌اینکه اطلاعات ایو در مورد دستگاه‌های کوانتومی آلیس و باب صفر خواهد بود. نقض نامساوی CHSH زمانی برقرار است که آلیس و باب دو کیوبیت خود را در حالت در هم‌تنیده ماکزیمم اندازه‌گیری کنند، در اینصورت امنیت پروتکل DIQKD برقرار است و این ایمنی کمترین مرزی روی اطلاعات ایو بصورت تابعی از مقدار CHSH می‌گذارد. لذا نتیجه‌ی کلی این است که نقض بل برای خروجی‌های تصادفی a و b بکار می-رود و ایو هیچ اطلاعاتی در مورد a و b نخواهد داشت.

۴-۶ حملات کلی استراق سمع‌کننده

در پروتکل‌های DIQKD، نه تنها فرض‌شده‌است که استراق سمع‌کننده(ایو) منبع را کنترل می-کند، بلکه دستگاه‌های اندازه‌گیری مربوط به سیستم آلیس و باب را نیز دستکاری می‌کند. با توجه به این مسئله، ایمنی پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه همچنان در برابر تهاجمات

استراق سمع کننده معتبر است. در این پروتکل‌های مستقل از دستگاه فرض بر اینست که؛ تنها ابزاری که در اختیار آلیس و باب است، که اطلاعات ایو را محدود کند، فقط ارتباط بین ورودی‌ها و خروجی-هایی است که ایو از آن‌ها اطلاعی ندارد. بنابراین هیچ فرض دیگری روی دستگاه‌های اندازه‌گیری کوانتومی و سیستم هایی که برای تولید آنها استفاده شده باشد، را درنظرنمی‌گیریم. با توجه به دسترسی بیش از حد ایو به سیستم‌های آلیس و باب، می‌خواهیم ثابت کنیم که این پروتکل‌ها همچنان ایمن هستند.

در حالت کاملاً کلی: اطلاعات قابل دسترسی ایو با سیستم کوانتومی‌ای معرفی می‌شود که با سیستم آلیس و باب همبسته است. یعنی اینکه ایو حالتش را با حالت‌های آلیس و باب به اشتراک می‌گذارد. بنابراین حالت $|\psi\rangle_{\mathrm{ABE}}$ (در حالت کوانتومی با ρ_{ABE} نشان می‌دهیم)، حالت مشترک سه کاربر آلیس و باب و ایو در فضای هیلبرت $H_A^{\otimes n}\otimes H_B^{\otimes n}\otimes H_E$ خواهند بود، که n تعداد بیت‌های کلید خام است. البته باید بدانیم که فضای هیلبرت d بعدی آلیس و باب -که اینگونه نمایش داده‌می‌شود، $\mathrm{H_A}=\mathrm{H_B}=\mathbb{C}^d$ - برای دو کاربر مجاز به‌نام‌های آلیس و باب نامشخص است و فقط ایو از آن اطلاع دارد (همانطور که پیش از این اشاره کردیم، ایو ذرات d بعدی را برای آلیس و باب توزیع کرده‌است و آلیس و باب از این رویداد هیچ آگاهی‌ای ندارند.چون: $\mathrm{tr}_{\varepsilon}\rho_{\mathrm{ABE}} = \rho_{\mathrm{AB}}$). بنابراین در این نوع پروتکل‌ها استراق سمع کننده حملات مختلفی را بکار می‌برد و ما حملات کلی را به چند طریق محدود می‌کنیم که دو نمونه را تعریف خواهیم کرد:

الف- حملات فردی[۱]: یکی از این حملات ایو، حملات فردی است. در این مورد از حملات فرض شده‌است که استراق سمع کننده اطلاعاتی را در مورد هر بیت از رشته کلید بدست می‌آورد و بطور مستقل به سیستم‌های آلیس و باب حمله می‌کند[۳۴].

۱. individual attacks

در این روش: ایو حالتی از سه ذره‌ی آلیس، باب و خودش را تهیه می‌کند. احتمال اندازه‌گیری $P(ab|xyz)$ خواهد بود که z نشان دهنده‌ی احتمال اندازه‌گیری توسط ایو روی سیستم خودش است و e نتیجه‌ی خروجی است. بنابراین

$$\sum_{e} P(abe|xyz) := P(ab|xy)$$

$$P(ab|xy) = \sum_{e} P_e \, P_e(ab|xy)$$

(۲۸-۴)

اطلاعات ایو با متغیر e مشخص می‌شود.

ب- حملات دسته جمعی[۱]: در نوع حملات که متفاوت با حملات فردی است ایمنی همچنان تضمین خواهد شد که توضیح مختصری در مورد آن خواهیم داد.

۴-۶-۱ حملات دسته جمعی استراق سمع کننده

حملات به گونه‌ای است که ایو بطور مستقل و یکسان، در هر دور از پروتکل به هر یک از دستگاه-های آلیس و باب حمله می‌کند و بطور همبسته در هر زمان روی این سیستم‌هایی که در اختیارش قرار گرفته است، عمل می‌کند. بنابراین ایمنی در حملات دسته جمعی به اینصورت است که ایو قادر نخواهد بود که اطلاعات را ذخیره کند.

فرض می‌کنیم که اگر یک رشته‌ی n بیتی داشته‌باشیم، در نتیجه حالت کلی سیستم که توسط سه کاربر مشترک می‌شود، اینگونه خواهد بود: $|\psi_{ABE}\rangle = |\psi_{ABE}\rangle^{\otimes n}$

حالت اولیه ρ_{ABE} بدین شکل است:

$$\rho_{ABE} = \sum_{x \in X} P(x) \, |x\rangle\langle x|_A \otimes \rho_{BE}$$

(۲۹-۴)

۱. collective attacks

همچنین اندازه‌گیری‌ها فقط تابعی از ورودی‌ها هستند. به عنوان مثال ورودی متعلق به آلیس $M_k = M(A_{jk})$ است. فرض کرده‌ایم که دستگاه‌ها بدون حافظه هستند و همچنین فرض شده‌است که ایو بطور یکسان و مستقل در هر دور از پروتکل به سیستم آلیس حمله می‌کند. بنابراین اندازه-گیری $M(A_j)$ بصورت A_j خواهد بود.

با توجه به محدود کردن استراق سمع کننده به حملات دسته جمعی نرخ کلید بدست می‌آید و ایمنی کامل را ارائه خواهد داد که محاسبه ایمنی نرخ کلید در حیطه این رساله نمی‌باشد[۳۶,۲۸].

۴-۶ نتیجه‌گیری

در پروتکل رایج و متداول توزیع کلید کوانتومی(QKD)، فرض شده‌است که آلیس و باب پایه-هایشان را از بهترین روش ممکن تنظیم کرده‌اند ولی دستگاه‌های کوانتومی در پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه(DIQKD) قابل اطمینان نیستند. در این نوع پروتکل‌ها آلیس و باب فقط به آشکارسازهایشان که اعداد تصادفی را بوجود می‌آورند، اطمینان دارند، یعنی اینکه ایو به همه اطلاعات دسترسی دارد، تنها چیزی که از آن اطلاع ندارد فقط ارتباط بین ورودی و خروجی‌های دستگاه‌های آلیس و باب است و همچنین فرض شده‌است که ایو روی سیستم‌های آلیس و باب بطور یکسان و مستقل حمله دسته جمعی انجام می‌دهد، با این حال ایمنی این پروتکل بسیار زیاد است. در حقیقت شکل کلی پروتکل‌های مستقل از دستگاه بگونه‌ای است که فرضیات را کاهش می‌دهد و اینکه دستگاه‌های کوانتومی نامطمئن هستند. در این نوع پروتکل‌ها ، ایو نه تنها منبع را کنترل می کند بلکه دستگاه‌های اندازه‌گیری آلیس و باب را هم هک می‌کند بطوریکه دستگاه‌های کوانتومی نا مطمئن خواهند شد. ما می‌خواهیم با ایو که محدود به قوانین فیزیک کوانتومی است مقابله کنیم.

هدف پروتکل‌های توزیع کلید کوانتومی مستقل از دستگاه، بوجود آوردن کلید سری بین دو کاربر است. ایمنی این پروتکل به احتمال اندازه‌گیری‌ها بستگی ندارد(احتمال اینکه آلیس چه اندازه‌گیری‌ای

انجام دهد و باب چه نتایجی را بدست آورد، به یکدیگر وابسته نیست). آلیس و باب از پایه‌های اندازه-گیری تصادفی استفاده می‌کنند و نتایجی را بوجود می‌آورند که برای استراق سمع کننده نامشخص خواهد بود. این نتایجِ اندازه‌گیری بطور محرمانه نگه‌داشته شده و کلید خام را تشکیل می‌دهند.

علاوه بر این، باید در نظر داشت که فرض ما بر آنست که دستگاه‌های کوانتومی هیچ حافظه داخلی ندارند یعنی اینکه حالت سیستم در مرحله j ام، هیچ اطلاعاتی (نه کلاسیکی و نه اطلاعات کوانتومی) را از مرحله j-1ام در خود ذخیره نمی‌کند.

همچنین ما در این رساله نشان داده‌ایم که اگر در این نوع پروتکل‌ها سیستم‌های کوانتومی، نامساوی بل را نقض کنند در این صورت ایمنی قویتری نسبت به طرح استاندارد(QKD) خواهد داشت. نقض نامساوی بل منجر به این نتیجه شده‌است که تمام اطلاعات در مورد خروجیِ کاربر اولی، باید برای کاربر دوم مشخص شده‌باشد. البته باید یادآوری کنیم که تمام آزمایشات تجربی بل که تاکنون انجام شده‌است، روی ذرات درهم‌تنیده صورت گرفته‌است.

۴-۷ پیشنهادات

کم کردن فرضیات کوانتومی برای ایمنی توزیع کلید کوانتومی مسئله‌ای است که توجه فیزیک-دانان را به خود جلب کرده‌است و با توجه به حداقل رساندن فرضیات، ایمنی نرخ کلید را بیشتر و بیشتر افزایش خواهند داد. بطوریکه اخیراً در مقاله‌ای نرخ کلید کوانتومی-یعنی تحمل آگاهی از نویز توسط استراق سمع کننده- را به ۴ برابر نرخ کلید کلاسیکی افزایش داده‌اند[۳۴]. بنابراین می‌توان پروتکل توزیع کلید کوانتومی مستقل را تعمیم داد و نتایج معقولی را بدست آورد که این ایده منجر به ایمنی بیشتر خواهد شد.

همچنین قبلاً بارها این مسئله مورد بررسی قرار گرفته بود که آلیس و باب هر کدام یک دستگاه اندازه‌گیری مختص به خود دارند. در آینده می‌توان با توجه به ساختار کلی پروتکل مستقل از دستگاه، N بیت را درنظرگرفت و اندازه‌گیری‌های آلیس و باب که از هم فاصله‌ی فضاگونه دارند، با N تا دستگاه انجام شود و در طی مدت اندازه‌گیری هیچ ارتباطی بین آنها رخ ندهد و در نهایت با توجه به حملات مختلف کلید خام بدست خواهد آمد[۳۵].

مراجع و کتاب نامه‌ها

[1] The Code book, Auther Simon Singh.

[2] Caezar Cipher History, page51 from “Secret code Brraker”.

[3] A.M.Turing.on computatable numbers.proc.Math.Soc.2,42:230 (1936).

[4] Solovay and v.s trassen.A fast Monte . F.Comput.6:84-85,(1976).

[5] D.Deutch. Quantum theory, and church-Turing principle & universal quantum computational . A,400.97.(1985).

[6] D.Deutch .Quantum computational net works.prac.R.Soc.Landon.A,425:73.(1989).

[7] P.W.Shor.Algoritms for quantum computation: discrete logarithms and factoring.In proceeding 35th Annual symposium on foundations of computer Science, IEEE press, Los Alamitos, CA,(1994).

[8] R.P.Feynman.Simulating physics with computers.Int.F.Theor.phys.21:4672(1992).

[9] W.K. Wootters and W.H. Zurek, Nature(London)299,802(1982).

[10] D.Dieks, phys. Leytt. 92A,271(1982).

[11] E.F. Galvao and L.Hardy, phys.Rev.A 62,1022301(2000).

[12] J.J. Sakurai. Modern Quantum Mechanics(1982).

[13] J. Perskill. Lecture notes for Ph 219.CS219(2001).

[14] Ch H. Bennet,phy. Rev.Lett.67,2881-2884(1992).

[15] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered, Phys. Rev. 47, no. 10, 777-780(1935).

[16] G. Auletta. Foundations and Interpretation of quantum mechanics. World Scientific, Singapore. New Jersey. London. Hong Kong(2001).

[17] J. S. Bell, On the Einstein Podolsky Rosen paradox, Physics 1, no. 3, 195-200(1964).

[18] A. Aspect, P. Grangier, and G. Roger, Experimental tests of realistic local theories via Bell's theorem, Phys. Rev. Lett. 47, no. 7, 460-463(1981).

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

[20] Wiesner. Proc IEEE int. Conference on computer, system and signal processing. SIGACT News 15,780(1983).

[21] V. Scarani, C. Kurtsiefer, arXiv: 0906.4547.

[22] Richard J. Hughes, Quantum Cryptography, PP. 8892. Quantum Computating and communication(1998).

[23] A. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67, no. 6, 661-663 (1991).

[۲۴] کریمی پور، درسنامه‌ی محاسبات کوانتومی، ۱۳۸۶

(http:/Sina.Sharif.edu/vahid/teaching QC.html)

[25] M. A. Nielson and I.L. Chuang, Quantum Computation and Quantum information, Cambridge university press, Cambridge (2000).

[26] C.E Shannon, A mathematical theory of communication, Bell System Technical Journal, (1948).

[27] R. Renner and R. Koenig, in Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Lecture Notes in Computer Science, edited by J. Kilian(Springer-Verlag, 2005), vol. 3378, pp. 407–425Brent Fultz and James Howe, *Transmission Electron Microscopy and Diffractometry of Materials*, Springer (2007).

[28] I. Devetak and A. Winter. Proc. R. Soc. A, 461:207, (2005).

[29] A. Acin, et al, Phys. Rev. Lett. 97, 120405, Device -Independent Quantum Key Distribution (2006).

[30] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, V. Scarani; New J. Phys. 11, 045021(2009).

[31] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani; Phys. Rev. Lett. 98, 230501 (2007).

[32] F. Xu, B. Qi, H.-K. Lo, arXiv:1005.2376.

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

[34] A. Acin, N. Gisin and Masanes L 2005 preprint quant. Ph/05010094(2005).

[35] L. Masanes, S. Piranio, A. Acin.arxiv: 1009.1567v1[quant-ph](2010).

[36] I. Csiszar, J. Kroner; IEEE Trans. Inf. Theory 24, 339 (1978).

Abstract:

One of the most important problem in quantum information that we faced, is information transfer as in secured. Therefore we introduce the protocol which as in usual Quantum Key Distribution protocols(QKD), the security relies on the lows of quantum physics and another thing is that no-information leakage from the legal parties labs. This scheme is named quantum key distribution protocol which is Device-Independent(DIQKD). The security proof is based on the minimal assumption rather than quantum key distribution schemes, it means that two parties would not only have no knowledge about the structure of their quantum devices but they would also distrust their measuring apparatuses or we don't assume that Alice and Bob's devices behave according to predetermined specifications, because the measuring devices may be modified by eavesdropper. We will show that the security of this kind of protocols follows from the combined facts that any Device – Independent protocol comparable to those of standard schemes is more secure, if it is based on the observation of a Bell inequality violation and In addition to this essential requirement, Eve is restricted by collective attack- in collective attack, where Eve is assumed to act independently and identically at each use of the devices. The aim of this protocol that we consider here, is distributing a secret key whose security relies on the laws of quantum physics, then in of the raw key satisfy this scheme we make an assumption on devices which any bits independence condition and don't influence each other, one could also defines space-like separated events and in consequence we use of this, to generate the secret key rate.

Shahrood University of Technology

Physics Department

Master science

In

Elementary Particle

Title:

Security in device-independent quantum key distribution protocols

By:

Toktam Kashani

Supervisor:

Dr. Hossein Movahedian

February 2012