
بسم الله الرحمن الرحیم

دانشکده فیزیک و مهندسی هسته‌ای

رشته فیزیک، گرایش ذرات بنیادی

پایان‌نامه کارشناسی ارشد

استفاده از درهم‌تنیدگی در ارتباط مستقیم کوانتومی و کاربرد آن در رمزنگاری کوانتومی

نگارنده: مریم نصیری

استاد راهنما

دکتر مصطفی عنابستانی

بهمن ۱۳۹۵

پیوست شماره ۲

دانشکده : فیزیک

گروه : ذرات بنیادی

پایان نامه کارشناسی ارشد آقای/ خانم مریم نصیری به شماره دانشجویی: ۹۳۱۷۴۹۴

تحت عنوان: استفاده ازدرهم تنیدگی درارتباط مستقیم کوانتومی وکاربرد آن دررمزنگاری کوانتومی

در تاریخ ۱۳۹۵/۱۱/۱۹ توسط کمیته تخصصی زیر جهت اخذ مدرک کارشناسی ارشد مورد ارزیابی و با درجه .....عالی..... مورد پذیرش قرار گرفت.

اساتید راهنما	امضاء	اساتید مشاور	امضاء
نام و نام خانوادگی :دکتر مصطفی عنابستانی		نام و نام خانوادگی :	
نام و نام خانوادگی :		نام و نام خانوادگی :	

اساتید داور	امضاء	نماینده تحصیلات تکمیلی	امضاء
نام و نام خانوادگی :دکتر کاظم بی‌تقصیرفدافن		نام و نام خانوادگی :دکتر مسلم سوهانی	
نام و نام خانوادگی :دکتر مرتضی رفیعی			
نام و نام خانوادگی :			
نام و نام خانوادگی :			

تقدیم به مهربان فرشتگانی که:
لحظات ناب باور بودن، لذت و غرور دانستن، جسارت خواستن، عظمت رسیدن و تمام تجربه‌های یکتا و زیبای زندگیم، مدیون حضور سبز آنهاست
تقدیم به خانواده عزیزم.

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

از استاد گرامیم جناب آقای دکتر عنابستانی بسیار سپاسگزارم چرا که بدون کمک‌ها و راهنمایی‌های ایشان تأمین این پایان‌نامه بسیار مشکل می‌نمود.

همچنین سپاسگزار و قدران همیشگی زحمات پدر و مادرم، آموزگارانی که برایم زندگی، بودن و انسانیت را معنا کردند از ابتدا تا ابد بوده و، هستم.

مریم نصیری

بهمن ۱۳۹۵

تعهد نامه

اینجانب **مریم نصیری** دانشجوی کارشناسی ارشد رشته **فیزیک فیزیک و مهندسی هسته‌ای** دانشگاه شاهرود، نویسنده پایان‌نامه با عنوان **استفاده از درهم‌تنیدگی در ارتباط مستقیم کوانتومی و کاربرد آن در رمزنگاری کوانتومی** ، تحت راهنمایی **مصطفی عنابستانی** متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش‌های دیگر پژوهش‌گران، به مرجع مورد استفاده استناد شده است.
- مطالب این پایان‌نامه، تا کنون توسط خود، یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ‌جا ارایه نشده است.
- حقوق معنوی این اثر، به دانشگاه صنعتی شاهرود تعلق دارد، و مقالات مستخرج با نام‌‌‌ دانشگاه صنعتی شاهرود‌‌‌ یا ‌‌‌Shahrood University of Technology ‌‌‌ به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به‌دست آوردن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند، در مقالات مستخرج از پایان‌نامه رعایت می‌گردد.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافت‌های آنها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته (یا استفاده شده است)، اصل رازداری و اصول اخلاق انسانی رعایت شده است.

مریم نصیری
بهمن ۱۳۹۵

مالکیت نتایج و حق نشر

- تمام حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه صنعتی شاهرود می‌باشد. این مطلب باید به نحو مقتضی، در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در این پایان‌نامه بدون ذکر منبع مجاز نمی‌باشد.

چکیده

توزیع یک کلید رمز کاملاً محرمانه بین دو کاربر قانونی که در فاصله‌ای از یکدیگر قرار دارند، مهم‌ترین هدف علم رمزنگاری است. در رمزنگاری کلاسیکی امنیت کلید رمز به سختی توابع ریاضی حاکم بر آن وابسته است. در حالی که در رمزنگاری کوانتومی یا به عبارتی توزیع کلید کوانتومی (QKD) این ایمنی به اصول بنیادین مکانیک کوانتومی وابسته است، که بر این اساس پروتکل‌های مختلفی برای توزیع کلید کوانتومی ارائه شده است. تقریباً تمام پروتکل‌های رمزنگاری کوانتومی بر اساس انتقال ذره حامل اطلاعات هستند، که از فرستنده به گیرنده منتقل می‌شود. در بررسی امنیت پروتکل‌ها معمولاً پس از اطمینان از امن بود کانال ارتباط کوانتومی، فرایند غربال داده‌ها به صورت حذف تعدادی از کیوبیت‌ها صورت می‌گیرد.

در سال ۲۰۰۳ بوستروم و فلبینگر یک ارتباط دو طرفه مستقیم کوانتومی را با توجه به مفهوم درهم‌تنیدگی یک جفت کیوبیت پیشنهاد دادند. از آنجایی که در پروتکل آن‌ها ارسال اطلاعات کوانتومی به صورت قطعی است، بنابراین کیوبیت‌ها دور ریخته نمی‌شوند و اطلاعات پس از انتقال رمزگشایی می‌شوند. در این پروتکل امنیت در مقابل حملات یک شنودکننده‌پنهان بواسطه‌ی مد کنترلی در ارتباط کوانتومی فراهم می‌شود.

در این پایان‌نامه، ابتدا مروری اجمالی بر مباحث مقدماتی استفاده شده در رمزنگاری خواهیم داشت. سپس در ادامه به توصیف نمایی کلی از توزیع کلید کوانتومی و چند پروتکل معروف توزیع کلید کوانتومی خواهیم پرداخت. در نهایت توضیحات کاملی در مورد پروتکل $Ping-Pong$ ارائه خواهیم داد و امنیت آن را در مورد حمله‌های مختلف بررسی خواهیم کرد.

کلمات کلیدی: رمزنگاری کلاسیکی، رمزنگاری کوانتومی، توزیع کلید کوانتومی ، درهم‌تنیدگی، کیوبیت

لیست مقالات مستخرج از پایان‌نامه

۱. مقاله اول: مصطفی عنابستانی، مریم نصیری ''توزیع کلید کوانتومی به روش حدس و غربال'' کنفرانس فیزیک ایران سال ۹۵(دانشگاه شیراز)

۲. مقاله دوم: مصطفی عنابستانی، مریم نصیری ''پایه‌های بهینه در پروتکل $BB84$'' کنفرانس فیزیک ریاضی ایران سال ۹۵(دانشگاه صنعتی قم)

فهرست مطالب

فهرست تصاویر

فصل ۱

رمزنگاری

۱.۱ مقدمه

رمزنگاری که از گذشته به منظور ارسال پیام‌ها یا اطلاعات محرمانه استفاده می‌شد دراصل دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز با استفاده از یک الگوریتم رمز است . دانشی که بدون آن کسی به جز شخص فرستنده و گیرنده پیام‌ها نتواند به محتویات آنها دسترسی داشته باشد، یعنی تنها اشخاصی که از کلید و الگوریتم رمز مطلع باشند قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشند و کسی که از یکی یا هر دوی آنها اطلاعات ندارد نتواند به اطلاعات دسترسی پیدا کند. در واقع می‌توان گفت که رمزنگاری علم کدها و رمزهاست. داستان استفاده از یک هنر قدیمی و جذاب برای حفاظت از اطلاعات محرمانه‌ای است که بین افراد مختلف مانند فرماندهان نظامی و جاسوسان و ... رد و بدل می‌شده و از هزاران سال پیش شروع شده و تاکنون مورد توجه بشر بوده است . به گونه‌ای که با ظهور و گسترش وسایل نوین ارتباطی که ویژگی بارز همه‌ی آنها سرعت و تنوع روابط است، دانش رمزنگاری وارد حوزه جدیدی از علوم به نام علوم رایانه شده است.

البته دانش رمزنگاری بر پایه‌ی مقدمات بسیاری از قبیل تئوری اطلاعات ، نظریه اعداد و آمار بنا شده است و امروزه به طور خاص در علم مخابرات مورد بررسی و استفاده قرار می‌گیرد. مخابره اطلاعات به شکل امن موضوع اصلی این علم بوده و همواره متخصصین این علم بدنبال بررسی و شناخت اصول و روش‌های انتقال یا ذخیره اطلاعات به صورت امن بوده و هستند، و در راستای این هدف متخصصین علم رمزنگاری برای ساختن طرح‌ها یا پروتکل‌هایی که بتوان به کمک آنها حتی در یک کانال ناامن (کانالی که در آن دشمن یا شنود کننده حضور دارد) نیز اطلاعات مهم را رد و بدل کرد، تلاش می‌کنند

[۱، ۲].

۲.۱ تاریخچه رمزنگاری

به مطالعات رمزنگاری Cryptography اطلاق می‌شود، که از واژه‌های یونانی Cryptos به معنی پنهان و $Graphan$ به معنی نوشتن تشکیل شده است. به علم ایجاد کدهای رمزنگاری و شکستن آنها به طور همزمان Cryptology و به فرآیند نوشتن پیام به صورت رمز شده به صورتی که تنها افراد مجاز قادر به رمزگشایی و خواندن آن باشند، Encryption گفته می‌شود [۳، ۴].

در گذشته رمزنگاری به شیوه‌های سنتی مانند استفاده از دود یا استفاده از سمبل‌ها به جای حروف و یا تغییر ترتیب حروف در متن مورد نظر و غیره صورت می‌گرفت. پس به طور طبیعی زمانی که پیام به مقصد می‌رسید، برای خوانده شدن نیاز به رمزگشایی داشت و از همین جا داستان جالب رمزنگاری آغاز می‌شود، و البته این داستان در عصر کنونی به شکل‌های جدیدتری همچنان ادامه دارد.

صدها و شاید هزاران سال پیش از رمزنگاری بیشتر در میدان‌های جنگ برای ارسال پیام به پشت جبهه استفاده می‌شد تا اگر جاسوسی به پیام دسترسی پیدا کرد اطلاعات مهم و حساس لو نرود. اگر چه در طول تاریخ ، رمزنگاری همواره جزئی از جنگ ، سیاست و حکومت داری بوده است ، اما امروزه کاربرد های رمزنگاری فراتر از علوم نظامی است و در موارد مختلفی از جمله تجارت الکترونیک [۱] کاربرد دارد [۵]. رمزنگاری و ابزارهای مربوط به آن در طی قرن‌ها رشد کردند و در الگوریتم‌های کامپیوتری و سیستم‌های مدرن امروزی به اوج خود رسیدند.

محافظت از ارتباطات همواره بخش حیاتی جنگ‌ها و نزاع‌های سیاسی محسوب می‌شود و به همین دلیل گسترش رمزنگاری مدرن تا حدود زیادی مدیون تحقیقاتی است که زیر فشار جنگ جهانی دوم برای شکستن کدهای رمزنگاری شده توسط ماشین انیگما [۲] انجام شده است.

۳.۱ مقدمات رمزنگاری

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی که برای محافظت از اطلاعاتی که بین فرماندهان نظامی و جاسوسان و ...ردوبدل می‌شده، مورد استفاده بوده است تا پیام‌های آنها محرمانه بماند.

رمزنگاری اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر آن به مقداری دانش ریاضیات نیاز است [۴].

- ✓ متن آشکار: پیام اصلی رمز نشده.
- ✓ متن رمز: پیام رمز شده.
- ✓ رمز: الگوریتم تبدیل متن آشکار به متن رمز.
- ✓ کلید: اطلاعاتی که در رمز مورد استفاده قرار می‌گیرد و فقط فرستنده و یا گیرنده پیام آن را می‌دانند.

[۱] Electronic business
[۲] Enigm Rotor

- ✓ رمزگذاری: تبدیل متن آشکار به متن رمز.
- ✓ رمزگشایی: استخراج متن آشکار از متن رمز.
- ✓ رمزنویسی: علم اصول روش‌های رمزگذاری.
- ✓ تحلیل رمز: علم اصول و روش‌های رمزگشایی متن رمز بدون اطلاع از کلید.
- ✓ رمزنگاری: علم حاصل از ترکیب رمزنویسی و تحلیل رمز.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها به عنوان استانداردها یا مقالات ریاضی منتشر شده‌اند.

کلید یک رشته از اعداد دودویی (صفر و یک) است که به خودی خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود، کلید است که باید مخفی نگه داشته شود، و کلید است که در مرحله پیاده‌سازی تغییر می‌کند. در رمزگشایی نیز از همان الگوریتم و کلید یا از الگوریتم و کلید متفاوتی استفاده می‌شود.

۴.۱ الگوریتم‌ها

طراحی الگوریتم‌های رمزنگاری مقوله‌ای برای متخصصان علم ریاضی است. طراحان سیستم‌هایی که در آنها از رمزنگاری استفاده می‌شود، باید از نقاط قوت و ضعف الگوریتم‌های موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم‌گیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون [۳] در اواخر دهه ۴۰ و اوایل دهه ۵۰ به شدت پیشرفت کرده است، اما کشف رمز نیز پابه‌پای رمزنگاری به پیش آمده است و الگوریتم‌های کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند.

به همین دلیل امروزه رمزنگاری مبتنی بر پنهان نگه‌داشتن الگوریتم رمز منسوخ شده است و در روش‌های جدید، فرض بر انتشار کامل اطلاعات الگوریتم رمزنگاری است و آنچه پنهان است فقط کلید رمز است. امنیت الگوریتم و پروتکل‌های رمزنگاری، متکی بر امنیت و پنهان ماندن کلید رمز است و جزئیات کامل این الگوریتم‌ها و پروتکل‌ها برای عموم منتشر می‌شود [۶، ۷].

برمبنای این تعریف رمزنگاری بر اساس ویژگی‌های کلید به دو دسته تقسیم می‌شود: رمزنگاری با کلید سری(متقارن) و رمزنگاری با کلید عمومی(نامتقارن).

۱.۴.۱ سیستم‌های کلید متقارن

رمزنگاری کلید متقارن یا تک کلیدی ، آن دسته از الگوریتم‌ها، پروتکل‌ها و سیستم‌های رمزنگاری است که در آن هر دو طرف ردوبدل کننده‌ی اطلاعات (که برای سادگی آنها را با نام‌های آلیس و باب می‌شناسیم) از یک کلید رمز یکسان برای عملیات رمزگذاری و رمزگشایی استفاده می‌کنند. در الگوریتم‌های رمزنگاری استاندارد شناخته می‌شود [۷]، فرستنده پیام یعنی آلیس آن را با استفاده از یک کلید رمزگذاری و گیرنده پیام یعنی باب آن را با استفاده از کپی همان کلید رمزگشایی می‌کند. در

[۳] Shannon

این قبیل سیستم‌ها یا کلیدهای رمزگذاری و رمزگشایی یکسان هستند و یا با رابطه‌ای بسیار ساده از یکدیگر قابل استخراج هستند، و در اصل رمزگذاری و رمزگشایی اطلاعات دو فرآیند معکوس یکدیگر هستند. این روش که اولین بار توسط گیلبرت ورنام [۴] در سال ۱۹۱۷ ارائه شد با عنوان روش رمزنگاری $One - time - pad$ شناخته شده است، و امنیت آن از لحاظ ریاضی توسط شانون اثبات شده و غیر قابل شکستن است. مراحل پروتکل ورنام به صورت زیر است:

۱ـ متن یا پیام اصلی به صورت رشته‌ای دودویی از ۰ و ۱ها نوشته می‌شود.

۲ـ کلید رمز یک رشته دودیی از ۰ و ۱ها با طولی برابر متن اصلی است که کاملاً تصادفی انتخاب می‌شود.

۳ـ با جمع کردن بیت‌های متن اصلی وکلید رمز در مد ۲، متن رمز شده بدست می‌آید.

اگر فرض کنیم که مجموعه‌ی P_i ها نشان دهنده‌ی متن اصلی و مجموعه‌ی K_i ها نشان دهنده‌ی کلید رمز باشند، آنگاه مجموعه‌ی C_i ها که نشان دهنده‌ی متن رمز شده است این گونه بدست می‌آید:

$$C_i = P_i \oplus K_i \tag{۱.۱}$$

که $i = ۱, ۲, ..., n$ و $\oplus$ ، نماد جمع در مبنای ۲ است.

به عنوان مثال فرض کنید که:

متن اصلی رمز شده توسط آلیس که آن را با P نشان می‌دهیم :

$$P = \ldots ۰۰۱۰۱۰۰۱۱ \ldots$$

کلید رمز به اشتراک گذاشته شده توسط آلیس و باب که با K نشان داده می‌شود :

$$K = \ldots ۱۰۰۱۱۱۰۱۰ \ldots$$

متن رمزی دریافت شده توسط باب که آن را با C نشان می‌دهیم :

$$C = \ldots ۱۰۱۱۰۱۰۰۱ \ldots$$

چون کلید رمز و متن رمز هر دو کاملاً تصادفی هستند لذا کد قابل شکستن نخواهد بود. باب پس از دریافت متن رمز شده با در اختیار داشتن کپی کلید رمز می‌تواند به متن اصلی دست پیدا کند. بنابراین کافیست که کلید رمز و متن رمز شده را دوباره در مبنای ۲جمع کند، یعنی :

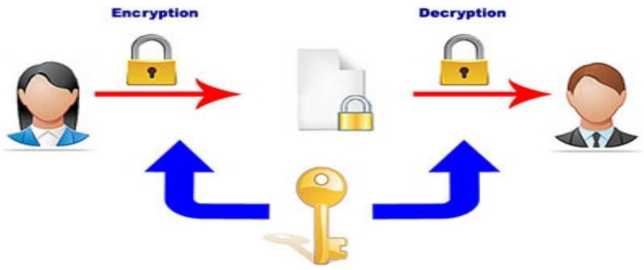
$$P_i = C_i \oplus K_i \tag{۲.۱}$$

تأکید می‌کنیم که در این روش که به عنوان $One - time - pad$ شناخته می‌شود ، کلید رمز تنها باید یکبار مورد استفاده قرار بگیرد. زیرا در این روش یک استراق سمع کننده [۵] یا همان جاسوس [۶]، برای حمله می‌تواند با دسترسی به متن رمز شده و جمع کردن متون رمز شده به مجموعه‌ی متن اصلی دسترسی پیدا کند، و با توجه به وجود کلمات مشترک در متون اصلی کل پیام را رمزگشایی کند.

[۴] Gilbert Vernam

[۵] Eavesdropper

[۶] Eve

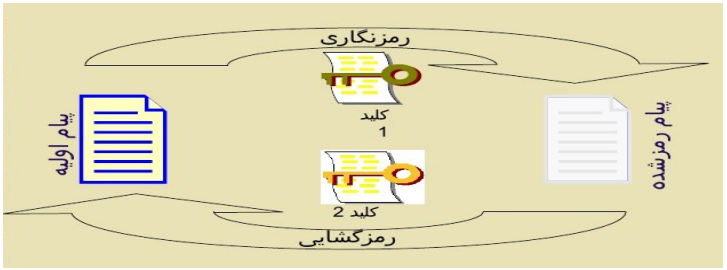


شکل ۱.۱: رمزنگاری کلید متقارن

در اصل در این نوع رمزگذاری باید یک کلید رمز مشترک بین دو طرف تعریف کرد، چون کلید رمز باید کاملاً محرمانه باقی بماند، برای ایجاد و ردوبدل کلید رمز مشترک باید از کانال امن استفاده نمود یا از روش‌های رمزنگاری نامتقارن استفاده کرد. نیاز به وجود کلید رمز به ازای هر دو نفر درگیر در رمزنگاری متقارن، موجب بروز مشکلاتی در مدیریت کلیدهای رمز می‌شود [۵].

۲.۴.۱ سیستم‌های کلیدهای نامتقارن

اصلی‌ترین مشکل رمزنگاری به روش متقارن مسئله توزیع کلید و ارسال آن است، که دیفی_ هلمن [۷] با ارائه ایده‌ای در سال ۱۹۷۰ این مشکل را حل کردند. در این روش از کلیدهای مختلفی برای رمزنگاری استفاده می‌شود، به این ترتیب که ابتدا گیرنده پیام یعنی باب یک زوج کلید، به نام‌های کلید عمومی [۸] و کلید خصوصی [۹] تولید می‌کند. کلید عمومی در دسترس همگان قرار می‌گیرد، و آلیس با استفاده از آن (کلید عمومی) می‌تواند تنها پیام خود را رمزگذاری کند ولی این کلید برای رمزگشایی کارایی ندارد. با استفاده از کلید خصوصی که فقط در اختیار باب است متن رمز شده، رمزگشایی می‌شود و امنیت رمزنگاری نیز به محرمانه بودن کلید خصوصی بستگی دارد.



شکل ۲.۱: رمزنگاری کلید نامتقارن

امنیت رمزنگاری با کلیدهای عمومی براساس پیچیدگی محاسباتی بنا شده است، که ایده آن را دیفی_ هلمن با معرفی روش توابع یک طرفه [۱۰] مطرح کردند [۵]. در این روش به سادگی می‌توان تابع

[۷] Diffe-Hellman
[۸] Key Public
[۹] Private key
[۱۰] One-way-Function

f را محاسبه کرد، ولی محاسبه تابع معکوس آن یعنی f^{-1} به سادگی ممکن نیست.

برای تعریف ساده است اگر تابع $f(x)$ با استفاده از متغییر داده شده x محاسبه شود ولی معکوس آن، یعنی محاسبه و بدست آوردن متغییر x از طریق تابع $f(x)$ مشکل به نظر می‌آید. منظور از مشکل بودن به این معنا است که زمان انجام چنین عملیاتی با توجه به تعداد بیت‌های ورودی به صورت نمایی افزایش می‌یابد.

متداول‌ترین روش رمزگذاری با کلید نامتقارن روشی موسوم به RSA [۱۱] است که اولین بار در سال ۱۹۷۷ ارائه شد.

شکستن الگوریتم RSA :

برای شکستن این الگوریتم باید بتوان N را به عوامل اولش تجزیه کرد، یعنی : $N = pq$

کلید عمومی N، به ترتیب حاصلضرب دو عدد اول بزرگ p و q است. حالا باید با استفاده از N بتوان عامل‌های p و q را حدس زد که مشکل‌ترین قسمت کار است. زیرا الگوریتم‌های ریاضی بدست آمده نشان می‌دهند که، اگر اعداد بزرگ عوامل اول کوچک‌تری داشته باشند ساده‌تر تجزیه می‌شوند تا اعداد بزرگی که عوامل اول بزرگتری دارند.

البته برای شکستن رمز اعداد بزرگ یا تجزیه‌ی آن‌ها به عوامل اول‌شان که با استفاده از الگوریتم‌های کلاسیکی رمز شده‌اند به زمان بسیار زیاد نیاز است. برای مثال شکستن کدهای RSA با بیش از ۱۲۸ بیت با کامپیوترهای کلاسیک حاضر بیشتر از عمر کیهان زمان لازم است. بنابراین در عمل این کدها غیرقابل شکستن هستند. اما نکته‌ای که حائزه اهمیت این است که با ساخت کامپیوترهای کوانتومی در آینده این زمان به کمتر از نیم ساعت خواهد رسید و اساساً تمام رمزهای کنونی بی‌فایده خواهند بود [۸].

۳.۴.۱ مقایسه الگوریتم رمزنگاری متقارن و نامتقارن

اصولاً این دو روش رمزنگاری دارای ماهیت متفاوتی هستند و کاربردهای متفاوتی نیز دارند. مقایسه این دو روش بدون توجه به کاربرد و سیستم مورد نظر کار دقیقی نخواهد بود. اما به طور خلاصه می‌توان گفت که الگوریتم متقارن بیشتر در رمزنگاری‌های ساده که حجم داده‌ها بسیار زیاد است و لازم است که داده‌ها با سرعت بالاتری رمزگذاری و رمزگشایی شوند مورد استفاده قرار می‌گیرد، و از الگوریتم نامتقارن که دارای امنیت بالاتری است در مواردی که نیاز به مدیریت برای توزیع و ارسال کلید است مورد استفاده قرار می‌گیرد. البته گاهی نیز از ترکیب هر دو الگوریتم استفاده می‌شود که به این الگوریتم‌ها، الگوریتم‌های ترکیبی [۱۲] گفته می‌شود [۹].

در جوامع امروزی اطلاعات و امنیت ارتباطات در بالاترین درجه اهمیت قرار دارد که با توجه به ویژگی‌های این دو نوع الگوریتم کلاسیکی و توسعه و گسترش فناوری در علم رمزنگاری بخصوص بعد از ظهور کامپیوتر و ورود آن به حوزه مکانیک کوانتومی این دو بخش مورد تهدید قرار می‌گیرند، پس برای در امان ماندن از این تهدیدات لازم است با نوع جدیدی از رمزنگاری یعنی رمزنگاری کوانتومی آشنا

[۱۱] Rivest- shamir- Adleman

[۱۲] Hybrid

شویم که در ادامه به آن خواهیم پرداخت.

۵.۱ رمزنگاری پیشرفته

با ظهور کامپیوترها و افزایش قدرت محاسباتی آن‌ها، دانش رمزنگاری وارد حوزه‌ی جدیدی از علوم به نام علوم کامپیوتر گردید و این پدیده، موجب بروز سه تغییر مهم در مسائل رمزنگاری شد:

۱ــ وجود قدرت محاسباتی بالا این امکان را پدید آورد که روش‌های پیچیده‌تر و مؤثرتری برای رمزنگاری به وجود آید.

۲ــ روش‌های رمزنگاری که تا قبل از آن اصولاً برای رمز کردن پیام به کار می‌رفتند، کاربردهای جدید و متعددی پیدا کردند.

۳ــ تا قبل از ورود کامپیوتر به این حوزه رمزنگاری عمدتاً روی اطلاعات متنی و با استفاده از حروف الفبا انجام می‌گرفت، اما ورود کامپیوتر باعث شد که رمزنگاری بر روی انواع اطلاعات و بر مبنای بیت انجام شود [۳].

ایده استفاده از سیستم‌های کوانتومی برای تأمین امنیت اطلاعات ریشه در پیشنهاد ویزنر، بنت و براسارد [۱۳] دارد. رمزنگاری کوانتومی در حقیقت بر پایه ترکیبی از علوم مانند، نظریه اطلاعات، رمزنگاری کلاسیکی، فیزیک کوانتومی و اپتیک کوانتومی تشکیل شده است و در نتیجه با همکاری دانشمندان متخصص در هر کدام از این زمینه‌ها در حال پیشرفت است [۵].

ورود به مبحث رمزنگاری کوانتومی را با مروری گذرا بر نظریه‌ی اطلاعات و قوانین فیزیک کوانتوم، شروع می‌کنیم و در ادامه چند پروتکل مشهور در زمینه رمزنگاری کوانتومی را معرفی و در نهایت به موضوع استفاده از درهم‌تنیدگی در ارتباط کوانتومی و کاربرد آن می‌پردازیم.

۶.۱ نظریه‌ی اطلاعات کوانتومی

کارهای ارزنده شانون منجر به پیدایش علم اطلاعات شد در حالی که دوازده سال پیش از آن نیز این علم با کارهای ارزنده تورینگ [۱۴] معرفی شده بود. علم رایانش و علم اطلاعات ، به عنوان پدیده‌هایی بسیار نو منجر به پیدایش تحول‌های بسیار بزرگی در تمام زمینه‌های علمی و اقتصادی شدند. علم اطلاعات و محاسبات کوانتومی شاخه جدید بین رشته‌ای است که با علم کامپیوتر، علم اطلاعات کلاسیک و مکانیک کوانتومی در ارتباط است. با نگاهی سطحی به این دو دستاورد علمی، یعنی علم رایانش و اطلاعات، می‌توان به سادگی وابستگی هر دوی آن‌ها را به علم فیزیک نشان داد. دستاوردهای اطلاعات و رایانش به ناچار باید در یک بستر فیزیکی پیاده‌سازی شوند ، از همین رو دور از تصور نیست که تغییرهای بنیادی در علم فیزیک منجر به پیدایش تغییرات اساسی در علم‌های رایانش و اطلاعات شود. چنانچه

[۱۳] S.Wiesner,C.Bennet,G.Brassward
[۱۴] Turing

که بکارگیری اطلاعات و محاسبات کوانتومی به ما چگونگی تفکر فیزیکی در مورد موضوع محاسبات و اطلاعات را می‌آموزد [۱۰، ۸].

البته نظریه‌ی اطلاعات کوانتومی خود از قسمت‌های دیگری تشکیل شده که عبارت است از [۸]:

- رایانش کوانتومی [۱۵] : علم جدیدی که پس از ساخت رایانه‌های کوانتومی بدنبال یافتن الگوریتم‌های مختلف اما سازگار با این رایانه‌ها است.
- محاسبات کوانتومی [۱۶]: محاسبات دانشی است که اساس آن در ریاضیات است، ولی با ساخت رایانه‌های کوانتومی که براساس مکانیک کوانتومی کار می‌کنند قدرت پردازش اطلاعات و محاسبات بسیار افزایش یافته است و متخصصین این علم در تلاش برای بدست آوردن پیچیدگی‌های الگوریتم‌های مختلف کوانتومی هستند.
- تصحیح خطای کوانتومی [۱۷]: در محاسبات کوانتومی برای محافظت از اطلاعات کوانتومی در مقابل خطاهای ناشی از ناهمدوسی و سایر اختلالات کوانتومی استفاده می‌شود.
- درهم‌تنیدگی کوانتومی [۱۸]: از دیدگاه نظریه اطلاعات به مطالعه درهم‌تنیدگی کوانتومی می‌پردازد.
- رمزنگاری کوانتومی [۱۹]: تعمیمی از ارتباطات کوانتومی است . هنر انتقال یک حالت کوانتومی از یک مکان به مکان دیگر است. رمزنگاری کوانتومی اولین کاربرد اطلاعات کوانتومی برای رسیدن به سطحی از پیشرفت در فن‌آوری روز، و به عنوان مثال برای مصارف تجاری است .

در این پایان نامه به رمزنگاری کوانتومی پرداخته شده است. اما پیش از آن به بررسی بخشی از تفاوت‌های دو نظریه اطلاعات کوانتومی و کلاسیکی می‌پردازیم.

کیوبیت

هر سیستم محاسباتی دارای یک پایه اطلاعاتی است که نماینده کوچک‌ترین میزان اطلاعات قابل نمایش چه به صورت پردازش شده و چه خام است. در محاسبات کلاسیکی این واحد ساختاری بیت [۲۰] نامیده می‌شود که گزیده واژه 'دودویی' [۲۱] است ، زیرا می‌تواند فقط یکی از دو مقدار مجاز "۰" و "۱" را در خود نگه دارد. در مقابل در محاسبات کوانتومی این واحد ساختاری کیوبیت [۲۲] نامیده می‌شود.

هر بیت کوانتومی یا کیوبیت عبارت است از یک سیستم دودویی که می‌تواند دو حالت [۲۳] مجزای $|۰\rangle$ و $|۱\rangle$ را داشته باشد. (که با استفاده از نماد دیراک کت، یعنی $|\rangle$ آن را نمایش می‌دهیم) همچنین یک سیستم دو بعدی کوانتومی با دو پایه‌ی مجزا را می‌توان به عنوان برداری در یک فضای برداری مختلط به نام فضای هیلبرت به صورت زیر توصیف کرد:

---

[۱۵] Quantum computing
[۱۶] Quantum computation
[۱۷] Quantum error correction
[۱۸] Quantum entangelmant
[۱۹] Quantum cryptography
[۲۰] Bit
[۲۱] Binary
[۲۲] Qubit
[۲۳] State

$$|۰\rangle = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \qquad |۱\rangle = \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} \tag{۳.۱}$$

و البته برخلاف یک بیت کلاسیک، که فقط می‌تواند در یکی از دو حالت ممکن خود یعنی ۰ و یا ۱ باشد، یک بیت کوانتومی می‌تواند در بیش از دو حالت $|۰\rangle$ و $|۱\rangle$ و در برهم‌نهی از دو حالت پایه به صورت،

$$|\psi\rangle = \alpha|۰\rangle + \beta|۱\rangle \tag{۴.۱}$$

باشد، که α و β هر دو عدد مختلط هستند. از طرفی مقدار یک بیت کلاسیک را می‌توان تعیین کرد اما مقدار بیت کوانتومی را نمی‌توان تعیین کرد، زیرا اندازه‌گیری از کیوبیت احتمال را به ما می‌دهد، به عبارتی رابطه زیر بین α و β برقرار است:

$$|\alpha|^۲ + |\beta|^۲ = ۱ \tag{۵.۱}$$

بر این اساس احتمال این که یک کیوبیت بعد از اندازه‌گیری مقدارش "۰" باشد، $|\alpha|^۲$ و مقدارش "۱" باشد، برابر $|\beta|^۲$ خواهد بود. همچنین می‌توان گفت در حالت کلی کیوبیت ناشناخته در برهم‌نهی از هر دو حالت پایه است، که با استفاده از مختصات کروی می‌توان حالت کیوبیت ناشناخته را به صورت زیر نوشت:

$$\alpha = cos\frac{\theta}{۲} \qquad \beta = e^{i\varphi}sin\frac{\theta}{۲} \tag{۶.۱}$$

$$|\psi\rangle = cos\frac{\theta}{۲}|۰\rangle + e^{i\varphi}sin\frac{\theta}{۲}|۱\rangle \tag{۷.۱}$$

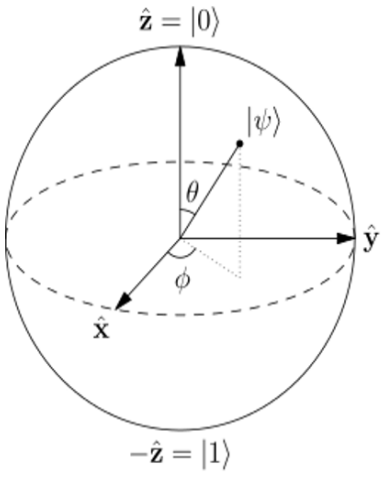
که $۰ \leq \theta \leq \pi$ و $۰ \leq \varphi \leq ۲\pi$ است.

هر حالت کوانتومی را می‌توان در یک فاز مثل $e^{i\varphi}$ ضرب کرد که به آن فاز کلی می‌گویند. به عبارتی حالت $e^{i\varphi}|\psi\rangle$ و حالت $|\psi\rangle$ هر دو برابر هستند زیرا احتمال هر دو حالت یکی است و تنها در یک عامل فازی جزئی $e^{i\varphi}$ با هم تفاوت دارند.

$$\langle e^{-i\varphi}\psi^{\dagger}|e^{i\varphi}\psi\rangle = ۱ \qquad \langle\psi|\psi\rangle = ۱ \tag{۸.۱}$$

بنابراین می‌توان گفت که در کیوبیت ناشناخته تا قبل از اندازه‌گیری بی‌نهایت اطلاعات نهفته است که به آن‌ها اطلاعات مخفی [۲۴] گفته می‌شود. اما پس از اندازه‌گیری، سیستم به یک حالت رمبش [۲۵] کرده و بقیه اطلاعات از بین می‌رود. این بی‌نهایت اطلاعات را می‌توان به شکل زیبایی در کره بلاخ [۲۶] دید. در مکانیک کوانتوم، کره بلاخ (شکل (۳.۱)) نمایشی هندسی از حالت یک سیستم کوانتومی دو

[۲۴] Hiden Information
[۲۵] Coullaps
[۲۶] Bloch Sphere



شکل ۳.۱: نمایش حالت با استفاده از کره بلاخ

حالته(کیوبیت) است. بنابراین هر حالتی از کیوبیت می‌تواند یک نقطه روی سطح کره بلاخ باشد.

از آنجا که θ و φ کمیت‌های پیوسته هستند بی‌نهایت حالت وجود دارد. بنابراین یک حالت ناشناخته می‌تواند هر نقطه‌ای روی سطح کره بلاخ باشد(همان مفهوم بی‌نهایت اطلاعات مخفی).

در مقابل نوع دیگری از فاز وجود دارد که به آن فاز نسبی [۲۷] می‌گویند. برای مثال دو حالت زیر را در نظر بگیرید:

$$|+\rangle = \frac{۱}{\sqrt{۲}}(|۰\rangle + |۱\rangle) \qquad |-\rangle = \frac{۱}{\sqrt{۲}}(|۰\rangle - |۱\rangle)$$

در این مثال احتمال بدست آوردن کیوبیت $|۱\rangle$، از دو حالت $|+\rangle$ و $|-\rangle$ مساوی و برابر $\frac{۱}{۲}$ است. در حالی که، علامت این کیوبیت در هر دو حالت با هم متفاوت است. برای چنین حالت‌های یکسانی می‌توان دو دامنه $\alpha_۱$ و $\alpha_۲$ را به گونه‌ای تعریف کرد که به وسیله‌ی یک فاز نسبی از هم متفاوت باشند. این فاز را به صورت $\alpha_۱ = e^{i\varphi}\alpha_۲$ تعریف می‌کنیم. در فاز نسبی برخلاف فاز کلی که هر دو دامنه‌ی یک حالت تحت تاثیر عامل فازی $e^{i\varphi}$ بودند، تنها یکی از دامنه‌ها تحت تأثیر عامل فازی $e^{i\varphi}$ بوده و دو حالت از یکدیگر متفاوت می‌باشند [۱۱].

عملگرهای خطی

کمیت‌های که در کلاسیک به نوعی متغییر بودند، در مکانیک کوانتومی می‌توانند با توجه به نوع فضا، یک عملگر یا اپراتور باشند و وقتی در فضای خاصی قرار می‌گیرند عمل کنند.

برای مثال x در فضای تکانه (p) یک عملگر، و در فضای خودش یک متغییر است.

برای تغییر یک حالت کوانتومی از عملگرهای خطی استفاده می‌شود و این عملگرها توابعی هستند که با تأثیر روی حالت کوانتومی، آن را به حالت کوانتومی دیگری تبدیل می‌کنند.

[۲۷] Relative phase

ویژگی‌های یک عملگر خطی:
۱ـ عملگر L یک عملگر خطی [۲۸] است، اگر

$$L[f(x)+g(x)] = Lf(x) + Lg(x) \tag{۹.۱}$$

۲ـاگر L یک عملگر خطی و C یک عدد ثابت باشد، آنگاه

$$L(cf(x)) = cLf(x) \tag{۱۰.۱}$$

البته می‌توان برای نمایش یک اپراتور یا عملگر از عمومی‌ترین شکل آن یعنی، نمایش ماتریسی استفاده کرد که عناصر ماتریس به شکل زیر تعریف می شوند:

$$\langle U_i|O|U_j\rangle = o_{ij} \tag{۱۱.۱}$$

نمایش ماتریسی عملگر O_{ij} به صورت زیر است:

$$O_{ij} \equiv \begin{pmatrix} o_{۱۱} & \dots & o_{۱n} \\ \vdots & \ddots & \vdots \\ o_{m۱} & \dots & o_{mn} \end{pmatrix} \tag{۱۲.۱}$$

عناصر ماتریس عملگر O، بر مبنای ویژه توابع U_i هستند [۱۲].
حال با استفاده از این نوع شکل نمایش ماتریسی برای عملگرها، می‌توان نمایش ماتریسی عملگرهای مهم در مبحث اطلاعات کوانتومی یعنی ماتریس‌های پائولی [۲۹] را که در پایه Z نوشته شده‌اند، به این شکل نشان داد:

$$X = \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \quad Y = \begin{pmatrix} ۰ & -i \\ i & ۰ \end{pmatrix} \quad Z = \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \tag{۱۳.۱}$$

البته در محاسبات کوانتومی ماتریس‌های پائولی، گیت‌های تک کیوبیتی هستند که مشهورترین آن‌ها، Z به عنوان یک گیت فاز برگردان [۳۰] و X به عنوان یک گیت بیت برگردان [۳۱]، مورد استفاده قرار می‌گیرند. برای مثال اثر عملگرهای فاز برگردان، و بیت برگردان Z و X روی حالت‌های $|۰\rangle$ و $|۱\rangle$ به صورت زیر است:

$$Z|۰\rangle = |۰\rangle \quad \longrightarrow \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \tag{۱۴.۱}$$

[۲۸] Linear Operators
[۲۹] Pauli matrices
[۳۰] Phase flip
[۳۱] Bit flip

$$Z|۱\rangle = -|۱\rangle \quad \longrightarrow \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} = \begin{pmatrix} ۰ \\ -۱ \end{pmatrix} \tag{۱۵.۱}$$

$$X|۰\rangle = |۱\rangle \quad \longrightarrow \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} = \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} \tag{۱۶.۱}$$

$$X|۱\rangle = |۰\rangle \quad \longrightarrow \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \tag{۱۷.۱}$$

با توجه به نوع اثر ماتریس عملگر پائولی X می‌توان این عملگر را معادل گیت NOT در محاسبات کوانتومی دانست، و البته ماتریس یکانی I که بصورت

$$I = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} \tag{۱۸.۱}$$

است و اعمال آن روی حالت کوانتومی تغییری در آن ایجاد نمی‌کند [۱۱].

ضرب داخلی

ضرب داخلی یا ضرب اسکالر [۳۲] در فضای اقلیدسی [۳۳] (جبر خطی) به صورت $\overrightarrow{a}.\overrightarrow{b}$ تعریف می‌شود، که حاصل آن یک عدد است. مشابه این تعریف در فیزیک، در فضای برداری که با آن سر و کار داریم یعنی فضای کت‌ها، متناظر با هر $|\alpha\rangle$ یک برا با نماد $\langle\alpha|$ وجود دارد که متعلق به فضای براست. فضای برا یک فضای برداریست؛ یعنی یک فضای برداری، دوگان [۳۴] فضای کت است و تناظر یک به یکی بین فضای کت و فضای برا، برقرار است.

در تشکیل ضرب داخلی نیز همواره یک بردار از فضای برا و یک بردار از فضای کت به شکل زیر در نظر گرفته می‌شود:

$$(\langle\beta|) \cdot (|\alpha\rangle) = \langle\beta|\alpha\rangle \tag{۱۹.۱}$$

ضرب داخلی دارای ۲ خاصیت است که به عنوان اصل موضوعه می‌پذیریم:

۱ــ حالت تناظر یک به یک در فضای دوگان

$$\langle\beta|\alpha\rangle = (\langle\alpha|\beta\rangle)^* \tag{۲۰.۱}$$

۲ــشرط تعامد و بهنجارش

$$\langle\alpha|\alpha\rangle \geqslant ۰ \tag{۲۱.۱}$$

[۳۲] Scalar multiplication
[۳۳] Euclidean space
[۳۴] Dual

حالت تساوی وقتی برقرار است که $|\alpha\rangle$ پوچ باشد.

چند تعریف در ارتباط با ضرب داخلی:

۱ـ در یک فضای برداری مانند γ، دو بردار $|\alpha\rangle$ و $|\beta\rangle$ متعامدند، اگر

$$\langle\beta|\alpha\rangle = \langle\alpha|\beta\rangle = ۰ \qquad (۲۲.۱)$$

و $(|\alpha\rangle, |\beta\rangle) \in \gamma$ است.

۲ـ با کت معلوم $|\alpha\rangle \neq ۰$، می‌توان کت بهنجار $|\tilde{\alpha}\rangle$ را به صورت زیر تعریف کرد:

$$|\tilde{\alpha}\rangle = (\frac{۱}{\sqrt{\langle\alpha|\alpha\rangle}})|\alpha\rangle \qquad (۲۳.۱)$$

که دارای خاصیت، $\langle\tilde{\alpha}|\tilde{\alpha}\rangle = ۱$ است.

در حالت کلی، در قیاس با اندازه یک بردار در فضای اقلیدسی $\sqrt{a.a} = |a|$، در فضای برداری، اندازه بردار $|\alpha\rangle$ به صورت $\left||\alpha\rangle\right| = \sqrt{\langle\alpha|\alpha\rangle}$ تعریف می‌شود که معمولاً با عنوان طول یا اندازه بردار شناخته می‌شود.

بنابراین می‌توان گفت اگر هر بردار $|\alpha_i\rangle$ یک بردار واحد باشد، حاصلضرب بردارهای، $|\alpha_i\rangle \in \overrightarrow{\alpha}$ به صورت زیر است:

$$\langle\alpha_i|\alpha_i\rangle = ۱ \qquad (۲۴.۱)$$

$$\langle\alpha_i|\alpha_j\rangle = ۰ \qquad i \neq j \qquad (۲۵.۱)$$

و $(i, j = ۱ \cdots n)$ است. با این تعریف چنین بردارهای کل فضا را شامل می‌شوند و هر بردار خارج از این فضا را می‌توان به صورت ترکیب خطی از این بردارهای پایه نوشت [۱۳].

ضرب خارجی

در جبر خطی ضرب خارجی دو بردار $\vec{A}$ و $\vec{B}$ را به صورت زیر تعریف می‌کنیم:

$$\vec{C} = \vec{A} \times \vec{B} \qquad (۲۶.۱)$$

که حاصل آن یک بردار است که بر صفحه هر دو بردار عمود است. برخلاف ضرب داخلی که حاصل آن یک عدد است.

در فضای برداری نیز ضرب خارجی [۳۵] یا ضرب پروانه‌ای را با استفاده از دو بردار کت $(\langle|)$ و برا $(|\rangle)$ به صورت زیر تعریف می‌کنیم که حاصل آن یک عملگر است و بنابراین اساساً با ضرب داخلی $\langle\beta|\alpha\rangle$ که حاصل آن یک عدد مختلط است، متفاوت می‌باشد.

[۳۵] Outer Products

$$|\alpha\rangle\langle\beta| = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} \begin{pmatrix} b_1^* & b_2^* & \dots & b_n^* \end{pmatrix} = \begin{pmatrix} a_1 b_1^* & \dots & a_1 b_n^* \\ \vdots & \ddots & \vdots \\ a_m b_1^* & \dots & a_m b_n^* \end{pmatrix} \tag{۲۷.۱}$$

به عنوان یکی از خواص این نوع ضرب می‌توان از خاصیت شرکت‌پذیری نام برد، که به صورت زیر نمایش داده می‌شود:

$$(|\alpha\rangle\langle\beta|)|\gamma\rangle = |\alpha\rangle(\langle\beta|\gamma\rangle) \tag{۲۸.۱}$$

که حاصل باز هم یک کت در فضای بردار α است. زیرا عبارت اول که همان $|\alpha\rangle$ و عبارت دوم (عبارت داخل پرانتز) ضرب داخلی دو بردار است که حاصل آن یک عدد مختلط است، و از جبر خطی می‌دانیم که حاصلضرب یک عدد در یک بردار همیشه یک بردار است، و در این‌جا این بردار در فضای بردار α است.

همچنین می‌توان با استفاده از تعریف ضرب خارجی، تعریف یکی از پرکاربردترین عملگرهای کوانتومی یعنی عملگر همانی یا رابطه‌ی کاملیت [۳۶] را بدست آورد [۱۳].

$$\sum_i |U_i\rangle\langle U_i| = I \tag{۲۹.۱}$$

ضرب تانسوری فضاهای برداری

هرگاه $(A_{i\times j})$ و $(B_{k\times l})$ دو ماتریس با ابعاد داده شده باشند می‌توان ضرب تانسوری [۳۷] آن‌ها را که ماتریسی با ابعاد $ik \times jl$ است به صورت زیر تعریف کرد:

$$(A \otimes B)_{ij,kl} := A_{ik} B_{jl} \tag{۳۰.۱}$$

تفسیر ضرب تانسوری در فضای برداری این است که با این ضرب یک فضای بزرگ‌تر از دو فضای کوچک‌تر ساخته می‌شود.

ضرب تانسوری را می‌توان به صورت ماتریسی به شکل زیر نوشت:

$$A \otimes B := \begin{pmatrix} a_{11} B & \dots & a_{1n} B \\ \vdots & \ddots & \vdots \\ a_{m1} B & \dots & a_{mn} B \end{pmatrix} \tag{۳۱.۱}$$

[۳۶] Comeleteness Relation
[۳۷] Tensor Products

اگر فضای برداری V با بردارهای پایه $\{|i\rangle, i = ۱, \ldots, n\}$ و فضای برداری W با بردارهای پایه $\{|j\rangle, j = ۱, \ldots, m\}$ را در نظر بگیریم، می‌توان ضرب تانسوری بردارهای پایه را این‌گونه تعریف کرد:

$$|i, j\rangle := |i\rangle \otimes |j\rangle \qquad i = ۱, \ldots, n \qquad j = ۱, \ldots, m \tag{۳۲.۱}$$

برای مثال: هرگاه V یک فضای برداری با پایه‌های

$$\left\{ |۰\rangle = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \quad , \quad |۱\rangle = \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} \right\} \tag{۳۳.۱}$$

باشد، آنگاه $V \otimes V$ یک فضای برداری ۴ بعدی با پایه‌های زیر است:

$$|۰, ۰\rangle := \begin{pmatrix} ۱ \\ ۰ \\ ۰ \\ ۰ \end{pmatrix} \quad |۰, ۱\rangle := \begin{pmatrix} ۰ \\ ۱ \\ ۰ \\ ۰ \end{pmatrix} \quad |۱, ۰\rangle := \begin{pmatrix} ۰ \\ ۰ \\ ۱ \\ ۰ \end{pmatrix} \quad |۱, ۱\rangle := \begin{pmatrix} ۰ \\ ۰ \\ ۰ \\ ۱ \end{pmatrix} \tag{۳۴.۱}$$

می‌توان ضرب تانسوری را در مورد عملگرهای خطی نیز تعریف کرد:
هرگاه $A : V \longrightarrow V$ و $B : W \longrightarrow W$ دو عملگر خطی باشند می‌توان ضرب تانسوری آن‌ها را به شکل زیر روی بردارهای پایه تعریف کرد:

$$(A \otimes B)(|i, j\rangle) := (A|i\rangle) \otimes (B|j\rangle) \tag{۳۵.۱}$$

و برای تعیین عناصر ماتریسی این عملگرها به طریق معمولی عمل می‌کنیم.

$$(A \otimes B)_{kl,ij} :\equiv \langle k, l|A \otimes B|i, j\rangle = \langle k|A|i\rangle\langle l|B|j\rangle = A_{ki}B_{lj} \tag{۳۶.۱}$$

که نشان می‌دهد ماتریس ضرب تانسوری عملگرها، از ضرب تانسوری ماتریس‌های دو عملگر بدست می‌آید [۱۱].

۷.۱ اندازه‌گیری کوانتومی

در مکانیک کوانتومی به تعریف دقیقی از اندازه‌گیری نیاز داریم. اندازه‌گیری یک شئ میکروسکوپیک ، در مکانیک کوانتومی، باعث تغییر در حالت آن می‌شود. بنابراین، اندازه‌گیری در مکانیک کوانتومی با اندازه‌گیری در مکانیک کلاسیک که در آن، مشاهده و اندازه‌گیری تأثیر زیادی بر جسم ندارد، تفاوت بسیاری دارد. در مفهوم کلاسیک اندازه‌گیری، همواره می‌توان فرض کرد که در محدوده‌ای معین(متناسب با دقت ابزار اندازه‌گیری) یک نتیجه برای اندازه‌گیری وجود دارد و مقادیر دیگر حاصل

از اندازه‌گیری صفر هستند. این ویژگی مفهوم کلاسیک اندازه‌گیری(نقش نداشتن احتمال در آن) مهم‌ترین تفاوت اندازه‌گیری کلاسیکی و کوانتومی است.

از سوی دیگر در اندازه‌گیری کلاسیک، اندازه‌گیری کمیت‌های گوناگون یک جسم اثری بر نتایج یکدیگر ندارند. اما در حوزه مکانیک کوانتومی این فرض درست نیست. برای مثال در مورد اندازه‌گیری مکان و تکانه خطی یک ذره، اندازه‌گیری کمیت‌های گوناگون بر اساس اصل عدم قطعیت هایزنبرگ [۳۸] بر هم اثر گذارند(اندازه‌گیری یکی بر دیگری اثر خواهد گذاشت).

اندازه‌گیری کوانتومی با استفاده از مجموعه‌ای مثل $\{M_m, \quad m = ۱, \cdots, K\}$ تعریف می‌شود، که M_m ها، عملگرهای اندازه‌گیری هستند و در شرط زیر صدق می‌کنند:

$$\sum_m M_m^\dagger M_m = I \tag{۳۷.۱}$$

با اعمال این عملگرهای اندازه‌گیری روی فضای حالت یک سیستم، آن را اندازه‌گیری می‌کنند. اگر $|\psi\rangle$ حالت اولیه‌ی سیستم قبل از اندازه‌گیری باشد آنگاه احتمال این که بعد از اندازه‌گیری نتیجه m بدست آید به صورت زیر است:

$$P(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{۳۸.۱}$$

و حالت سیستم بعد از اندازه‌گیری خواهد بود:

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \tag{۳۹.۱}$$

معادله‌ی (۳۷.۱) یا معادله‌ی کاملیت بیان می‌کند که مجموعه تمام احتمالات برابر ۱ است:

$$\sum_m P(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = ۱ \tag{۴۰.۱}$$

و این رابطه به ازای تمام $|\psi\rangle$ ها برقرار است.

علاوه بر این، اندازه‌گیری کوانتومی در پایه‌های محاسباتی یک فضای برداری مختلط دو بعدی(فضای کیوبیت‌ها) یعنی $\langle۰|$ و $\langle۱|$ بسیار مهم است، و بر این اساس دو عملگر اندازه‌گیری $M_۰$ و $M_۱$، به شکل زیر تعریف می‌شود:

$$M_۰ = |۰\rangle\langle۰| = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix} \qquad M_۱ = |۱\rangle\langle۱| = \begin{pmatrix} ۰ & ۰ \\ ۰ & ۱ \end{pmatrix} \tag{۴۱.۱}$$

با بکار بردن روابط، $M_۱^۲ = M_۱, \quad M_۰^۲ = M_۰, \quad M_۱^\dagger = M_۱, \quad M_۰^\dagger = M_۰$ برای دو عملگر اندازه‌گیری $M_۰$ و $M_۱$، و با فرض این که حالت کیوبیت قبل از اندازه‌گیری به صورت $|\psi\rangle = \alpha|۰\rangle + \beta|۱\rangle$ باشد آنگاه احتمال بدست آوردن نتایج ۰ و ۱ از اندازه‌گیری کیوبیت به صورت زیر خواهد بود:

$$P(۰) = \langle\psi|M_۰^\dagger M_۰|\psi\rangle = \langle\psi|M_۰|\psi\rangle = \tag{۴۲.۱}$$

[۳۸] Heisenberg's uncertainty principle

$$P(0) = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$P(0) = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$P(0) = \alpha^*\alpha + 0 = |\alpha|^2$$

و به طور مشابه احتمال آن که نتیجه اندازه‌گیری برابر ۱ باشد: $P(1) = |\beta|^2$

بنابراین حالت کیوبیت بعد از اندازه‌گیری در یکی از دو حالت زیر است:

$$|\acute{\psi}\rangle = \frac{M_0|\psi\rangle}{\sqrt{\langle\psi|M_0^\dagger M_0|\psi\rangle}} = \frac{\alpha}{|\alpha|}|0\rangle \qquad (۴۳.۱)$$

$$|\acute{\psi}\rangle = \frac{M_1|\psi\rangle}{\sqrt{\langle\psi|M_1^\dagger M_1|\psi\rangle}} = \frac{\beta}{|\beta|}|1\rangle \qquad (۴۴.۱)$$

ضرایب $\frac{\alpha}{|\alpha|}$ و $\frac{\beta}{|\beta|}$ طول واحد دارند، و در صورت بهنجار بودن سیستم قابل چشم پوشی هستند [۱۴].

۸.۱ عملگر چگالی

حالت یک سیستم فیزیکی بسته(سیستمی که از محیط اطرافش مستقل باشد) با یک بردار در یک فضای هیلبرت ($|\psi\rangle \in H$) توصیف می‌شود. حالت یک سیستم وقتی قابل توصیف است که روی آن اندازه‌گیری انجام شود. در غیاب هر نوع اندازه‌گیری در مورد یک آنسامبل [۳۹]، یعنی اجتماعی از سیستم‌های فیزیکی تنها می‌توان به اطلاعات آماری در مورد توزیع این حالت‌ها بسنده کرد. در مورد حالت‌های خالص می‌توان آنسامبلی را فرض کرد که، همه اعضاء با یک حالت یکسان مثلاً $|\alpha\rangle$ مشخص می‌شوند و اگر حالت همه اعضاء یکسان نباشد راه دیگر توصیف حالت‌های کوانتومی عملگر چگالی [۴۰] (ماتریس چگالی) است. تمام اطلاعاتی که می‌توان در چارچوب مکانیک کوانتومی از این حالت‌ها استخراج کرد در ماتریس چگالی آن‌ها نهفته است. به همین دلیل ماتریس چگالی را ماتریس حالت می‌گوییم.

اگر حالت یک سیستم کوانتومی دقیقاً معلوم و برابر $|\psi\rangle$ باشد، سیستم کوانتومی در حالت خالص [۴۱] قرار دارد. در این صورت عملگر چگالی آن خواهد بود:

$$\rho = |\psi\rangle\langle\psi| \qquad (۴۵.۱)$$

در غیر این صورت می‌گوییم سیستم در حالت آمیخته [۴۲] قرار دارد و تنها می‌توان آن را با عملگر چگالی به صورت زیرتوصیف کرد:

$$\rho = \sum_i P_i|\psi_i\rangle\langle\psi_i| \qquad (۴۶.۱)$$

[۳۹] Ensamble
[۴۰] Density Operator
[۴۱] Pure state
[۴۲] Mixed State

که $\{|\psi_i\rangle\}$ مجموعه حالات ممکن و $\{P_i\}$ توزیع احتمالات است.

چنین ماتریس چگالی دارای ویژگی‌های زیر است:

✓یک عملگر چگالی یا اپراتور چگالی هرمیتی است یعنی: $\rho = \rho^\dagger$

✓$Tr(\rho) = ۱$ که نشان می‌دهد مجموع احتمالات هر مجموعه کامل برابر ۱ است.(Tr [۴۳] یا رد، یعنی حاصل جمع عناصر روی قطر اصلی)

✓عملگر چگالی یک عملگر مثبت [۴۴] است، یعنی برای هر بردار حالت $|v\rangle$ رابطه $\langle v|\rho|v\rangle \geqslant ۰$ صادق است.

✓یک سیستم در حالت خالص است، اگر و فقط اگر $\rho^۲ = \rho$ ، یا به صورت معادل $\rho(\rho - ۱) = ۰$ باشد، و بنابراین تنها برای آنسامبل‌های خالص، علاوه بر $Tr(\rho) = ۱$ خواهیم داشت: $Tr(\rho^۲) = ۱$، که نشان می‌دهد برای یک آنسامبل خالص ، ویژه مقادیر عملگر چگالی صفر و یک هستند، و بنابراین ماتریس حالت خالص ρ قطری خواهد بود.

اما در مورد یک آنسامبل آمیخته $Tr(\rho^۲)$، عددی مثبت و کوچک‌تر از یک است [۱۳].

۹.۱ حالت‌های درهم‌تنیده

درهم‌تنیدگی [۴۵] یکی از مفاهیم مهم و اصلی در نظریه‌ی اطلاعات کوانتومی است، که نقش اساسی در شاخه‌های گوناگون این علم مانند رایانش کوانتومی، ارتباطات کوانتومی [۴۶]، رمزنگاری کوانتومی و دوربری کوانتومی [۴۷] بازی می‌کند. درهم‌تنیدگی یکی از جنبه‌های منحصر به فرد مکانیک کوانتومی است که از اصل موضوعه‌ی آن نتیجه‌گیری می‌شود و نمونه‌ای در فیزیک کلاسیک ندارد [۵].

حالت درهم‌تنیده، حالتی از سیستم است که نمی‌توان آن را بر حسب حالت زیر سیستم‌های آن توصیف کرد. از دیدگاه ریاضی نیز حالت درهم‌تنیده به حالتی اطلاق می‌شود که نمی‌توان آن را به صورت ضرب تانسوری دو بردار نوشت. برای توضیح بیشتر به بیان تفاوت دو حالت غیر درهم‌تنیده و درهم‌تنیده می‌پردازیم.

حالت خالص $|\psi\rangle$ را که از دو سیستم کوانتومی a و b تشکیل شده است در نظر می‌گیریم. می‌توان این حالت ترکیبی [۴۸] را به صورت ضرب تانسوری دو حالت،

$$|\psi\rangle = |\lambda\rangle_a \otimes |\varphi\rangle_b \qquad (۴۷.۱)$$

نوشت و ماتریس چگالی آن را که در فضای هیلبرت [۴۹]، دو زیر سیستم به شکل $H_{ab} = H_a \otimes H_b$، ساخته می‌شود را به صورت زیر در نظر گرفت:

$$\hat{\rho_{ab}} = \hat{\rho_a} \otimes \hat{\rho_b} \qquad (۴۸.۱)$$

---

[۴۳] Trace
[۴۴] Positive
[۴۵] Entanglement
[۴۶] Quantum Communications
[۴۷] Quantum Teleportation
[۴۸] composite
[۴۹] Hilbert

در حالت $|\psi\rangle$ می‌توان حالت زیر سیستم‌های a و b را به صورت حالت مجزا یا جدایی‌پذیر [۵۰] در نظر گرفت ، یعنی با یک ضرب تانسوری می‌توان زیر سیستم‌ها را از هم جدا کرد. پس حالت $|\psi\rangle$ یک حالت غیر درهم‌تنیده است.

اصل برهم‌نهی مکانیک کوانتومی بیان می‌کند که هر برهم‌نهی از حالت‌های ترکیبی مثل حالت (۴۷.۱) نیز یک حالت مجاز برای دو زیر سیستم خواهد بود. برای مثال حالت دو کیوبیتی زیر را در نظر بگیرید:

$$|\psi\rangle = \frac{۱}{\sqrt{۲}}(|۰\rangle_a|۰\rangle_b + |۱\rangle_a|۱\rangle_b) \qquad (۴۹.۱)$$

این حالت یک برهم‌نهی از حالت‌های ترکیبی است و نمی‌توان آن را مانند حالت $|\psi\rangle$ در رابطه‌ی (۴۷.۱) به صورت حاصل‌ضرب تانسوری دو زیر سیستم a و b نوشت. چنین حالتی را یک حالت درهم‌تنیده می‌نامند.

با این وجود نمی‌توان هر سیستمی را که به صورت برهم‌نهی از حالت‌های ترکیبی نوشته شده است را، به عنوان یک حالت درهم‌تنیده در نظر گرفت. برای مثال، حالت ترکیبی زیر را در نظر بگیرید:

$$|\psi\rangle = \frac{۱}{۲}(|۰\rangle_a|۰\rangle_b + |۱\rangle_a|۰\rangle_b + |۰\rangle_a|۱\rangle_b + |۱\rangle_a|۱\rangle_b) \qquad (۵۰.۱)$$

$$= \frac{۱}{\sqrt{۲}}(|۰\rangle_a + |۱\rangle_a) \otimes \frac{۱}{\sqrt{۲}}(|۰\rangle_b + |۱\rangle_b)$$

حالت $|\psi\rangle$ به صورت برهم‌نهی از دو زیر سیستم a و b است ولی می‌توان آن را به صورت حاصل ضرب تانسوری، حالت دو زیر سیستم a و b نوشت.

بنابراین، استفاده از عملگر چگالی راهی برای تشخیص یک سیستم درهم‌تنیده از یک سیستم غیردرهم‌تنیده است. به این منظور می‌توان عملگر چگالی را تشکیل داد و با گرفتن ”رد“ آن روی یکی از زیرسیستم‌ها ماتریس چگالی کاهش یافته [۵۱] را بدست آورد. برای یک حالت غیردرهم‌تنیده مانند حالت (۴۷.۱) ماتریس چگالی به صورت زیر خواهد بود:

$$\hat{\rho}_{ab} = |\lambda\rangle\langle\lambda| \otimes |\varphi\rangle\langle\varphi| \qquad (۵۱.۱)$$

با محاسبه رد آن روی حالت b ماتریس چگالی کاهش یافته برای حالت خالص a بدست می‌آید و با محاسبه رد آن روی حالت a ماتریس چگالی کاهش یافته برای حالت خالص b بدست می‌آید:

$$\hat{\rho}_a = |\lambda\rangle\langle\lambda| \qquad (۵۲.۱)$$

$$\hat{\rho}_b = |\varphi\rangle\langle\varphi|$$

و با توجه به این که دو شرط، $\hat{\rho}_a^{۲} = \hat{\rho}_a$ و $Tr(\hat{\rho}_a^{۲}) = ۱$ برای ماتریس چگالی یک حالت خالص صادق است. هر حالت خالص غیر درهم‌تنیده را می‌توان به فرم معادله (۴۷.۱) نوشت و شرط $Tr(\hat{\rho}_a^{۲}) = ۱$ برای آن برقرار است. در حالی که برای یک حالت درهم‌تنیده این شرط، $Tr(\hat{\rho}_a^{۲}) \neq ۱$ برقرار است.

[۵۰] Separable
[۵۱] Reduced Density Matrice

یک حالت متشکل از دو زیر سیستم a و b را می‌توان به صورت زیر نوشت:

$$|\psi\rangle = \sum_n a_n |\lambda_n\rangle_a |\phi_n\rangle_b \qquad (۵۳.۱)$$

که حالت‌های $\{|\lambda_n\rangle\}$ و $\{|\phi_n\rangle\}$ به ترتیب مجموعه‌های متعامد بهنجار [۵۲] برای سیستم‌های a و b هستند. در این‌جا هر حالت $\{|\lambda_n\rangle\}$ از سیستم a منحصراً وابسته به یک حالت $\{|\phi_n\rangle\}$ از سیستم b است، که به تجزیه اشمیت [۵۳] معروف است. اگر فقط یکی از a_n ها غیر صفر باشد حالت $|\psi\rangle$ جدایی‌پذیر می‌باشد، اما اگر بیشتر از یک a_n غیر صفر باشد می‌تواند نشانه‌ای از درهم‌تنیدگی باشد به تعداد ضرایب غیر صفر a_n عدد اشمیت می‌گویند که عدد اشمیت مخالف ۱ می‌تواند تحت شرایطی نشان از وجود درهم‌تنیدگی باشد.

در میان مجموعه حالت‌های درهم‌تنیده‌ی ممکن، حالت‌های بل دو کیوبیتی [۵۴] به دلیل سادگی و دیگر این که از آزمایشات متعدد نتیجه شده‌اند و نیز این‌که این حالت‌ها، حالت‌هایی با بیشینه‌ی درهم‌تنیدگی‌اند ، بسیار با اهمیت هستند [۱۴]. چهار حالت بل به صورت زیر در نظر گرفته می‌شوند:

$$|\psi^-\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle \otimes |۱\rangle - |۱\rangle \otimes |۰\rangle\Big) \qquad (۵۴.۱)$$

$$|\psi^+\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle \otimes |۱\rangle + |۱\rangle \otimes |۰\rangle\Big)$$

$$|\phi^-\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle \otimes |۰\rangle - |۱\rangle \otimes |۱\rangle\Big)$$

$$|\phi^+\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle \otimes |۰\rangle + |۱\rangle \otimes |۱\rangle\Big)$$

۱۰.۱ اصل عدم کپی برداری

در مکانیک کوانتومی برخلاف مکانیک کلاسیک حالت‌ها قابل کپی شدن نیستند، یعنی نمی‌توان حالت یک سیستم فیزیکی را کپی کرد مگر این که برهم عمود باشند. این امر در مکانیک کوانتومی نتیجه‌ی اصل عدم کپی برداری از حالت‌های کوانتومی یعنی نظریه‌ای $No-cloning$ است که اولین بار توسط زورک [۵۵]، ووترز [۵۶] و دیک [۵۷] مطرح شد.

فرض کنید که بتوان از حالت‌های کوانتومی با استفاده از یک دستگاه کپی کوانتومی کپی تهیه کرد. اگر این کار امکان‌پذیر باشد باید بتوان آن را با یک عملگر تحول یکانی مانند U انجام داد. برای مثال فرض کنید که یک دستگاه کپی با دو ورودی A و B وجود دارد. ورودی A، ورودی داده است که محل

[۵۲] Orthonormal
[۵۳] Schmidt
[۵۴] Bell states
[۵۵] Zurek
[۵۶] Wooters
[۵۷] Dick

ورودی یک حالت کوانتومی ناشناخته مثل $|\psi\rangle$ است. هدف کپی کردن حالت $|\psi\rangle$ روی حالت $|v\rangle$ در ورودی دوم B است.

بااین توضیحات حالت اولیه دستگاه کپی به صورت زیر خواهد بود:

$$|\psi\rangle \otimes |v\rangle \tag{۵۵.۱}$$

فرایند کپی کردن دستگاه با استفاده از عملگر تحول یکانی U به صورت زیر است:

$$|\psi\rangle \otimes |v\rangle \rightarrow U(|\psi\rangle \otimes |v\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{۵۶.۱}$$

حال فرض کنید که این عملیات کپی کردن روی دو $|\psi\rangle$ و $|\varphi\rangle$ انجام شود در این صورت خواهیم داشت:

$$U(|\psi\rangle \otimes |v\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{۵۷.۱}$$

$$U(|\varphi\rangle \otimes |v\rangle) = |\varphi\rangle \otimes |\varphi\rangle \tag{۵۸.۱}$$

با ضرب داخلی این دو معادله خواهیم داشت:

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^{۲} \tag{۵۹.۱}$$

اما می‌دانیم که از حل معادله‌ی $x = x^{۲}$ دو جواب خواهیم داشت: $x = ۰$ و $x = ۱$. بنابراین اگر $\langle\psi|\varphi\rangle = ۱$ یعنی $|\psi\rangle = |\varphi\rangle$ و اگر $\langle\psi|\varphi\rangle = ۰$ یعنی $|\psi\rangle$ بر $|\varphi\rangle$ عمود است. پس می‌توان نتیجه گرفت که اگر یک دستگاه کپی کوانتومی وجود داشته باشد تنها می‌تواند حالت‌هایی را کپی کند که بر هم عمود باشند و یک دستگاه کپی کوانتومی کلی نمی‌تواند وجود داشته باشد [۱۱، ۵].

فصل ۲

توزیع کلید کوانتومی

در این فصل ابتدا نمایی از یک پروتکل توزیع کلید کوانتومی را معرفی و در ادامه چند پروتکل مهم در این زمینه را مورد بررسی قرار می‌دهیم.

۱.۲ نمایی از توزیع کلید کوانتومی

پیشرفت‌های فیزیک کوانتومی، به ویژه ایده‌ی ساخت و تحقق رایانه‌های کوانتومی رمزنگاران را به سمت طراحی شیوه‌های جدیدی برای تضمین امنیت در ارتباطات سوق داده است و به نظر می‌رسد که سیستم‌های رمزنگاری جدید پاسخی به این مسئله باشند. البته امنیت برای این سیستم‌های رمزنگاری به اثبات رسیده است و تنها مسئله، توزیع امن کلید است [۱۵].

در این مورد نیز رمزنگاری کوانتومی با استفاده از فناوری توزیع کلید کوانتومی (QKD) [۱] بر اساس قوانین فیزیک کوانتومی، به جای فرضیات پیچیده محاسباتی مسائل ریاضی، قادر به تولید کلیدهای رمزنگاری امن و توزیع آن از طریق یک کانال ناامن(کانالی که ممکن است ایو [۲] یا همان جاسوس به آن دسترسی داشته باشد) است [۱۶].

مفهوم توزیع کلید کوانتومی دقیق‌تر از رمزنگاری کوانتومی است. بنابراین در این بخش به تشریح مراحل یک پروتکل توزیع کلید کوانتومی می‌پردازیم:

مرحله‌ی اول با انتقال فوتون‌ها از آلیس(فرستنده) به باب(گیرنده) آغاز می‌شود، فوتون‌ها نمایش

[۱] Quantum Key Distribution

[۲] EVe

دهنده‌ی ذره‌ی کوانتومی یعنی همان کیوبیت هستند و چون نسبت به سایر سیستم‌های کوانتومی در دسترس‌تر می‌باشند و به سختی با یکدیگر برهم‌کنش می‌کنند پس برای انتقال در مسیرهای طولانی گزینه‌ی مناسبی هستند. این انتقال از طریق کانالی که خاصیت کوانتومی ذره را حفظ کند یعنی کانال کوانتومی [۳] صورت می‌گیرد (البته تفاوت در چگونگی روش‌های انتقال خود باعث شکل‌گیری پروتکل‌های مختلف توزیع کلید می‌شود). مرحله بعد ارتباط از طریق کانال کلاسیکی یا همان کانال عمومی [۴] است که می‌تواند یک کانال قراردادی مانند تلفن باشد. در این مرحله اندازه‌گیری کیوبیت‌ها توسط باب باعث تولید دو رشته بیت متفاوت در دست آلیس و باب می‌شود که هنوز نمی‌توان آن را به عنوان کلید مشترک در نظر گرفت. چون امکان شنود در این کانال وجود دارد. پس آلیس و باب برای اجتناب از شنود مکالمات خود توسط جاسوس یا جلوگیری از حمله معروف به حمله مرد میانی (DOS) [۵]، باید مرحله غربال‌گری [۶] بیت‌ها را انجام دهند. در این مرحله آلیس و باب در مورد این که کدام بیت‌ها را نگه داشته و کدام بیت‌ها را حذف کنند تصمیم می‌گیرند. پس از توافق در مورد بیت‌ها و اطمینان اولیه از عدم حضور جاسوس در مسیر انتقال ذره(کانال کوانتومی)، آن‌ها وارد مرحله اصلاح [۷] یا مرحله‌ی تصحیح خطا [۸] می‌شوند. چون کانال کوانتومی بدون اختلال [۹] نیست، پس آلیس و باب یک رشته بیت یکسان را به اشتراک نگذاشته‌اند. بخش کوچکی از خطا در رشته بیت باب است که در این مرحله تصحیح می‌شود. پس از اصلاح آلیس و باب یک رشته یکسان را با احتمال بسیار بالا به اشتراک می‌گذارند. اما این رشته هنوز نمی‌تواند به عنوان کلید مورد استفاده باشد. زیرا جاسوس امکان دسترسی به رشته تصحیح شده را دارد پس آلیس وباب باید میزان اطلاعات جاسوس از کلید را تا حد ممکن کم و به میزان صفر برسانند، از این رو آن‌ها با استفاده از یکی از روش‌های تقویت محرمانگی [۱۰] باید رشته بیت خود را به زیر مجموعه‌های کوچک‌تری تقسیم کنند تا اطلاعات جاسوس را به صفر کاهش دهند. پس از پایان این مرحله آلیس و باب باید در مرحله‌ی بعد تأیید هویت [۱۱] کنند. تا آلیس به اشتباه به صورت مستقیم با جاسوس به جای باب ارتباط برقرار نکند. پس از این مرحله آلیس و باب می‌توانند کلید محرمانه‌ای را که تنها برای خودشان شناخته شده است با اطمینان به اشتراک بگذارند [۱۱].

پس از توصیف نمای کلی توزیع کلید کوانتومی در ادامه به توضیح مختصری در مورد کانال‌های ارتباطی و انواع مدل‌های رمزنگاری و سپس استراتژی های حمله می‌پردازیم.

کانال‌ها

کانال‌ها ابزاری پایه برای ارتباطات و رمزنگاری هستند، که به جهت برقراری ارتباط و انتقال پیام‌های خاص بین دو یا چند نفر مورد استفاده قرار می‌گیرند. برای مثال یک کانال ممکن است تنها برای انتقال

[۳] Quantum Channel
[۴] Public Channel
[۵] Man-in-the-middle Attack
[۶] Sifting Phase
[۷] Reconciliation Phase
[۸] Error Correction Phase
[۹] Noiseless Channel
[۱۰] Privacy Amplification
[۱۱] Authentication

پیام‌های کلاسیکی یا برای انتقال حالت‌های کوانتومی مورد استفاده قرار بگیرد. اما نکته مهم در مورد یک کانال ایمنی و مورد تأیید بودن آن از طرف دو شخص فرستنده(آلیس) و گیرنده(باب) پیام است. به این معنی که گیرنده‌ی پیام پس از دریافت آن بداند که این پیام از طرف آلیس است، و پیامی از طرف ایو یا همان جاسوس نیست.

در حالت کلی کانال‌ها ۲ دسته شنودکننده دارند. شنودکننده‌های مجاز یا همان کاربران قانونی یعنی آلیس و باب که می‌خواهند از طریق دو کانال کوانتومی(مورد استفاده برای انتقال فوتون‌ها یا حالت کوانتومی) و کانال کلاسیکی(برای اعلام پیام‌های مخابره شده بین اشخاص مجاز) امن با هم در ارتباط باشند و شنودکننده غیرمجاز یا همان جاسوس که می‌خواهد در مورد پیام‌های ارسال شده از کانال‌ها اطلاعات به دست آورد. البته به کانال‌های عمومی همه دسترسی دارند و شنودکننده غیرمجاز نیز نمی‌تواند مانع از ارتباط در این کانال شود، اما در مورد کانال کوانتومی جاسوس قادر است که مانع از انتقال فوتون ارسالی فرستنده از طریق کانال اصلی شده و آن را از طریق کانال مورد نظر خودش عبور دهد، و یا در کانال کوانتومی، برای دسترسی به اطلاعات یک سیگنال کمکی به سیستم اضافه کند و به این صورت استراتژهای مختلفی برای حمله فراهم کند که در ادامه به آن‌ها خواهیم پرداخت [۱۷].

۲.۲ طبقه‌بندی حملات شنود

به جهت اثبات امنیت پروتکل‌های QKD باید حملات شنود یا استراق سمع را مورد توجه قرار دهیم. زیرا یک شنودکننده یا جاسوس با در اختیار داشتن بالاترین سطح امکانات و تکنولوژی می‌تواند استراتژی‌های نامحدودی برای مقابله با پروتکل‌های QKD طراحی و اجرا کند و از این طریق امنیت پروتکل را به خطر بیندازد و مشکلاتی را در مسیر ارتباط کوانتومی ایجاد کند. البته این کارشکنی‌ها از طریق بروز خطاها برای کاربران قانونی آشکار می‌شود و آن‌ها پی به حضور شنودکننده می‌برند از این رو جاسوس به دنبال استفاده از روش‌های است که بتواند حمله به پروتکل توزیع کلید کوانتومی را پنهان نگه دارد، که می‌توان آن‌ها را به صورت زیر طبقه‌بندی کرد [۱۸].

✓ حمله‌های مستقل [۱۲] : نوعی از حمله که در آن جاسوس به هر سیگنال ارسالی از طرف فرستنده به صورت مستقیم حمله می‌کند. حمله‌ی سدسازی و بازارسال [۱۳] نمونه‌ای از این نوع حمله است.

✓ حمله‌های جمعی [۱۴] : حمله‌های جمعی یک نوع کلی از حملات شنود هستند. در این نوع حمله جاسوس با استفاده از یک سیستم کوانتومی کمکی که عموماً ترکیبی از یک سیگنال منفرد و یک فضای کمکی است به هر سیگنال ارسالی از طرف فرستنده حمله می‌کند و اجازه می‌دهد که این دو حالت(حالت کمکی و حالت ارسالی) با هم برهم‌کنش کنند. سپس او حالت اصلی را برای باب می‌فرستد و حالت کمکی را نزد خود نگه‌می‌دارد. وقتی که همه‌ی سیگنال‌ها انتقال داده شدند ایو صبر می‌کند تا بیشترین اطلاعات ممکن را از مکالمات عمومی بدست آورد تا بهترین اندازه‌گیری را روی حالت کمکی خودش انجام دهد.

---

[۱۲] Individual Attacks
[۱۳] Intercept-Resend Attack
[۱۴] Collective Attacks

✓ حمله‌های الحاقی [۱۵] :کلی‌ترین نوع حمله‌های جمعی حمله‌های الحاقی هستند. در این نوع حمله جاسوس مجاز به اعمال هر عملگر کوانتومی بر روی سیگنال انتقالی(حالت ارسالی بین آلیس و باب) و استفاده از هر حالت کمکی ممکنی است. به این معنی که در این نوع از حمله ایو به جای برهم‌کنش با هر سیگنال انتقالی به صورت مستقل، با تمام سیگنال‌های انتقالی به صورت یک سیستم کوانتومی منفرد برهم‌کنش می‌کند . سپس جاسوس هر دو حالت سیگنال منفرد و حالت کمکی خودش را به صورت یک سیستم منفرد در نظر گرفته و مکالمات عمومی بین آلیس و باب را شنود می‌کند و در مورد اندازه‌گیری بر روی حالت کمکی خودش تصمیم می‌گیرد [۱۱].

۳.۲ پروتکل‌های گسسته

پروتکل‌های گسسته حداقل یک اندازه‌گیری کوانتومی دارند که نتایج اندازه‌گیری‌ها معمولاً از یک مجموعه‌ی محدود گسسته ناشی می‌شود. به طور کلی، این پروتکل‌ها به صورت ایده‌آل بیت‌های کلاسیکی را در حالت‌های با بعد محدود رمزگذاری می‌کنند.

در این قسمت پروتکل‌های گسسته‌ای را که در آن‌ها از کیوبیت‌ها به عنوان حالت کوانتومی استفاده می‌شود و از طریق کانال کوانتومی ارسال می‌شوند را توصیف می‌کنیم [۱۹].

۱.۳.۲ پروتکل BB۸۴

$BB۸۴$ اولین پروتکل توزیع کلید کوانتومی است که توسط بنت [۱۶] و براسارد [۱۷] در ۱۹۸۴ ارائه شده‌است، واز این رو به نام $BB۸۴$ شناخته می‌شود. در این پروتکل، نه با تکیه برپیچیدگی مسائل ریاضی بلکه برپایه‌ی مکانیک کوانتومی، مبنای متفاوتی برای رمزنگاری کوانتومی معرفی شده است.

در پروتکل $BB۸۴$ از پلاریزاسیون پالس‌های نوری استفاده می‌شود، که هر پالس حاوی یک فوتون منفرد است. آلیس و باب بوسیله‌ی یک کانال کوانتومی مانند فیبرنوری و یک کانال کلاسیک عمومی مانند یک خط تلفن و یا اینترنت با هم در ارتباط هستند. در عمل این دو کانال همان لینک مشترک مورد استفاده آلیس و باب است، و البته تفاوت آن‌ها در شدت پالس‌های فوتون‌های نوری است: یعنی برای کانال کوانتومی یک فوتون در هر بیت و برای کانال کلاسیکی صدها فوتون در هر بیت وجود دارد.

در این پروتکل آلیس و باب به جهت یک ارتباط امن و کدگذاری کیوبیت‌ها از پلاریزاسیون فوتون‌ها در سه حالت یا پایه‌ی نامتعامد زیر استفاده می‌کنند:

پایه‌های افقی: $|\leftrightarrow\rangle = |۱\rangle$ پایه‌های عمومی: $|\updownarrow\rangle = |۰\rangle$

$$|۱\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{۲}} \qquad |۰\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{۲}}$$

و پایه‌های قطری $\pm ۴۵^\circ$:

[۱۵] Joint Attacks
[۱۶] Charles H. Bennett
[۱۷] Gilles Brassard

شکل ۱.۲: پروتکل BB۸۴

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

آلیس به صورت تصادفی و با احتمال برابر یکی از حالت‌های پلاریزاسیون $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ را برای هر فوتون انتخاب می‌کند، و پیش از ارسال حالت قطبش و مقدار بیت متناظر با هر حالت ارسالی را برای خودش ثبت می‌کند و در نهایت حالت متناظر با آن کیوبیت را برای باب ارسال می‌کند. باب نیز حالت کیوبیت دریافتی را به صورت تصادفی و با احتمال برابر در یکی از پایه‌های X یا Z، اندازه‌گیری می‌کند و پس از اندازه‌گیری، او نیز پایه انتخابی و بیت بدست آمده را برای خود ثبت می‌کند. اگر پایه‌های انتخابی آلیس و باب یکسان باشد آن‌ها نتایج حالت‌ها با پایه‌های یکسان را نزد خود نگه می‌دارند. در حالی که اگر پایه‌های انتخابی باب متفاوت با آلیس باشد او هیچ اطلاعاتی در مورد حالت فوتون بدست نخواهد آورد و این حالت‌ها کنار گذاشته می‌شوند. برای مثال، اگر آلیس پلاریزاسیون فوتون را افقی $|\longleftrightarrow\rangle$ انتخاب کند و باب در پایه‌های قطری اندازه‌گیری کند، با احتمال مساوی ۵۰٪ هر یک از پلاریزاسیون فوتون‌های $\pm ۴۵^\circ$ را بدست خواهد آورد. اما نکته مهم در این پروتکل آن است که اگر باب بعد از اندازه‌گیری متوجه شود که پایه را اشتباه انتخاب کرده است ، نمی‌تواند حالت پلاریزاسیون ارسالی آلیس را تعیین کند.

- **مراحل پروتکل $BB۸۴$:**

۱ـ آلیس به صورت تصادفی و با احتمال برابر برای هر بیت ارسالی یک قطبش در نظر می‌گیرد و قطبش متناظر با آن(دو حالت $|\circlearrowleft\rangle$ و $|+\rangle$ در پایه‌های خود بیانگر مقدار بیت ۰ و دو حالت $|\circlearrowright\rangle$ و $|-\rangle$ در پایه‌های خود بیانگر مقدار بیت ۱ هستند.) را از طریق کانال کوانتومی برای باب ارسال می‌کند.

۲ـ باب هم به صورت کاملاً مستقل و تصادفی و با احتمال برابر یکی از دو پایه X یا Z را برای اندازه‌گیری هر فوتون انتخاب می‌کند و در آن پایه اندازه‌گیری می‌کند.

۳ـ برای هر بیت باب از طریق کانال کلاسیکی عمومی، پایه‌های انتخابی و فوتونی را که ثبت کرده است را اعلام می‌کند. البته، باب نتیجه‌ای را که بدست آورده است را آشکار نمی‌کند.

۴ـ بعد از مقایسه پایه‌های انتخابی، آلیس و باب بیت‌های را که در پایه‌های یکسان اندازه‌گیری شده‌اند را نگه می‌دارند و بقیه بیت‌ها را کنار می‌گذارند، و چون پایه‌ها را به صورت تصادفی و با احتمال

برابر انتخاب می‌کنند با احتمال مساوی نتایج را یا درست و یا نادرست بدست می‌آورند. بنابراین، تقریباً ۵۰٪ از کلید اولیه یا کلید خام [۱۸] حذف می‌شود. بنابراین، طول کلید کوتاه‌تر می‌شود این کلید کوچک شده، ''کلید غربال شده'' [۱۹] نامیده می‌شود.

۵ـ آلیس و باب در مرحله‌ی تصحیح بعضی از بیت‌های باقی‌مانده را جهت بررسی میزان خطا به صورت تصادفی انتخاب و پس از بررسی آن‌ها را دور می‌ریزند. به دو دلیل می‌تواند میزان خطا متفاوت با مقدار انتظاری آن‌ها باشد: اشکال فنی در آشکارسازها و وجود شنودکننده پنهان. پس برای اطمینان در مورد کلید محرمانه، آلیس و باب باید خطاها را تصحیح کنند تا اطلاعات ایو یا همان شنودکننده پنهان را کاهش دهند و در نهایت رشته بیت باقی‌مانده همان ''کلید محرمانه'' [۲۰] است.

توجه کنید که کلید محرمانه واقعاً تصادفی است. چون نه آلیس و نه باب نمی‌توانند در مورد نتایج کلید تصمیم بگیرند، زیرا آن‌ها پایه‌ها را به صورت کاملاً تصادفی انتخاب می‌کنند [۱۵].

Alice's polar. states	$\nearrow$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$	$\searrow$	$\searrow$	$\updownarrow$	$\nearrow$	$\leftrightarrow$
Alice's bit value	1	0	0	1	0	0	0	1	1
Bob's basis	⊗	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕
Bob's measured states	$\nearrow$	$\nearrow$	$\updownarrow$	$\nearrow$	$\leftrightarrow$	$\searrow$	/	$\updownarrow$	$\leftrightarrow$
Bob's bit value	1	1	0	1	1	0	/	0	1
Same basis?	Y	N	Y	N	N	Y	/	N	Y
Bit sequence	1	/	0	/	/	0	/	/	1
Test Eve?	N	/	N	/	/	Y	/	/	N
Secret key	1		0						1

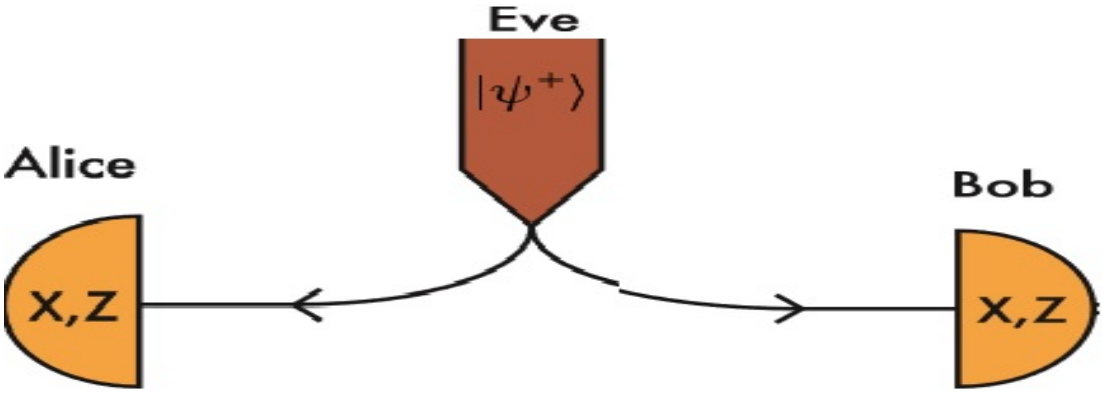
شکل ۲.۲: مراحل پروتکل BB۸۴

۲.۳.۲ پروتکل E۹۱

در سال ۱۹۹۱ آرتور ایکرت [۲۱] روش متفاوتی را برای توزیع کلید کوانتومی براساس درهم‌تنیدگی ذرات پیشنهاد کرد. که به پروتکل $E۹۱$ معروف است. براین اساس یک منبع ساطع کننده‌ی فوتون یک جفت کیوبیت در بیشینه حالت درهم‌تنیدگی مانند $|\psi^+\rangle = \frac{۱}{\sqrt{۲}}(|۰۱\rangle + |۱۰\rangle)$ را در پایه‌های بل [۲۲] تولید می‌کند، سپس آلیس یکی از کیوبیت‌ها و باب کیوبیت دیگر را می‌گیرد. در مراحل بعدی پروتکل مشابه پروتکل $BB۸۴$ است، یعنی آلیس و باب مشابه با این پروتکل به طور کاملاً تصادفی و با احتمال

[۱۸] Raw key
[۱۹] Sifted Key
[۲۰] Secret Key
[۲۱] Artur K. Ekert
[۲۲] Bell States

برابر یکی از پایه‌های X و Z را برای اندازه‌گیری انتخاب می‌کنند و سپس پایه‌های انتخابی را بررسی، و مراحل رسیدن به کلید محرمانه را مشابه با پروتکل $BB۸۴$ طی می‌کنند.



شکل ۳.۲: پروتکل E۹۱

به عبارتی می‌توان گفت: پروتکل ایکرت که در ارتباط مستقیم با پارادوکس EPR یا همان پروتکل انیشتین، پودولسکی و روزن [۲۳] است، به شرح زیر می‌باشد:

۱ـ یک منبع، یک جفت کیوبیت در بیشینه حالت درهم‌تنیدگی مانند $|\psi^+\rangle$ را ساطع می‌کند.

$$|\psi^+\rangle = \frac{۱}{\sqrt{۲}}(|۰۱\rangle + |۱۰\rangle)$$

۲ـ آلیس و باب قطبش را در چهار زاویه‌ی $۰^\circ, \pm ۴۵^\circ, ۹۰^\circ$ اندازه‌گیری می‌کنند.

۳ـ بعد از انتقال کیوبیت‌ها، آلیس و باب پایه‌های انتخابی برای اندازه‌گیری را اعلام عمومی می‌کنند. از نتایج اندازه‌گیری هر یک از آن‌ها سه گروه تشکیل می‌شود:

- گروه اول: متشکل از اندازه‌گیری در پایه‌های متفاوت
- گروه دوم: متشکل از اندازه‌گیری در پایه‌های مشابه
- گروه سوم: نتایج اندازه‌گیری‌های که در آن حداقل یکی از آن دو به یکی از دلایل اشکال فنی در آشکارسازها و یا وجود شنودکننده موفق به ثبت فوتونی نشده‌اند.

توجه کنید که از نتایج گروه اول برای تست نامساوی بل و از نتایج گروه دوم برای ساختن کلید محرمانه استفاده می‌شود. در حالی که نتایج گروه سوم دور ریخته می‌شود.

۴ـ در نهایت، آلیس و باب نتایج گروه اول را اعلام عمومی می‌کنند. بنابراین ، آن‌ها می‌توانند وجود شنودکننده را بررسی کنند، به این معنی که اگر شنودکننده‌ای نباشد سیستم آشفتگی یا اختلال ندارد، و نامساوی برقرار است و درهم‌تنیدگی بین ذرات از بین نرفته‌است، و در آخر آلیس و باب می‌توانند از اندازه‌گیری‌های گروه دوم رشته بیت محرمانه یا همان کلید رمز را بدست آورند [۱۱].

[۲۳] Albert Einstein, Boris Podolsky and Nathan Rosen

۳.۳.۲ نسخه‌های از BB۸۴

انواع متفاوتی از پروتکل $BB۸۴$ وجود دارد. دو مثال مهم پروتکل شش حالته [۲۴] [۲۰] و پروتکل $SARG$ [۲۵] [۲۱] هستند.

پروتکل شش حالته شکلی از پروتکل $BB۸۴$ برای چهار حالت $\{|۰\rangle, |۱\rangle, |+\rangle, |-\rangle\}$ است، که با اضافه کردن دو حالت

$$|-i\rangle := \left(\frac{|۰\rangle - i|۱\rangle}{\sqrt{۲}}\right) \qquad |i\rangle := \left(\frac{|۰\rangle + i|۱\rangle}{\sqrt{۲}}\right)$$

حاصل می‌شود که $\{|-i\rangle, |i\rangle\}$ پایه‌های Y هستند و Y مجموعه‌ای از ویژه بردارهای ماتریس پائولی است که به صورت زیر تعریف می‌شود:

$$\sigma_Y = \begin{pmatrix} ۰ & -i \\ i & ۰ \end{pmatrix} \tag{۱.۲}$$

پروتکل شش حالته از پروتکل $BB۸۴$ کارآمدتر است زیرا تعداد پایه‌های اندازه‌گیری به سه پایه‌ی X, Y, Z افزایش یافته است [۲۰]، پس باب می‌تواند یکی از سه پایه را به صورت تصادفی و با احتمال یکسان برای اندازه‌گیری انتخاب کند، همچنین آلیس و باب می‌توانند پس از مرحله‌ی غربال کردن پایه‌ها هر اندازه‌گیری را که پایه‌های هر دو یکسان نیستند را کنار بگذارند.

اما پروتکل $SARG$ به عنوان یک جایگزین برای پروتکل $BB۸۴$ معرفی شد تا حمله‌ای را که ایو به پروتکل $BB۸۴$ انجام می‌دهد را خنثی کند [۲۲، ۲۳، ۲۴، ۲۵]. پروتکل $SARG$ مشابه با پروتکل $BB۸۴$ عمل می‌کند به جز آن که در این پروتکل نقش حالت‌ها و پایه‌ها معکوس شده است. اگر آلیس حالتی را در پایه‌ی Z ارسال کند معرف بیت ۰ و اگر حالتی را در پایه‌ی X ارسال کند معرف بیت ۱ خواهد بود و رشته بیت باب رشته‌ای پیچیده خواهد بود که در ادامه توضیح داده خواهد شد.

بنابراین بیت ارسالی آلیس شامل پایه Z (۰) و پایه X (۱) خواهد بود، بنابراین انتخاب آلیس یکی از حالات $\{|۰\rangle, |-\rangle\}$،$\{|۰\rangle, |+\rangle\}$،$\{|۱\rangle, |-\rangle\}$،$\{|۱\rangle, |+\rangle\}$ خواهد بود. از آنجایی که این مجموعه‌ها تعدادی حالت مشترک دارند، آلیس بطور یکسان و تصادفی مجموعه‌ای را انتخاب می‌کند که با حالت ارسالی او سازگار باشد و سپس مجموعه انتخابی را به باب اعلام می‌کند. بنابراین باب می‌تواند حالت ارسالی آلیس را با احتمال $\frac{۱}{۲}$ مشخص کند. برای مثال، اگر آلیس مجموعه‌ای $\{|۰\rangle, |+\rangle\}$ را انتخاب کند و حالت $|+\rangle$ را ارسال کره باشد، و باب در پایه‌ی Z اندازه‌گیری کند و نتیجه $|۱\rangle$ را بدست‌آورد، او می‌داند که آلیس باید حالت $|+\rangle$ را ارسال کرده باشد، و بنابراین باب بیت ۱، را ثبت می‌کند. بطور مشابه اگر آلیس حالت $|۰\rangle$ را از همان مجموعه‌ی اعلام شده‌ی قبلی ارسال کند، و باب در پایه‌ی X اندازه‌گیری کند ونتیجه‌ی $|-\rangle$ را بدست‌آورد، او می‌داند که آلیس باید حالت $|۰\rangle$ را ارسال کرده‌باشد، بیت ۰، را ثبت می‌کند.

در ادامه آلیس و باب مانند پروتکل $BB۸۴$ مرحله‌ی غربال پایه‌ها را انجام می‌دهند. اگر نتیجه‌ای که باب از اندازه‌گیری بدست می‌آورد در مجموعه‌ی اعلام شده‌ی آلیس نباشد، این مرحله بی‌نتیجه

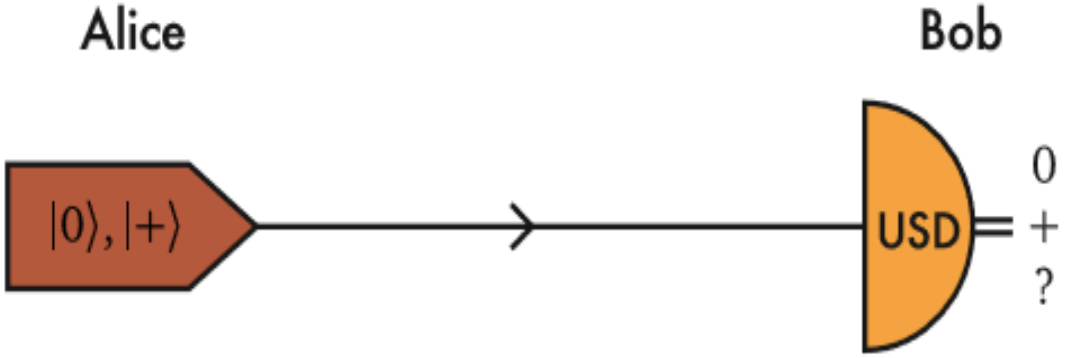
[۲۴] six-state protocol

[۲۵] Valerio Scarani, Antonio Acin,Gregoire Ribordy and Nicolas Gisin

است(مانند بدست‌آوردن نتیجه‌ی $|۰\rangle$ از همان مجموعه‌ی اعلام شده $\{|۰\rangle, |+\rangle\}$). پس باب به آلیس اعلام می‌کند و آن‌ها نتیجه‌ی این اندازه‌گیری را کنار می‌گذارند.

۴.۳.۲ پروتکل B۹۲

پروتکل $B۹۲$ یا پروتکل BBM نوع دیگری از پروتکل $BB۸۴$ است که در سال ۹۲ توسط بنت و براسارد و مرمین [۲۶] ارائه شد [۲۳]. $B۹۲$ پروتکلی پیشرفته‌تر نسبت به پروتکل $BB۸۴$ است که تنها به دلیل استفاده از دو حالت غیر متعامد $|+\rangle$ و $|۰\rangle$ با پروتکل $BB۸۴$ متفاوت است(شکل (۴.۲) را ببینید). البته گاهی اوقات دو حالت غیرمتعامد غیر از $|+\rangle$ و $|۰\rangle$ استفاده می‌شوند، اما در اینجا ما برای سادگی از



شکل ۴.۲: پروتکل B۹۲

دو حالت $|+\rangle$ و $|۰\rangle$ استفاده می‌کنیم. همچنین، در این پروتکل باب فقط یک اندازه‌گیری ساده انجام می‌دهد،او پایه‌ای را انتخاب نمی‌کند، به این معنی که در این پروتکل نیازی به مرحله‌ی غربال پایه‌ها نیست.

اندازه‌گیری باب یک حالت مشخص و تمیزپذیراست [۲۶]، که برای حالت‌های $|+\rangle$ و $|۰\rangle$ اندازه‌گیری باب بوسیله‌ی سه عملگر اندازه‌گیری مثبت $(POVM)$ [۲۷]

$$F_۰ = \frac{\sqrt{۲}}{۱+\sqrt{۲}}|-\rangle\langle -| \qquad F_۱ = \frac{\sqrt{۲}}{۱+\sqrt{۲}}|۱\rangle\langle ۱| \qquad F_? = ۱ - F_۰ - F_۱ \qquad (۲.۲)$$

توضیح داده‌می‌شود(F_m مجموعه‌ای از عملگرهای خطی و مثبت هستند که باید در شرط $\sum_m F_m = I$ صدق کنند).

با این اندازه‌گیری، باب می‌داند که چه وقت نتیجه‌ی ۰ را بدست می‌آورد، پس نمی‌تواند حالت $|+\rangle$ را داشته باشد، چون حالت‌های $|+\rangle$ و $|-\rangle$ متعامد هستند($\langle +|-\rangle = ۰$). به طور مشابه وقتی که باب نتیجه‌ی ۱ را بدست می‌آورد، او نمی‌تواند حالت $|۰\rangle$ را داشته باشد. همچنین اگر باب نتیجه را مبهم یعنی "?" بدست آورد پس او نمی‌داند که چه حالتی را دریافت کرده است. اما باب تعدادی از این

[۲۶] Mermin
[۲۷] Positive operator valued measure

نتایج اندازه‌گیری را نگه می‌دارد، زیرا این نتایج ("?") برای کشف حضور جاسوس مهم هستند. چون جاسوس تنها می‌تواند یک اندازه‌گیری مشابه با باب و قبل از او انجام دهد، و همیشه نتیجه‌ای را که باب از اندازه‌گیری بدست خواهد آورد می‌داند. بنابراین، اگر جاسوس اندازه‌گیری مشابه‌ای با باب انجام دهد، باب نتایج تعداد زیادی از اندازه‌گیری‌ها را به صورت ("?") بدست خواهد آورد، پس باب نتیجه‌ی اندازه‌گیری حالت‌های را که ("?") بدست می‌آورد را به آلیس اعلام می‌کند تا آلیس این رشته بیت‌ها را کنار بگذارد، و اگر تعداد پیشامدهای ("?") بیش‌تر از حد معینی باشد پروتکل آلیس و باب بی‌نتیجه خواهد ماند.

در مقابل پروتکل‌های توزیع کلید کوانتومی، جاسوس نیز استراتژی‌های برای حمله انتخاب می‌کند که در ادامه به تشریح آن‌ها خواهیم پرداخت.

۴.۲ مقدمه‌ای بر استراتژای‌های حمله

براساس مقدار اطلاعاتی که جاسوس از کلید محرمانه‌ی مشترک بین آلیس و باب بدست می‌آورد حمله به پروتکل QKD تعریف می‌شود. البته هدف آلیس و باب کم کردن مقدار این اطلاعات برای جاسوس است. معمولاً اطلاعات جاسوس از کلید محرمانه شامل دو قسمت است: اطلاعاتی که از اندازه‌گیری روی سیگنال انتقالی بدست آورده و اطلاعاتی که در مورد پایه‌های انتخابی آلیس و باب بدست آورده است. قسمت دوم نشان می‌دهد که آیا جاسوس اندازه‌گیری صحیحی بر روی کیوبیت مربوطه انجام داده است یا خیر؟ پس بهترین روش برای بیان آن، استفاده از احتمال شرطی $p(s|m)$ است. در این‌جا s، مقدار بیت فرستاده شده‌ی آلیس و m مقدار بیت بدست آمده از اندازه‌گیری جاسوس است. مقدار $p(s|m)$ را می‌توان به سادگی و با استفاده از احتمال $p(m|s)$ محاسبه کرد. احتمال شرطی $p(m|s)$ یعنی این که جاسوس نتیجه‌ی m را بدست آورد در صورتی که آلیس بیت s را فرستاده باشد، پس احتمال $p(s|m)$ با استفاده از فرمول زیر بدست می‌آید:

$$p(s|m) = \frac{p(m|s)}{\sum_{s'} p(m|s')} \qquad (۳.۲)$$

کمیت مورد توجه بعدی، احتمال آن است که جاسوس نتیجه‌ی مشابه‌ای با آلیس بدست آورد که احتمال برخورد نامیده می‌شود.

$$p_c(s|m) = \sum_s p(s|m)^۲ \qquad (۴.۲)$$

چشمداشتی احتمال برخورد، از اندازه‌گیری جاسوس برروی تمام m خروجی ممکن به صورت زیر تعریف می‌شود:

$$\langle p_c \rangle = \sum_m p(m) p_c(s|m) \qquad (۵.۲)$$

مقدار اطلاعات جاسوس از بیت آلیس با استفاده از دو آنتروپی، یکی آنتروپی شانون [۲۸] (H)، و دیگری آنتروپی رینی [۲۹] (R) ، مشخص می‌شود. البته این اطلاعات به نتیجه‌ی اندازه‌گیری جاسوس بستگی دارد، و به ترتیب با استفاده از نسخه شرطی این دو آنتروپی یعنی $H(S|M)$ و $R(S|M)$ قابل محاسبه است. آنتروپی شانون تعریف می‌شود:

$$H(S|M=m) = -\sum_{m} p(s|m)\log p(s|m) \qquad (۶.۲)$$

و از آنتروپی شانون روی احتمال‌های نتایج جاسوس میانگین گرفته می‌شود:

$$H(S|M) = \sum_{m} p(s|m)H(S|M=m) \qquad (۷.۲)$$

به طور مشابه آنتروپی رینی تعریف می‌شود:

$$R(S|M=m) = -\log p_c(s|m) = -\log \sum_{s} p(s|m)^{۲} \qquad (۸.۲)$$

و میانگین احتمالات خواهد بود:

$$R(S|M) = \sum_{m} p(m)R(S|M=m) \qquad (۹.۲)$$

با استفاده از آنتروپی شانون می‌توان عدم قطعیت یک توزیع احتمال را تخمین زد و بنابراین اختلاف آنتروپی شانون را می‌توان به عنوان اطلاعات بدست آمده تفسیر کرد. برای توزیع احتمال اولیه‌ی X و توزیع احتمال بعدی Y، اطلاعات بدست آمده به صورت

$$I = H(X) - H(Y) \qquad (۱۰.۲)$$

است، که می‌توان آن را به عنوان مقدار اطلاعات بدست آمده برای جاسوس در حمله‌های مشخص توصیف کرد. در این قسمت چون آلیس رشته بیت خودش را به صورت تصادفی انتخاب می‌کند جاسوس اطلاعات اولیه‌ای از کلید محرمانه ندارد و بنابراین $H = ۱$ است. از این رو مقدار اطلاعاتی که جاسوس پس از اجرای پروتکل بدست خواهد آورد $I = ۱ - H(S|M)$ است.

سؤال مهم بعدی این است که چه مقدار از کلید باید حذف شود تا اطلاعات جاسوس از کلید مینیمم شود؟ این مقدار بخش حذف شدنی τ نامیده می‌شود و با استفاده از مقدار چشمداشتی احتمال برخورد قابل محاسبه است [۲۷].

$$\tau = ۱ + \log\langle p_c\rangle^{\frac{۱}{n}} \qquad (۱۱.۲)$$

براساس این معادله یک رشته بیت با طول n باید در طی مرحله‌ی تقویت محرمانگی به $n\tau$ بیت کاهش یابد تا حداکثر جاسوس ۱ بیت از کل کلید (اطلاعات کلید) را بدون توجه به طول آن در اختیار داشته باشد [۱۱].

[۲۸] Shannon Entropy
[۲۹] Renyi Entropy

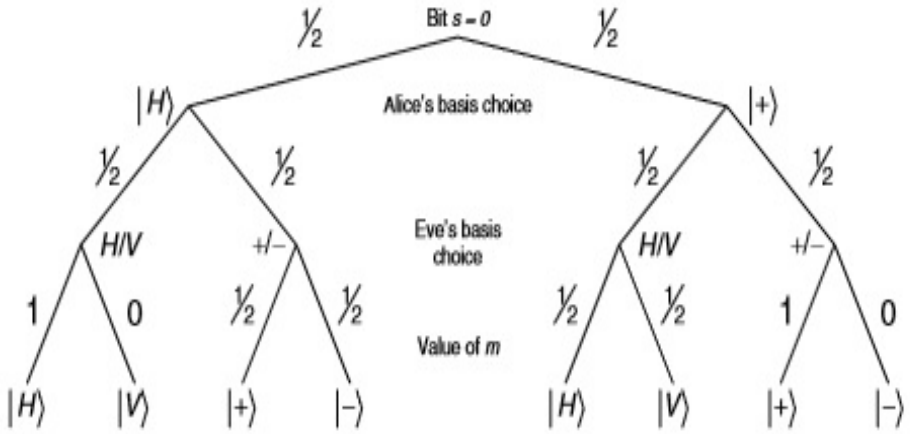
۵.۲ استراتژای حمله در یک محیط واقعی

حمله‌ی سدسازی و باز ارسال ساده

از رایج‌ترین نوع حمله‌های مستقل، حمله‌ی سدسازی و بازارسال ساده [۳۰] را می‌توان نام برد که در این نوع حمله هدف جاسوس آن است که هر فوتون ارسال شده از طرف آلیس را نزد خود نگه داشته و آن را در پایه‌ای از پیش تعریف شده اندازه‌گیری کند و سپس با توجه به نتیجه بدست آمده یک فوتون جدید آماده و آن را برای باب ارسال کند. به طور کلی کیوبیت آلیس در هر یک از پایه‌های افقی، عمودی و قطری، یعنی در یکی از این چهار حالت $|H\rangle$ ، $|V\rangle$، $|+\rangle$ یا $|-\rangle$ خواهد بود.

$$|+\rangle = \frac{۱}{\sqrt{۲}}(|H\rangle + |V\rangle) \qquad |-\rangle = \frac{۱}{\sqrt{۲}}(|H\rangle - |V\rangle) \tag{۱۲.۲}$$

آلیس برای فرستادن بیت صفر با احتمال مساوی آن را در پایه‌های $|H\rangle$ یا $|+\rangle$ کدگذاری می‌کند، جاسوس بدون اطلاع از کدگذاری آلیس به صورت تصادفی بین پایه‌های V/H و $+/-$ انتخاب خواهد کرد. بنابراین، اگر آلیس در پایه‌ی $|H\rangle$ بیت را بفرستد و جاسوس در پایه‌های H/V اندازه‌گیری کند و یا آلیس در پایه‌ی $|+\rangle$ بیت را ارسال کند و جاسوس در پایه‌های $+/-$ اندازه‌گیری کند نتیجه‌ای درست بدست خواهد آورد. هر ترکیب دیگری، خروجی اندازه‌گیری کاملاً تصادفی را نتیجه خواهد داد.



شکل ۵.۲: استراتژی حمله‌یI&R

حالا فرض کنید که جاسوس به مکالمه‌ی عمومی بین آلیس و باب گوش نمی‌کند. بنابراین او نمی‌داند در چه مواردی اندازه‌گیریش اشتباه است. پس برای احتمال شرطی $p(m|s)$ چهار نتیجه ممکن به صورت زیر است:

$$p(m = |H\rangle|s = ۰) = p(m = |+\rangle|s = ۰) = (\frac{۱}{۲})^۳ + (\frac{۱}{۲})^۲(۱) = \frac{۳}{۸} \tag{۱۳.۲}$$

[۳۰] Naive Intercept and Resend

$$p(m=|V\rangle|s=۰)=p(m=|-\rangle|s=۰)=(\frac{۱}{۲})^۳+(\frac{۱}{۲})^۲(۰)=\frac{۱}{۸}$$

و برای $p(m|s=۱)$ نیز نتایج به همین صورت قابل محاسبه است. به ازای احتمالات شرطی $p(s|m)$ مجموع $\sum_s p(m|s)=\frac{۱}{۲}$، ما $p(s|m)=۲p(m|s)$ بدست می‌آوریم. بنابراین، احتمال برخورد در نسخه ساده حمله‌ی $I\&R$ به صورت زیر است:

$$P_c(s|m=|H\rangle)=(\frac{۳}{۴})^۲+(\frac{۱}{۴})^۲=\frac{۵}{۸} \qquad (۱۴.۲)$$

به همین ترتیب برای $m=|V\rangle$، $m=|+\rangle$ و $m=|-\rangle$ نتایج میانیگن احتمال برخورد به صورت زیر محاسبه می‌شود:

$$\langle P_c\rangle=\sum_m \frac{۱}{۴}P_c(s|m)=۴(\frac{۱}{۴})[(\frac{۱}{۴})^۲+(\frac{۳}{۴})^۲]=\frac{۵}{۸} \qquad (۱۵.۲)$$

در نتیجه می‌توان قسمت حذفی از احتمال برخورد را به صورت $۱+\log\langle P_c\rangle$ محاسبه کرد. که در نتیجه‌ی آن $\tau\simeq ۰٫۳۲۲$ است. به این ترتیب، تنها $\frac{۱}{۳}$ از کلید باید حذف شود و این تضمین می‌کند که جاسوس کمتر از یک بیت اطلاعات از کل کلید دارد.

با نگاهی به آنتروپی شرطی شانون برای $M=|H\rangle$ این نتایج را بدست خواهیم آورد:

$$H(S|M=|H\rangle)=-\frac{۳}{۴}\log\frac{۳}{۴}-\frac{۱}{۴}\log\frac{۱}{۴}=۰٫۸۱۱ \qquad (۱۶.۲)$$

آنتروپی‌های دیگر $H(S|M=|V\rangle)$، $H(S|M=|+\rangle)$، $H(S|M=|-\rangle)$ برابر است با:

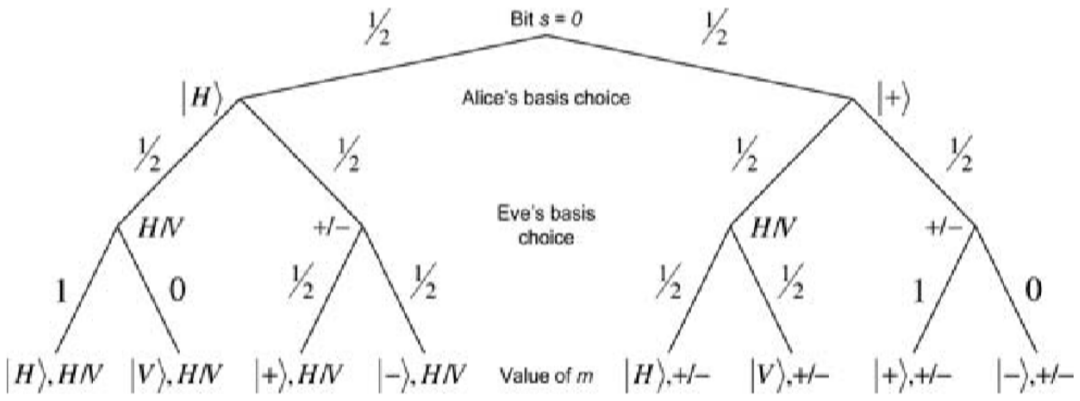
$$H(S|M)=\sum_m(\frac{۱}{۴}H(S|M=m)=۴\frac{۱}{۴}(-\frac{۳}{۴}\log\frac{۳}{۴}-\frac{۱}{۴}\log\frac{۱}{۴})=۰٫۸۱۱ \qquad (۱۷.۲)$$

کل اطلاعاتی که جاسوس در نهایت از هر بیت خواهد داشت: $۱-H(S|M)\backsimeq ۰٫۲$ است که نتیجه نامطلوبی برای جاسوس است. بنابراین، جاسوس از استراتژی‌های دیگری برای بدست آوردن اطلاعات بیشتر استفاده خواهد کرد.

حمله‌ی سدسازی و باز ارسال کامل

در حمله‌های نوع سدسازی و بازارسال کامل [۳۱] جاسوس یکی از پایه‌های H/V و $+/-$ را به صورت تصادفی انتخاب می‌کند تا فوتون‌های دریافت شده از طرف آلیس را اندازه‌گیری کند. سپس نتایج خود را برای آلیس ارسال می‌کند و مکالمه‌ی عمومی بین آلیس و باب در مرحله‌ی تصفیه(غربال) را شنود می‌کند. فرض کنید که آلیس بیت ۰ را به صورت $|H\rangle$ کدگذاری و ارسال می‌کند، حال اگر جاسوس با پایه H/V اندازه‌گیری کند مطمئناً نتیجه‌ی $|H\rangle$ را بدست خواهد آورد و هیچ خطای از خود باقی نخواهد گذاشت. در صورتی که اگر پایه انتخابی جاسوس $+/-$ باشد به احتمال مساوی هر یک از نتایج $|+\rangle$ یا $|-\rangle$ را از اندازه‌گیری بدست خواهد آورد.

[۳۱] Full Intercept and Resend



شکل ۶.۲: استراتژی حمله‌ی سدسازی و بازارسال کامل

مقایسه نمودار دو شکل (۵.۲) و (۶.۲) نشان می‌دهد که جاسوس می‌تواند دو پیشامد موجود برای $S = ۰$ را حذف کند، به این معنی که احتمال بدست آوردن حالت $|V\rangle$ در صورتی که آلیس از پایه‌های H/V استفاده کرده باشد و احتمال بدست آوردن حالت $|-\rangle$ در صورتی که از پایه‌های $+/-$ استفاده کرده باشد، صفر است. آگاهی از این احتمال موجب افزایش اطلاعات جاسوس در مقایسه با حمله‌ی $I\&R$ می‌شود. به طور جزئی احتمالات شرطی $p(m|s)$ برابرند با:

$$p\Big(m = (|H\rangle, H/V)|s = ۰\Big) = (\frac{۱}{۲})^۲(۱) = \frac{۱}{۴} = p\Big(m = (|+\rangle, +/-)|s = ۰\Big) \quad (۱۸.۲)$$

$$p\Big(m = (|V\rangle, H/V)|s = ۰\Big) = (\frac{۱}{۲})^۲(۰) = ۰ = p\Big(m = (|-\rangle, +/-)|s = ۰\Big)$$

$$p\Big(m = (|+\rangle, H/V)|s = ۰\Big) = (\frac{۱}{۲})^۳ = \frac{۱}{۸} = p\Big(m = (|H\rangle, +/-)|s = ۰\Big)$$

$$p\Big(m = (|-\rangle, H/V)|s = ۰\Big) = (\frac{۱}{۲})^۳ = \frac{۱}{۸} = p\Big(m = (|V\rangle, +/-)|s = ۰\Big)$$

و مقادیر مشابهی برای $s = ۱$ بدست می‌آید. به صورتی که برای مجموع $p(m|s)$ خواهیم داشت؛ $\sum_s p(m|s) = \frac{۱}{۴}$ و برای $p(s|m) = ۴p(m|s)$ است. با توجه به این نتایج احتمال برخورد ۱ است، اگر جاسوس در پایه‌های درست اندازه‌گیری کند و اگر جاسوس پایه‌های متفاوتی با پایه‌های آلیس انتخاب کند نتیجه $\frac{۱}{۲}$ است. به این ترتیب احتمال برخورد میانگین خواهد بود:

$$\langle P_c\rangle = \frac{۱}{۴} + (۴)\frac{۱}{۱۶} + \frac{۱}{۴} = \frac{۳}{۴} \quad (۱۹.۲)$$

و احتمال برخورد میانگین برای آنتروپی شانون ۰ است، اگر جاسوس پایه‌ها را یکسان با آلیس انتخاب کند، و در غیر این صورت $\frac{۱}{۲}$ است. بنابراین آنتروپی شانون میانگین خواهد بود:

$$H(S|M) = ۴(\frac{۱}{۸}) = \frac{۱}{۲} \quad (۲۰.۲)$$

با این استراتژی حمله جاسوس نسبت به حمله‌ی $I\&R$ ساده اطلاعات بیشتری بدست می‌آورد [۱۱].

۶.۲ حمله در پایه‌ی درهم‌تنیدگی

۱.۶.۲ پروتکل مشابه BB۸۴

استراتژی دیگر برای جاسوس استفاده از درهم‌تنیدگی برای برهم کنش با سیگنال ارسالی توسط آلیس است. در این مورد جاسوس برای هر سیگنال یک حالت کمکی آماده می‌کند و این حالت کمکی را با سیگنال ارسالی درهم‌تنیده می‌کند وسپس سیگنال اصلی را برای باب ارسال می‌کند. بعد از آن، جاسوس قادر به انجام اندازه‌گیری یا اعمال هر عملگر کوانتومی دیگری بر روی حالت کمکی خود است تا اطلاعاتی در مورد سیگنال اصلی بدست آورد.

با توجه به پروتکل $BB۸۴$ یک استراتژی ساده برای جاسوس استفاده از یک زوج درهم‌تنیده در یکی از حالت‌های بل است.

$$|\varphi^{\pm}\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰۰\rangle \pm |۱۱\rangle\Big) \qquad |\psi^{\pm}\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰۱\rangle \pm |۱۰\rangle\Big) \tag{۲۱.۲}$$

جاسوس یک اندازه‌گیری در پایه‌ی بل بر روی فوتون رسیده از طرف آلیس و یکی از فوتون‌های درهم‌تنیده‌ی خودش انجام می‌دهد. تا با توجه به آن‌چه که گفته شد اطلاعاتی در مورد سیگنال اصلی بدست آورد. این کار معادل با یک طرح دوربری کوانتومی [۳۲] است که حالت یک سیگنال ناشناخته به حالت کمکی جاسوس دوربری می‌شود.

$$\begin{aligned}&(\alpha|H\rangle + \beta|V\rangle)\,\frac{۱}{\sqrt{۲}}(|HH\rangle + |VV\rangle) = \\ &\frac{۱}{۲}\Big(|\varphi^{+}\rangle(\alpha|H\rangle + \beta|V\rangle) + |\varphi^{-}\rangle(\alpha|H\rangle - \beta|V\rangle) \\ &+ |\psi^{+}\rangle(\alpha|V\rangle + \beta|H\rangle) + |\psi^{-}\rangle(\alpha|V\rangle - \beta|H\rangle\Big)\end{aligned} \tag{۲۲.۲}$$

جاسوس می‌تواند حالت کمکی خود را نگه دارد تا زمانی که آلیس پایه‌ی انتخابی خود را آشکار کند و سپس جاسوس آن را در پایه درست اندازه‌گیری کند و تمام اطلاعات را بدست آورد. با در نظر گرفتن احتمال برخورد میانیگن و اطلاعات شانون جاسوس در مورد بیت آلیس خواهیم دید که:

$$\langle P_c\rangle = ۱ \qquad ۱ - H(S|M) = ۱ \tag{۲۳.۲}$$

و این یعنی جاسوس تمام اطلاعات در مورد بیت ارسالی آلیس را دارد. هر چند سیگنالی را که جاسوس برای باب ارسال می‌کند یک زیر سیستم از حالت بل است، اما سیگنال همه‌ی اطلاعاتش در مورد پایه‌ی انتخابی آلیس را از دست داده است و در یک حالت کاملاً مخلوط است. بنابراین باب در هر یک از دو پایه H/V یا $+/-$ اندازه‌گیری کند نتیجه‌ای کاملاً تصادفی بدست می‌آورد که به سهولت از احتمال برخورد میانگین باب قابل مشاهده است $\langle P_c\rangle = \frac{۱}{۲}$. بنابراین آلیس و باب در مرحله‌ی تصفیه، خطای بیشتری را آشکار می‌کنند(تقریباً ٪۵۰) و بنابراین پروتکل بی‌نتیجه باقی می‌ماند.

[۳۲] Quantum Teleportation Scheme

همان طور که می‌بینیم جاسوس با استفاده از استراتژی حمله تمام اطلاعات در مورد بیت آلیس را بدست می‌آورد. اما احتمال برخورد میانگین با استراتژی حمله‌ی سدسازی و بازارسال کامل مشابه است. بنابراین، با این استراتژی حمله جاسوس نمی‌تواند اطلاعات بیشتری بدست آورد.

۲.۶.۲ حمله‌ی کنترلی CNOT

اما اگر آلیس و باب از حالت‌های درهم‌تنیده مانند پروتکل $E۹۱$ برای ارتباط استفاده کنند، چه می‌شود؟ یک استراتژی برای جاسوس در این مورد آن است که حالت کمکی خود را در حالت $|H\rangle$ آماده کند و عملگر کنترلی NOT $(CNOT)$ را بر روی سیگنال و حالت کمکی خودش اعمال کند.

$$CNOT_{۱۲} = |H\rangle\langle H|\otimes I + |V\rangle\langle V|\otimes(|۰\rangle\langle ۱|+|۱\rangle\langle ۰|) \qquad (۲۴.۲)$$

عملگر $(CNOT)$ یک عملگر کوانتومی است که بر روی دو کیوبیت، منبع و کیوبیت هدف عمل می‌کند. اگر حالت کیوبیت منبع $|V\rangle$ باشد، عملگر NOT یا عملگر بیت برگردان بر روی کیوبیت هدف اثر می‌کند. توجه کنید به اندیس‌های که در معادله‌ی (۲۴.۲) است. اندیس اول، نشان دهنده‌ی کیوبیت منبع و اندیس دوم نشان دهنده‌ی کیوبیت هدف است. این ساده است اگر عملگر $(CNOT)$ را بر روی یک حالت مرکب با بیش از دو کیوبیت برای اجتناب از اشتباه بکار ببریم. با اعمال عملگر $CNOT$ بر روی سیگنال دریافتی از آلیس حالت کمکی جاسوس به صورت زیر تغییر خواهد کرد:

$$CNOT_{۲۳}(|\varphi^+\rangle_{۱۲}\otimes|H\rangle_{۳}) = \frac{۱}{\sqrt{۲}}(|HHH\rangle_{۱۲۳} + |VVV\rangle_{۱۲۳}) \qquad (۲۵.۲)$$

نتیجه حالت، یک حالت GHZ است با خاصیتی ویژه که اگر یکی از فوتون‌ها اندازه‌گیری شود دو فوتون دیگر سریعاً به حالتی مشخص مربوط به نتیجه اندازه‌گیری رمبش [۳۳] می‌کنند. در مورد معادله‌ی (۲۵.۲) اگر آلیس در پایه‌های H/V اندازه‌گیری کند و باب و جاسوس هم در همان پایه اندازه‌گیری کنند، نتیجه‌ای مشابه با آلیس بدست خواهند آورد. در مواردی که آلیس از پایه‌های $+/-$ استفاده کند، نتیجه‌ی اندازه‌گیری باب در پایه‌ی مشابه در ۵۰٪ موارد با نتیجه‌ی آلیس متناظر نخواهد بود. این به این معنی است که اگر آلیس و باب در پایه‌های H/V اندازه‌گیری کنند احتمال برخورد و اطلاعات شانون به شکل زیر خواهد بود:

$$\langle P_c\rangle = ۱ \qquad ۱ - H(S|M) = ۱ \qquad (۲۶.۲)$$

و اگر پایه‌های $+/-$ انتخاب شوند، باب نتیجه‌ی مشابه با آلیس را با احتمال $\langle P_c\rangle = \frac{۱}{۲}$ بدست می‌آورد. بنابراین همه‌ی اطلاعاتی که جاسوس از بیت محرمانه بدست می‌آورد $۱ - H(S|M) = ۰/۷۵$ است، که به طور قابل توجهی در مقایسه با استراتژی $I\&R$ بیشتر است. با این وجود، هر زمان که آلیس و باب پایه‌های $+/-$ را استفاده کنند خطا با احتمال $\frac{۱}{۲}$ مشخص می‌شود. بروز عدم تعادل ناشی از خطا به سادگی باعث می‌شود که آلیس و باب حضور جاسوس را تشخیص دهند.

[۳۳] Collapse

۷.۲ حمله‌های مستقل در محیط‌های واقعی

پروتکل‌ها و حمله‌های توصیف شده در بخش‌های قبلی با فرض حضور در یک محیط ایده‌آل بودند. به این معنی که منابع ساطع کننده فوتون تنها سیگنال‌های تک فوتون را گسیل می‌کنند و بازده آشکارسازها ۱۰۰٪ است. اما با توجه به شرایط تکنولوژی امروز استفاده از چنین مجموعه‌های غیر ممکن است. زیرا آشکارسازها خیلی حساس هستند و اغلب بدون این که حتی هیچ فوتونی ارسال شده باشد کیلیک می‌کنند(این پدیده را شمارش تاریک [۳۴] می‌نامند). این پدیده در مرحله‌ی تصحیح خطا و تقویت محرمانگی(افزایش حریم خصوصی) مشخص می‌شود.

علاوه براین هیچ منبع گسیل کننده تک فوتونی وجود ندارد، از طرفی یک پالس سیگنال معمولی اغلب شامل تعداد زیادی فوتون است. این مشکل با استفاده از پالس‌های همدوس ضعیف (WCP) [۳۵] در دستگاه‌های رمزنگاری کوانتومی واقعی حل می‌شود، و به صورت زیر توصیف می‌شوند:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \qquad (۲۷.۲)$$

که بر هم‌نهی از حالت‌هایی با تعداد فوتون‌های از ۰ تا n هستند. در چنین پالس‌های میانگین تعداد فوتون‌ها یعنی (μ) نسبتاً کم است، یعنی احتمال یافتن یک فوتون در یک پالس از توزیع پوآسون [۳۶] زیر پیروی می‌کند:

$$P(n,\mu) = \frac{\mu^n}{n!} e^{-\mu} \qquad (۲۸.۲)$$

(μ) میانگین تعداد فوتون‌ها را نمی‌توان به صورت دلخواه کاهش داد زیرا وضعیت بازده پروتکل را کاهش می‌دهد. عدم وجود سیگنال‌های تک فوتونی و آشکارسازی‌های ایده‌آل راه را برای ارائه پروتکل‌های حمله، مانند حمله‌ی PNS یا حمله‌ی تقسیم تعداد فوتون [۳۷] و حمله‌ی اسب تروژن [۳۸] باز می‌کند [۱۱].

---

[۳۴] Dark count
[۳۵] Weak coherent pulses
[۳۶] Poissonian Distribution
[۳۷] Photon Number Splitting
[۳۸] Trojan-Horse Attack

فصل ۳

پروتکل توزیع کلید کوانتومی به روش Ping-Pong

۱.۳ مقدمه

با وجود تاریخ طولانی علم مکانیک کوانتومی و ظهور آن در یک قرن پیش، و همچنین مسائل و تعابیر حل نشده‌ی مربوط به آن این شاخه از علم فیزیک نقش بسیار مهم و انکارناپذیری در پیدایش بسیاری از علوم امروزی و پیشرفت‌های اهداف بشر امروزی داشته است و در همین زمینه نیز پدیده‌های بسیار مهم و متعددی را به دنیای علم معرفی کرده که در محدودی فیزیک کلاسیک قابل توصیف نیستند.

انتقال اطلاعات به صورت امن یکی از زمینه‌هایی است که مکانیک کوانتومی می‌تواند به شیوه‌ای بسیار مؤثر در آن نقش داشته باشد. به این منظور در این فصل به تشریح یکی از پروتکل‌های توزیع کلید کوانتومی $(Ping - Pong)$ می‌پردازیم که در آن ارتباط بین فرستنده و گیرنده به صورت مستقیم و برمبنای مفهومی بسیار جالب و پیچیده به نام درهم‌تنیدگی ذرات است، و در ادامه معایب و مزایای این پروتکل را مورد بررسی قرارمی‌دهیم.

۲.۳ توزیع کلید کوانتومی بدون اندازه‌گیری متناوب

دو هدف اصلی از رمزنگاری برای دو شخص دور از هم آلیس و باب آن است که بتوانند به‌گونه‌ای با هم ارتباط داشته باشند که برای طرف سوم(جاسوس) نامفهوم باشد، و جاسوس نتواند در هنگام انتقال،

پیام را تغییر دهد. این دو هدف می‌تواند با موفقیت انجام شود اگر هم آلیس و هم باب یک کلید، یک دنباله‌ی تصادفی محرمانه‌ی مشابه از بیت‌ها را در اختیار داشته باشند. بنابراین یکی از مسائل مهم در رمزنگاری مسئله‌ی توزیع کلید است، که آلیس و باب چگونه آن را انجام دهند، که هیچ اطلاعات محرمانه‌ای به اشتراک گذاشته نشود، و به مرحله‌ی در اختیار داشتن کلید محرمانه برسند در حالی که مطمئن باشند که جاسوس هیچ اطلاعاتی از کلید را بدست نیاورده است. این مشکل نمی‌تواند با استفاده از مفاهیم کلاسیک حل شود، اما با استفاده از مکانیک کوانتومی می‌تواند حل شود زیرا در حالی که اطلاعات در شکل کلاسیکی ذخیره شده‌اند می‌توانند بررسی و کپی شوند اما اگر اطلاعات در یک حالت ناشناخته‌ی کوانتومی ذخیره شوند براساس نظریه‌ی $(No-Cloning)$ قابل بررسی و کپی شدن نیستند. تأمین امنیت در پروتکل‌های $BB۸۴, E۹۱, B۹۲$ و پروتکل‌های دیگر بر این اساس تضمین می‌شود که آلیس و باب باید به صورت تصادفی بین دو اندازه‌گیری ممکن انتخاب کنند. اما در توزیع کلید کوانتومی بدون اندازه‌گیری تناوبی به انتخاب آلیس و باب نیازی نیست. این طرح براساس جابه‌جایی درهم‌تنیدگی بین دو زوج از کیوبیت‌ها حالات بل است که حالت‌های بل ۴ حالت متعامد به شکل زیر هستند($|xy\rangle_{ij}$ نمادی برای حالت‌های بل است و نباید با ضرب تانسوری $|x\rangle|y\rangle$ اشتباه شود.)

$$|\varphi^+\rangle_{ij} \equiv |۰۰\rangle_{ij} = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle_i \otimes |۰\rangle_j + |۱\rangle_i \otimes |۱\rangle_j\Big) \qquad (۱.۳)$$

$$|\varphi^-\rangle_{ij} \equiv |۰۱\rangle_{ij} = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle_i \otimes |۰\rangle_j - |۱\rangle_i \otimes |۱\rangle_j\Big) \qquad (۲.۳)$$

$$|\psi^+\rangle_{ij} \equiv |۱۰\rangle_{ij} = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle_i \otimes |۱\rangle_j + |۱\rangle_i \otimes |۰\rangle_j\Big) \qquad (۳.۳)$$

$$|\psi^-\rangle_{ij} \equiv |۱۱\rangle_{ij} = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle_i \otimes |۱\rangle_j - |۱\rangle_i \otimes |۰\rangle_j\Big) \qquad (۴.۳)$$

جابه‌جایی درهم‌تنیدگی بدین صورت است که: یک جفت از کیوبیت‌های i و j را در یکی از چهار حالت بل برای مثال حالت $(|\psi^-\rangle_{ij})$ $|۱۱\rangle_{ij}|$ آماده کرده و سپس جفت دوم از کیوبیت‌های k و l را در حالت بل دیگر برای مثال $(|\psi^+\rangle_{ij})$ $|۱۰\rangle_{kl}|$ آماده می‌کند. اگر عمگر اندازه‌گیری بل روی i و k عمل کند، چهار نتیجه ممکن $(۰۰, ۰۱, ۱۰, , ۱۱)$ با احتمال یکسان رخ می‌دهد در حقیقت نتیجه‌ی اندازه‌گیری کاملاً تصادفی است. فرض کنید که نتیجه (۰۰) بدست آید، به تبع آن حالت زوج i و k بعد از اندازه‌گیری $|\varphi^+\rangle_{ik} = |۰۰\rangle_{ik}|$ خواهد بود و حالت j و l خواهد شد $|۱۰\rangle_{jl} = |\psi^+\rangle_{jl}|$، بنابراین حالت j و l درهم‌تنیده می‌شود اگرچه آن‌ها هیچگاه برهم‌کنشی باهم نداشتند. به‌عنوان توضیحی برای طرح توزیع کلید کوانتومی QkD ارائه شده، این مثال را در نظر می‌گیریم که در ابتدا:

(i) آلیس کیوبیت‌های ۱ و ۲ را در حالت بل $|\varphi^+\rangle_{۱۲} = |۱۱\rangle_{۱۲}|$ و کیوبیت‌های ۳ و ۵ را در حالت بل $|\psi^+\rangle_{۳۵} = |۱۰\rangle_{۳۵}|$ آماده می‌کند. باب نیز در یک مکان دورتر کیوبیت‌های ۴ و ۶ را در حالت بل $|\psi^+\rangle_{۴۶} = |۱۰\rangle_{۴۶}|$ آماده می‌کند البته همه‌ی این اطلاعات به صورت عمومی منتشر می‌شود. در مرحله‌ی بعد :

(ii) آلیس با استفاده از یک کانال عمومی کیوبیت ۲ را به باب انتقال می‌دهد. این کانال یک واسطه‌ی انتقالی است که حالت کیوبیت را از برهم‌کنش با محیط حفظ می‌کند.

(iii) آلیس با اعمال عملگر بل روی کیوبیت‌های ۱ و ۳ آن‌ها را اندازه می‌گیرد، باب نیز با اعمال عملگر بل روی کیوبیت‌های ۲ و ۴ آن‌ها را اندازه می‌گیرد. نتایج هر دو اندازه‌گیری همبسته هستند، اگرچه آلیس و باب هنوز نمی‌دانند از چه طریقی؟ در مرحله‌ی بعد توضیح می‌دهیم که چگونه نتایج بدون افشای عمومی هریک از آن‌ها همبسته هستند.

(iv) باب کیوبیت ۶ را با استفاده از یک کانال عمومی به آلیس انتقال می‌دهد. سپس آلیس با اعمال عملگر بل روی کیوبیت‌های ۵ و ۶ آن‌ها را اندازه‌گیری و نتیجه را اعلام عمومی می‌کند. فرض کنید که آلیس از اندازه‌گیری روی کیوبیت‌های ۱ و ۳ نتیجه‌ی $(\psi^-)_{۱۳} = (۱۱)$ را بدست آورد، و چون آلیس می‌داند که حالت اولیه‌ی $۱, ۲, ۳, ۵$ به صورت زیر بوده است:

$$\Big(|۱۱\rangle_{۱۲} \otimes |۱۰\rangle_{۳۵}\Big) = \frac{۱}{۲}\Big(|\varphi^-\rangle_{۱۳}|\varphi^+\rangle_{۲۵} - |\varphi^+\rangle_{۱۳}|\varphi^-\rangle_{۲۵} + |\psi^-\rangle_{۱۳}|\psi^+\rangle_{۲۵} - |\psi^+\rangle_{۱۳}|\psi^-\rangle_{۲۵}\Big) \tag{۵.۳}$$

با استفاده از جدول (۱.۳) می‌داند که حالت کیوبیت‌های $(۲, ۵)$ خواهد بود $|۱۰\rangle_{۲۵} (= |\psi^+\rangle_{۲۵})$.

باب نیز پس از دریافت کیوبیت ۲ از طرف آلیس روی کیوبیت‌های ۲ و ۴ اندازه‌گیری بل انجام می‌دهد و حالت $|\varphi^+\rangle_{۲۴} = |۰۰\rangle_{۲۴}$ را بدست می‌آورد. در نتیجه کیوبیت‌های ۵ و ۶ در حالت $|\varphi^+\rangle_{۵۶} = |۰۰\rangle_{۵۶}$ درهم‌تنیده می‌شوند.

$$\Big(|۱۰\rangle_{۲۵} \otimes |۱۰\rangle_{۴۶}\Big) = \frac{۱}{۲}\Big(|\varphi^+\rangle_{۲۴}|\varphi^+\rangle_{۵۶} - |\varphi^-\rangle_{۲۴}|\varphi^-\rangle_{۵۶} + |\psi^+\rangle_{۲۴}|\psi^+\rangle_{۵۶} - |\psi^-\rangle_{۲۴}|\psi^-\rangle_{۵۶}\Big) \tag{۶.۳}$$

سپس باب کیوبیت ۶ را برای آلیس می‌فرستد و او کیوبیت‌های ۵ و ۶ را در پایه‌ی بل اندازه‌گیری می‌کند و نتیجه را اعلام عمومی می‌کند. از طرفی آلیس با استفاده از جدول شکل (۱.۳) می‌داند که باب از اندازه‌گیری کیوبیت‌های $۲, ۴$ نتیجه‌ی $|\varphi^+\rangle_{۲۴} = ″۰۰″$ را بدست آورده است، همین طور باب نیز می‌تواند بفهمد که نتیجه‌ی اندازه‌گیری آلیس بر روی کیوبیت‌های ۱ و ۳ به صورت $|\varphi^+\rangle_{۱۳} = ″۱۱″$ است، از طرفی آلیس و باب از قبل توافق می‌کنند که دنباله‌ای از نتایج اندازه‌گیری مخفیانه‌ی آلیس را بعنوان کلید انتخاب کنند. بنابراین نتیجه‌ی $|\varphi^+\rangle_{۱۳} = ″۱۱″$ آلیس، دو بیت اولیه‌ای از کلید است؛ اما اطلاعات عمومی به اشتراک گذاشته شده به وسیله‌ی آلیس و باب برای جاسوس کافی نیست تا آگاهی از نتیجه‌ی هر یک از طرفین بدست آورد.

با استفاده از اطلاعات به اشتراک گذاشته شده جاسوس تنها می‌داند که یکی از نتایج چهار ترکیب ممکن زیر از اندازه‌گیری مخفیانه‌ی آلیس و باب رخ داده است: نتیجه‌ی $|\varphi^-\rangle = ″۰۱″$ برای آلیس و نتیجه‌ی $|\psi^+\rangle = ″۱۰″$ برای باب، متقابلاً نتیجه‌ی $|\psi^+\rangle = ″۱۰″$ برای آلیس و نتیجه‌ی $|\varphi^-\rangle = ″۰۱″$ برای باب و نتیجه‌ی $|\psi^-\rangle = ″۱۱″$ و نتیجه‌ی $|\varphi^+\rangle = ″۰۰″$ برای باب، بنابراین این مقدار اطلاعات برای آگاهی جاسوس از نتیجه‌ای هر یک از طرفین ناکافی است.

Initial state $\|ijkl\rangle$				Possible final states $\|ikjl\rangle$			
0000	0101	1010	1111	0000	0101	1010	1111
0001	0100	1011	1110	0001	0100	1011	1110
0010	0111	1000	1101	0010	0111	1000	1101
0011	0110	1001	1100	0011	0110	1001	1100

شکل ۱.۳: در سمت چپ حالت اولیه‌ی کیوبیت‌های $|i,j,k,l\rangle$ و در سمت راست تمام حالت‌های نهایی ممکن کیوبیت‌های $|ik,jl\rangle$ پس از اعمال عملگر اندازه‌گیری بل نشان داده شده‌اند.

پس می‌توان برای توزیع کلید کوانتومی در دو مکان دور از هم از ایده‌ی جابه‌جایی درهم‌تنیدگی [۱] بین جفت‌های (EPR) [۲] برای تولید یک دنباله‌ی مشابه از بیت‌های تصادفی با ویژگی‌های زیر استفاده کرد که براساس آن:

(a) نیازی به اندازه‌گیری‌های تناوبی آلیس وباب نیست، از این‌رو نرخ [۳] بیت‌های تولید شده به واسطه‌ی انتقال کیوبیت‌ها بهتر می‌شود.

(b) این به آلیس و باب اجازه می‌دهد که یک کلید با طول دلخواه را با استفاده از یک سیستم کوانتومی منفرد(سه زوج EPR)، به‌جای یک دنباله‌ی طولانی از بیت‌ها تولید کنند.

(c) کشف جاسوس به مقایسه‌ی تعداد بیت کمتری نیاز دارد.

(d) این طرح که با فرض قابل اطمینان بودن عملگر اندازه‌گیری بل است اساساً بر پایه‌ای درهم‌تنیدگی کوانتومی است. به این معنا که، از خاصیت درهم‌تنیدگی برای هدف توزیع کلید کوانتومی با ویژگی‌های بیان شده (a,b,c) می‌توان استفاده کرد و این طرح توزیع کلید کوانتومی بدون درهم‌تنیدگی امکان‌پذیر نمی‌باشد.

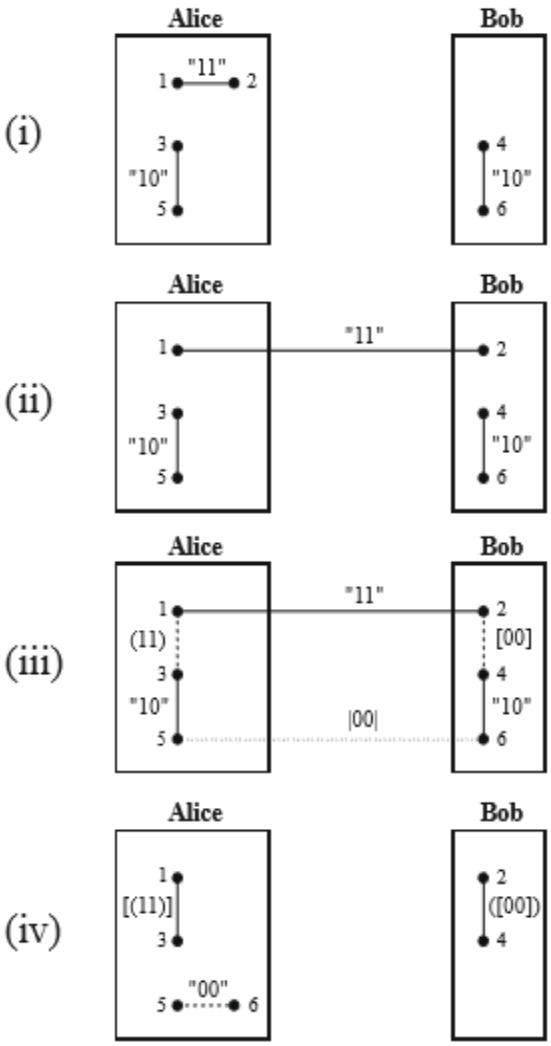
اما براساس استراتژی حمله‌ای که در ادامه توضیح داده می‌شود یعنی استراتژی حمله در پایه‌ای درهم‌تنیدگی، جاسوس می‌تواند از نتایج محرمانه‌ی آلیس آگاهی یابد. با توجه به شکل (۳.۳)، در ادامه به تشریح سناریوی این حمله می‌پردازیم.

(a) جاسوس دو کیوبیت ۷ و ۸ را در یک حالت بل، برای مثال در حالت $|\varphi^+\rangle_{۷۸} = |۰۰\rangle_{۷۸}$ آماده می‌کند.

$(۱b)$ جاسوس کیوبیت ۲ را که آلیس برای باب ارسال می‌کند را سد و عملگر اندازه‌گیری بل را روی کیوبیت‌های ۲ و ۸ اعمال می‌کند. سپس کیوبیت‌های ۱ و ۷ در یک حالت شناخته شده‌ای بل(برای جاسوس) درهم‌تنیده می‌شوند.

---

[۱] Entanglement swapping
[۲] Einstein-Podolsky-Rosen
[۳] Entanglement swapping



شکل ۲.۳: طرح توزیع کلید کوانتومی براساس جابه‌جایی درهم‌تنیدگی. در این طرح خطوط پررنگ نشان‌دهنده‌ی کیوبیت‌ها در حالت بل هستند و خطوط مقطع نشان‌دهنده‌ی حالت‌های اندازه‌گیری شده با عملگر اندازه‌گیری بل است، خطوط نقطه‌چین نشان‌دهنده‌ی حالت‌های بل که با جابه‌جایی درهم‌تنیده شده‌اند. حالت ″۰۰″ حالت بل $|۰۰\rangle$ را نمایش می‌دهد که اعلام عمومی شده و حالت (۰۰) نشان‌دهنده‌ی حالتی که فقط آلیس آن را می‌شناسد حالت [۰۰] نشان‌دهنده‌ی حالتی که تنها باب آن را می‌شناسد و حالت $|۰۰|$ نشان‌دهنده‌ی حالت ناشناخته برای آلیس و باب است، و حالت [(۰۰)] نشان‌دهنده‌ی حالت شناخته شده برای هر دو آنهاست.

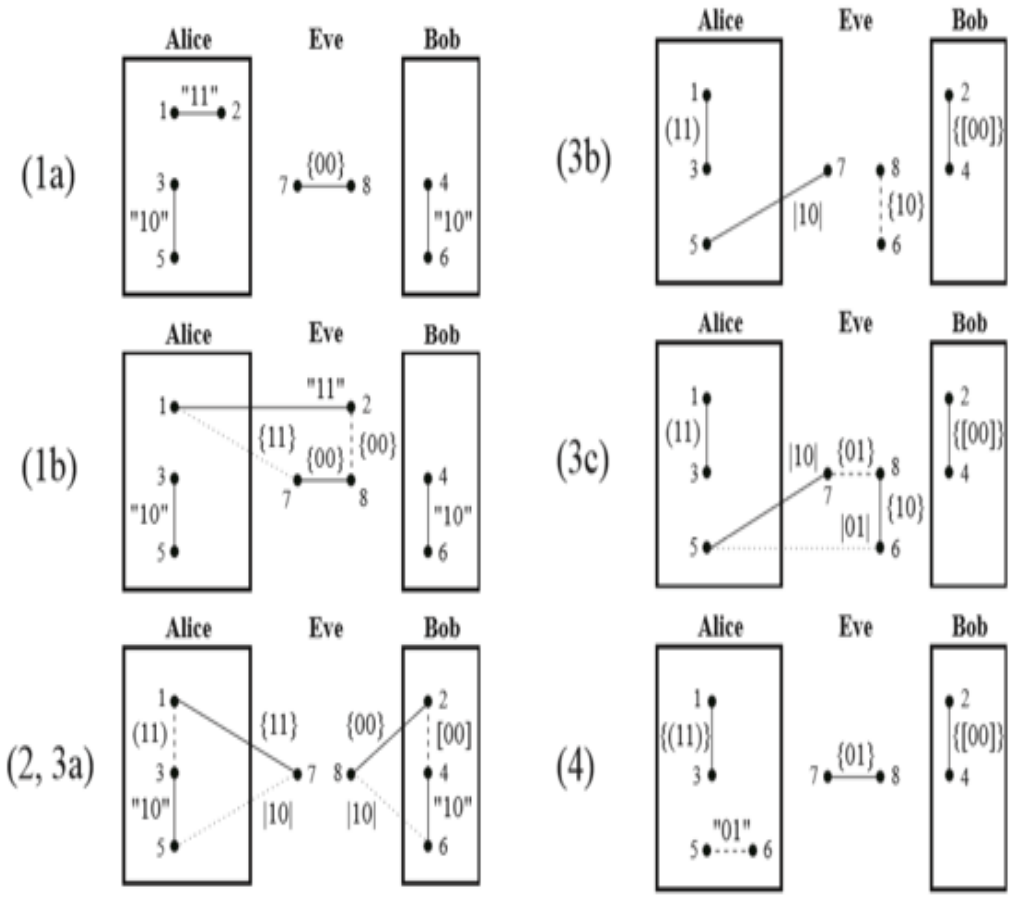
(۲) برای مثال جاسوس حالت ۲ و ۸ را بعد از اندازه‌گیری $|\varphi^+\rangle_{۷۸} = |۰۰\rangle_{۲۸}|$ و حالت درهم‌تنیده‌ی ۱ و ۷ را در حالت $|\psi^-\rangle_{۷۸} = |۱۱\rangle_{۱۷}|$ بدست می‌آورد.

$(۳a)$ در این سناریوی جدید، بعد از اندازه‌گیری آلیس(باب) روی کیوبیت‌های ۱ و ۳ (۲, ۴) حالت کیوبیت‌های ۵ و ۷ (۶,۸) یک حالت بل می‌شود. برای مثال، اگر آلیس(باب) ″۱۱″ (۰۰) را بدست آورد حالت کیوبیت‌های ۵ و ۷ (۶,۸) خواهد شد ″۱۰″ (۱۰). با این حال، این حالت‌ها برای جاسوس ناشناخته هستند، زیرا او هنوز از نتایج اندازه‌گیری آلیس و باب بی‌اطلاع است.

(۳b) جاسوس کیوبیت ۶ را که باب برای آلیس ارسال می‌کند را سد کرده و عملگر اندازه‌گیری بل را روی کیوبیت‌های ۶ و ۸ اعمال می‌کند سپس جاسوس می‌تواند از نتیجه‌ی باب آگاه شود. برای مثال، جاسوس "۱۰" را خواهد یافت و خواهد دانست که نتیجه‌ی باب "۰۰" است.

(۳c) جاسوس عملگر اندازه‌گیری بل را روی کیوبیت‌های ۷ و ۸ اعمال می‌کند. سپس کیوبیت‌های ۵ و ۶ در یک حالت بل که هنوز برای جاسوس ناشناخته است درهم‌تنیده می‌شوند، چون او نتیجه‌ی محرمانه‌ی آلیس را نمی‌داند. برای مثال، اگر جاسوس "۰۱" را بدست آورد پس کیوبیت‌های ۵ و ۶ در حالت $|\varphi^-\rangle_{۵۶} = |۰۱\rangle_{۵۶}$ خواهند بود.

(۴) جاسوس کیوبیت ۶ را برای آلیس ارسال می‌کند، و او روی کیوبیت‌های ۵ و ۶ اندازه‌گیری و نتیجه را اعلام می‌کند. سپس جاسوس می‌تواند از حالت ۵ و ۷ $|\varphi^-\rangle_{۵۷} = (|۱۰\rangle_{۵۷})$ و نتیجه‌ی اندازه‌گیری آلیس بر روی کیوبیت‌های ۱ و ۳ $|\psi^-\rangle_{۱۳} = (|۱۱\rangle_{۱۳})$ آگاهی یابد.



شکل ۳.۳: استراتژی جاسوس برای اطلاع از نتایج محرمانه‌ی آلیس

با این حال، مداخله‌ی جاسوس باعث تغییر همبستگی مورد انتظار از نتایج محرمانه‌ی آلیس و باب

می‌شود. برای نمونه در مثال مطرح شده باب با توجه به نتیجه‌ی خودش و نتیجه‌ی اعلام عمومی آلیس حالت "۱۰" را به‌عنوان دو بیت اولیه‌ی کلید در نظر می‌گیرد.

البته همانند پروتکل‌های قبلی QKD، در این طرح نیز آلیس و باب می‌توانند مداخله‌ی جاسوس را بوسیله‌ی مقایسه‌ی عمومی یک زیر مجموعه‌ی تصادفی بقدر کافی بزرگ از دنباله‌ی بیت‌هایشان کشف کنند، که متعاقباً این بیت‌ها کنار گذاشته می‌شوند. همچنین اگر آنها بعد از مقایسه، یک زیر مجموعه‌ی تصادفی یکسان را بیابند می‌توانند کلید را تشکیل دهند. به نوعی در این طرح نیز می‌توان مشابه پروتکل $BB۸۴$ وجود جاسوس را آشکار کرد؛ تنها با این تفاوت که در $BB۸۴$ احتمال کشف حضور جاسوس پس از مقایسه بیت‌ها $\frac{۱}{۴}$ است؛ اما در این طرح احتمال این که مقایسه‌ای آلیس و باب حضور جاسوس را آشکار کند، $\frac{۳}{۴}$ است [۲۸].

اما در سال ۲۰۰۱ ژانگ، لی و گوا [۴] یک استراتژی حمله در مورد این طرح ارائه کردند؛ که براساس استراتژی حمله‌ی آن‌ها یعنی (ZLG)، ایو می‌تواند تمام اطلاعات در مورد کلید محرمانه‌ی بین آلیس و باب را بدست آورد. ایده این استراتژی بدین شکل است که پس از اندازه‌گیری آلیس بر روی کیوبیت‌های $(۱,۳)$ و ارسال کیوبیت ۲ برای باب، همانگونه که در تصویر (۴.۳) دیده می‌شود ایو کیوبیت ارسالی ۲ را دریافت کرده و به جای آن کیوبیت ۸ از حالت درهم‌تنیده‌ی $|\varphi^+\rangle_{۷۸}$ را برای باب ارسال می‌کند. متقابلاً باب حالت‌های $(۴,۸)$ را اندازه‌گیری می‌کند که در نتیجه‌ی آن حالت‌های $(۶,۷)$ درهم تنیده می‌شوند.

$$\Big(|\varphi^+\rangle_{۷۸}\otimes|\psi^+\rangle_{۴۶}\Big)= \tag{۷.۳}$$
$$\frac{۱}{۲}\Big(|\varphi^+\rangle_{۴۸}\psi^+\rangle_{۶۷}+|\varphi^-\rangle_{۴۸}|\psi^-\rangle_{۶۷}+|\psi^+\rangle_{۴۸}|\varphi^+\rangle_{۶۷}+|\psi^-\rangle_{۴۸}|\varphi^-\rangle_{۶۷}\Big)$$

از آنجا که جاسوس حالت

$$|\psi^+\rangle_{۲۵}=\frac{۱}{\sqrt{۲}}\Big(|۰۱\rangle_{۲۵}+|۱۰\rangle_{۲۵}\Big)$$

را که مطابق با نتیجه‌ی اندازه‌گیری آلیس است در اختیار دارد، پس او نتیجه‌ی اندازه‌گیری دقیق باب را می‌داند(با توجه به مرحله‌ی ۵ در شکل (۴.۳)) علاوه بر این، او می‌داند که چگونه حالت کیوبیت‌های ۲ و ۵ را تغییر دهد تا حالت کیوبیت‌های ۵ و ۶ مطابق با نتایج اندازه‌گیری آلیس و باب شود. به این جهت یکی از ۴ عملگرهای پائولی $(I,\sigma_x,\sigma_y,\sigma_z)$ را روی کیوبیت ۲ در حالت $|\psi^+\rangle_{۲۵}$ اعمال می‌کند، تا کیوبیت ۲ در وضعیت کیوبیت ۶ در حالت

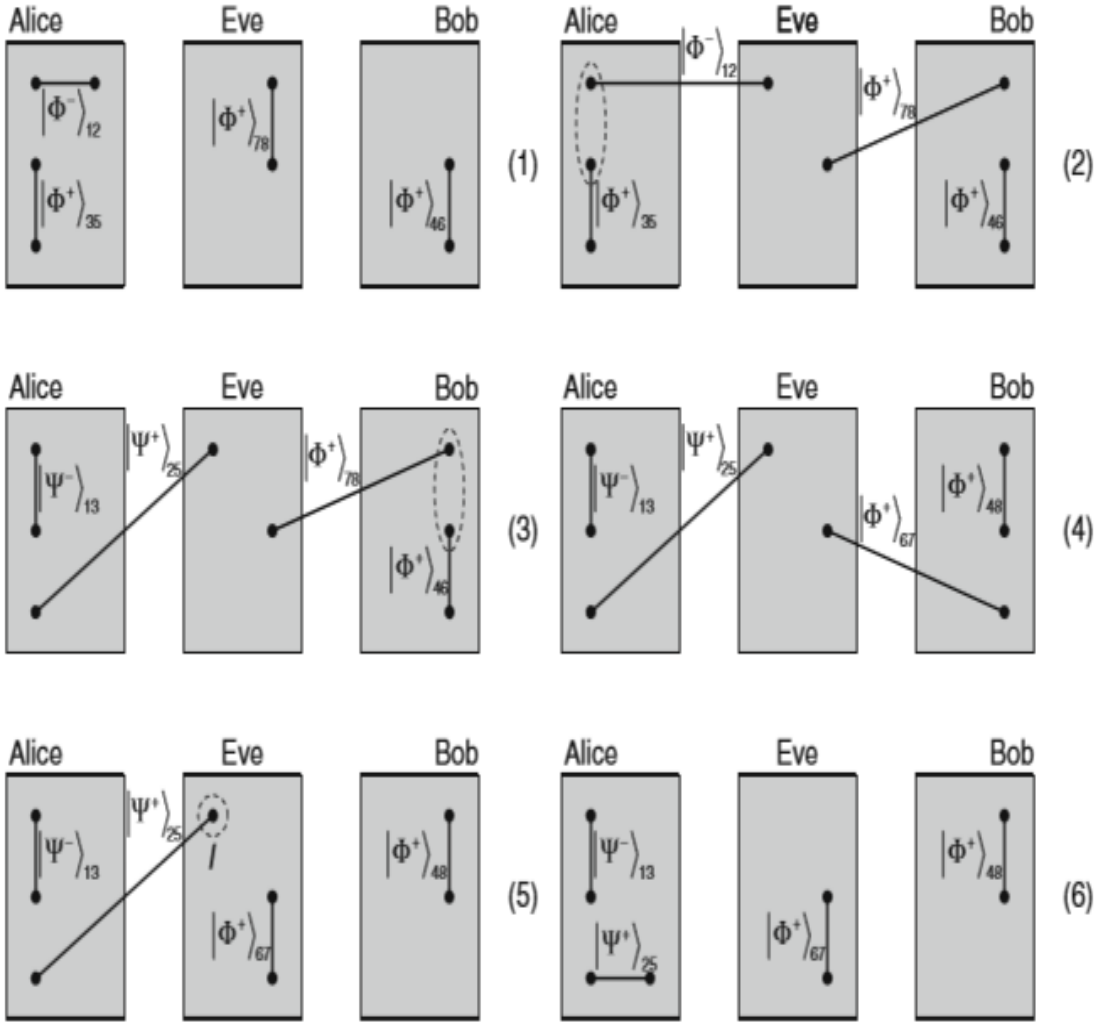
$$|\psi^+\rangle_{۶۷}=\frac{۱}{\sqrt{۲}}\Big(|۰۱\rangle_{۶۷}+|۱۰\rangle_{۶۷}\Big)$$

قرار بگیرد، یعنی:

$$I|\psi^+\rangle_{۲۵}=\frac{۱}{\sqrt{۲}}\Big(|۰۱\rangle_{۲۵}+|۱۰\rangle_{۲۵}\Big)$$

و سپس کیوبیت ۲ را به آلیس برمی‌گرداند. آلیس نیز یک اندازه‌گیری انجام می‌دهد و نتیجه را همبسته(مطابق) با نتیجه‌ی اندازه‌گیری باب بدست می‌آورد، و از آن‌جا که حالت کیوبیت‌های ایو یعنی $|\varphi^+\rangle_{۶۷}$ با حالت

[۴] Zhang, Li, and Guo



شکل ۴.۳: طرح حمله‌ی ZLG

کیوبیت‌های باب یعنی $|\varphi^+\rangle_{۴۸}$ مشابه می‌باشد او می‌تواند تمام اطلاعات در مورد کلید مشترک بین آلیس و باب را بدست آورد.

بدنبال این طرح در سال ۲۰۰۱ کابلو [۵] با ارائه‌ی یک راه حل مشکل ایمنی این پروتکل را در مقابل حمله‌ی (ZLG) برطرف نمود. به نظر او برای حل این مسئله می‌توان از عملگر هادامارد H [۶] به صورت زیر استفاده کرد:

$$H|\varphi^{\pm}\rangle = \frac{۱}{\sqrt{۲}}\Big(|\varphi^{\mp}\rangle \pm |\psi^{\pm}\rangle\Big) = |\omega^{\pm}\rangle \qquad (۸.۳)$$
$$H|\psi^{\pm}\rangle = \frac{۱}{\sqrt{۲}}\Big(|\psi^{\mp}\rangle \pm |\varphi^{\pm}\rangle\Big) = |\chi^{\pm}\rangle$$

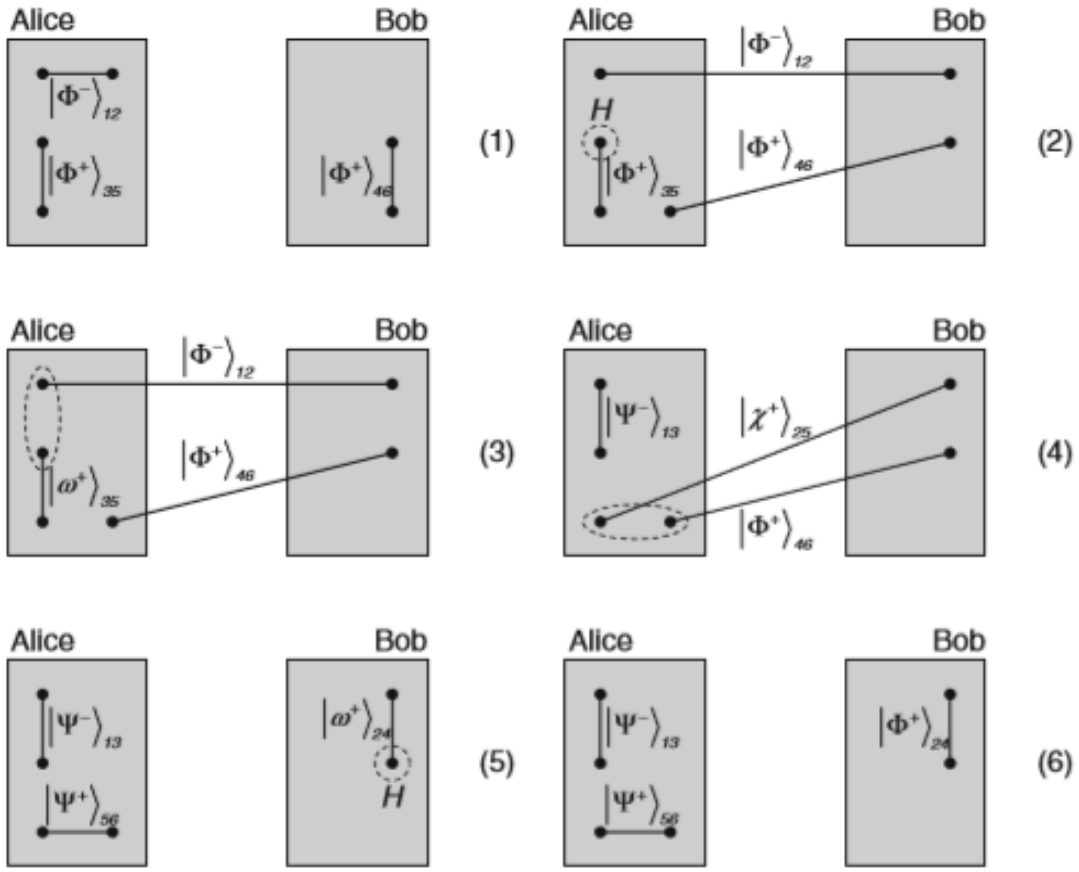
در این روش آلیس و باب مانند پروتکل اصلی کیوبیت‌های ۲ و ۶ را مبادله می‌کنند و پس از آن اندازه‌گیری

[۵] Adan Cabello
[۶] Hadamard operation

بل انجام می‌دهند، همچنین آلیس به صورت تصادفی برای اعمال یا عدم اعمال عملگر هادامارد روی کیوبیت ۳ تصمیم می گیرد، یعنی:

$$\left(|\psi^-\rangle_{۱۲}|\chi^+\rangle_{۳۵}\right) = \tag{۹.۳}$$
$$\frac{۱}{۲}\left(|\varphi^-\rangle_{۱۳}|\omega^+\rangle_{۲۵} - |\varphi^+\rangle_{۱۳}|\omega^-\rangle_{۲۵} + |\psi^-\rangle_{۱۳}|\chi^+\rangle_{۲۵} - |\psi^+\rangle_{۱۳}|\chi^-\rangle_{۲۵}\right)$$

سپس آلیس نتایج انتخاب‌ها و اندازه‌گیری‌های خودش بر روی کیوبیت‌های ۵ و ۶ را با هم اعلام می‌کند. اما اگر آلیس عملگر هادامارد را استفاده نکند، هر دو نفر پروتکل اصلی را دنبال می‌کنند. در غیر این صورت، باب هم عملگر هادامارد را بر روی کیوبیت ۴ اعمال می‌کند تا اثر آن را خنثی کند. سپس عملگر اندازه‌گیری بل را روی کیوبیت‌های ۲ و ۴ اعمال می‌کند، و در نتیجه‌ی استفاده از عملگر هادامارد جاسوس نمی‌تواند عملگر پائولی درست را در هنگام حمله‌ی (ZLG) انتخاب کند، و بنابراین نتایج اندازه‌گیری آلیس و باب ناهمبسته نخواهند بود. اما نکته‌ی مهم وقابل توجه در این طرح احتمال کشف



شکل ۵.۳: اعمال عملگر هادامارد در حمله‌ی ZLG

حضور جاسوس است، که جاسوس با احتمال $\frac{۳}{۴}$ کشف می‌شود. بنابراین برای مثال اگر نتایج n جفت $(N = ۲n)$ بیت با هم مقایسه شوند، احتمال کشف جاسوس $(۱ - (\frac{۱}{۲})^N)$ خواهد بود [۱۱].

۳.۳ پروتکل Ping-Pong

پروتکل‌های رمزنگاری کوانتومی براساس مکانیک کوانتومی معمولاً غیر قطعی یا پیش‌بینی‌ناپذیر [۷] هستند. به این معنا که آلیس به عنوان فرستنده می‌تواند یک بیت کلاسیکی را در یک حالت کوانتومی رمزگذاری کند و سپس آن را برای باب یا همان گیرنده‌ی پیام بفرستد، اما او نمی‌تواند مقدار بیتی را که در نهایت باب رمزگشایی می‌کند ، پیش‌بینی کند. با این وجود، این ارتباط غیرقابل پیش‌بینی می‌تواند برای به اشتراک گذاری یک کلید محرمانه‌ی تصادفی بین آلیس و باب استفاده شود، که پیام‌ها با استفاده از این کلید رمزگذاری و از طریق یک کانال کلاسیکی عمومی ارسال می‌شوند.

در سال ۲۰۰۲ یک پروتکل ارتباط کوانتومی جدید توسط بیج [۸] و همکارانش ارائه شد، در این پروتکل طرفین می‌توانند به صورت مستقیم با یکدیگر ارتباط برقرار کنند یعنی آن که پیام مستقیماً از طریق کانال کوانتومی بین طرفین مخابره شود. پس از آن‌ها بوستروم و فلبینگر [۹] پروتکل ارتباط کوانتومی به نام $Ping-Pong$ را براساس ویژگی درهم‌تنیدگی ذرات و بر مبنای یک ارتباط مستقیم و قطعی ارائه کردند. ایده اصلی این پروتکل رمزنگاری اطلاعات بوسیله‌ی اعمال عملگرهای جایگزیده بر روی حالت‌های بل یا یک زوج EPR است، که پیش از این توسط بنت و ویزنر [۱۰] مطرح شده بود.

• طرح پروتکل Ping-Pong

هنگامی که دو فوتون در درجه‌ی آزادی قطبششان با یکدیگر به صورت بیشینه درهم‌تنیده می‌شوند آنگاه نمی‌توان هر یک از فوتون‌ها را به صورت منفرد درهم‌تنیده در نظر گرفت. اگر حالت قطبش عمودی و افقی را به ترتیب با حالت‌های $|۰\rangle$ و $|۱\rangle$ نمایش دهیم، آنگاه حالت‌های بل $|\psi^{\pm}\rangle$ را می‌توان به صورت زیر نمایش داد:

$$|\psi^{\pm}\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰۱\rangle \pm |۱۰\rangle\Big)$$

از آن جا که حالت‌های بل در بیشینه‌ی درهم‌تنیدگی در فضای هیلبرت دو ذره به شکل

$$H = H_A \otimes H_B$$

هستند. اندازه‌گیری از قطبش یکی از فوتون‌ها منجر به یک نتیجه‌ی کاملاً تصادفی می‌شود. این واقعیت به علت، یک ماتریس چگالی کاهش یافته متناظر با یک نتیجه‌ی کاملاً مخلوط برای هر فوتون به صورت

$$\rho_A^{\pm} = Tr_B\{|\psi^{\pm}\rangle\langle\psi^{\pm}|\} = \frac{۱}{۲}I_A$$

است. چون حالت‌های $|\psi^{\pm}\rangle$ بر یکدیگر عمود هستند پس کسی که فقط به یکی از دو فوتون درهم‌تنیده دسترسی دارد نمی‌تواند بدون اندازه‌گیری حالت‌های $|\psi^{+}\rangle$ و $|\psi^{-}\rangle$ را از یکدیگر متمایز کند. بنابراین می‌توان یک بیت از اطلاعات را در حالت‌های $|\psi^{\pm}\rangle$ رمزگذاری کرد به گونه‌ای که حالت کیوبیت برای کسی که تنها به یکی از دو کیوبیت دسترسی دارد نامشخص باشد.

---

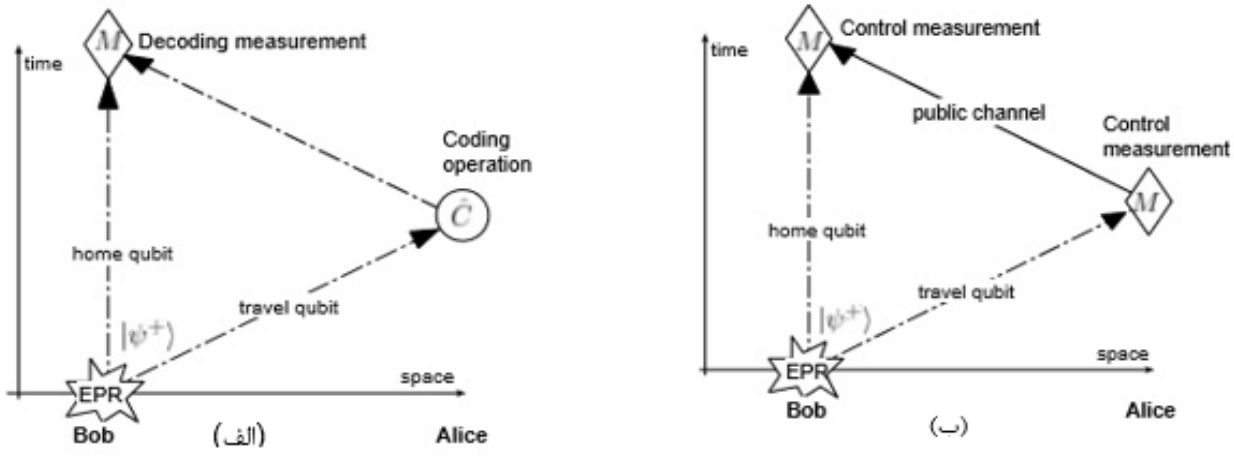
[۷] Non-Deterministic
[۸] Beige
[۹] Bostrom & Felbinger
[۱۰] Bennett and Wiesner

با استفاده از اپراتور یکانی و فاز برگردان

$$\sigma_z^A \equiv \left(\sigma_z^A \otimes I\right) = \left(|۰\rangle\langle۰| - |۱\rangle\langle۱|\right) \otimes I$$

و اعمال آن بر روی حالت‌های $|\psi^{\pm}\rangle$ می‌توان حالت $|\psi^{+}\rangle$ را به حالت $|\psi^{-}\rangle$ (و بالعکس) تبدیل کرد. اگر چه عملگر σ_z^A به صورت موضعی [۱۱] تنها بر روی یک فوتون عمل می‌کند ولی اثر آن غیرموضعی [۱۲] و بر روی کل حالت بل است. یعنی کسی که فقط به یک فوتون دسترسی دارد می‌تواند یک بیت از اطلاعات را رمزگذاری کند، اما نمی‌تواند آن را رمزگشایی کند، زیرا او به فوتون دیگر دسترسی ندارد. بنابراین، این وضعیت کاملاً برای یک سناریوی رمزنگاری مناسب است. در این سناریو ابتدا باب دو فوتون را در حالت $|\psi^{+}\rangle$ آماده می‌کند. او یک فوتون را نزد خود نگه داشته و فوتون دیگر را برای آلیس ارسال می‌کند. آلیس در مورد اعمال یا عدم اعمال اپراتور σ_z بر روی کیوبیت دریافتی تصمیم می‌گیرد، البته عدم اعمال اپراتور به مفهوم اعمال اپراتور همانی I بر روی کیوبیت دریافتی از باب است. سپس او کیوبیت را مجدداً برای باب ارسال می‌کند. باب، که حالا هر دو کیوبیت را دارد در پایه‌ی بل اندازه‌گیری انجام می‌دهد که با توجه به این که آلیس چه اپراتوری را بر روی کیوبیت اعمال کرده است یکی از نتایج $|\psi^{+}\rangle$ یا $|\psi^{-}\rangle$ برای باب حاصل می‌شود. بنابراین، در رفت و برگشت یک کیوبیت از آلیس به باب(پینگ_پنگ) یک بیت اطلاعات از آلیس به باب منتقل شده، و باب یک بیت اطلاعات از آلیس بدست آورده است.

برای ایجاد امنیت در این پروتکل، ارسال پیام‌ها در دو مد مختلف به نام‌های مد پیام (برای ارسال حالت‌های کوانتومی) و مد کنترل (جهت کشف جاسوس یا شنودکننده) انجام می‌شود، به طور پیش فرض آلیس و باب در مد پیام هستند و به صورت توضیح داده شده با یکدیگر ارتباط برقرار می‌کنند.



شکل ۶.۳: الف:نمایی از مد پیام، ب:نمایی از مد کنترل

[۱۱] Local
[۱۲] Non-Local

با احتمال c، آلیس به جای اعمال اپراتور، روی کیوبیت دریافتی مد کنترل را سوئیچ می‌کند و یک اندازه‌گیری در پایه‌ی $B_z = \{|0\rangle, |1\rangle\}$ انجام می‌دهد، و نتیجه را با استفاده از کانال عمومی برای باب می‌فرستد، سپس او نیز مد کنترل را سوئیچ می‌کند و یک اندازه‌گیری در پایه‌ی مشابه B_z انجام می‌دهد. باب نتیجه‌ی خودش را با نتیجه آلیس مقایسه می‌کند، در صورت منطبق بودن نتایج در مد کنترل باب متوجه حضور شنودکننده روی خط می‌شود و ارتباط را متوقف می‌کند.

به عبارتی دیگر می‌توان الگوریتم این پروتکل را برای دو مد کنترل و مد پیام در مراحل زیر خلاصه کرد:

$p\cdot 0$) هدف انتقال رشته پیام $x^N = (x_1, ..., x_N)$ است، که $x \in \{0, 1\}$ و در مرتبه اول پروتکل $n = 0$ است.

$p\cdot 1$) در مرحله‌ی بعد $n = n + 1$، و آلیس و باب در مد پیام هستند. باب دو کیوبیت را در حالت بل $|\psi^+\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big)$ آماده می‌کند.

$p\cdot 2$) باب یک کیوبیت را نزد خود نگه داشته، و کیوبیت دیگر را از طریق کانال کوانتومی برای آلیس ارسال می‌کند.

$p\cdot 3$) آلیس کیوبیت ارسالی را دریافت می‌کند، و با احتمال c مد کنترل را سوئیچ می‌کند و برای مرحله‌ی اول مد کنترل $(c\cdot 1)$ اقدام می‌کند، در غیر این صورت برای مرحله‌ی اول مد پیام $(m\cdot 1)$ اقدام می‌کند.

$c\cdot 1$) آلیس کیوبیت انتقالی را در پایه‌ی B_z اندازه‌گیری می‌کند و با احتمال مساوی نتیجه را $i \in \{0, 1\}$ بدست می‌آورد.

$c\cdot 2$) او نتیجه‌ی i را از طریق کانال عمومی به باب اعلام می‌کند.

$c\cdot 3$) باب پس از دریافت نتیجه‌ی i، مد کنترل را سوئیچ و کیوبیت خود را در پایه‌ی B_z اندازه‌گیری می‌کند و مقدار j را نتیجه می‌گیرد.

$c\cdot 4$) اگر $(i = j)$: حضور شنودکننده آشکار می‌شود و انتقال بی‌نتیجه می‌ماند. در غیر این صورت اگر $(i \neq j)$ است؛ پس $n = n - 1$ و پروتکل به مرحله‌ی $p\cdot 1$) باز می‌گردد.

$m\cdot 1$) در این مد دو عملگر $(\hat{C}_0 := I, \hat{C}_1 := \hat{\sigma}_z)$ را برای عملیات رمزگذاری $x_n \in \{0, 1\}$ تعریف می‌کنیم. آلیس یکی از عملگرهای $\hat{C}_{x_n}$ را روی کیوبیت انتقالی اعمال می‌کند و مجدداً آن را برای باب می‌فرستد.

$m\cdot 2$) باب کیوبیت انتقالی را دریافت می‌کند و یک اندازه‌گیری بل روی هر دو کیوبیت انجام می‌دهد، در نتیجه حالت نهایی را به‌صورت $|\acute{\psi}\rangle \in \{|\psi^+\rangle, |\psi^-\rangle\}$ بدست می‌آورد، که

$$|\acute{\psi}\rangle = \begin{cases} |\psi^+\rangle \Longrightarrow x_n = 0 \\ |\psi^-\rangle \Longrightarrow x_n = 1 \end{cases} \qquad (10.3)$$

$m\cdot 3$) اگر $(n < N)$: پروتکل به مرحله‌ی $p\cdot 1$، برمی‌گردد و اگر $(n = N)$: مرحله‌ی $p\cdot 4$، انجام می‌شود.

$p\cdot 4$) رشته پیام x^N از آلیس به باب با موفقیت منتقل شده، و ارتباط پایان می‌پذیرد.

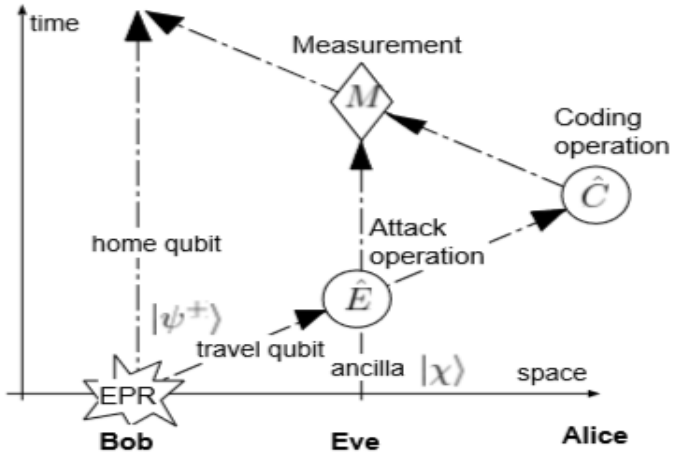
• امنیت پروتکل

برای اثبات ایمنی این پروتکل به این سؤال پاسخ داده‌می‌شود که یک شنودکننده‌ی پنهان تا قبل از آشکار شدن چه میزان اطلاعات را می‌تواند از این ارتباط بدست آورد؟ چرا که یک شنودکننده پنهان(ایو) [۱۳] می‌تواند تمام دستگاه‌های را که به واسطه‌ی قوانین مکانیک کوانتومی مجاز هستند را بسازد، و هدف او از شنود در این پروتکل تنها کشف عملگر اعمالی آلیس است. از آنجایی که جاسوس به کیوبیت باب دسترسی ندارد، بنابراین همه‌ی آنچه که او می‌تواند بدست آورد محدود به کیوبیت انتقالی بین آلیس و باب است. حالتی که بواسطه‌ی ترکیب کامل $\rho_A = Tr_B\{|\psi^+\rangle\langle\psi^+|\} = \frac{1}{2}I_A$ برای جاسوس غیرقابل تشخیص است. پس جاسوس به منظور بدست آوردن اطلاعات درباره‌ی عملگر آلیس، ابتدا با استفاده از عملگر یکانی $(\hat{E})$ کیوبیت انتقالی آلیس به باب را با کیوبیت خودش درهم‌تنیده می‌کند:

$$\hat{E}|0\rangle|x\rangle = \alpha|0\rangle|x_0\rangle + \beta|1\rangle|x_1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1 \qquad (۱۱.۳)$$

$$\hat{E}|1\rangle|x\rangle = \acute{\alpha}|0\rangle|\acute{x_0}\rangle + \acute{\beta}|1\rangle|\acute{x_1}\rangle \qquad |\acute{\alpha}|^2 + |\acute{\beta}|^2 = 1 \qquad (۱۲.۳)$$

سپس جاسوس اجازه می‌دهد تا سیستم مرکب به دست آلیس برسد، و او عملگر رمزگذاری $\hat{C}$ را روی کیوبیت انتقالی اعمال کند و مجدداً آن را برای باب بفرستد، در بین راه جاسوس حالت کمکی خود را اندازه‌گیری می‌کند تا بدین ترتیب اطلاعات رمزگذاری شده توسط آلیس را بدست آورد. از آنجا که حضور



شکل ۷.۳: نمایی از حمله‌ی شنودکننده پنهان

جاسوس تنها با کنترل مشخص می‌شود، طراحان این پروتکل این مد(مد کنترل) را در نظر گرفته‌اند. زیرا که در این مد با فرض ارسال حالت $|0\rangle$ از طرف باب و در غیاب ایو نتیجه همیشه "۰" خوانده می‌شود، اما در صورت حضور جاسوس و حمله به کیوبیت انتقالی، احتمال کشف این حمله در مسیر کنترل خوانده می‌شود:

$$d = |\beta|^2 = 1 - |\alpha|^2 \qquad (۱۳.۳)$$

[۱۳] Eve

در مد پیام با حمله‌ی جاسوس به کیوبیت انتقالی باب به آلیس، حالت سیستم به شکل زیر خواهد بود:

$$\begin{aligned}\acute{\rho} = |\acute{\psi}\rangle\langle\acute{\psi}| &= \Big(\alpha|۰, x_۰\rangle + \beta|۱, x_۱\rangle\Big)\Big(\alpha^*\langle۰, x_۰| + \beta^*\langle۱, x_۱|\Big) \\ &= |\alpha|^۲|۰, x_۰\rangle\langle۰, x_۰| + \alpha\beta^*|۰, x_۰\rangle\langle۱, x_۱| \\ &+\beta^*\alpha|۱, x_۱\rangle\langle۰, x_۰| + |\beta|^۲|۱, x_۱\rangle\langle۱, x_۱|\end{aligned} \tag{۱۴.۳}$$

یا

$$\acute{\rho} = \begin{pmatrix} |\alpha|^۲ & \alpha\beta^* \\ \alpha^*\beta & |\beta|^۲ \end{pmatrix} \tag{۱۵.۳}$$

سپس جاسوس این سیستم مرکب را برای آلیس ارسال می‌کند و آلیس به ترتیب با احتمال $p_۰$ و $p_۱$ عملگرهای $\hat{c}_۰ = I$ یا $\hat{c}_۱ = \hat{\sigma}_z$ را برای به رمز در آوردن کیوبیت انتقالی بکار می‌برد و آن را به باب برگشت می‌دهد. جاسوس حالت برگشتی آلیس را مجدداً دریافت و روی آن اندازه گیری انجام می‌دهد.

$$\begin{aligned}\rho'' &= P_۰\Big(I|\psi'\rangle\langle\psi'|I^\dagger\Big) + P_۱\Big(\sigma_z|\psi'\rangle\langle\psi'|\sigma_z^\dagger\Big) \\ &= \begin{pmatrix} |\alpha|^۲ & \alpha\beta^*(P_۰ - P_۱) \\ \alpha^*\beta(P_۰ - P_۱) & |\beta|^۲ \end{pmatrix}\end{aligned} \tag{۱۶.۳}$$

بیشینه اطلاعات کلاسیکی $(I_۰)$ که بوسیله‌ی آنتروپی وان نیومن [۱۴] می‌تواند از این حالت بدست آورد:

$$I_۰ = S(\rho'') \equiv -Tr\{\rho'' \log_۲ \rho''\}$$

با محاسبه‌ی ویژه مقدار λ، بیشینه اطلاعات کلاسیکی از ماتریس چگالی ρ'' بدست می‌آید.

$$\det(\rho'' - \lambda I) = ۰ \tag{۱۷.۳}$$

بنابراین

$$\lambda_{۱,۲} = \frac{۱}{۲}\Big(۱ \pm \sqrt{۱ - ۴|\alpha\beta|^۲[۱ - (P_۰ - P_۱)^۲]}\Big) \tag{۱۸.۳}$$

و $I_۰$ خواهد بود:

$$I_۰ = -\lambda_۱ \log_۲ \lambda_۱ - \lambda_۲ \log_۲ \lambda_۲ \tag{۱۹.۳}$$

در نتیجه احتمال کشف جاسوس با استفاده از معادله‌ی (۱۳.۳)

$$|\alpha\beta|^۲ = (۱ - |\beta|^۲)|\beta|^۲ = (d - d^۲)$$

و ویژه مقادیر خواهند بود:

$$\lambda_{۱,۲} = \frac{۱}{۲} \pm \frac{۱}{۲}\sqrt{۱ - (۴d - ۴d^۲)[۱ - (P_۰ - P_۱)^۲]} \tag{۲۰.۳}$$

[۱۴] von-Neumann

حالا فرض کنید که باب حالت $|۱\rangle$ را به جای حالت $|۰\rangle$ می‌فرستد. محاسبات بالا را می‌توان در مشابهتی کامل انجام داد، نتیجه در تشابهی کامل روابط (۱۹.۳) و (۲۰.۳) است.

اما اگر جاسوس تلاش کند تا احتمال آشکار شدنش یعنی $(d = ۰)$ باشد، آنگاه $\lambda_۱ = ۱$ و $\lambda_۲ = ۰$ خواهد بود و در نتیجه جاسوس نمی‌تواند هیچ اطلاعاتی بدست آورد $I_۰ = ۰$.

همچنین اگر آلیس از دو عملگر رمزگذاری I و σ_z به ترتیب با احتمال مساوی $P_۰ = P_۱ = \frac{۱}{۲}$ استفاده کند، در این صورت

$$\lambda_{۱,۲} = \frac{۱}{۲} \pm |\frac{۱}{۲} - d|$$

یا $\lambda_۱ = d$ و $\lambda_۲ = ۱ - d$ خواهد بود، و ماکزیمم اطلاعات بدست آمده خواهد شد:

$$I_۰(d) = -d \log_۲ d - (۱ - d) \log_۲ (۱ - d) \qquad (۲۱.۳)$$

بنابراین اگر جاسوس تمام اطلاعات را بدست آورد یعنی $I_۰ = ۱$، آنگاه احتمال کشف ایو $d(I_۰ = ۱) = \frac{۱}{۲}$ است.

از این‌رو می‌توان گفت در مقایسه با دیگر پروتکل‌های توزیع کلید کوانتومی مانند پروتکل $BB۸۴$ پروتکل $Ping - Pong$، امکان انتقال قطعی بیت‌ها و ارتباط مستقیم پیام از آلیس به باب را فراهم کرده است، ولی این امکان وجود دارد که جاسوس مقداری از اطلاعات را بدست آورد پس این ارتباط شبه امن است، ضمن این که در مقایسه با پروتکل $BB۸۴$ احتمال کشف جاسوس در این پروتکل بهتر شده است، در این پروتکل در شرایطی که $I_۰ = ۱$ باشد $d = \frac{۱}{۲}$ است، در حالی که در پروتکل $BB۸۴$ احتمال کشف $\frac{۱}{۴} = \frac{۱}{۲} * \frac{۱}{۲} = d$ است. علاوه براین در پروتکل $BB۸۴$ با احتمال $\frac{۱}{۲}$ بیت منتقل شده بدلیل انتخاب پایه‌ی اشتباه از سوی هر دو طرف کنار گذاشته می‌شود، در صورتی که در این پروتکل امکان انتقال قطعی بیت‌ها فراهم شده است.

در این پروتکل با فرض $r = ۱ - c$ یعنی نرخ [۱۵] انتقال مؤثر بیت‌ها، احتمال کشف نشدن جاسوس خواهد بود:

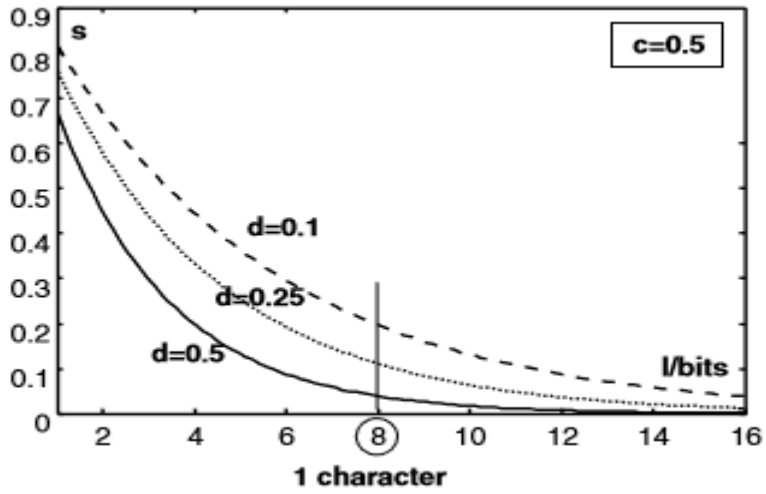
$$\begin{aligned} S(c,d) &= (۱ - c) + c(۱ - d)(۱ - c) + c^۲(۱ - d)^۲(۱ - c) + \cdots \qquad (۲۲.۳) \\ &= \frac{۱ - c}{۱ - c(۱ - d)} \end{aligned}$$

که نمودار (۸.۳) به وضوح این مورد را نشان می‌دهد.

اگر بعد از n بار اجرای پروتکل، جاسوس بتواند $nI_۰(d)$ اطلاعات بدست آورد، با احتمال S^n روی خط باقی می‌ماند، پس اطلاعات بدست آمده برای جاسوس و احتمال شنود بیت‌ها خواهد بود: $I = nI_۰$ و $S^n = S^{\frac{I}{I_۰}}$

$$S(I,c,d) = \Big(\frac{۱ - c}{۱ - c(۱ - d)}\Big)^{\frac{I}{I_۰}} \qquad (۲۳.۳)$$

[۱۵] Rate



شکل ۸.۳: نمودار احتمال شنود موفق جاسوس به عنوان تابعی از ماکزیمم اطلاعات بدست آمده

که البته $I_{\circ}(d)$ بوسیله‌ی (۲۱.۳) محاسبه می‌شود و برای $d > \circ$ و $c > \circ$، این مقدار به صورت نمایی کاهش می‌یابد و در حد $n \longrightarrow \infty$، خواهیم داشت $S \longrightarrow \circ$. بنابراین ایمنی پروتکل مجانبی است [۲۹].

پس از ارائه پروتکل $Ping - Pong$ پروتکل‌های متعددی در زمینه‌ی بررسی امنیت این پروتکل مطرح شدند که در ادامه به مرور تعدادی از آن‌ها خواهیم پرداخت.

۴.۳ بررسی امنیت و طرح‌های حمله به پروتکل Ping-Pong

۱.۴.۳ ارتقا ظرفیت پروتکل بوستروم ـ فلبینگر

در مقاله‌ای که بوستروم و فلبینگر در سال ۲۰۰۳ تحت عنوان پروتکل $Ping - Pong$ ارائه کردند، اطلاعات محرمانه را می‌توان براساس درهم‌تنیدگی یک جفت کیوبیت، در یک روش مستقیم منتقل کرد. اما در این پروتکل اشکالاتی وجود دارد. برای مثال یک شنودکننده‌ی پنهان(جاسوس) می‌تواند اطلاعات را شنود کند، اگر کانال کوانتومی نویز(اختلال) [۱۶] داشته باشد. همچنین می‌توان به این پروتکل بدون استراق سمع حمله کرد. علاوه براین حالت درهم‌تنیده شده در هر بار اجرای مد پیام تنها می‌تواند یک بیت از اطلاعات کلاسیکی را از طریق کانال کوانتومی عبور دهد، یعنی ظرفیت کانال محدود است. اما در سال ۲۰۰۴ لی و کای [۱۷] با ارائه مقاله‌ی سعی کردند تا این اشکال پروتکل $Ping - Pong$ را بر طرف کنند. در این روش یک حالت درهم‌تنیده در هر بار اجرای مد پیام می‌تواند دو بیت اطلاعات کلاسیکی را حمل کند و امنیت آن از طریق بکار بردن پایه‌های اندازه‌گیری مزدوج مختلط [۱۸] در مد

[۱۶] Noisy
[۱۷] Qing-yu Cai and Bai-wen Li
[۱۸] Conjugate Measurement Bases

کنترل تضمین می‌شود.

در این روش در هر بار اجرای مد پیام، آلیس یک بیت را بر روی کیوبیت انتقالی رمزگذاری می‌کند. البته، چهار حالت بل به صورت $|\psi^{\pm}\rangle$ و $|\varphi^{\pm}\rangle$ وجود دارند که متقابلاً هرحالت با یک حالت دیگر متعامد است، و تنها بوسیله‌ی عملگرهای یونیتاری موضعی می‌توان این چهار حالت را به یکدیگر انتقال داد. این چهار حالت را می‌توان به صورت زیر در نظر گرفت:

$$|\varphi^{+}\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle|۰\rangle + |۱\rangle|۱\rangle\Big) = \frac{۱}{\sqrt{۲}}\Big(|+\rangle|+\rangle + |-\rangle|-\rangle\Big) \qquad (۲۴.۳)$$

$$|\varphi^{-}\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle|۰\rangle - |۱\rangle|۱\rangle\Big) = \frac{۱}{\sqrt{۲}}\Big(|+\rangle|-\rangle + |-\rangle|+\rangle\Big) \qquad (۲۵.۳)$$

$$|\psi^{+}\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle|۱\rangle - |۱\rangle|۰\rangle\Big) = \frac{۱}{\sqrt{۲}}\Big(|+\rangle|+\rangle - |-\rangle|-\rangle\Big) \qquad (۲۶.۳)$$

$$|\psi^{-}\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle|۱\rangle - |۱\rangle|۰\rangle\Big) = \frac{۱}{\sqrt{۲}}\Big(|+\rangle|-\rangle - |-\rangle|+\rangle\Big) \qquad (۲۷.۳)$$

که $|-\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle - |۱\rangle\Big)$ و $|+\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰\rangle + |۱\rangle\Big)$ است. حالا فرض کنید که باب یک جفت (EPR) را در حالت $|\psi^{-}\rangle$ آماده می‌کند.

در مد پیام، آلیس عملگر یونیتاری U_{ij} را روی اطلاعات کدگذاری شده‌ی خودش اعمال می‌کند، که U_{ij} ها هستند:

$$U_{۰۰} = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} \qquad U_{۰۱} = \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \qquad (۲۸.۳)$$

$$U_{۱۰} = \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \qquad U_{۱۱} = \begin{pmatrix} ۰ & ۱ \\ -۱ & ۰ \end{pmatrix}$$

این چهار عملگر می‌توانند برای مثال حالت $|\psi^{-}\rangle$ را به ترتیب به حالت‌های $\{|\varphi^{-}\rangle, |\varphi^{+}\rangle, |\psi^{+}\rangle, |\psi^{-}\rangle\}$ انتقال دهند:

$$U_{۰۰}|\psi^{-}\rangle = \Big(|۰\rangle\langle۰| - |۱\rangle\langle۱|\Big)\frac{۱}{\sqrt{۲}}\Big(|۰\rangle|۱\rangle - |۱\rangle|۰\rangle\Big) = |\psi^{-}\rangle$$

وقتی که باب کیوبیت انتقالی را دریافت می‌کند، یک اندازه‌گیری در پایه‌ی بل انجام می‌دهد تا اطلاعات آلیس را رمزگشایی کند. بنابراین، یک حالت درهم‌تنیده می‌تواند در هر بار اجرای مد پیام دو بیت اطلاعات کلاسیکی را منتقل کند.

برای این که تضمین شود پیام منتقل شده در این روش امن است باید مد کنترل اصلاح شود. وقتی که آلیس مد پیام را به مد کنترل سوئیچ می‌کند، او یک اندازه‌گیری تصادفی در یکی از پایه‌های مزدوج

مختلط [۱۹] $B_z = \{|۰\rangle, |۱\rangle\}$ یا $B_x = \{|+\rangle, |-\rangle\}$ انجام می‌دهد. سپس او پایه‌ای را که بکار برده و نتیجه‌ی اندازه‌گیری‌اش را از طریق کانال عمومی اعلام می‌کند. باب نیز مد کنترل را سوئیچ می‌کند و یک اندازه‌گیری در همان پایه‌ی آلیس انجام می‌دهد. اگر هر دو نتیجه منطبق شد، باب می‌فهمد که جاسوس روی خط است و ارتباط متوقف می‌شود. در غیر این صورت باب کیوبیت بعدی را برای آلیس ارسال می‌کند.

البته جاسوس می‌تواند به کیوبیت انتقالی آلیس به باب حمله کند، ولی از آنجا که حالت این کیوبیت پس از عملیات کدگذاری تصادفی آلیس به صورت

$$\rho_A^{\pm} = Tr_B\{|\psi^{\pm}\rangle\langle\psi^{\pm}|\} = Tr_B\{|\varphi^{\pm}\rangle\langle\varphi^{\pm}|\}$$

است، جاسوس نمی‌تواند هیچ یک از حالت‌های بل را تشخیص دهد. بنابراین اطلاعاتی که جاسوس می‌تواند از ماتریس چگالی ρ بدست آورد بوسیله‌ی مرز هولو [۲۰] که کمیتی برای مشخص کردن حداکثر اطلاعات دریافتی است، محدود شده است [۲۶]. در مقابل مقدار اطلاعات کلاسیکی منتقل شده در مد پیام، به واسطه‌ی عملگرهای کدگذاری یکانی موضعی دو برابر شده است. همچنین استفاده از دو پایه‌ای اندازه‌گیری مزدوج مختلط در مد کنترل و همین طور پیام احراز هویت در این مد، پروتکل را در مقابل حمله‌های جاسوس محافظت می‌کند [۳۱].

۲.۴.۳ حمله به پروتکل Ping-Pong بدون استراق سمع

در سال ۲۰۰۴ کای [۲۱] مقاله‌ی را تحت عنوان حمله به پروتکل $Ping-Pong$ بدون استراق سمع منتشر کرد که هدف از ارائه آن را اصلاح پروتکل $Ping-Pong$ عنوان کرد. در این پروتکل که براساس درهم‌تنیدگی جفت کیوبیت‌ها است. یک کیوبیت بین آلیس و باب در رفت و آمد است، اما نکته قابل توجه در مورد همین کیوبیت انتقالی است که اطلاعات آلیس را به باب منتقل می‌کند. امااین اطلاعات دریافتی برای باب قابل اطمینان نیست چرا که پیام نمی‌تواند با موفقیت از آلیس با باب منتقل شود اگر این پروتکل اصلاح نشود.

همان‌طور که در بخش قبل توضیح داده شد در این پروتکل باب دو کیوبیت را در یکی از حالت‌های بل، برای مثال $|\psi^+\rangle = \frac{۱}{\sqrt{۲}}\Big(|۰۱\rangle + |۱۰\rangle\Big)$ آماده می‌کند، سپس یک کیوبیت را برای خودش نگه داشته و کیوبیت دیگر را از طریق کانال کوانتومی برای آلیس ارسال می‌کند. آلیس به صورت تصادفی بین دو مد پیام و کنترل سوئیچ می‌کند. در مد پیام آلیس از عملگر σ_z برای رمزگذاری بیت "۱" و از عملگر I برای رمزگذاری بیت "۰" استفاده می‌کند و سپس آنرا به باب برگشت می‌دهد. باب نیز می‌تواند با اندازه‌گیری بل روی هر دو کیوبیت اطلاعات آلیس را بدست آورد. اما در مد کنترل آلیس یک اندازه‌گیری در پایه‌ی $B_z = \{|۰\rangle, |۱\rangle\}$ انجام می‌دهد و نتیجه را از طریق کانال عمومی به باب اطلاع می‌دهد. باب نیز مد کنترل را سوئیچ و کیوبیت خودش را در پایه‌ی B_z اندازه‌گیری می‌کند، و سپس هر دو نتیجه را با هم مقایسه می‌کند اگر هر دو نتیجه منطبق بود، باب متوجه می‌شود که جاسوس روی

[۱۹] conjugate bases
[۲۰] Holevo bound
[۲۱] Qing-yu Cai

خط است و ارتباط متوقف می‌شود و در غیر این صورت باب کیوبیت بعدی را برای آلیس ارسال می‌کند و ارتباط ادامه می یابد. با این حال، هر اطلاعاتی که جاسوس بدست آورد در حقیقت احتمال کشف او را غیر صفر می‌سازد. بنابراین نادیده گرفتن حمله‌ی که جاسوس بدون استراق سمع می‌تواند نسبت به این ارتباط کوانتومی انجام دهد، باعث خواهد شد که اطلاعاتی که باب از آلیس بدست می‌آورد غیر قابل اطمینان باشد.

فرض کنید که جاسوس روی خط باشد. در مد کنترل جاسوس اقدامی را بر روی کیوبیت انتقالی که آلیس به باب برگشت می‌دهد، انجام نمی‌دهد چون آلیس نتیجه‌ی این مد را اعلام عمومی می‌کند. در مد پیام جاسوس کیوبیت انتقالی را که آلیس به باب برگشت می‌دهد را گرفته و یک اندازه‌گیری در پایه‌ی B_z انجام می‌دهد و سپس این کیوبیت را برای باب ارسال می کند. در این صورت آلیس و باب قادر به کشف حضور جاسوس نیستند. پس باب اجازه می‌دهد تا این ارتباط ادامه یابد، اما نتیجه‌ی هر اندازه‌گیری او بی‌معنی خواهد بود چرا که دو کیوبیت بعد از حمله‌ی اندازه‌گیری جاسوس از یکدیگر مستقل شده‌اند و نتیجه‌ی اندازه‌گیری باب به صورت تصادفی در یکی از حالت‌های $|\psi^{\pm}\rangle$ است. تا زمانی که ارتباط قطع شود، باب چیزی جز یک دنباله‌ی تصادفی بی‌معنی از بیت‌ها را بدست نخواهد آورد.

در اصل حمله به پروتکل $Ping-Pong$ بدون استراق سمع، حالت خاصی از یک حمله‌ی DoS [۲۲] است، البته هدف جاسوس از این حمله بدست آوردن اطلاعات نیست بلکه هدف از این حمله تنها مختل کردن پروتکل است، از این‌رو برای شناسایی چنین حمله‌ای که توضیح داده شد پروتکل $Ping-Pong$ باید اصلاح شود. به این منظور آلیس برای مانع شدن از رسیدن جاسوس به هدفش می‌تواند از استراتژی مشابه این حالت استفاده کند که:

در مد کنترل با احتمال C_0 آلیس کیوبیت انتقالی را در پایه‌ی B_z اندازه‌گیری کند و نتیجه را از طریق کانال عمومی به باب اطلاع دهد، اما در مد پیام، با احتمال $1-C_0$ آلیس به جای رمزگذاری، کیوبیت انتقالی را مستقیماً برای باب ارسال کند. بعد از این که باب کیوبیت را دریافت کرد، بهتر است باب در مورد اعلام وصول کیوبیت انتقالی از طریق کانال عمومی به آلیس اطلاع دهد. چون اگر آلیس عملگرش را بدون خبر اعلام وصول باب منتشر کند، جاسوس می‌تواند کیوبیت را مستقیماً ارسال کند، و باعث ایجاد اختلال در ارتباط بین آلیس و باب شود. پس بهتر است بعد از خبر اعلام وصول از طرف باب، آلیس در مورد عملگر خود به او اطلاع دهد تا اگر باب نتیجه‌ی اندازه‌گیری خود را در حالت $|\psi^{-}\rangle$ بدست آورد، حضور جاسوس آشکار شود. در این وضعیت باب با احتمال $\frac{1}{2}$ حمله‌ی جاسوس را کشف خواهد کرد. هر چند می‌توان پیام احراز هویت ، در یک کانال عمومی قابل اطمینان را جایگزین این روش کرد و بدین ترتیب پروتکل را در مقابل حمله‌ی DoS محافظت نمود.

با این وجود چون هدف از یک ارتباط امن، آن است که بتوان پیام را با موفقیت و به صورت ایمن انتقال داد اگر پروتکل ارتباط کوانتومی $Ping-Pong$ اصلاح نشود انتقال پیام تحت حمله‌ی DoS نمی‌تواند انجام شود. در حالی که در پروتکل‌های قبلی مانند $BB84$ چنین مشکلی وجود ندارد، و امنیت در این پروتکل‌ها براساس نظریه‌ی عدم کپی برداری و این که حالت‌های کوانتومی نامتعامد را نمی‌توان با اطمینان تشخیص داد، تضمین می‌شود، بنابراین کای هدف از طرح این حمله را نشان دادن

[۲۲] Denial-of-Service

شکاف موجود در پروتکل مذکور و بر طرف نمودن آن مطرح می‌کند [۳۰].

۳.۴.۳ شنود در مسیر پروتکل ارتباط کوانتومی Ping-Pong

بعد از کار پیشگامان بنت و براسارد که در سال ۱۹۸۴ منتشر شد، انواع پروتکل‌های ارتباط کوانتومی محرمانه ارائه شدند. اگرچه ویژگی‌های پروتکل‌ها متفاوت بود، اما تقریباً تمام آن‌ها بدنبال تحقق بخشیدن به یک سناریوی رمزنگاری کوانتومی بودند.

تا این‌که در سال ۲۰۰۳ بوستروم و فلبینگر پروتکل رمزنگاری کوانتومی کاملاً متفاوت $Ping-Pong$ را مطرح کردند، که به ادعای نویسندگان آن به تولید کلید قطعی و ارتباط مستقیم امن اجازه می‌داد و امنیت آن از طریق سوئیچ تصادفی بین دو مد پیام (مدی برای انتقال پیام) و مد کنترل (مدی برای کشف استراق‌سمع‌کننده) تضمین می‌شد. اما برخلاف باور آن‌ها ووچیک [۲۳] مدعی بود که امنیت پروتکل می‌تواند از طریق کانال کوانتومی در نظر گرفته شده آسیب قابل توجهی ببیند. همچنین کلید ساخته شده بین آلیس و باب غیرقطعی است اگر و فقط اگر برنتایج اندازه‌گیری انجام شده در مد کنترل منطبق باشد، زیرا تنها پارامتری که جهت شناسایی کردن استراق‌سمع‌کننده دراین مد بررسی می‌شود رابطه بین بیت‌های تولید شده در مد کنترل است که ناکافی است. از این‌رو طرح حمله‌ی ارائه شده توسط ووچیک برای نشان دادن اشکالات این پروتکل است.

در این طرح شنود که با توجه به شکل اصلی پروتکل $Ping-Pong$ است. ووچیک طرح حمله‌ی خود را براساس بازده کانال طراحی کرده است.

- **طرح حمله‌ی ووچیک**

اساس طرح بدین شکل است که، جاسوس برای حمله همزمان از فضای دو مد کمکی x و y و یک تک فوتون در حالت $|۰\rangle$ استفاده می‌کند و دو بار به کانال کوانتومی حمله می‌کند. بار اول هنگام انتقال فوتون از باب به آلیس(حمله‌ی $B-A$) و بار دوم هنگام انتقال از آلیس با باب(حمله‌ی $A-B$). به این منظور جاسوس دو مد کمکی x و y را در حالت $|vac\rangle_x|۰\rangle_y$ آماده می‌کند، که حالت $|vac\rangle$ به معنی مد خالی است.

جاسوس برای حمله به این صورت عمل می‌کند که، ابتدا دو مد کمکی خود را به حالت ارسالی باب اضافه می‌کند

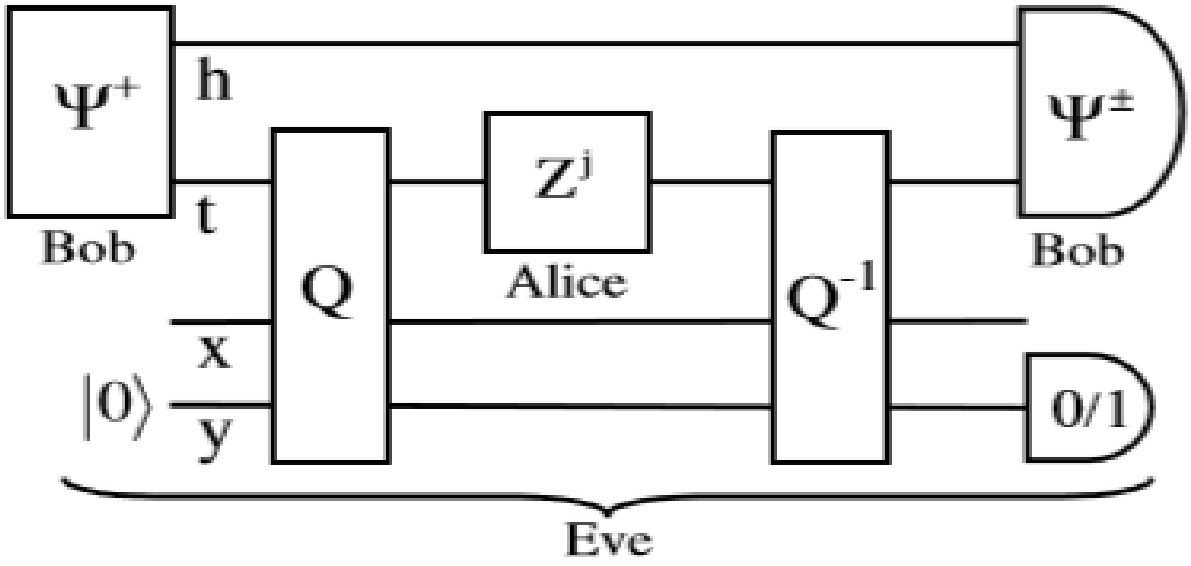
$$|initial\rangle = |\psi^+\rangle_{ht}|vac\rangle_x|۰\rangle_y \qquad (۲۹.۳)$$

سپس عملگر یونیتاری Q را بر روی سه مد y, x, t، (t مد فوتون انتقالی را نشان می‌دهد) اعمال می‌کند.

عملگر Q هست:

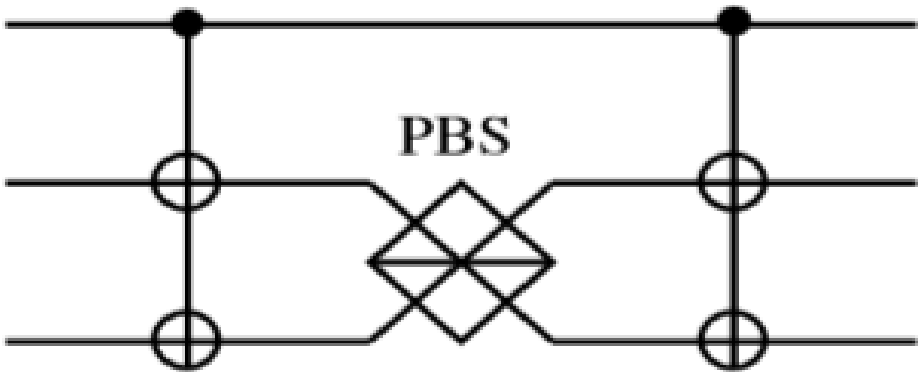
$$Q_{txy} = (SWAP)_{tx}(CPBS)_{txy}H_y \qquad (۳۰.۳)$$

[۲۳] Antoni Wôjcik



شکل ۹.۳: طرح حمله‌ی شنود ووچیک در پروتکل Ping-Pong

و بنابر تعریف ارائه شده در معادله‌ی (۳۰.۳) عملگر Q از گیت هادامارد H، گیت $SWAP$ و گیت $CPBS$ که آن را گیت شکافنده پرتو قطبیده کنترل شده [۲۴] می‌نامند، تشکیل شده است. ساختار گیت $CPBS$ در شکل (۱۰.۳) مشخص است که از یک شکافنده پرتو (PBS) و دو عملگر کنترلی سه‌تایی تشکیل شده است.



شکل ۱۰.۳: ساختار گیت CPBS

البته با توجه به شکل (۱۰.۳)، گیت $CPBS$ موجب انتقال‌های زیر برای حالت‌های کوانتومی

[۲۴] Controlled Polarizing Beam Splitter

می‌شود؛

$$
\begin{aligned}
|\circ\rangle_t|vac\rangle_x|\circ\rangle_y &\longrightarrow |\circ\rangle_t|\circ\rangle_x|vac\rangle_y \\
|\circ\rangle_t|vac\rangle_x|\text{۱}\rangle_y &\longrightarrow |\circ\rangle_t|vac\rangle_x|\text{۱}\rangle_y \\
|\text{۱}\rangle_t|vac\rangle_x|\circ\rangle_y &\longrightarrow |\text{۱}\rangle_t|vac\rangle_x|\circ\rangle_y \\
|\text{۱}\rangle_t|vac\rangle_x|\text{۱}\rangle_y &\longrightarrow |\text{۱}\rangle_t|\text{۱}\rangle_x|vac\rangle_y
\end{aligned}
$$

و بنابراین با بکار بردن عملگر Q انتقال‌های زیر برای حالت‌های کوانتومی خواهد بود:

$$
\begin{aligned}
|\circ\rangle_t|vac\rangle_x|\circ\rangle_y &\longrightarrow |\circ\rangle_t|\circ\rangle_x|vac\rangle_y + |vac\rangle_t|\circ\rangle_x|\text{۱}\rangle_y \\
|\circ\rangle_t|vac\rangle_x|\text{۱}\rangle_y &\longrightarrow |\circ\rangle_t|\circ\rangle_x|vac\rangle_y - |vac\rangle_t|\circ\rangle_x|\text{۱}\rangle_y \\
|\text{۱}\rangle_t|vac\rangle_x|\circ\rangle_y &\longrightarrow |vac\rangle_t|\text{۱}\rangle_x|\circ\rangle_y + |\text{۱}\rangle_t|\text{۱}\rangle_x|vac\rangle_y \\
|\text{۱}\rangle_t|vac\rangle_x|\text{۱}\rangle_y &\longrightarrow |vac\rangle_t|\text{۱}\rangle_x|\circ\rangle_y - |\text{۱}\rangle_t|\text{۱}\rangle_x|vac\rangle_y
\end{aligned}
\tag{۳۱.۳}
$$

از این جهت حالت سیستم در اولین حمله جاسوس در مسیر $(B-A)$ و پس از اعمال عملگر Q خواهد شد:

$$|B-A\rangle = Q_{txy}|\psi^+\rangle_{ht}|vac\rangle_x|\circ\rangle_y$$

$$
\begin{aligned}
|B-A\rangle = \frac{\text{۱}}{\text{۲}}|\circ\rangle_h\Big(|vac\rangle_t|\text{۱}\rangle_x|\circ\rangle_y + |\text{۱}\rangle_t|\text{۱}\rangle_x|vac\rangle_y\Big) \\
+\frac{\text{۱}}{\text{۲}}|\text{۱}\rangle_h\Big(|vac\rangle_t|\circ\rangle_x|\text{۱}\rangle_y + |\circ\rangle_t|\circ\rangle_x|vac\rangle y\Big)
\end{aligned}
\tag{۳۲.۳}
$$

بنابراین اگر کیوبیت انتقالی در حالت $|\circ\rangle_t(|\text{۱}\rangle_t)$ باشد، پس حالت فوتون کمکی $|\circ\rangle$ به مد $x(y)$ می‌رود در حالی که حالت $|\text{۱}\rangle$ به مد $y(x)$ می‌رود، و سرانجام مدهای t و x جابه‌جا می‌شوند و فوتون انتقالی اصلی به واسطه‌ی حمله‌ی جاسوس به مد x منتقل می‌شود. حالا اگر آلیس مد کنترل را سوئیچ کند و حالت مد t را اندازه‌گیری کند، طبق معادله‌ی (۳۲.۳) آلیس با احتمال $\frac{\text{۱}}{\text{۲}}$ فوتونی را آشکار نمی‌کند $(P_{|vac\rangle_t} = \frac{\text{۱}}{\text{۲}})$؛ و اگر فوتونی هم آشکار شود حالت آن کاملاً با حالت فوتون باب ناهمبسته است. پس طبق پروتکل اصلی $Ping-Pong$ باب می‌تواند فوتون بعدی را برای آلیس ارسال کند. بنابراین حضور جاسوس با احتمال صفر آشکار می‌شود.

در مرحله‌ی بعد با فرض سوئیچ مد پیام از طرف آلیس و اعمال عملگر کدگذاری Z_t^j در این مد مطابق با پروتکل $Ping-Pong$، جاسوس خود را برای حمله‌ی دوم یعنی $(A-B)$ و اعمال عملگر $Q_{txy}^{-\text{۱}}$ آماده می‌کند که در نتیجه‌ی این حمله حالت سیستم خواهد بود:

$$|A-B\rangle = Q_{txy}^{-\text{۱}}Z_t^j|B-A\rangle$$

یا به عبارتی جاسوس حمله‌ی خود را بدین شکل انجام می‌دهد

$$|A-B\rangle = H_y^{-1} CPBS_{txy}^{-1} SWAP_{tx}^{-1} \Big\{ \frac{1}{2}|0\rangle_h \Big(|vac\rangle_t |1\rangle_x |0\rangle_y + |1\rangle_t |1\rangle_x |vac\rangle_y \Big) + \frac{1}{2}|1\rangle_h \Big(|vac\rangle_t |0\rangle_x |1\rangle_y + |0\rangle_t |0\rangle_x |vac\rangle_y \Big) \Big\} = \frac{1}{\sqrt{2}} \Big(|0\rangle_h |1\rangle_t |j\rangle_y + |1\rangle_h |0\rangle_t |0\rangle_y \Big) |vac\rangle_x \quad (۳۳.۳)$$

که $j \in \{0,1\}$ و در نهایت جاسوس قطبش حالت فوتون y را اندازه‌گیری می‌کند. در حالی‌که نتیجه‌ی این اندازه‌گیری برای باب با $m = 0(1)$ مشخص می‌شود که مطابق با نتیجه‌ی یکی از حالت‌های کوانتومی $|\psi^+\rangle(|\psi^-\rangle)$ خواهد بود. همچنین می‌توان معادله‌ی (۳۳.۳) را به این شکل بازنویسی کرد:

$$|A-B\rangle = \frac{1}{2} \Big(|\psi^+\rangle_{ht} |j\rangle_y + |\psi^-\rangle_{ht} |j\rangle_y + |\psi^+\rangle_{ht} |0\rangle_y - |\psi^-\rangle_{ht} |0\rangle_y \Big) |vac\rangle_x \quad (۳۴.۳)$$

و با در نظر گرفتن معادله‌ی (۳۴.۳) تنها احتمالات غیر صفر یعنی P_{jkm}، به ترتیب حاصل از نتایج اندازه‌گیری احتمالات ممکن آلیس، جاسوس و باب برای مقادیر مختلف j (با توجه به این نکته که آلیس هر دو مقدار j را با احتمال یکسان $\frac{1}{2}$ می‌فرستد) بدست می‌آید:

$$P_{000} = \frac{1}{2} \Big| \Big(\langle 0|_y \langle \psi^+|_{ht} \Big) \Big(\frac{1}{2}(|\psi^+\rangle_{ht} + |\psi^-\rangle_{ht})|j\rangle_y + \frac{1}{2} \Big((|\psi^+\rangle_{ht} - |\psi^-\rangle_{ht})|0\rangle_y \Big) \Big|^2 = \frac{1}{2}$$

یا

$$P_{000} = \frac{1}{2} \quad (۳۵.۳)$$
$$P_{100} = P_{101} = P_{110} = P_{111} = \frac{1}{8}$$

بنابراین می‌توان جهت بررسی حضور جاسوس اطلاعات متقابل [۲۵] بین (آلیس و جاسوس) و (آلیس و باب) همچنین (باب و جاسوس) را با استفاده از رابطه‌ی

$$I(x,y) = -\sum P(x,y) \log_2 \frac{P(x,y)}{P_x P_y}$$

و احتمالات غیر صفر محاسبه کرد:

$$I_{AE} = I_{AB} = \frac{3}{4} \log_2 \frac{3}{4} \approx 0.311 \quad (۳۶.۳)$$
$$I_{BE} = 1 + \frac{5}{8} \log_2 5 - \frac{3}{2} \log_2 3 \approx 0.074$$

از دیدگاه دیگر می‌توان گفت که اطلاعات متقابل بین جاسوس و آلیس مساوی اطلاعات متقابل بین باب و آلیس است. از طرفی این طرح شنود با توجه به احتمالات غیر صفر یعنی؛ $\sum_k (P_{0k1} + P_{1k0})$ باعث میزان خطای بیت کوانتومی $(QBER)$ [۲۶] در سطح $\frac{1}{4}$ می‌شود. البته مقدار اطلاعات بدست آمده برای

[۲۵] Mutual Information
[۲۶] Quantumn Bit Error Rate

جاسوس و $(QBER)$ به مقدار بیت تولید شده توسط آلیس وابسته است ولی این به مفهوم متقارن [۲۷] بودن طرح نیست. از این‌رو، جاسوس به منظور رفع مشکل عدم تقارن با احتمال $\frac{۱}{۲}$ از یک عملگر یونیتاری مانند عملگر S_{ty} بعد از اعمال عملگر $Q_{txy}^{-۱}$ در هنگام حمله‌ی $A-B$ استفاده می‌کند که این کار باعث ایجاد تقارن می‌شود. عملگر S_{ty} از عملگرهای Z، منفی X و عملگر کنترلی $CNOT$ منفی تشکیل شده است.

$$S_{ty} = X_t Z_t CNOT_{ty} X_t \qquad (۳۷.۳)$$

با اعمال عملگر S_{ty} حالت نهایی سیستم خواهد بود

$$|A-B\rangle^{(s)} = S_{ty}|A-B\rangle$$

$$|A-B\rangle^{(s)} = \frac{۱}{۲}\Big(|\psi^+\rangle_{ht}|j\rangle_y + |\psi^-\rangle_{ht}|j\rangle_y - |\psi^+\rangle_{ht}|۱\rangle_y + |\psi^-\rangle_{ht}|۱\rangle_y\Big) \qquad (۳۸.۳)$$

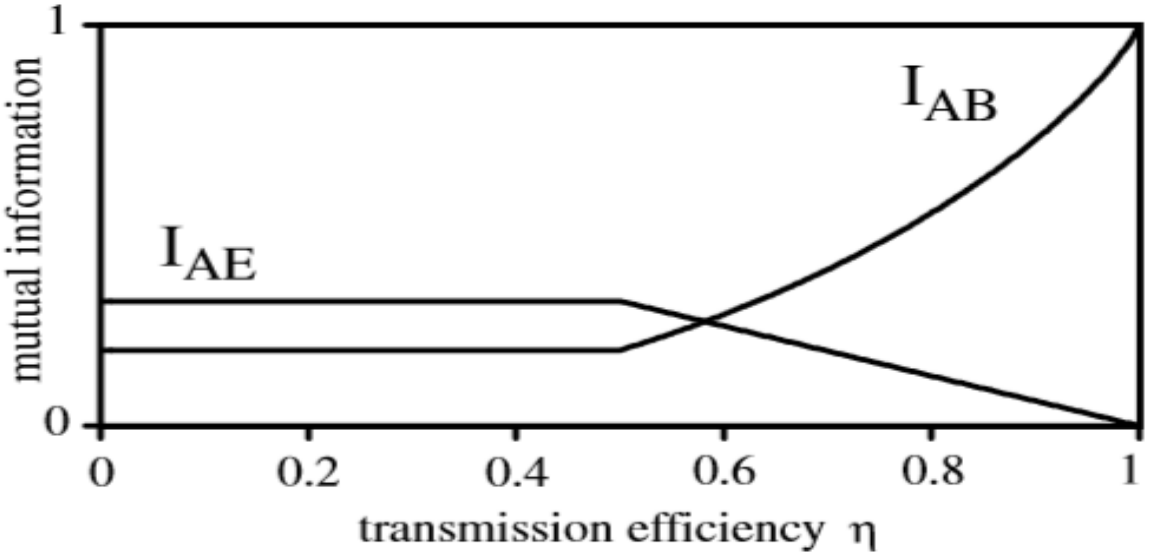
مشخصاً فرایند متقارن‌سازی یک عنصر حیاتی برای طرح شنود نیست، اما باعث می‌شود که اطلاعات متقابل بین آلیس و باب کاهش یابد، در حالی که تأثیری بر روی $(QBER)$ ندارد یا به بیانی دیگر می‌توان گفت که تقارن ارتباط بین آلیس و باب را مختل می‌کند. بنابراین مقدار اطلاعات متقابل بین آلیس و باب در نتیجه‌ی این حمله‌ی تقارنی، کاهش یافته و برابر خواهد بود با:

$$I_{AB} = \frac{۳}{۴}\log_۲ ۳ - ۱ \approx ۰/۱۸۹ \qquad (۳۹.۳)$$

طرح شنود ارائه شده توسط ووچیک ضایعات و خطاهای را تولید می‌کند اما منجر به تولید نتایج همبسته در مد کنترل نمی‌شود، بنابراین جاسوس می‌تواند حضور خود را در ضایعات کانال پنهان کند. برای مثال اگر ایو کانال کوانتومی اصلی با بازده η را با کانالی با بازده انتقالی دو برابر $(\eta = ۲\eta)$ جایگزین کند، آلیس از محاسبه‌ی بازده کانال اصلی مقدار η را بدست می‌آورد، و این در حالی است که، بازده کانال انتقالی باب‌ـآلیس‌ـباب در مد پیام $\eta^۲$ خواهد بود و نه مقدار $۴\eta^۲$. پس در مد پیام جاسوس باید $(=\frac{۳}{۴})$ ۷۵ ٪ از فوتون‌های دریافتی باب را فیلتر کند، بنابراین اثری از حضور جاسوس با توجه به نتایج مد کنترل نخواهد بود. با این حال اگر بازده کانال اصلی η بیش از ۵۰٪ باشد، ممکن است که شنود کشف نشود؛ یا حتی اطلاعات متقابل I_{AE} به مقدار داده شده در معادله‌ی (۳۶.۳) نرسد. در این مورد جاسوس می‌تواند کانال اصلی را با یک کانال ایده‌ال جایگزین کند، اما تنها می‌تواند $\mu = ۲(۱-\eta)$ از بیت‌های انتقالی را شنود کند. در نتیجه همان‌طور که در شکل (۱۱.۳) دیده می‌شود اگر بازده انتقالی کانال بیش از ۶۰٪ باشد، اطلاعات متقابل بین آلیس و جاسوس نمی‌تواند از اطلاعات متقابل بین باب و آلیس بیشتر باشد.

در پایان ووچیک با توجه به طرح حمله‌ی شنود خود پیشنهاداتی را برای اصلاح امنیت پروتکل $Ping-Pong$ مطرح می‌کند. برای مثال، او پیشنهاد می‌کند که به منظور ایجاد امنیت در پروتکل می‌توان قسمتی از کلید را به منظور تخمین زدن $(QBER)$، قربانی کرد، و یا به جهت حفاظت از پروتکل

[۲۷] Symmetric



شکل ۱۱.۳: نمودار بازده انتقال کانال کوانتومی و اطلاعات متقابل

$Ping-Pong$ در مقابل حملات شنود با توجه به این که حمله‌ی جاسوس وابسته به مد انتخابی آلیس است(مد پیام یا مد کنترل)، در مورد حمله‌ی $A-B$ باید در نظر داشت اگر جاسوس حمله‌ی $A-B$ را اعمال کند در حالی که آلیس مد کنترل را انتخاب کرده باشد می‌تواند حالتی بوجود آید که هم آلیس و هم باب فوتون را در حالت انتقال t بیابند این آشکارسازی فوتون برای هر دو نفر می‌تواند به عنوان شاهدی برای وجود جاسوس در نظر گرفته شود. بنابراین بهتر است که آلیس با تأخیر مد انتخابی خود را اعلام کند. از طرف دیگر باب نیز می‌تواند با اندازه‌گیری قطبش فوتون خود، وجود یک فوتون دیگر را در مد انتقال بررسی کند، تا پروتکل امن بماند [۳۲].

در ادامه ژانگ [۲۸] و همکارانش طرح شنود ووچیک بر روی بازده کانال را با استفاده از همان سیستم‌های کمکی، اما عملگرهای متفاوت اصلاح کردند. برای مثال در مسیر حمله‌ی $(B-A)$ آن‌ها به جای عملگر Q_{txy} در رابطه‌ی (۳۰.۳) از عملگر W_{txy} بدین شکل استفاده کردند

$$W_{txy} = U_{txy}V_{txy}Q_{txy} \qquad (۴۰.۳)$$

$$U_{txy} = |۰\rangle\langle۰|_y \otimes SWAP_{tx} + (I_y - |۰\rangle\langle۰|_y) \otimes I_{tx} \qquad (۴۱.۳)$$

$$V_{txy} = |۱\rangle\langle۱|_y \otimes SWAP_{tx} + (I_y - |۱\rangle\langle۱|_y) \otimes I_{tx} \qquad (۴۲.۳)$$

که I عملگر همانی است و Q_{txy} همان عملگر تعریف شده در معادله‌ی (۳۰.۳) است. پس حالت سیستم با انجام عملیات حمله‌ی جاسوس در مسیر $(B-A)$ خواهد بود:

$$|B-A\rangle = W_{txy}\Big(|\psi^+\rangle_{ht}|vac\rangle_x|۰\rangle_y\Big)$$

[۲۸] Zhan-jun Zhang

$$= \frac{۱}{۲}|۰\rangle_h|۱\rangle_t\Big(|vac\rangle_x|۰\rangle_y + |۱\rangle_x|vac\rangle_y\Big) \quad (۴۳.۳)$$
$$+ \frac{۱}{۲}|۱\rangle_h|۰\rangle_t\Big(|vac\rangle_x|۱\rangle_y + |۰\rangle_x|vac\rangle_y\Big)$$

در این مرحله اگر آلیس مد کنترل را سوئیچ کند و مد t را اندازه‌گیری کند، مطابق معادله‌ی (۴۳.۳) با احتمال ۱۰۰٪ حالت این مد را ناهمبسته با حالت مد h بدست خواهد آورد. بنابراین احتمال کشف جاسوس براساس مشاهده‌ی نتایج همبسته صفر است، که این دقیقاً مطابق با طرح ووچیک است. البته ضایعات کانال ناشی از شنود در این طرح صفر است ($P_{|vac\rangle_t} = ۰$) در حالی که ضایعات شنود در طرح ووچیک در این مرحله ۵۰٪ ($P_{|vac\rangle_t} = \frac{۱}{۲}$) است، و این به معنی افزایش دامنه‌ی حمله‌ی جاسوس به بازه بیت‌های منتقل شده $[۰, ۱۰۰٪]$ در این طرح نسبت به طرح قبلی $[۰, ۵۰٪]$ است.

تفاوت دیگر این طرح با طرح قبلی در مد پیام و پس از حمله‌ی جاسوس است، در طرح فعلی حالت سیستم پس از حمله جاسوس خواهد بود:

$$|A-B\rangle_j = W_{txy}^{-۱} Z^j |B-A\rangle \quad (۴۴.۳)$$
$$= \frac{۱}{۲}\Big[(-۱)^j(\psi_{ht}^+ + \psi_{ht}^-)|j\rangle_y + (\psi_{ht}^+ - \psi_{ht}^-)|۰\rangle_y\Big]|vac\rangle_x$$

و همان طور که دیده می‌شود تفاوت این معادله با معادله‌ی (۳۳.۳) در وجود عامل فاز جزئی $(-۱)^j$ است.

همچنین در این طرح نیز برای رفع مشکل عدم تقارن از همان عملگر یونیتاری S_{ty}، تنها با یک تفاوت کوچک استفاده شده است

$$S_{ty} = X_t Z_t CNOT_{ty} X_t Z_t$$

پس حالت سیستم خواهد بود:

$$|A-B\rangle_j^{(s)} = S_{ty}|B-A\rangle_j \quad (۴۵.۳)$$
$$= \frac{۱}{۲}\Big[(\psi_{ht}^+ + \psi_{ht}^-)|j\rangle_y + (-۱)^j(\psi_{ht}^+ - \psi_{ht}^-)|۱\rangle_y\Big]|vac\rangle_x$$

و چون جاسوس می‌داند که چه وقت از عملگر S_{ty} استفاده کرده است، تقارن تولیده شده اطلاعات متقابل بین آلیس و جاسوس را کاهش نمی‌دهد در حالی که ارتباط بین آلیس و باب را مختل می‌کند و اطلاعات متقابل بین آلیس و باب را مطابق معادله‌ی (۳۹.۳) کاهش می‌دهد.

تا اینجا، طرح اصلاح شده تقریباً همان طرح شنود ووچیک است مگر برای ضایعات کانال ناشی از شنود، که در این مورد دامنه‌ی η برای حمله‌های جاسوس به تمام بیت‌های منتقل شده از $[۰, ۵۰٪]$ به $[۰, ۱۰۰٪]$ گسترده شده است، از این جهت پروتکل $Ping-Pong$ در نسخه اصلی خودش قابل شنود و ناامن است، حتی در یک کانال ایده‌ال. سایر موارد پیشنهادی برای ایجاد امنیت پروتکل $Ping-Pong$ در این طرح و طرح شنود ووچیک یکی است، تنها پیشنهاد می‌شود که برای مشخص شدن میزان خطای بیت کوانتومی در پروتکل $Ping-Pong$ آلیس و باب به طور کلی از روش، دو پایه‌ی اندازه‌گیری در مد کنترل استفاده کنند [۳۳].

۴.۴.۳ امنیت پروتکل بوستروم ـ فلبینگر

پس از ارائه پروتکل $Ping-Pong$ مقالات متعددی در زمینه امنیت این پروتکل در هر یک از کانال‌های کوانتومی کامل و ناقص ارائه شد، همچنین امنیت این پروتکل در مقابل حمله‌های متعدد مورد بررسی قرارگرفت که به ادعای برخی از آنها این پروتکل ناامن است. از این‌رو بوستروم و فلبینگر با ارائه مقاله‌ی در سال ۲۰۰۸ مدعی شدند که تمام ادعاها در زمینه ناامنی پروتکل $Ping-Pong$ نادرست هستند.

طراحان پروتکل مدعی بودند که پروتکل $Ping-Pong$، یک پروتکل رمزنگاری کوانتومی منحصر به‌فرد است که ویژگی‌های خاصی دارد مانند: انتقال قطعی بیت‌ها و این که کیوبیت‌ها در این روش دور ریخته نمی‌شوند(برخلاف پروتکل‌های قبلی)، بازده انتقال در مقایسه با پروتکل‌های غیرقطعی مثل $BB۸۴$ و $E۹۱$ که تنها $\frac{۱}{۲}$ از بیت‌های منتقل شده را می‌توان برای اهداف ارتباطی استفاده کرد، دو برابر شده است. در یک کانال کوانتومی کامل وقتی که ایو سعی می‌کند تمام اطلاعات را بدست آورد(یعنی $I_{\circ}=۱$ بیت به ازای هر بیت پیام)، احتمال کشف جاسوس برای هر بیت کنترلی $d=\frac{۱}{۲}$ است، در حالی که در یک سناریوی کاملاً مشابه وقتی جاسوس به همه‌ی بیت‌های منتقل شده حمله می‌کند، در پروتکلی مثل $BB۸۴$ احتمال کشف ایو $d=\frac{۱}{۴}$ است. همچنین به سبب ماهیت پروتکل که براساس درهم‌تنیدگی جفت کیوبیت‌ها است، توزیع کلید کوانتومی مجانبی و ارتباط مستقیم و شبه امن امکان‌پذیر است. به این معنی که احتمال برای این که یک شنودکننده کشف نشده باقی بماند، با طول پیام منتقل شده به صورت نمایی کاهش می‌یابد. همچنین ویژگی دیگر پروتکل آن است که حامل اطلاعات یک کیوبیت منفرد است که به جلو وعقب بین فرستنده و گیرنده سفر می‌کند، که دلیل نام‌گذاری پروتکل $Ping-Pong$ است. به علاوه از دیگر ویژگی‌های پروتکل آن است که فرستنده و گیرنده به صورت تصادفی بین دو مد پیام وکنترل سوئیچ می‌کنند، که در مد پیام تنها یک بیت پیام منتقل می‌شود و در مد کنترل با احتمال قطعی می توان شنودکننده را کشف کرد، و البته واقعیت این است که شنودکننده تنها وقتی متوجه این مد می‌شود که برای فرار از کشف شدن خیلی دیر است و این نکته بسیار مهمی برای امنیت پروتکل است و لازم است که در پیاده‌سازی‌های عملی پروتکل مورد توجه قرار گیرد.

بنابراین به بررسی وضعیت امنیت پروتکل $Ping-Pong$ پس از تلاش‌های متعدد برای حمله به آن در هر یک از کانال‌های کوانتومی کامل و ناقص با توجه به پروتکل‌های رمزنگاری پیشنهادی جایگزین، در امتداد طرح پروتکل اصلی $Ping-Pong$ می‌پردازیم که امکان افزایش بازده یا امکان پیاده‌سازی تجربی آن را ممکن می‌داند. البته با توجه به این نکته که امنیت همه‌ی این پروتکل‌ها براساس امنیت پروتکل اصلی است.

برای مثال، حمله‌ی DOS [۲۹] که کای [۳۰] آن را برای بررسی امنیت پروتکل $Ping-Pong$ پیشنهاد می‌کند و در بخش‌های قبلی به آن پرداختیم نمونه‌ای از این حمله‌ها است. در این حمله جاسوس می‌تواند بدون این که اطلاعات انتقالی قابل آشکارسازی باشند و بدون این که هیچ‌گونه مفهوم اطلاعاتی آشکار شود پروتکل را مختل کند.

در مد پیام جاسوس هر کیوبیت انتقالی برگشتی از آلیس به باب را دریافت کرده و آن را در پایه‌ی

[۲۹] Denial-Of-Service
[۳۰] Qing-yu Cai

Z اندازه‌گیری می‌کند. زیرا با توجه به پروتکل هیچ چک امنیتی در این مسیر وجود ندارد، از این‌رو حمله کشف نشده باقی می‌ماند. چون حمله درهم‌تنیدگی کیوبیت باب و آلیس را از بین می‌برد، از این‌رو بیت خوانده شده توسط باب کاملاً با بیت کدگذاری شده توسط آلیس ناهمبسته است. بنابراین پیام بهم‌ریخته است و از آن‌جا که نتیجه‌ی اندازه‌گیری جاسوس کاملاً تصادفی است، او هیچ اطلاعاتی از پیام بدست نمی‌آورد، اما می‌تواند پروتکل را مختل کند.

البته کای، خود پیشنهاد می‌کند که برای محافظت از پروتکل در مقابل این نوع حمله بهتر است که هم در مکانیک کوانتومی مکانیزم کنترل را اندکی اصلاح کنیم، و هم در مکانیک کلاسیک از یکی از روش‌های استاندارد مانند پیام احراز هویت استفاده کنیم.

اما طراحان پروتکل برای اثبات ایمنی آن حتی پیشنهاد می‌کنند که این حمله اندکی اصلاح شود، و به جاسوس اجازه داده شود که اطلاعات انتقالی در کانال را با معکوس کردن بیت‌های پیام به انتخاب خودش تغییر دهد و به جای اندازه‌گیری کیوبیت، جاسوس از عملگر σ_z استفاده کند بدین ترتیب جاسوس قادر است که اطلاعات پیام را تغییر دهد هرچند به روشی کور، اما بازهم جاسوس قادر به بدست آوردن اطلاعاتی از پیام نیست و پروتکل در شکل اصلی خود امن بوده ومی‌تواند از محرمانگی پیام محافظت کند، اگرچه نه به تمامیت(درست مثل رمزنگاری کلاسیکی یک بار مصرف [۳۱])، که این درست همان ادعای طراحان است که مدعی بودند، امنیت در این پروتکل در مورد توزیع کلید مجانبی و در مورد ارتباط مستقیم شبه امن است.

تا این مرحله اثبات امنیت پروتکل $Ping-Pong$ تنها برای مورد کانال کوانتومی کامل بوده است، وجود هر نقص در کانال به طور بالقوه، دری را برای حمله‌ی جاسوس باز می‌کند، و از آنجا که همه‌ی پروتکل‌های رمزنگاری کوانتومی با چنین مشکلی مواجه هستند روش استاندارد، معرفی مراحل بیشتری برای تصحیح خطا و افزایش حریم خصوصی با استفاده از یک کانال عمومی برای خالص سازی یک کلید کاملاً امن مجانبی است. این روش می‌تواند کاملاً مفید باشد اگراطلاعات متقابل بین فرستنده و گیرنده بیشتر از اطلاعات متقابل بین فرستنده و شنودکننده باشد.

طرح حمله‌ی هوشمندانه‌ی ووچیک بر روی کانال کوانتومی پر اتلاف بر همین اساس است، و شنودکننده را قادر می‌سازد که اطلاعات پیام را بدون آشکار شدن بدست آورد.

ایده اصلی این طرح که در بخش قبل توضیح داده شد، براین اساس است که اگر بازده کانال $\eta <$ ۵۰٪ باشد، جاسوس اتلاف کانال را با یک کانال بهتر جایگزین می‌کند به طوری که اتلاف کانال دقیقاً مشابه با انتظار آلیس و باب باشد. به این ترتیب جاسوس می‌تواند به همه‌ی بیت‌های منتقل شده حمله کند مادامی که غیر قابل کشف باقی بماند، و مقدار اطلاعات متقابل بین خودش و آلیس را نسبت به اطلاعات متقابل بین آلیس و باب افزایش دهد. از این‌رو حتی با تصحیح خطا و افزایش حریم خصوصی، پروتکل ایمن نخواهد بود. بنابراین اگر ۶۰٪ $< \eta <$ ۵۰٪ باشد جاسوس می‌تواند به $\mu = ۲(۱ - \eta)$ قسمت از کیوبیت‌ها حمله کند. ولی اگر بازده کانال بیش از ۶۰٪ باشد، همان طور که در شکل (۱۱.۳) دیده می‌شود اطلاعات متقابل بین آلیس و جاسوس کمتر از اطلاعات متقابل بین آلیس و باب است، پس در این مورد تصحیح خطا و افزایش حریم خصوصی می‌تواند امنیت پروتکل را برقرار کند.

[۳۱] one-time pad

با این حال طراحان پروتکل می‌پذیرند که در مورد وجود حفره‌ی امنیتی در پروتکل راه‌حل پیشنهادی ووچیک برای حفاظت از پروتکل، یعنی تخمین زدن نرخ خطای کیوبیت‌ها که آلیس و باب را مجبور می‌کند تا تعدادی از بیت‌های پیام را قربانی کنند سود مند است. همین طور راه حل دیگر ووچیک یعنی به تأخیر انداختن اعلان آلیس از مد انتقالی تا زمانی که باب بررسی کند، که آیا یک فوتون اضافی در مد انتقال وجود دارد یا خیر؟ برای کشف حمله مفید است، و به این ترتیب می‌توان خلأ امنیتی پروتکل را بر طرف کرد. اما به نظر فلبینگر و بوستروم حمله‌ی ZLM [۳۲] بر روی کانال کوانتومی کامل که در تکمیل طرح شنود ووچیک برای بازده کانال بیش از ۸۰٪ مطرح شده است اشکالاتی دارد. در طرح حمله‌ی مطرح شده، برای مثال در دومین حمله‌ی جاسوس یعنی در زمان برگشت کیوبیت از آلیس به باب و پس از اعمال عملگر کدگذاری آلیس نویسندگان حالت سیستم را

$$|A-B\rangle_j = W_{txy}^{-1} Z^j |B-A\rangle \qquad (۴۶.۳)$$
$$= \frac{1}{2}\Big[(-1)^j(\psi_{ht}^+ + \psi_{ht}^-)|j\rangle_y + (\psi_{ht}^+ - \psi_{ht}^-)|0\rangle_y\Big]|vac\rangle_x$$

می‌دانند که اشتباه است. چرا که حالت سیستم پس از عملگر کدگذاری آلیس بر روی فوتون انتقالی t خواهد بود:

$$Z_t^j |B-A\rangle_j = \frac{1}{\sqrt{2}}\Big[(-1)^j|0,1\rangle_{ht}|x_1\rangle_{xy} + |1,0\rangle_{ht}|x_0\rangle_{xy}\Big] \qquad (۴۷.۳)$$

که

$$|x_1\rangle_{xy} = \frac{1}{\sqrt{2}}\Big(|vac,0\rangle_{xy} + |1,vac\rangle_{xy}\Big) \qquad (۴۸.۳)$$

$$|x_0\rangle_{xy} = \frac{1}{\sqrt{2}}\Big(|vac,1\rangle_{xy} + |0,vac\rangle_{xy}\Big) \qquad (۴۹.۳)$$

هستند، و همان طور که می‌دانیم جاسوس به کیوبیت باب یعنی حالت فوتون h دسترسی ندارد، بنابراین حالت ناشناخته‌ی ماتریس چگالی کل بعد از عملگر کدگذاری آلیس

$$\rho_j = Z_t^j |B-A\rangle\langle B-A| Z_t^{j\dagger} \qquad (۵۰.۳)$$
$$= \frac{1}{2}\Big[|0,1\rangle_{ht}|x_1\rangle_{xy}\langle 0,1|_{ht}\langle x_1|_{xy} + (-1)^j|0,1\rangle_{ht}|x_1\rangle_{xy}\langle 1,0|_{ht}\langle x_0|_{xy}$$
$$+ (-1)^j|1,0\rangle_{ht}|x_0\rangle_{xy}\langle 0,1|_{ht}\langle x_1|_{xy} + |1,0\rangle_{ht}|x_0\rangle_{xy}\langle 1,0|_{ht}\langle x_0|_{xy}\Big]$$

است. هر چند حالت سیستم قابل دسترس برای جاسوس یعنی حالت فوتون t و حالت دو مد کمکی xy بوسیله‌ی رد جزئی بر روی فوتون باب مشخص می‌شود،

$$\rho_j^{(Eve)} = Tr_h\{\rho_j\} \qquad (۵۱.۳)$$

[۳۲] Zhan-jun Zhang, Zhong-xiao Man, and Yong Li

$$\rho_j^{(Eve)} = \frac{1}{2}\Big[|1\rangle_t|x_1\rangle_{xy}\langle 1|_t\langle x_1|_{xy} + |0\rangle_t|x_0\rangle_{xy}\langle 0|_t\langle x_0|_{xy}\Big] \qquad (۵۲.۳)$$

اما با توجه به این که $\rho_j^{(Eve)}$ از مقدار j مستقل است، هیچ اطلاعاتی از پیام برای جاسوس قابل دسترس نیست. همچنین حالت سیستم پس از دومین حمله‌ی جاسوس بدین صورت است:

$$|A-B\rangle_j = W_{txy}^{-1} Z^j |B-A\rangle \qquad (۵۳.۳)$$
$$= \frac{1}{2}\Big[(-1)^j(\psi_{ht}^+ + \psi_{ht}^-) + (\psi_{ht}^+ - \psi_{ht}^-)\Big]|0, vac\rangle_{xy}$$

و همان طور که دیده می‌شود این معادله با معادله‌ی (۴۶.۳) متفاوت است. بنابراین تفسیر ارائه شده در مقاله‌ی مذکور، براساس یک محاسبه‌ی اشتباه انجام شده است: و طرح حمله‌ی ژانگ و همکارانش امنیت پروتکل $Ping-Pong$ را مختل نمی‌کند و مؤثر نیست [۳۴].

۵.۴.۳ امنیت توزیع کلید کوانتومی پروتکل Ping-Pong

در پروتکل ارتباط کوانتومی $Ping-Pong$ برخلاف پروتکل‌های $BB84$ و $E91$ کاربران قانونی، آلیس و باب سعی می‌کنند تا کلید محرمانه‌ای را با استفاده از یک کانال کوانتومی دو طرفه به اشتراک بگذارند: باب یک سیستم تک کیوبیت را برای آلیس ارسال می‌کند و او بعد از کدگذاری یک بیت، به صورت تعیین شده و قطعی آن کیوبیت را به باب برگشت می‌دهد. پس، باب با احتمال ۱ در غیاب یک شنودکننده‌ی پنهان کیوبیت را بدست می‌آورد. بنابراین، آنها می‌توانند بدون اصلاح پایه‌ها، یک کلید محرمانه را به اشتراک بگذارند(در حالی که در $BB84$ یا $E91$ در همین شرایط آنها نیاز به اصلاح پایه‌ها دارند). چنین پروتکل QKD بدون نیاز به اصلاح پایه‌ها، یک پروتکل توزیع کلید کوانتومی قطعی $(DQKD)$ [۳۳] نامیده می‌شود. اما در حضور یک شنودکننده‌ی پنهان(ایو) ارتباط می‌تواند مختل شود. بنابراین، اختلال ایجاد شده توسط ایو می‌تواند امنیت پروتکل را تهدید کند، از این رو بوستروم و فلبینگر جهت تحلیل امنیت پروتکل $Ping-Pong$ ارتباط بین اطلاعات بدست آمده برای جاسوس و نرخ خطای ایجاد شده در مد کنترل را بررسی کردند و با استفاده از مرز هولو [۳۴]، که کمیتی برای مشخص کردن حداکثر اطلاعات دریافتی است؛ نشان دادند که اطلاعات دریافتی جاسوس محدود است. چنین مسئله‌ی را یوشیدا [۳۵] و همکارانش در مقاله‌ای که در سال ۲۰۱۳ منتشر کردند با استفاده از مفهوم رد فاصله [۳۶] اثبات کردند [۳۵].

به منظور اثبات تئوری امنیت بدون قید و شرط پروتکل $Ping-Pong$ براساس نظریه‌ای اطلاعات اختلالی، در اولین گام آنها به این شکل اقدام کردند که: در کانال کوانتومی کامل [۳۷] از باب به آلیس، یک شنودکننده‌ی پنهان هر سیستم برگشتی H_A (سیستم مربوط به آلیس) را نگه داشته و یک عملگر کوانتومی روی آن اعمال می‌کند و سپس سیستم مرکب را اندازه‌گیری می‌کند، تا اطلاعاتی در مورد کلید محرمانه بدست آورد.

---

[۳۳] Deterministic Quantum Key Distribution
[۳۴] Holevo bound
[۳۵] Yoshida
[۳۶] Trace distance
[۳۷] Perfect Quantum Channel

از این جهت یوشیدا و همکارانش با توجه به وجود دو مد کنترل و پیام در این پروتکل حمله را طراحی می‌کنند و اجازه می‌دهند تا جاسوس به مانند پروتکل $Ping-Pong$ عمل کند. یعنی جاسوس سیستم کوانتومی H_E را در حالت $|\Omega\rangle$ آماده می‌کند و عملگر تحول یونیتاری U_{AE} را بر روی سیستم دو قسمتی $H_A \otimes H_E$ اعمال می‌کند:

$$U_{AE}|۰\rangle|x\rangle = \alpha|۰\rangle_A|x_۰\rangle + \beta|۱\rangle_A|x_۱\rangle$$
$$U_{AE}|۱\rangle|x\rangle = \acute{\alpha}|۰\rangle_A|\acute{x_۰}\rangle + \acute{\beta}|۱\rangle_A|\acute{x_۱}\rangle$$

$$|\varphi\rangle = U_{AE}\Big(|\psi^+\rangle|\Omega\rangle\Big) \qquad (۵۴.۳)$$
$$= \frac{۱}{\sqrt{۲}}\Big\{|۰\rangle\Big(\alpha|۰\rangle|x_۰\rangle + \beta|۱\rangle|x_۱\rangle\Big) + |۱\rangle\Big(\acute{\alpha}|۰\rangle|\acute{x_۰}\rangle + \acute{\beta}|۱\rangle|\acute{x_۱}\rangle\Big)\Big\}$$

که $|\alpha|^۲ + |\beta|^۲ = ۱$ و $|\acute{\alpha}|^۲ + |\acute{\beta}|^۲ = ۱$ هستند و $\Big(|x_۰\rangle, |x_۱\rangle, |\acute{x_۰}\rangle, |\acute{x_۱}\rangle\Big)$ بوسیله‌ی عملگر U_{AE} تعیین می‌شوند.

مشابه پروتکل $Ping-Pong$ در مد کنترل آلیس از اندازه‌گیری بر روی فوتون‌ها فهرستی از خروجی‌ها را به صورت $i = \{۰, ۱\}$ بدست می‌آورد، و پس از اعلام مد انتخابی خود، باب نیز مد کنترل را سوئیچ و از اندازه‌گیری فوتون‌ها $\acute{i} = \{۰, ۱\}$ را نتیجه می‌گیرد، بنابراین اگر نتایج این دو اندازه‌گیری نامساوی باشند یعنی $i \neq \acute{i}$ آنگاه (P_e) احتمال نرخ خطا به ازای یک بیت، در مد کنترل توسط باب خوانده می‌شود:

$$P_e := ۱ - \frac{۱}{۲}\Big(|\alpha|^۲ + |\acute{\beta}|^۲\Big) \qquad (۵۵.۳)$$

در این صورت می‌توان با استفاده از مد کنترل آلیس و باب وجود ایو را آشکار کرد اگر و فقط اگر $P_e > ۰$ باشد، که (P_e) دقیقاً تابعی برای تعیین مقدار بازده است، اگر به طور پیش فرض و قرار دادی پارامتر امنیتی تعیین شده برای تشخیص حضور جاسوس $P_s = ۰$ باشد.

اما در مد پیام با توجه به انتخاب عملگر آلیس از مجموعه‌ی $S \in \{۰, ۱\}$ که $S = ۰ = I$ و $S = ۱ = Z$ است، حالت سیستم مرکب $H_A \otimes H_E$ خواهد بود:

$$(I \otimes I \otimes I)|\varphi\rangle = |\varphi\rangle \qquad (۵۶.۳)$$

و

$$(I \otimes Z \otimes I)|\varphi\rangle = |\varphi^-\rangle \qquad (۵۷.۳)$$
$$= \frac{۱}{\sqrt{۲}}\Big\{|۰\rangle\Big(\alpha|۰\rangle|x_۰\rangle - \beta|۱\rangle|x_۱\rangle\Big) + |۱\rangle\Big(\acute{\alpha}|۰\rangle|\acute{x_۰}\rangle - \acute{\beta}|۱\rangle|\acute{x_۱}\rangle\Big)\Big\}$$

سپس جاسوس یک اندازه‌گیری بر روی هر حالت انجام می‌دهد تا اطلاعاتی در مورد کلید بدست آورد، نتیجه‌ای این اندازه‌گیری جاسوس دو ماتریس چگالی کاهشی $\rho_۰$ و $\rho_۱$ است.

$$\rho_۰ : = tr_{BA}|\varphi\rangle\langle\varphi| \qquad \rho_۱ : = tr_{BA}|\varphi^-\rangle\langle\varphi^-|$$

البته به جهت محاسبه‌ی میزان اطلاعات بدست آمده برای جاسوس باید اطلاعات متقابل بین آلیس و جاسوس را تخمین زد، در این مقاله یوشیدا وهمکارانش این کار را با استفاده از مفهوم رد فاصله انجام می‌دهند. رد فاصله معیاری برای تمیزناپذیری دو حالت کوانتومی است؛ و برای دو حالت کوانتومی ρ و σ به این شکل تعریف می‌شود که:

$$\|\rho-\sigma\|:=\frac{۱}{۲}tr|\rho-\sigma|$$

همچنین این کمیت(رد فاصله) مقادیر ۰ تا ۱ را می‌گیرد، و $\|\rho-\sigma\|=۰$ اگر و فقط اگر $\rho=\sigma$ باشد.

از این رو یوشیدا و همکارانش امنیت پروتکل $Ping-Pong$ را با توجه به مفهوم رد فاصله و رابطه‌ی بین اطلاعات دریافتی برای جاسوس و بازه خطای ایجاد شده در مد کنترل، این‌گونه تحلیل می‌کنند که:

$$\begin{aligned}I(A:E)\leqslant\|\rho_{۰}-\rho_{۱}\|&=\frac{۱}{۲}tr|\rho_{۰}-\rho_{۱}| \qquad (۵۸.۳)\\ &=\frac{۱}{۲}tr\Big|\alpha\bar{\beta}|۰\rangle|x_{۰}\rangle\langle۱|\langle x_{۱}|+\bar{\alpha}\beta|۱\rangle|x_{۱}\rangle\langle۰|\langle x_{۰}|\\ &\quad+\acute{\alpha}\bar{\acute{\beta}}|۰\rangle|\acute{x}_{۰}\rangle\langle۱|\langle\acute{x}_{۱}|+\bar{\acute{\alpha}}\acute{\beta}|۱\rangle|\acute{x}_{۱}\rangle\langle۰|\langle\acute{x}_{۰}|\Big|\\ &=\frac{۱}{۲}\Big\{tr\Big|\alpha\bar{\beta}|۰\rangle|x_{۰}\rangle\langle۱|\langle x_{۱}|+\bar{\alpha}\beta|۱\rangle|x_{۱}\rangle\langle۰|\langle x_{۰}|\\ &\quad+\acute{\alpha}\bar{\acute{\beta}}|۰\rangle|\acute{x}_{۰}\rangle\langle۱|\langle\acute{x}_{۱}|+\bar{\acute{\alpha}}\acute{\beta}|۱\rangle|\acute{x}_{۱}\rangle\langle۰|\langle\acute{x}_{۰}|\Big|\Big\}\\ &=|\alpha\beta|+|\acute{\alpha}\acute{\beta}|\end{aligned}$$

و رابطه‌ی (۵۸.۳) با جایگزینی P_e (نرخ خطا) خواهد شد:

$$I(A:E)\leqslant ۲\sqrt{P_e} \qquad (۵۹.۳)$$

بنابراین می‌توان نتیجه گرفت که نامساوی رد فاصله دو معنی دارد:

۱) جاسوس اطلاعاتی از کلید بدست می‌آورد، اگر و فقط اگر $P_e>۰$ باشد. همچنین اگر $I(A:E)>۰$ باشد، جاسوس بدون آشکار شدن نمی‌تواند اطلاعاتی بدست آورد.

۲) نامساوی رد فاصله به معنی ارتباط بین اطلاعات بدست آمده برای جاسوس و نرخ خطاست. برای مثال، اگر بازده خطای حمله‌ی جاسوس بیش از اطلاعات بدست آمده برای جاسوس است، در نتیجه‌ی نرخ بازده خطای بزرگ ، جاسوس آشکار می‌شود.

پس همان‌طور که از تفسیر نامساوی رد فاصله می‌توان دید امنیت پروتکل $Ping-Pong$ در مورد این حمله نیز همچنان برقرار است.

فصل ۴

نتیجه‌گیری

هدف از ارائه این پایان‌نامه بررسی استفاده از ویژگی درهم‌تنیدگی در یک پروتکل ارتباط کوانتومی مستقیم و کاربرد آن در رمزنگاری کوانتومی است. لذا به عنوان مقدمه در فصل اول به بیان تاریخچه‌ای از رمزنگاری و اصول و کاربردهای آن در ادوار مختلف تاریخ پرداخته شد، در ادامه با در نظر گرفتن ناکارآمدی این نوع از رمزنگاری کلاسیکی همزمان با پیدایش و ظهور سرعت و قدرت محاسباتی بالا در کامپیوترها و اهمیت امنیت اطلاعات و ارتباطات با توجه به پیشرفت فناوری‌های روز، و افزایش احتمال سریع استفاده از کامپیوترهای کوانتومی، و جایگزینی نوع جدیدی از رمزنگاری پرداختن به مبحث نظریه‌ی محاسبات و اطلاعات کوانتومی و بیان تفاوت‌های این نوع رمزنگاری با نمونه کلاسیکی آن در ادامه این فصل ضروری دیده شد. در فصل دوم ضمن توصیف نمایی کلی از پروتکل توزیع کلید کوانتومی و طبقه بندی حملات شنود، چند پروتکل توزیع کلید کوانتومی با ویژگی‌های مختلف مورد بررسی قرار گرفت. برای مثال پروتکل $BB۸۴$ با ویژگی انتقال کیوبیت‌های مستقل، و نیز پروتکل‌های مشابه آن مانند $B۹۲$ و پروتکل $E۹۱$ بر مبنای درهم‌تنیدگی کوانتومی مورد بحث و بررسی قرار گرفت.

توزیع کلید و برقراری ارتباط در پروتکل‌های توصیف شده و بسیاری از پروتکل‌های دیگر برمبنای انتقال ذرات کوانتومی یعنی همان فوتون‌ها است. البته این پروتکل‌ها براساس اصل عدم قطعیت در مکانیک کوانتومی غیر قطعی هستند. اما پروتکل توصیف شده در فصل سوم یعنی پروتکل $Ping-Pong$ با توجه به مفهوم درهم‌تنیدگی کیوبیت‌ها و برمبنای یک ارتباط مستقیم و قطعی است؛ به این معنا که کیوبیت‌ها یا همان ذرات حامل اطلاعات، در این پروتکل به صورت قطعی منتقل شده و کنار گذاشته نمی‌شوند. ایده این پروتکل رمزنگاری بوسیله‌ی اعمال عملگرهای جایگزیده بر روی یک زوج EPR است. بنابراین می‌توان یک بیت اطلاعات را، در یکی از حالت‌های بل مثلاً $|\psi^{\pm}\rangle$ رمزگذاری کرد به‌گونه‌ای

که حالت کیوبیت برای کسی که تنها به یکی از دو کیوبیت دسترسی دارد نامشخص باشد. همچنین این پروتکل از دو مد ارتباطی پیام و کنترل بهره می‌برد که در مد پیام کیوبیت انتقال داده می‌شود و از مد کنترل جهت کشف شنودکننده پنهان و امنیت پروتکل استفاده می‌شود. البته استراتژی‌های زیادی در مورد حمله به این پروتکل با توجه به این دو مد ارتباطی مطرح شدند که به چند نمونه از آن‌ها پرداخته شد، و امنیت پروتکل در مقابل این استراتژی‌های حمله به اثبات رسید. این بررسی‌ها نشان می‌دهد که پروتکل $Ping - Pong$ همانند ادعای طراحان آن یک پروتکل ارتباط کوانتومی است که به توزیع کلید مجانبی امن و ارتباط مستقیم شبه امن اجازه می‌دهد.

مراجع

[1] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, (India), p. 175, 1984.

[3] J. Katz and Y. Lindell, "Introduction to modern cryptography: Principles and protocols," p. 553.

[4] H. H. Clark and E. F. Schaefer, "Concealing one's meaning from overhearers," *Journal of Memory and Language*, vol. 26, no. 2, pp. 209 – 225, 1987.

[5] S. M. Barnett, *Quantum information*. Oxford Master Series in Atomic, Optical and Laser Physics, Oxford Univ. Press, 2009.

[6] S. Goldwasser and M. Bellare, "Lecture notes on cryptography," 2001.

[7] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2 ed., 2008.

[8] X. Ma, "Quantum cryptography: theory and practice," *arXiv preprint arXiv:0808.1385*, 2008.

[9] R. Tripathi and S. Agrawal, "Comparative study of symmetric and asymmetric cryptography techniques," *International Journal of Advance Foundation and Research in Computer (IJAFRC), ISSN*, pp. 2348–4853, 2014.

[10] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007.

[11] C. Kollmitzer and M. Pivk, *Applied quantum cryptography*, vol. 797. Springer, 2010.

[12] G. Stephen, *Quantum physics*. Wiley, 2003.

[13] J. J. Sakurai, *Modern Quantum Mechanics (Revised Edition)*. Addison Wesley, revised ed., Sept. 1993.

[14] D. McMahon, *Quantum Computing Explained*. Dec 04 2007, 2007.

[15] P. Pajic, "Quantum cryptography," 2013.

[16] A. Mink, S. Frankel, and R. A. Perlner, "Quantum key distribution (QKD) and commodity security protocols: Introduction and integration," *CoRR*, vol. abs/1004.0605, 2010.

[17] N. J. Beaudry, "Assumptions in Quantum Cryptography," *ETH Zurich*, no. 22269, p. 221, 2014.

[18] H.-K. Lo and Y. Zhao, "Quantum cryptography," *arXiv preprint arXiv:0803.2507*, 2008.

[19] N. J. Beaudry, "Assumptions in quantum cryptography," *arXiv preprint arXiv:1505.02792*, 2015.

[20] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, pp. 3018–3021, Oct 1998.

[21] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical review letters*, vol. 92, no. 5, p. 057901, 2004.

[22] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Physical Review Letters*, vol. 85, no. 6, p. 1330, 2000.

[23] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.

[24] M. Dušek, O. Haderka, and M. Hendrych, "Generalized beam-splitting attack in quantum cryptography with dim coherent states," *Optics communications*, vol. 169, no. 1, pp. 103–108, 1999.

[25] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, pp. 1863–1869, Mar 1995.

[26] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

[27] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, Apr 2000.

[28] A. Cabello, "Addendum to"quantum key distribution without alternative measurements"," *arXiv preprint quant-ph/0009051*, 2000.

[29] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, p. 187902, Oct 2002.

[30] Q.-y. Cai, "The "ping-pong" protocol can be attacked without eavesdropping," *Phys. Rev. Lett.*, vol. 91, p. 109801, Sep 2003.

[31] Q.-y. Cai and B.-w. Li, "Improving the capacity of the boström-felbinger protocol," *Phys. Rev. A*, vol. 69, p. 054301, May 2004.

[32] A. Wójcik, "Eavesdropping on the "ping-pong" quantum communication protocol," *Phys. Rev. Lett.*, vol. 90, p. 157901, Apr 2003.

[33] Z.-j. Zhang, Y. Li, and Z.-x. Man, "Improved wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss," *Physics Letters A*, vol. 341, no. 5, pp. 385–389, 2005.

[34] K. Boström and T. Felbinger, "On the security of the ping-pong protocol," *Physics Letters A*, vol. 372, no. 22, pp. 3953–3956, 2008.

[35] M. Yoshida, T. Miyadera, and H. Imai, "On the security of quantum key distribution ping-pong protocol," *Journal of Quantum Information Science*, vol. 3, no. 01, p. 16, 2013.

واژه‌نامه فارسی به انگلیسی

رمزنگاری ..... Cryptography
رمزنگاری کلاسیکی ..... Classical Cryptography
رمزنگاری کوانتومی ..... Quantum Cryptography
توزیع کلید کوانتومی ..... Quantum Key distribution
درهم‌تنیدگی ..... Entanglement
کیوبیت ..... Qubits
حمله‌های جاسوس ..... Eve attacks
استراتژی حمله ..... Attack strategy
استراق سمع کننده ..... Eavesdropper
ارتباط کوانتومی ..... Quantum communication
الگوریتم ..... Algorithm

واژه‌نامه انگلیسی به فارسی

رمزنگاری ..... cryptography
رمزنگاری کلاسیکی ..... classical cryptography
رمزنگاری کوانتومی ..... Quantum Cryptography
توزیع کلید کوانتومی ..... Quantum key distribution
درهم تنیدگی ..... Entanglement
کیوبیت ..... Qubits
حمله‌های جاسوس ..... Eve attacks
استراتژی حمله ..... Attack strategy
استراق سمع کننده ..... Eavesdropper
ارتباط کوانتومی ..... Quantum communication
الگوریتم ..... Algorithm

Abstract

Distributing a secure key between two legitimate users over a distance, is the main task of cryptography. In classical cryptography, security of secret key is based on the difficulty of math functions, while, in quantum cryptography or quantum key distribution(QKD), security depends on fundamental principals of quantum mechanics. Several protocols have been introduced for QKD which almost all of them use carrying particle to send information from sender to reciever. The security of QKD protocols provided by several steps such as authentication, sifting process and privacy amplification processes.

In 2003, Bostrom and Felbinger presented a direct two-way quantum communication based on entangled qubits. Since the information is transferred in a deterministic manner, no qubits have to be discarded and therefore the information can be decoded after the transmission. In this protocol security against eavesdropping attacks is provided by the control mode in quantum communication.

In this thesis, first we have review some basic concepts used in cryptography. Then we have a general overview of quantum key distribution and some well-known quantum key distribution protocols. Finally we presented a complete explanation of Ping-Pong protocol and investigate its security against different kinds of attacks.

keywords: Classical Cryptography, Quantum Cryptography, Quantum Key Distribution, Entanglement, Qubits

Shahrood University of Technology

Faculty Of Physics and Nuclear Engineering

MSc Thesis in: Particle Physics

Using Entanglement in direct Quantum Communication and its application in Quantum Cryptography

By: Maryam Nasiri

Supervisor

Dr. M. Annabestani

February 2017