دانشکده فیزیک

گروه ذرات بنیادی

پایان‌نامه کارشناسی ارشد

مطالعه روش و بررسی امنیت توزیع کلید کوانتومی در پروتکل $N۰۹$

معصومه گل‌آرا

استاد راهنما

دکتر مصطفی عنابستانی

بهمن ۱۳۹۴


بسم الله الرحمن الرحيم

این دیده نیست، لایق دیدار روی تو
چشمی دگر بده، که تماشا کنم تورا...
اللهم عجل لولیک الفرج

تقدیم به پدر و مادر عزیز و مهربانم
که همواره در زندگی پشتیبانی محکم و مطمئن برایم هستند.
و برادران و خواهرانم
امیر، علی، آزاده و عاطفه

سپاس خدای را که هر چه دارم از اوست به امید آنکه توفیق یابم جز خدمت به خلق او نکوشم.

از استاد گرامیم جناب آقای دکتر عنابستانی بسیار سپاسگزارم چرا که بدون راهنمایی‌ها و سعه صدر مثال زدنی ایشان، به ثمر رسیدن این پایان نامه ممکن نبود.

همچنین سپاسگزار همیشگی پدر و مادرم از ابتدا تا ابد بوده و هستم و در این پایان نامه حمایت، ذکر و دعاهای آن‌ها بود که فرش مسیر تلاشم شد.

معصومه گل آرا
بهمن ۱۳۹۴

تعهدنامه

اینجانب **معصومه گل‌آرا** دانشجوی کارشناسی ارشد رشته **ذرات بنیادی دانشکده فیزیک** دانشگاه شاهرود، نویسنده پایان‌نامه با عنوان **مطالعه روش و بررسی امنیت توزیع کلید کوانتومی در پروتکل** $N۰۹$ ، تحت راهنمایی **دکتر 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 شاهرود متعلق دارد، و مقالات مستخرج با نام " دانشگاه شاهرود " یا " Shahrood University " 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.

معصومه گل‌آرا
بهمن ۱۳۹۴

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 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

امروزه رمزنگاری کوانتومی به طور گسترده مورد توجه قرار گرفته است. زیرا برخلاف نمونه‌ی کلاسیکی آن، می‌تواند با به کارگیری قوانین فیزیکی بدون آنکه نیازی به محاسبات ریاضی پیچیده داشته باشد، امنیت یک ارتباط را تأمین کند. توزیع کلید کوانتومی (QKD) یکی از مهمترین بخش‌ها در رمزنگاری کوانتومی است که در آن دو شخص دور از هم (مانند آلیس و باب) می‌توانند یک کلید رمز را بین خود به اشتراک بگذارند تا در آینده بتوانند از آن به عنوان کلید برای یک پیام کلاسیکی استفاده کنند.

از اولین طرح توزیع کلید کوانتومی ارائه شده توسط بِنِت و بِراسارد در سال ۱۹۸۴ ($BB۸۴$) تا چند سال گذشته همه پروتکل‌ها براساس انتقال ذرات حامل اطلاعات از طریق یک کانال کوانتومی بنا شده‌اند. در سال ۲۰۰۹ یک فیزیکدان کره‌ای به نام نُه (Noh) با استفاده از ایده **اندازه‌گیری بدون برهمکنش** یک پروتکل توزیع کلید کوانتومی جدید ارائه داد. درواقع پروتکل پیشنهادی وی با سایر پروتکل‌ها تفاوت عمده‌ای داشت. زیرا کلید خام این پروتکل از رویدادهایی انتخاب می‌شوند که در آن فوتون‌ها از کانال کوانتومی عبور نکرده‌اند. در نتیجه شنودکننده قادر نیست به هیچ یک از فوتون‌هایی که به عنوان کلید خام انتخاب می‌شوند دسترسی داشته باشد. همین امر سبب می‌شود که از لحاظ امنیتی پروتکل $N۰۹$ مورد توجه ویژه‌ای قرار بگیرد. هرچند بازه تولید کلید در آن کم باشد.

در این پایان نامه، ابتدا پیشینه رمزنگاری کلاسیکی و انواع آن عنوان می‌شود. سپس با بیان مقدمه‌ای از نظریه اطلاعات کوانتومی به بررسی مراحل یک پروتکل توزیع کلید کوانتومی می‌پردازیم. در ادامه سه پروتکل مهم در زمینه رمزنگاری کوانتومی را مطرح کرده و امنیت آن‌ها را به طور مختصر بررسی می‌کنیم. در نهایت توضیحات کاملی درباره روند اجرای پروتکل $N۰۹$ ارائه خواهیم داد و به بررسی امنیت آن خواهیم پرداخت.

کلمات کلیدی: رمزنگاری، توزیع کلید کوانتومی، حمله سدسازی و بازارسال، امنیت پروتکل، اندازه‌گیری، اندازه‌گیری بدون برهمکنش.

لیست مقالات مستخرج از پایان‌نامه

۱. مصطفی عنابستانی، معصومه گل‌آرا " توزیع کلید کوانتومی بر پایه دوربری کوانتومی " کنفرانس فیزیک ایران سال ۹۴ (دانشگاه فردوسی مشهد)
شهریور ماه ۱۳۹۴

فهرست مطالب

فهرست تصاویر د

۱ مقدمه ۱

۱.۱ رمزنگاری ۲

۱.۱.۱ رمزنگاری با کلید سری(متقارن) ۳

۲.۱.۱ رمزنگاری با کلید عمومی(نامتقارن) ۶

۲.۱ رمزنگاری کوانتومی ۸

۳.۱ نظریه اطلاعات کوانتومی ۸

۱.۳.۱ کیوبیت ۹

۲.۳.۱ عملگرهای خطی ۱۲

۳.۳.۱ ضرب داخلی ۱۳

۴.۳.۱ ضرب خارجی ۱۵

۵.۳.۱ ضرب تانسوری ۱۶

۶.۳.۱ اندازه‌گیری کوانتومی ۱۷

۷.۳.۱ عملگر چگالی؛ حالتهای مخلوط و خالص ۱۸

۸.۳.۱ حالت‌های درهم‌تنیده ۱۹

۹.۳.۱ اصل عدم کپی برداری ۲۲

۲ توزیع کلید کوانتومی و امنیت آن ۲۵

۱.۲ نمای کلی توزیع کلید کوانتومی ۲۶

۲.۲ استراتژی های حمله ۲۷

۱.۲.۲ تعاریف مورد نیاز ۲۸

۳.۲ پروتکل BB۸۴ . . . . . ۳۰

۴.۲ پروتکل $E۹۱$ ۳۸

۵.۲ پروتکل **Ping-Pong** ۴۰

۶.۲ استراتژی‌های حمله در محیط واقعی ۴۶

۱.۶.۲ حمله **PNS** ۴۷
۲.۶.۲ حمله اسب تروژان ۴۸

۳ پروتکل توزیع کلید کوانتومی به روش$N09$ ۵۱
۱.۳ مقدمه ۵۲
۲.۳ اندازه‌گیری بدون برهم‌کنش ۵۲
۳.۳ آزمایش نتیجه منفی رنینگر ۵۴
۴.۳ اندازه‌گیری بدون برهم‌کنش الیتزور و وایدمن ۵۵
۵.۳ پروتکل $N09$ ۵۹
۶.۳ بررسی امنیت پروتکل$N09$ ۶۵
۱.۶.۳ امنیت در مقابل حمله$I\&R$ ساده ۶۸
۲.۶.۳ تشخیص کانال کوانتومی ۷۱
۳.۶.۳ امنیت در مقابل سایر حمله ها ۷۴

۴ نتیجه‌گیری ۷۷

مراجع ۸۰

نمایه ۸۵

فهرست تصاویر

۱.۱ فراوانی استفاده از حروف در زبان انگلیسی[۱] ۳
۲.۱ رمزنگاری با کلید متقارن ۵
۳.۱ رمزنگاری با کلید نا متقارن ۷
۴.۱ کره بلاخ؛ نمایش یک کیوبیت ۱۱

۱.۲ حمله $I\&R$ ساده ۳۴
۲.۲ حمله $I\&R$ کامل ۳۵
۳.۲ الف: نمایی از مُد پیام ؛ ب: نمایی از مُد کنترل ۴۳

۱.۳ آزمایش نتیجه منفی رنینگر[۳۲] ۵۴
۲.۳ تداخل سنج ماخ-زندر ۵۵
۳.۳ اندازه‌گیری بدون برهم‌کنش الیتزور و وایدمن ۵۷
۴.۳ نمای پروتکل $N۰۹$ ۶۰
۵.۳ نحوه عملکرد یک شکافنده پرتو قطبشی ۶۱
۶.۳ نحوه عملکرد آشکارساز قطبشی ۶۲
۷.۳ نمایش دیگری از پروتکل$N۰۹$ ۶۲

فصل ۱

مقدمه

۱.۱ رمزنگاری

کریپتوگرافی یا رمزنگاری از دو واژه (crypt) به معنای رمز و (graphy) به معنای نگارش پدید آمده است. هدف این علم ساختن طرح‌ها یا پروتکل‌هایی است که بتوان با کمک آنها حتی در حضور دشمن یا شنودکننده [۱] نیز اطلاعات مهمی را ردوبدل کرد. رمزنگاری پیشینه بسیار طولانی و درخشانی دارد که به هزاران سال قبل برمی‌گردد. از علوم نظامی در زمان یونان باستان گرفته تا مسائل امنیتی در اقتصاد، سیاست و حتی در دنیای امروز اینترنت، مخابره اطلاعات به صورت ایمن مدیون پیشرفت در زمینه رمزنگاری است. یکی از اولین استفاده‌کنندگان از رمزنگاری جولیس سزار سردار روم باستان است. روش رمزنگاری او روشی بسیار ساده است. به این ترتیب که او تمام حروف الفبا در متن موردنظر را به اندازه مشخصی جابه‌جا کرد. برای مثال اگر اندازه جابه‌جایی، یک درنظر گرفته شده باشد، آنگاه A به صورت B رمزی می‌شود و $B \to C$ و به همین ترتیب...$Y \to Z$ و در نهایت $Z \to A$ رمزی می‌شود.

روند کار در رمزنگاری به این صورت است که متن اصلی پیام که با اصطلاح متن آشکار [۲] مطرح می‌شود، با استفاده از کلید رمز [۳] که تنها برای گیرنده و فرستنده مشخص است، به متن دیگری به نام متن رمز [۴] تبدیل می‌شود. این متن رمز، غالبا ظاهری نامفهوم و تصادفی دارد که از فرستنده به گیرنده فرستاده می‌شود. به همین ترتیب گیرنده با داشتن کلید رمز، متن رمز را رمزگشایی می‌کند و پی به متن اصلی می‌برد.

در مدل رمزنگاری سزار، کلید یکی از ۲۵ عدد صحیح اول می‌تواند باشد (تعداد حروف الفبایی انگلیسی ۲۶ است) که به عنوان مقدار جابه‌جایی درنظر گرفته می‌شود. نقطه ضعف بارز رمزنگاری به شیوه سزار محدود بودن تعداد کلیدهای ممکن است که در پی آن هر شخصی می‌تواند با امتحان کردن تک تک امکان‌ها پی به متن اصلی ببرد. روش دیگری که در تکمیل روش سزار مطرح می‌شود روش جابه جایی است. در رمزنگاری به روش جابه‌جایی هر حرف از حروف الفبا با یکی از حروف دیگر جابه‌جا می‌شود که در نتیجه تعداد کلید های ممکن چیزی در حدود $۴ \times ۱۰^{۲۶} \approx ۲۶!$ می‌تواند باشد. واضح است در این روش کشف متن اصلی به روش امتحان کردن کار طاقت فرسایی است. هرچند این

[۱] evasdropper
[۲] plaintext
[۳] secret key
[۴] cipher

روش از مدل سزار قوی‌تر است ولی باز هم دارای نقطه ضعف است. حروف به کار رفته در یک متن دارای فراوانی‌های مشخص هستند. این فراوانی‌ها به متن مربوطه مرتبط است اما به طور کلی در زبان انگلیسی استفاده از حروف دارای یک فراوانی نسبی است که در جدول زیر آورده شده است:

A	8.2%	J	0.1%	S	6.3%
B	1.5%	K	0.8%	T	9.0%
C	2.8%	L	4.0%	U	2.8%
D	4.2%	M	2.4%	V	1.0%
E	12.7%	N	6.7%	W	2.4%
F	2.2%	O	7.5%	X	0.1%
G	2.0%	P	1.9%	Y	2.0%
H	6.1%	Q	0.1%	Z	0.1%
I	7.0%	R	6.0%		

شکل ۱.۱: فراوانی استفاده از حروف در زبان انگلیسی[۱]

از جدول مشخص است که حروفی نظیر E،T،A،I و O پراستفاده‌ترین حروف هستند. با دانستن این اطلاعات و همچنین حدس زدن موضوع متن پیام، یک شنودکننده می‌تواند اقدام به رمزگشایی متن پیام رمزی شده کند [۱].

به طور کلی رمزنگاری براساس ویژگی‌های کلید رمز به دو دسته تقسیم می‌شود: رمزنگاری با کلید سری و رمزنگاری با کلید عمومی.

۱.۱.۱ رمزنگاری با کلید سری(متقارن)

در رمزنگاری به روش متقارن تنها توسط یک کلید، متن اصلی رمزنگاری شده [۵] و با استفاده از همان کلید رمزگشایی [۶] می‌شود. برای سادگی می‌توان این گونه فرض کرد که فرستنده (که معمولا در این علم با نام آلیس [۷] از او یاد می‌شود) یک پیام را با یک کلید قفل می‌کند و می‌فرستد و در طرف دیگر گیرنده (شخصی به نام باب[۸]) با در اختیار داشتن کپی همان کلید، قفل پیام را می‌گشاید. این روش رمزنگاری

[۵] encryption
[۶] decryption
[۷] Alice
[۸] Bob

که با عنوان $one-time-pad$ شناخته شده است، اولین بار توسط گیلبرت وِرنام [۹] در سال ۱۹۱۷ ارائه شد. امنیت این روش از لحاظ ریاضی توسط شانون[۱۰] اثبات شده و غیر قابل شکسته شدن است. مراحل پروتکل وِرنام به صورت زیر است:

- متن اصلی به صورت رشته‌ای دودویی از ۰ها و ۱ها نوشته می‌شود.
- کلید رمز رشته دودویی به طول متن اصلی است که کاملا تصادفی انتخاب می‌شود.
- متن رمزی شده با جمع کردن در مد ۲ بیتهای متن اصلی و کلید رمز بدست می‌آید.

اگر $\{p_۱, p_۲, ..., p_n\}$ نشاندهنده‌ی متن اصلی (به طوری که p_iها ارقام بر مبنای دو باشند) و اگر $\{k_۱, k_۲, ..., k_n\}$ کلید رمز باشد، آنگاه متن رمزی شده $\{c_۱, c_۲, ..., c_n\}$ این گونه بدست می‌آید که :

$$c_i = p_i \oplus k_i$$

که $i = ۱, ۲, ..., n$ و $\oplus$. نماد جمع مُد دو است که به صورت زیر تعریف می‌شود:

$$\begin{aligned} ۰ \oplus ۰ &= ۰ \qquad ۱ \oplus ۰ = ۱ \\ ۰ \oplus ۱ &= ۱ \qquad ۱ \oplus ۱ = ۰ \end{aligned} \tag{۱.۱}$$

برای مثال فرض کنید

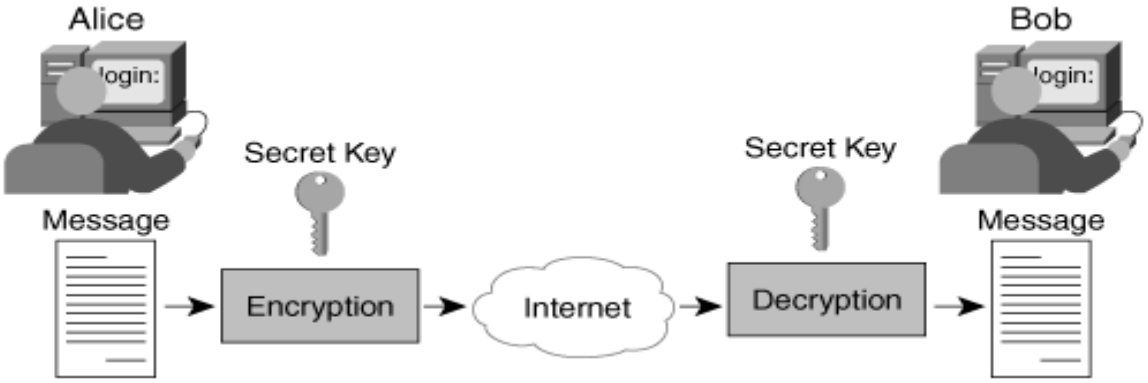
۰۰۱۰۱۰۰۱۱ متن اصلی

۱۰۰۱۱۱۰۱۰ کلید رمز

۱۰۱۱۰۱۰۰۱ متن رمز

از آنجایی‌که کلید رمز کاملا تصادفی است بنابراین متن رمز هم کاملا تصادفی می‌شود لذا کد غیر قابل شکستن خواهد بود. کلید رمز از قبل به نحوی بین آلیس و باب به اشتراک گذاشته شده است در نتیجه وقتی پیام رمز به دست گیرنده (باب) می‌رسد او می‌تواند به متن اصلی دست پیدا کند. کافیست باب متن رمز را دوباره با کلید(در مبنای دو) جمع کند.

$$p_i = c_i \oplus k_i$$



شکل ۲.۱: رمزنگاری با کلید متقارن

باید تاکید شود که کلید رمز تنها باید یکبار مورد استفاده قرار بگیرد. به همین دلیل این نوع از رمزنگاری را با عنوان $one - time - pad$ هم ذکر می‌کنند. اگر کلید دوبار مورد استفاده قرار بگیرد و شنودکننده بتواند به متن رمز دسترسی داشته باشد آنگاه او می‌تواند با جمع کردن متن‌های رمز به مجموع متن‌های اصلی دست پیدا کند و با توجه به وجود کلمات مشترک در متون اصلی می‌تواند کل پیام را رمزگشایی کند.

از همین رو مشکل اصلی رمزنگاری تنها انتقال متن رمز نیست بلکه **توزیع کلید** بین دو طرف است. این توزیع نیازمند یک مسیر امن است. همین مسئله، مشکل امنیت ارتباطات را به مشکل امنیت کلید تبدیل می‌کند. در واقع مسئله این است که شنودکننده (متعارف است وی را با نام ایو [۱۱] معرفی می‌کنند.)روشی را پیدا می‌کند تا به کلید دسترسی پیدا کند بدون آنکه از خودش اثری برجای بگذارد. بنابراین آلیس و باب هرگز از امنیت کامل کلید رمز اطمینان نخواهند داشت. در آینده نشان خواهیم داد که مکانیک کوانتومی برای حل این مسئله راه حل‌هایی را ارائه می‌دهد. از طرفی ایراد دیگر این نوع رمزنگاری طول بلند کلید است که همین موضوع انتقال آن را نیز سخت تر می‌کند. چون در رمزنگاری ورنام طول کلید باید هم اندازه طول کل پیام باشد [۲].

[۹] Gilbert Vernam

[۱۰] shannon

[۱۱] Eve

۲.۱.۱ رمزنگاری با کلید عمومی(نامتقارن)

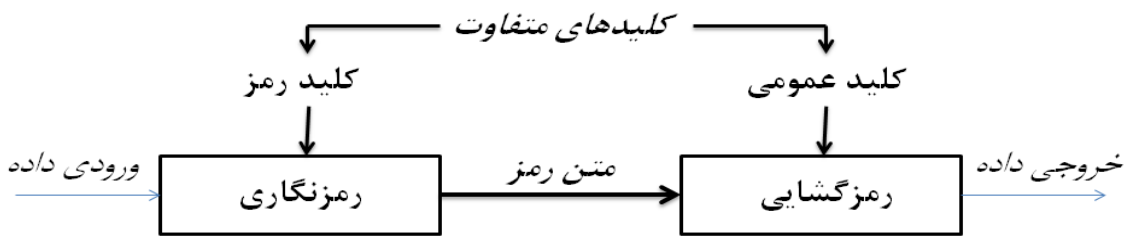
از آنجایی که در رمزنگاری ورنام برای هر پیام نیاز به تولید کلید رمزِ تصادفی جدید است، این روش رمزنگاری تنها برای ارتباطات دیپلماتیکِ مهم مورد استفاده قرار می‌گیرد. برای اموری با درجه اهمیت کمتر سیستم رمزنگاری کلید عمومی جایگزین می‌شود که اصول آن در اواسط دهه ۱۹۷۰ توسط دِفی[۱۲] و هِلمن[۱۳] کشف شد.

تفاوت اصلی بین رمزنگاری کلید خصوصی و کلید عمومی در این است که در روش اول آلیس پیام خود را توسط یک کلید رمزنگاری می‌کند سپس متن رمز برای باب فرستاده می‌شود. باب با در دست داشتن همان کلید می‌تواند متن را رمزگشایی کند. بنابراین امنیت پیام به امنیت کلید وابسته است. نهایتا این کلید رمز باید در یک زمانی بین آلیس و باب توزیع شود اما همیشه احتمال دسترسی ایو به کلید، در حین توزیع آن وجود دارد. این در حالیست که در رمزنگاری کلید عمومی آلیس و باب لازم نیست بین خود کلید رمزی را تبادل کنند. در این روش باب یک کلید عمومی طراحی می‌کند که در دسترس همگان می‌تواند قرار بگیرد. آلیس با استفاده از همان کلید پیام خود را رمزنگاری می‌کند ولی دیگر برای رمزگشایی، کلید عمومی کاربردی ندارد بلکه تنها باب با استفاده از کلید شخصی خود می‌تواند به متن اصلی دسترسی پیدا کند. یک مثال پرکاربرد از این نوع رمزنگاری سیستم پست الکترونیکی است. در پست الکترونیکی یک نام کاربری و یک کلید رمز عبور طراحی می‌شود. نام کاربری همان کلید عمومی است که در اختیار هر کسی می‌تواند باشد. پیام به آدرس این نام کاربری فرستاده می‌شود ولی تنها دریافت کننده، صاحب نام کاربری است که رمز عبور در اختیار اوست تا با استفاده از آن بتواند به متن پیام دسترسی داشته باشد[۲].

امنیت رمزنگاری با کلید عمومی بر اساس پیچیدگی‌های محاسباتی است. ایده اصلی، استفاده از تابع‌های یک طرفه است. توابعی مانند f که به راحتی محاسبه می‌شوند ولی معکوس آنها f^{-1} به سختی بدست می‌آیند. برای مثال با داشتن متغیر x تابع$f(x)$ به راحتی محاسبه می‌شود ولی بدست آوردن x از $f(x)$ سخت است. در اینجا مفهوم عبارت "سخت" آن است که زمان انجام محاسبات با تعداد بیت‌های ورودی به صورت نمایی افزایش پیدا می‌کند. به عنوان مثال کسری از ثانیه کافیست تا دو عدد اول ۷۱ و ۶۷ را در هم ضرب کرد ولی تجزیه عدد ۴۷۵۷ به عوامل اولش زمان به مراتب بیشتری را به

[۱۲] Diffie

[۱۳] Hellman



شکل ۳.۱: رمزنگاری با کلید نا متقارن

خود اختصاص می‌دهد[۳].

یکی از مشهورترین پروتکل‌های رمزنگاری کلید عمومی پروتکل RSA است[۴] .RSA اولین بار توسط رایوِست[۱۴] ، شمیر[۱۵] و اَدلمن[۱۶] در سال ۱۹۷۷ ارائه شد. همانطورکه توضیح داده شد، این پروتکل ازکلید عمومی مانند N استفاده می‌کند که حاصلضرب دو عدد اول بزرگ است. یک روش برای شکستن رمزنگاری RSA تجزیه عدد N است. در شکستن رمز با بزرگ شدن اعداد، تجزیه آنها زمان زیادی را می‌طلبد به طوری که هیچ الگوریتم کلاسیکی وجود ندارد که در زمانی کمتر از مرتبه $O((logN)^k)$ (به ازای هر k)تجزیه را انجام دهد. این در حالیست که پیتر شور[۱۷] الگوریتمی را بر مبنای کار رایانه‌های کوانتومی ارائه داده است که تجزیه اعداد را به عوامل اولشان در زمانی از مرتبه $O(logN)$ انجام می‌دهد و این به معنای نا امن بودن پروتکل RSA و سایر پروتکل‌های مشابه آن است[۵]. همان طورکه مطرح شد پیاده‌سازی الگوریتم شور به وجود کامپیوترهای کوانتومی وابسته است که در حال حاضر هنوز به طور گسترده این فناوری در دسترس نیست.

اگر این فناوری توسعه یابد تامین امنیت اطلاعات به روش حال حاضر مورد تهدید قرار می‌گیرد. برای مصون ماندن از این تهدید،در مقابل رمزنگاری کلاسیکی امروزه در نظریه اطلاعات کوانتومی نوعی از رمز نگاری با عنوان **رمزنگاری کوانتومی** یا در واقع توزیع کلید کوانتومی ارائه شده است که در ادامه به آن خواهیم پرداخت.

[۱۴] Rivest
[۱۵] Shamir
[۱۶] Adleman
[۱۷] Peter Shor

۲.۱ رمزنگاری کوانتومی

رمزنگاری کوانتومی یا توزیع کلید کوانتومی(QKD[۱۸])با به کار بردن قوانین فیزیک کوانتومی نوید ایجاد یک ارتباط امن را می‌دهد. در توزیع کلید کوانتومی دو شخص دور از هم درصدد ایجاد ارتباط با یکدیگرند (این بار هم با نام‌های آلیس و باب شناخته می‌شوند). بدین منظور آنها باید علاوه بر کانال کلاسیکی مرسوم، یک کانال کوانتومی را تدارک ببینند تا از طریق آن رشته بیتی را که در قالب سیستم کوانتومی در آمده است بین خود به اشتراک بگذارند. این رشته بیت همان کلید رمز مورد نظر آنها خواهد بود که می‌تواند بعدها برای چندین پیام رمزی شده مورد استفاده قرار بگیرد چون آنها بعد از طی کردن مراحل امنیتی با توجه به قوانین فیزیک کوانتومی از امنیت کلید خود مطمئن خواهند بود[۱].

هرچند امروزه امنیت پروتکل‌های توزیع کوانتومی تنها به طور نظری امری قابل اثبات است اما به لحاظ آزمایشگاهی برای رسیدن به امنیت مطلوب به پیشرفت‌های تکنولوژی بیشتری در گذر زمان نیاز است.

رمزنگاری کوانتومی آخرین ایده در تاریخ امنیت ارتباطات است که اگر پیشرفت لازم در آن صورت گیرد رقیب جدی برای سیستم‌های امنیتی امروزی خواهد بود.

برای وارد شدن به مبحث رمزنگاری ابتدا با معرفی و مروری کوتاه بر قوانین فیزیک کوانتومی زمینه را برای بررسی چند پروتکل مشهور آماده می‌کنیم و در نهایت پروتکل $N۰۹$ را مطرح و امنیت آن را بررسی می‌کنیم.

۳.۱ نظریه اطلاعات کوانتومی

نظریه اطلاعات کوانتومی ترکیبی از دو علم به روز دنیا یعنی فیزیک کوانتومی و نظریه اطلاعات است. در واقع نظریه اطلاعات کوانتومی دانش به کارگیری مکانیک کوانتوم در پردازش اطلاعات می باشد. این نظریه شامل موضوعات مختلف نظری و عملی در ایجاد ارتباطات و مدل های محاسباتی، با استفاده از محدودیت‌های فیزیک کوانتومی است. امروزه اطلاعات کوانتومی مورد توجه طیف وسیعی از دانشمندان قرار گرفته است، دانشمندانی از حوزه‌هایی مانند نظریه اطلاعات، فیزیک، مهندسی، علوم کامپیوتر و

[۱۸] Quantum key distribution

ریاضیات به بررسی ابعاد مختلف عملی و تئوری آن می‌پردازند.

اطلاعات کوانتومی دارای زیر شاخه های متعددی است. چند نمونه از این زیر شاخه عبارتند از[۵]:

- **رایانش کوانتومی** [۱۹]، که در آن از طرفی به بررسی چگونگی ساخت یک رایانه کوانتومی می پردازد و از طرف دیگر در جستجوی بدست آوردن الگوریتم هایی برای نشان دادن قدرت این رایانه ها هستند.

- **محاسبات کوانتومی** [۲۰]، که پیچیدگی‌های محاسباتی الگوریتم‌های مختلف کوانتومی را بدست می‌آورد.

- **تصحیح خطای کوانتومی**، که در رایانش کوانتومی مورد استفاده قرار می گیرد تا از اطلاعات کوانتومی در برابر خطاهای ناشی از ناهمدوسی و سایر نوفه های کوانتومی مواظبت کند.

- **درهم‌تنیدگی کوانتومی**، که به مطالعه درهم‌تنیدگی از منظر نظریه اطلاعات می‌پردازد.

- **رمزنگاری کوانتومی**، یا بطور عمومی ارتباطات کوانتومی، هنر انتقال اطلاعات به صورت حالت های کوانتومی از مکانی به مکان دیگر است. رمزنگاری اولین کاربرد اطلاعات کوانتومی است که با توجه به تکنولوژی روز دنیا قابل انجام است. در این پایان نامه به بررسی این شاخه از نظریه اطلاعات کوانتومی پرداخته شده است.

دو نظریه اطلاعات کوانتومی و اطلاعات کلاسیکی دارای تفاوت‌های بنیادین با یکدیگر هستند. در این بخش به بررسی این تفاوت‌ها می‌پردازیم.

۱.۳.۱ کیوبیت

یک بیت، عددی در مبنای دو است که پایه و اساس نظریه اطلاعات کلاسیکی را شکل می‌دهد. یک بیت سیستمی است که می‌تواند دو مقدار ”۰“ و ”۱“ را داشته باشد. در بیان ساده‌تر، به طور کلاسیکی می‌توان بیت را یک کلید مکانیکی در نظرگرفت که می‌تواند بین دو حالت کاملا قابل تشخیص از هم قرار

[۱۹] quantum computing

[۲۰] quantum computation

بگیرد؛ حالت روشن یا خاموش. نظریه اطلاعات کوانتومی در مقابل بیت، سیستم دیگری به نام **کیوبیت** [۲۱] را معرفی می‌کند.

یک بیت کوانتومی یا یک کیوبیت، یک واحد از اطلاعات کوانتومی است. برای کیوبیت مشابه بیت کلاسیکی دو حالت [۲۲] $|۰\rangle$ و $|۱\rangle$ ممکن است.[نماد $|\rangle$ نماد دیراک (یا کِت) نامیده می‌شود و نمادی استاندارد برای توصیف حالت‌های کوانتومی است] تفاوت عمده ی بین بیت کلاسیکی و کیوبیت در آن است که کیوبیت قادر است حالتی فرای دو حالت $|۰\rangle$ و $|۱\rangle$ را بپذیرد و آن برهم‌نهی از این دو حالت پایه است. به طور کلی یک کیوبیت را به صورت زیر نمایش می‌دهند:

$$|\Psi\rangle = \alpha\,|۰\rangle + \beta\,|۱\rangle \qquad (۲.۱)$$

که در آن $\alpha, \beta \in C$ چون ضرایب α و β اعداد مختلط هستند، یک کیوبیت را می‌توان به عنوان برداری در یک فضای برداری مختلط دو بعدی توصیف کرد که این فضا را فضای هیلبرت[۲۳] می‌نامند. دو حالت $|۰\rangle$ و $|۱\rangle$ پایه‌های محاسباتی این فضا را تشکیل می‌دهند که بر هم عمود هستند. برای مثال $|۰\rangle = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix}$ و $|۱\rangle = \begin{pmatrix} ۰ \\ ۱ \end{pmatrix}$. از آنجایی که کیوبیت یک بردار واحد است، یعنی طول آن به ۱ بهنجار شده است باید معادله زیر برای ضرایب α و β برقرار باشد.

$$|\alpha|^۲ + |\beta|^۲ = ۱ \qquad (۳.۱)$$

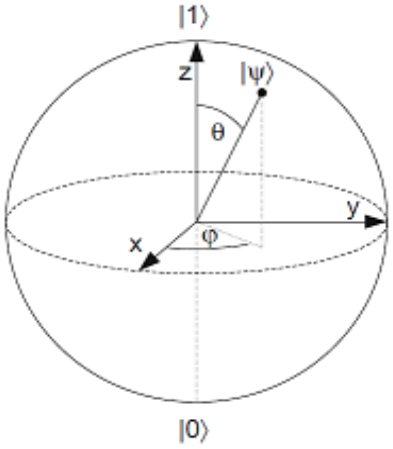
با استفاده از این حقیقت می‌توان حالت یک کیوبیت را به این صورت بازنویسی کرد:

$$|\Psi\rangle = \cos\frac{\theta}{۲}\,|۰\rangle + e^{i\varphi}\sin\frac{\theta}{۲}\,|۱\rangle \qquad (۴.۱)$$

که θ و φ اعداد حقیقی هستند و یک نقطه از کره‌ای موسوم به کره بلاخ[۲۴] را توصیف می‌کنند.

اندازه‌گیری کیوبیت‌ها مسئله مهمی است. در حالت خاص وقتی α یا β صفر هستند ، کیوبیت به یک بیت کلاسیکی نگاشته می‌شود و نتیجه ۰ یا ۱ خواهد بود. اما اگر $\alpha, \beta \neq ۰$ باشند، یک برهم‌نهی اتفاق می‌افتد و این بار بعد از اندازه‌گیری کیوبیت به یکی از دو حالت $|۰\rangle$ یا $|۱\rangle$ ریزش [۲۵] می‌کند با

[۲۱] qubit
[۲۲] state
[۲۳] Hilbert
[۲۴] bloch sphere
[۲۵] collapse



شکل ۴.۱: کره بلاخ؛ نمایش یک کیوبیت

توجه به فرمول ۳.۱ احتمال آنکه یک کیوبیت بعد از اندازه‌گیری ۰ باشد، $|\alpha|^2$ و ۱ باشد، $|\beta|^2$ خواهد بود. در مکانیک کوانتومی به اعداد α و β دامنه احتمال $|0\rangle$ و $|1\rangle$ نیز می‌گویند[۶].

عبارت دیگری نیز برای توصیف یک کیوبیت وجود دارد و آن فاز[۲۶] است. حالت $e^{i\varphi}|\psi\rangle$ را در نظر بگیرید که $|\psi\rangle$ یک بردار حالت است و φ یک عدد حقیقی. با توجه به عامل فاز کلی[۲۷] می‌توان گفت که $e^{i\varphi}|\psi\rangle$ با $|\psi\rangle$ برابر است. به عبارت دیگر یعنی اندازه‌گیری برای این دو حالت از منظر آماری با یکدیگر یکسان است.

نوعی فاز دیگر وجود دارد و آن فاز نسبی[۲۸] است. دو حالت زیر را در نظر بگیرید:

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

در حالت $|+\rangle$ دامنه $|1\rangle$ مقدار $\frac{1}{2}$ است و در حالت $|-\rangle$ دامنه $|1\rangle$ اندازه مشابهی دارد ولی علامت آن متفاوت است. می‌توان دو دامنه α_1 و α_2 را برای برخی حالتها به گونه‌ای تعریف کرد که با یک فاز نسبی متفاوت باشند درصورتی که یک φ حقیقی وجود داشته باشد، به طوریکه $\alpha_1 = e^{i\varphi}\alpha_2$ باشد. برخلاف فاز کلی که هر دو دامنهٔ یک حالت، تحت تاثیر عامل فاز $e^{i\varphi}$ بودند، فاز نسبی تنها یکی از دامنه‌ها را توسط عامل $e^{i\varphi}$ از دیگری متفاوت می‌کند [۸].

هرسیستم فیزیکی دو حالته‌ی کوانتومی می‌تواند برای توصیف یک کیوبیت مورد استفاده قرار بگیرد.

[۲۶] phase
[۲۷] global phase factor
[۲۸] relative phase

سیستم هایی که امروزه در آزمایشگاه‌ها مورد استفاده قرار می‌گیرند سیستم‌هایی نظیر: دو حالت قطبش عمود بر هم فوتون(برای مثال قطبش افقی برای حالت $|۰\rangle$ و عمودی برای$|۱\rangle$)، جهت گیری یک ذره با اسپین نیمه صحیح، دو حالت پایه و برانگیخته اتم یا یون و... هستند.

۲.۳.۱ عملگرهای خطی

در زبان مکانیک کوانتومی برای تغییر حالت یک کیوبیت از عملگرهای خطی استفاده می‌شود. به زبان ریاضی عملگرها توابعی هستند که با تاثیر روی یک بردار آن را به بردار دیگری تبدیل می‌کند. مرسوم ترین روش برای نمایش یک عملگر نمایش ماتریسی است.

چهار ماتریسی که در اطلاعات کوانتومی بسیار مورد استفاده قرار می‌گیرند ماتریس‌های پاولی هستند. ماتریس‌های پاولی ماتریس‌های ۲×۲ هستند که برخی تغییرات مورد نیاز را روی کیوبیت‌ها به وجود می‌آورند. این ماتریس‌ها عبارتند از:

$$X = \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \qquad Y = \begin{pmatrix} ۰ & -i \\ i & ۰ \end{pmatrix}$$
$$Z = \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \qquad I = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} \tag{۵.۱}$$

ماتریس چهارم ماتریس یکانی است که اعمال آن روی کیوبیت تغییری در آن ایجاد نمی‌کند. عملگرهای پاولی X و Z معمولا با عنوان‌های بیت برگردان [۲۹] و فاز برگردان [۳۰]مورد استفاده قرار می‌گیرد. اگر X روی یک کیوبیت اثر داده شود مشاهده می‌شود که $|۰\rangle$ را به $|۱\rangle$ و بالعکس تغییر می‌دهد:

$$X|۰\rangle = \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} = \begin{pmatrix} ۰ \\ ۱ \end{pmatrix}$$

$$X|۱\rangle = \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \tag{۶.۱}$$

[۲۹] bit flip

[۳۰] phase flip

عملگر Z یا عملگر فاز برگردان، فاز حالت $|۱\rangle$ را از طریق علامت آن تغییر می‌دهد:

$$Z|+\rangle = \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \begin{pmatrix} \sqrt{۲} \\ \sqrt{۲} \end{pmatrix} = \begin{pmatrix} \sqrt{۲} \\ -\sqrt{۲} \end{pmatrix}$$

$$Z|-\rangle = \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \begin{pmatrix} \sqrt{۲} \\ -\sqrt{۲} \end{pmatrix} = \begin{pmatrix} \sqrt{۲} \\ \sqrt{۲} \end{pmatrix} \quad (۷.۱)$$

برای نشان دادن تاثیر عملگر Y روی کیوبیت‌ها لازم است عناصر ماتریس در i ضرب شود زیرا بهتراست ماتریس‌هایی با اعداد طبیعی مورد استفاده قرارگیرند. بنابراین عملگر iY را تعریف می کنیم که برابر با ضرب دوماتریس Z و X است.

$$iY = ZX = \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} = \begin{pmatrix} ۰ & ۱ \\ -۱ & ۰ \end{pmatrix} = i \begin{pmatrix} ۰ & i \\ -i & ۰ \end{pmatrix} \quad (۸.۱)$$

حاصل اعمال این عملگر روی کیوبیت‌ها نتیجه‌ای ترکیب از هر دو عملگر بیت برگردان و فاز برگردان را می‌دهد:

$$iY|۰\rangle = \begin{pmatrix} ۰ & ۱ \\ -۱ & ۰ \end{pmatrix} \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} = \begin{pmatrix} ۰ \\ -۱ \end{pmatrix}$$

$$iY|۱\rangle = \begin{pmatrix} ۰ & ۱ \\ -۱ & ۰ \end{pmatrix} \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \quad (۹.۱)$$

۳.۳.۱ ضرب داخلی

یک ضرب داخلی (یا ضرب نرده‌ای[۳۱]) در جبرخطی به صورت $\langle v|\ w\rangle$ برای دو بردار $|v\rangle$ و $|w\rangle$ نمایش داده می‌شود و آن تابعی است که ورودی آن دو بردار از فضای برداری و خروجی آن یک عدد مختلط

[۳۱] scalar

خواهد بود. برای مثال ضرب داخلی دو بردار n بعدی به صورت زیر تعریف می‌شود.

$$\langle v|\ w\rangle = \sum_i a_i^* b_i = \begin{pmatrix} a_1^* & \cdots & a_n^* \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \qquad (۱۰.۱)$$

دو خاصیت بنیادی برای ضرب داخلی تعریف می‌شود :

- $\langle v|\ w\rangle = \langle w|\ v\rangle^*$
- $\langle v|\ v\rangle \geq 0$

که حالت مساوی تنها وقتی بدست می‌آید که $|v\rangle = 0$ باشد.

در ادامه چند تعریف در ارتباط با ضرب داخلی آورده شده است.

تعریف) در یک فضای برداری مانند V دو بردار $|v\rangle\ , |w\rangle \in V$را متعامد گویند اگر :

$$\langle v|\ w\rangle = 0$$

تعریف) در فضای برداری V نُرم بردار $|v\rangle$ به صورت $||v\rangle| = \sqrt{\langle v|\ v\rangle}$ تعریف می‌شود نُرم یک بردار معمولا با عنوان طول یا اندازه بردار شناخته می‌شود.

تعریف) در فضای برداری V حالت بهنجار یک بردار معلوم $|v\rangle$ به صورت زیر تعریف می‌شود:

$$|\tilde{v}\rangle = (\frac{|v\rangle}{\sqrt{\langle v|\ v\rangle}})$$

که در پی آن

$$\langle \tilde{v}|\ \tilde{v}\rangle = 1$$

تعریف) در فضای برداری V زیر مجموعه‌ای از بردارهای $|v_i\rangle \in V$بردارهای متعامد بهنجار[۳۲] نامیده می‌شوند، اگر هر بردار $|v_i\rangle$ یک بردار واحد باشند و بردارها متمایز بر یکدیگر عمود باشند:

$$\langle v_i|\ v_j\rangle = 0$$

که در آن $i, j = 1, ..., n$ و $i \neq j$

[۳۲] orthonormal

در تعیین پایه‌های محاسباتیِ یک فضای برداری آخرین تعریف باید برقرار باشد. به طوریکه چنین بردارهایی کل فضای برداری را جاروب[۳۳] می‌کنند و هر برداری خارج از این فضا را می‌توان به صورت ترکیب خطی از این بردارهای پایه نوشت.

۴.۳.۱ ضرب خارجی

در مقابل ضرب داخلی، ضرب خارجی دو بردار تعریف می‌شود که خروجی آن یک عملگر(ماتریس) خواهد بود:

$$|v\rangle\langle w| = A_{ij} = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \cdot \begin{pmatrix} b_1^* & \cdots & b_n^* \end{pmatrix} = \begin{pmatrix} a_1 b_1^* & \cdots & a_1 b_n^* \\ \vdots & \ddots & \vdots \\ a_m b_1^* & \cdots & a_m b_n^* \end{pmatrix}$$

نمایش ضرب خارجی به صورت بِرا و کِت برای نمایش عملگرهای خطی روشی بسیار پر کاربرد است به طوریکه سبب می‌شود اثر عملگرها روی حالات، به محاسبه ضرب داخلی ساده تبدیل شود. فرض کنید $|v_i\rangle$ یک بردار در فضای ضرب داخلی V و $|w_i\rangle$ یک بردار در فضای ضرب داخلی W باشد. آنگاه $|w\rangle\langle v|$ را عملگر خطی تبدیل فضا از V به W تعریف می‌شود به طوری که:

$$(|w\rangle\langle v|)(|v'\rangle) = |w\rangle\langle v|\,v'\rangle = \langle v|\,v'\rangle\,|w\rangle$$

دو برداشت را می‌توان از رابطه بالا داشت: از یک طرف بیانگر آن است که بردار $|v'\rangle$ توسط یک ماتریس($|w\rangle\langle v|$)به یک بردار در فضای برداری W نگاشت شده است و از طرف دیگر بیانگر بردار $|w\rangle$ است که در یک عدد مختلط ضرب شده است.

یکی از کاربردهای ضرب خارجی استفاده آن در نتیجه‌ی مهمی با عنوان رابطه کاملیت[۳۴] برای بردارهای متعامد بهنجار است. فرض کنید $|v_i\rangle$ها پایه‌های متعامد بهنجار[۳۵] فضای برداری V باشند آنگاه رابطه زیر باید همیشه برقرار باشد:

$$\sum_i |v_i\rangle\langle v_i| = I$$

[۳۳] span

[۳۴] completeness relation

[۳۵] orthonormal

۵.۳.۱ ضرب تانسوری

ضرب تانسوری عملیاتی است که طی آن یک فضای برداری بزرگتر از دو فضای برداری کوچکتر تشکیل می‌شود. اگر دوفضای برداری V و W با ابعاد به ترتیب m و n باشند آنگاه $V \otimes W$ یک فضای برداری mn بعدی است که مولفه‌های آن ترکیب خطی از ضرب تانسوری مولفه‌های $|v\rangle \in V$ و $|w\rangle \in W$ هستند. برای مثال ضرب تانسوری دو بردار $(۱, ۲)$ و $(۳, ۴)$ برداری است به صورت :

$$\begin{pmatrix} ۱ \\ ۲ \end{pmatrix} \otimes \begin{pmatrix} ۳ \\ ۴ \end{pmatrix} = \begin{pmatrix} ۱ \times ۳ \\ ۱ \times ۴ \\ ۲ \times ۳ \\ ۲ \times ۴ \end{pmatrix} = \begin{pmatrix} ۳ \\ ۴ \\ ۶ \\ ۸ \end{pmatrix}$$

در این مثال ضرب تانسوری روی بردارهایی از فضای دو بعدی انجام شد در حالیکه این عملیات می‌تواند روی عملگرهای خطی نیز انجام شود. فرض کنید $A : V \to V'$ و $B : W \to W'$ آنگاه $A \otimes B : V \otimes W \to V' \otimes W'$ خواهد بود. A را یک ماتریس $m \times n$ بعدی و B را یک ماتریس $p \times q$ بعدی در نظر بگیرید. نمایش ماتریس حاصلضرب تانسوری به صورت زیر است:

$$A \otimes B = \begin{pmatrix} A_{۱۱}B & \dots & A_{۱n}B \\ \vdots & \ddots & \vdots \\ A_{m۱}B & \cdots & A_{mn}B \end{pmatrix}$$

که $A_{۱۱}B$ بیانگر یک زیرماتریس $p \times q$ بعدی است. برای مثال ضرب تانسوری ماتریس‌های پاولی X و Y به صورت زیر خواهد بود:

$$X \otimes Y = \begin{pmatrix} ۰Y & ۱Y \\ ۱Y & ۰Y \end{pmatrix} = \begin{pmatrix} ۰ & ۰ & ۰ & -i \\ ۰ & ۰ & i & ۰ \\ ۰ & -i & ۰ & ۰ \\ i & ۰ & ۰ & ۰ \end{pmatrix}$$

۶.۳.۱ اندازه‌گیری کوانتومی

یک سیستم کوانتومی بسته، توسط تحول‌های یکانی[۳۶] (نوعی خاص از عملگرهای خطی) بدون آنکه با محیط بیرون برهمکنش داشته باشند، تغییر می‌کند. اما گاهی لازم است که یک سیستم کوانتومی اندازه‌گیری شود تا کمیتی بدست آید، که در آن صورت باید با محیط (مثلا دستگاه‌های آزمایشگاه و ...) برهم کنش داشته باشد. این برهمکنش سبب می‌شود که دیگر سیستم بسته نباشد و از حالت کوانتومی خود خارج شود و به یک موجود کلاسیکی تبدیل شود.

اندازه‌گیری کوانتومی با مجموعه $\{M_m\}$ توصیف می‌شود که مجموعه عملگرهای اندازه‌گیری نام دارند. با اعمال این عملگرها روی فضای حالت یک سیستم، آن را اندازه‌گیری می‌کنند. اگر حالت یک سیستم کوانتومی قبل از اندازه‌گیری $|\psi\rangle$ باشد آنگاه احتمال آنکه بعد از اندازه‌گیری نتیجه m بدست آید به صورت زیر تعریف می‌شود :

$$P(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

و حالت سیستم بعد از اندازه‌گیری به صورت زیر در می‌آید:

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

عملگرهای اندازه‌گیری در رابطه کاملیت صدق می‌کنند:

$$\sum_m M_m^\dagger M_m = I$$

رابطه کاملیت این حقیقت را بیان می‌کند که مجموع همه‌ی احتمال‌ها برابر با یک است.

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

این معادله به ازای همه $|\psi\rangle$ برقرار است.

یک مثال ساده از اندازه‌گیری کوانتومی، اندازه‌گیری یک کیوبیت در پایه‌های محاسباتی است. این اندازه‌گیری روی یک کیوبیت توسط دو عملگر $M_۰ = |۰\rangle\langle۰|$ و $M_۱ = |۱\rangle\langle۱|$ توصیف می‌شود. فرض کنید حالت کیوبیت قبل از اندازه‌گیری به صورت $|\psi\rangle = a|۰\rangle + b|۱\rangle$ باشد آنگاه احتمال آنکه نتیجه

[۳۶] unitary transformation

اندازه‌گیری صفر باشد خواهد بود :

$$P(۰) = \langle\psi| M_۰^\dagger M_۰ |\psi\rangle = \langle\psi| M_۰ |\psi\rangle = |a|^۲$$

به طور مشابه،احتمال آنکه نتیجه اندازه‌گیری ۱ باشد $P(۱) = |b|^۲$ خواهد بود.

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

- $$\frac{M_۰ |\psi\rangle}{|a|} = \frac{a}{|a|} |۰\rangle$$

- $$\frac{M_۱ |\psi\rangle}{|b|} = \frac{b}{|b|} |۱\rangle$$

ضرایب $\frac{a}{|a|}$ و $\frac{b}{|b|}$ در صورت بهنجار بودن قابل چشم پوشی هستند. بنابراین خروجی اندازه‌گیری یک کیوبیت که برهم‌نهی از حالت‌های $|۰\rangle$ و $|۱\rangle$ است در نهایت به یکی از دو حالت $|۰\rangle$ یا $|۱\rangle$ ریزش می‌کند[۳۷] [۶].

۷.۳.۱ عملگر چگالی؛ حالتهای مخلوط و خالص

در بعضی از مواقع به جای در نظر گرفتن یک سیستم کوانتومیِ تنها، نیاز داریم تا روی تعداد زیاد و یا مجموعه‌ای از سیستم‌ها که به عنوان آنسامبل[۳۸] شناخته شده است، مطالعه داشته باشیم. علاوه بر این اعضای یک آنسامبل می‌توانند در یک یا دو و یا تعداد متفاوتی از حالت‌های کوانتومی باشند. برای آنکه هر عضو از آنسامبل مشخص باشد که در کدام حالت ممکن است پیدا شود، به آن یک احتمال نسبت داده می‌شود [۱۱]. برای واضح‌تر شدن بحث لازم است در اینجا عملگر چگالی[۳۹] یا ماتریس چگالی ρ را معرفی می‌کنیم.

$$\rho = \sum_n P_n |\psi_n\rangle \langle\psi_n| \qquad (۱۱.۱)$$

[۳۷] collapse

[۳۸] ensamble

[۳۹] density operator

اگر یکی از احتمال‌ها برابر یک باشد به آن معنی است که آنگاه عملگر چگالی به فرم ساده‌تر $\rho = |\psi_n\rangle\langle\psi_n|$ تبدیل می‌شود. به عملگر چگالی به این فرم که در آن یک بردار حالت مشخص است، عملگر چگالی حالت خالص یا حالت‌های خالص[۴۰] اطلاق می‌شود.عملگرهای چگالی به فرم معادله ۱۱.۱ نشان دهندهٔ مخلوطی از حالت‌ها یا حالت‌های مخلوط[۴۱] هستند[۱].

عملگرهای چگالی دارای ویژگی‌های مشخصی هستند:

- یک عملگر چگالی هرمیتی است یعنی $\rho = \rho^\dagger$.
- $Tr(\rho) = ۱$ که نشان می‌دهد مجموع احتمالات هر مجموعه کامل برابر ۱ است. (Tr نمایش عملگر رد[۴۲] است که جمع عناصر روی قطر یک ماتریس را محاسبه می‌کند)
- عملگر چگالی یک عملگر مثبت[۴۳] است، یعنی برای هر بردار حالت $|u\rangle$ رابطه $\langle u|\rho|u\rangle \geq ۰$ برقرار است.
- برای یک حالت خالص همواره $\rho = \rho^۲$ و بنابراین $Tr(\rho^۲) = ۱$ است. اما برای یک حالت مخلوط این روابط برقرار نیست، بلکه $Tr(\rho^۲)$ برای یک حالت مخلوط همواره کوچکتر از ۱ است.

۸.۳.۱ حالت‌های درهم‌تنیده

درهم‌تنیدگی[۴۴] یک ویژگی ارتباطی بین دو یا چند سیستم کوانتومی است. این ویژگی نمونه‌ای در فیزیک کلاسیک ندارد و ذاتا پدیده‌ای کوانتومی است. به همین دلیل درهم‌تنیدگی نقش مهمی را در ارتقا و پیشرفت نظریه اطلاعات کوانتومی ایفا می‌کند.

برای ورود به بحث حالت‌های درهم‌تنیده ابتدا یک حالت خالص از دو سیستم کوانتومی با برچسب‌های

---

[۴۰] pure states
[۴۱] mixed states
[۴۲] trace
[۴۳] positive
[۴۴] entanglement

a و b درنظرمی‌گیریم این حالت ترکیبی[۴۵] را می‌توان به صورت ضرب تانسوری دو حالت نوشت :

$$|\psi\rangle = |\lambda\rangle_a \otimes |\varphi\rangle_b \qquad (۱۲.۱)$$

در حالت $|\psi\rangle$ می‌توان حالت زیر سیستم‌های a و b را به صورت مجزا در نظر گرفت یعنی با یک ضرب تانسوری می‌توان زیرسیستم‌ها را از هم جدا کرد.

اصل برهم‌نهیِ مکانیک کوانتومی این طور بیان می‌کند که هر برهم‌نهی از حالت‌های ترکیبی مثل حالت ۱.۲ نیز یک حالت مجاز برای دو زیرسیستم خواهد بود. برای مثال حالت دو کیوبیتی زیر را در نظر بگیرید:

$$|\psi\rangle = \frac{۱}{\sqrt{۲}}(|۰\rangle_a|۰\rangle_b + |۱\rangle_a|۱\rangle_b) \qquad (۱۳.۱)$$

این حالت دربردارنده‌ی یک برهم نهی از حالت‌های ترکیبی است و نمی‌توان مانند حالت $|\psi\rangle$ در ۱۲.۱ آن را به صورت حاصلضرب تانسوری دو زیر سیستم a و b نوشت. حالت‌هایی با این ویژگی که نمی‌توان آنها را مانند حالت‌های ترکیبی ۱۲.۱ نوشت را حالت‌های در هم‌تنیده می‌نامند.

برای یک حالت درهم‌تنیده تنها آنکه بتوان آن را به صورت برهم نهی از حالت‌های ترکیبی نوشت کافی نیست. به عنوان مثال حالت زیر را در نظر بگیرید:

(۱۴.۱)

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

این حالت یک برهم‌نهی از سیستم a و b است ولی می‌توان آن را به صورت ضرب تانسوری حالت‌های دو زیرسیستم a و b نوشت بنابراین درهم‌تنیده نیست.

برای آنکه راحت‌تر بتوان تشخیص داد که یک سیستم درهم‌تنیده هست یا خیر از عملگرهای چگالی استفاده می‌شود. برای هر حالت می‌توان عملگرهای چگالی را تشکیل داد و با گرفتن "رد" آن روی یکی از زیرسیستم‌ها ماتریس چگالی کاهش یافته[۴۶] را بدست آورد. برای یک حالت غیر درهم‌تنیده مثل حالت ۱۲.۱ ماتریس چگالی به صورت زیر خواهد بود:

$$\hat{\rho}_{ab} = |\lambda\rangle\langle\lambda| \otimes |\varphi\rangle\langle\varphi|$$

[۴۵] composite

[۴۶] reduced density matrice

با محاسبه رد آن روی حالت b ماتریس چگالی کاهش یافته برای سیستم a به این صورت بدست می‌آید:

$$\hat{\rho}_a = |\lambda\rangle\langle\lambda|$$

که یک ماتریس چگالی برای یک حالت **خالص** است. واضح است که $\hat{\rho}_a^2 = \hat{\rho}_a$ و $Tr(\hat{\rho}_a^2) = 1$. هرحالت خالص غیر درهم‌تنیده را می‌توان به فرم معادله ۱۲.۱ نوشت و در نتیجه شرط $Tr(\hat{\rho}_a^2) = 1$ هم برای آن برقرار خواهد بود. این یک علامت برای تشخیص حالت غیر درهم‌تنیده است به همین ترتیب اگر برای یک حالت **خالص** $Tr(\hat{\rho}_a^2) \neq 1$ باشد آنگاه حالت درهم‌تنیده است.

یک حالت درهم‌تنیدهٔ دو سیستم a و b را همیشه می‌توان به صورت زیر نوشت:

$$|\psi\rangle = \sum_n \alpha_n |\lambda_n\rangle_a \otimes |\varphi_n\rangle_b \qquad (۱۵.۱)$$

که حالت‌های $\{|\lambda_n\rangle\}$ و$\{|\varphi_n\rangle\}$ به ترتیب مجموعه‌های متعامد بهنجار برای سیستم‌های a و b هستند. در اینجا هر حالت $|\lambda_n\rangle$ سیستم a تنها با حالت $|\varphi_n\rangle$ سیستم b در ارتباط است. این نوع از نوشتن حالت‌ها با عنوان بسط اشمیت[۴۷] مشهور است.

در میان خیل حالت‌های درهم‌تنیده‌ی ممکن، حالت‌های بِل[۴۸] دو کیوبیتی دارای اهمیت ویژه‌ای هستند. دلیل آن یکی سادگی آن‌ها و دیگری اینکه در بسیاری از آزمایشات توانسته‌اند به آن‌ها عینیت ببخشند. چهار حالت بل را معمولاً به صورت زیر درنظر می‌گیرند:

$$\begin{aligned}
|\psi^-\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \\
|\psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) \\
|\phi^-\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \\
|\phi^+\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)
\end{aligned} \qquad (۱۶.۱)$$

مشخص است که حالت بل اول نسبت به جابه‌جایی ترتیبِ کیوبیت‌ها نامتقارن و سایر حالت‌ها، متقارن هستند [۱].

[۴۷] schmidt decomposition

[۴۸] Bell states

۹.۳.۱ اصل عدم کپی برداری

یکی از ویژگی‌های بیت‌های کلاسیکی آن است که اگر در بین مسیر انتقال، (به هر نحوی) بتوان به آنها دسترسی پیدا کرد و از آن کپی گرفت هیچ کس متوجه این کار نخواهد شد. در مقابل یک کیوبیت ناشناخته، با توجه به خاصیت کوانتومی که با خود به همراه دارد قادر به کپی شدن نخواهد بود مگر آنکه روی آن اندازه‌گیری انجام شود و انجام اندازه‌گیری یعنی از بین بردن حالت کوانتومی کیوبیت و تبدیل آن به یک بیت کلاسیکی. این امر سبب می‌شود حضور یک شنودکننده در هنگام بررسی امنیت کلید رمز به اشتراک گذاشته شده توسط آلیس و باب ، به سادگی تشخیص داده شود.

نظریه‌ای که عدم امکان کپی برداری یک کیوبیت ناشناخته را اثبات می‌کند، **اصل عدم کپی برداری**[۴۹] است که اولین بار توسط ووترز[۵۰] ، دیک[۵۱] و زورِک[۵۲] عنوان شد[۱۲]. فرض کنید یک ماشین کوانتومی با دو ورودی وجود دارد. ورودی اول (A) ، ورودی داده است که محل ورود یک حالت کوانتومی ناشناخته مثل $|\psi\rangle$ است. هدف ماشین آن است که حالت $|\psi\rangle$ را روی حالت مفروض در ورودی دوم (B) کپی کند.

با این توضیحات حالت اولیه دستگاه کپی به صورت زیر خواهد بود:

$$|\psi\rangle \otimes |s\rangle$$

فرایند کپی کردن دستگاه را به صورت یک عملگر تحول یکانی U در نظر می‌گیریم:

$$|\psi\rangle \otimes |s\rangle \rightarrow U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

فرض کنید این عملیات کپی برداری روی دو حالت $|\psi\rangle$ و $|\phi\rangle$ انجام شود آنگاه خواهیم داشت:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle \qquad (۱۷.۱)$$

[۴۹] no-cloning
[۵۰] Wooters
[۵۱] Dick
[۵۲] Zurek

با انجام ضرب داخلی دو معادله بالا خواهیم داشت:

$$\langle\psi|\,\varphi\rangle = |\langle\psi|\,\varphi\rangle|^{۲} \qquad (۱۸.۱)$$

می دانیم که معادله $x = x^{۲}$ تنها دو جواب دارد: $x = ۰$ و $x = ۱$. بنابراین جواب‌های معادله ۱۸.۱ یا $|\psi\rangle = |\varphi\rangle$ است ($\langle\psi|\,\varphi\rangle = ۱$) یا $|\psi\rangle$ بر $|\varphi\rangle$ عمود است(زیرا $\langle\psi|\,\varphi\rangle = ۰$). می‌توان نتیجه گرفت که اگر یک دستگاه کپی برداری موجود باشد تنها می‌تواند حالت‌هایی را کپی کند که بر هم عمودند و یک دستگاه کپی برداری کلی برای همه حالت‌ها نمی‌تواند وجود داشته باشد[۸].

فصل ۲

توزیع کلید کوانتومی و امنیت آن

در این فصل بعد از ارائه نمای کلی از مراحل یک پروتکل توزیع کلید کوانتومی به معرفی چند پروتکل مهم در عرصه رمزنگاری کوانتومی می‌پردازیم و سپس نقش شنودکننده در خرابکاری و استراق سمع از ارتباط بین آلیس و باب را مورد بررسی قرار می‌دهیم. در آخر چند نمونه از استراتژی های حمله به پروتکل‌ها توسط ایو را معرفی می‌کنیم.

۱.۲ نمای کلی توزیع کلید کوانتومی

یک پروتکل در توزیع کلید کوانتومی سلسله مراتبی دارد که به اختصار آنها را بیان می‌کنیم. اولین مرحله انتقال ذره کوانتومی از طریق یک کانال کوانتومی از فرستنده(آلیس) به گیرنده(باب) است. اصولاً در پروتکل‌ها فوتون به عنوان سیستم کوانتومی برای عینیت بخشیدن به مفهوم کیوبیت به کار می‌رود چون نسبت به سایر سیستم‌های کوانتومی در دسترس تر است، به سختی با یکدیگر برهم کنش می‌کنند و می‌توان آنها را با فیبرهای نوری در مسیرهای طولانی انتقال داد. چگونگی انتقال ذره کوانتومی از کانالی که خاصیت کوانتومی ذره را حفظ کند(یعنی همان کانال کوانتومی)، روش‌های متفاوتی دارد که همین تفاوت‌ها در نحوه انتقال ذرات، پروتکل‌های مختلف را شکل می‌دهند. در آخر مرحله‌ی اندازه‌گیری کیوبیت‌ها توسط باب است که منجر به شکل‌گیری دو رشته بیت در دست آلیس و باب می‌شود که آنها هنوز نمی‌توانند آن را به عنوان کلید در نظر بگیرند. آنها باید این رشته بیت‌ها را با استفاده از مراحل کلاسیکی بعدی پالایش کنند. به همین منظور پس از اتمام مرحله اول، ارتباطات از کانال کوانتومی به کانال کلاسیکی تغییر می‌کند. آلیس و باب این طور فرض می‌کنند که مکالماتشان از طریق کانال کلاسیکی ممکن است در اختیار شنودکننده(ایو) قرار گیرد، از این رو کانال کلاسیکی را کانال عمومی نیز می‌نامند.

پس از ورود به کانال کلاسیکی ابتدا مرحله تصفیه[۱] در پیش روست. مرحله‌ای که در آن آلیس و باب تصمیم می‌گیرند کدام بیت‌ها را نگه داشته و کدامشان را حذف کنند. بعد از توافق بر سر بیت‌ها و اطمینان اولیه از عدم حضور ایو در طول کانال کوانتومی، آنها وارد مرحله اصلاح[۲] یا تصحیح خطا[۳] می‌شوند. از آنجایی‌که کانال‌های کوانتومی حتما دارای نوفه هستند آلیس و باب رشته بیت یکسانی را

[۱] sifting

[۲] reconciliation

[۳] error correction

به اشتراک نگذاشته‌اند. حتماً مقداری خطا در رشته بیت باب وجود دارد که در این مرحله به اصلاح آنها می‌پردازند. با عبور از مرحله تصحیح خطا آلیس و باب هر کدام یک رشته بیت در اختیار دارند که با احتمال بالا با یکدیگر یکسانند ولی هنوز هم این رشته بیت را به عنوان کلید در نظر نمی‌گیرند. آنها باید میزان اطلاعاتی که ممکن است ایو از کلید رمز نهایی بدست آورده باشد را به کمترین میزان ممکن یعنی صفر برسانند. ایو ممکن است در طول انتقال ذره یا تصحیح خطا اطلاعاتی را بدست آورده باشد، به همین خاطر آلیس و باب رشته بیت خود را باید به یک زیرمجموعه کوچکتر تقلیل دهند تا دانسته‌های ایو را به صفر برسانند. این مرحله را تقویت محرمانگی[۴] می‌نامند. پس از این مرحله یک کلید رمز که تنها برای آلیس و باب شناخته شده است با اطمینان بین آنها مشترک می‌شود[۹].

درآخر باید تاکید شود که در هر پروتکل توزیع کلید کوانتومی باید روش‌هایی برای تایید هویت[۵] بین آلیس و باب وجود داشته باشد. اگر چنین نباشد ممکن است آلیس به جای آنکه طرف او باب باشد، به صورت مستقیم با ایو ارتباط برقرار کند.

۲.۲ استراتژی های حمله

یکی از اساسی‌ترین مشکلات موجود در ایجاد یک ارتباط کوانتومی، کارشکنی‌های شنودکننده یا همان ایو است. ایو با برخوردار بودن از بالاترین سطح تکنولوژی همواره در پی بدست آوردن بیشترین اطلاعات از رشته بیت تبادلی بین آلیس و باب است. مزیت رمزنگاری کوانتومی سبب می‌شود که بسیاری از این کارشکنی‌های ایو در قالب خطا آشکار شود و آلیس و باب پی به وجود یک شنودکننده در بین مسیر انتقال پیام ببرند ولیکن بازهم ممکن است ایو روش‌هایی را برای حمله به پروتکل‌های توزیع کلید کوانتومی پیدا کند که از چشم آنها پنهان بماند. در این فصل پس از معرفی هر پروتکل توزیع کلید کوانتومی به بررسی چند نمونه از روش‌های حمله‌ای که ممکن است ایو روی آن‌ها اعمال کند، می‌پردازیم. ابتدا امنیت پروتکل‌ها را درشرایطی در نظر می‌گیریم که چشمه‌های ساطع کننده کیوبیت و سایر دستگاه‌های استفاده شده در اجرای پروتکل ایده‌آل باشد و در آخر فصل امنیت پروتکل‌های QKD را در محیط واقعی با در نظر گرفتن محدودیت‌های فیزیکیِ دستگاه‌ها مورد بررسی قرار می‌دهیم.

[۴] privacy amplification

[۵] authentication

بررسی امنیت در این فصل محدود به حمله‌های مستقل[۶] می‌شوند. زیرا حملات مستقل از ساده‌ترین استراتژی‌های حمله روی پروتکل‌های QKD است که بیشترین مطالعه روی آن ها صورت گرفته است. نکته اصلی در این گونه حمله‌ها این است که شنودکننده با هر سیگنال آمده از طرف آلیس به طور جداگانه برهم‌کنش[۷] می‌کند. برخی استراتژی ها برپایه این حقیقت هستند که ایو می‌تواند برهمکنش با کیوبیت را تا بعد از مرحله تصفیه و تصحیح خطا و یا تا هر وقت که لازم بداند به تعویق بیندازد تا بیشترین اطلاعات ممکن از مکالمات عمومی را بدست آورد. همچنین ایو می‌تواند به جای استفاده از این روش، اندازه‌گیری روی حالت را فوراً انجام دهد و در ادامه از اطلاعات مرحله تصفیه و تصحیح خطا استفاده کند.

درمقابل حمله‌های مستقل، حمله‌های جمعی [۸] قرار دارد که در آن ایو برای هر کیوبیت آمده از طرف آلیس، یک حالت کمکی آماده می‌کند و اجازه می‌دهد تا هر حالت با یک کیوبیت برهم‌کنش کند. سپس ایو حالت‌های اصلی را به دست باب می‌رساند و حالت‌های کمکی را نزد خود نگه می‌دارد. وقتی همه کیوبیت‌ها انتقال داده شدند، ایو صبر می‌کند تا بیشترین اطلاعات ممکن را از مکالمات عمومی بدست آورد و آن‌گاه بهترین اندازه‌گیری را روی همهٔ حالت‌های کمکی خود انجام می‌دهد تا بدین ترتیب به اطلاعات ارسال شده پی ببرد.

۱.۲.۲ تعاریف مورد نیاز

هر حمله‌ای که روی پروتکل‌های QKD تعریف می‌شود از روی مقدار اطلاعاتی است که ایو از کلید رمز به اشتراک گذاشته بین آلیس و باب بدست می‌آورد. هدف آلیس و باب این است که دسترسی به این اطلاعات را کمینه کنند. معمولاً اطلاعات ایو درباره کلید رمز شامل دو بخش است: اطلاعاتی که از اندازه‌گیری‌هایش روی سیگنال در حال تبادل بدست می‌آورد و اطلاعات درباره پایه‌های انتخابی آلیس و باب. بخش دوم به ایو نشان می‌دهد که آیا اندازه گیری درستی بر روی کیوبیت موردنظر اعمال کرده است یا خیر. بهترین راه نشان دادن آن این است که از احتمال شرطی $p(s|m)$ استفاده شود. در اینجا sمقدار بیتی است که آلیس فرستاده و m خروجی اندازه‌گیری ایو است. مقدار$p(s|m)$ به سادگی

[۶] Individual attacks

[۷] interaction

[۸] collective attacks

از احتمال $p(m|s)$ قابل محاسبه است. $p(m|s)$ یعنی احتمال آنکه ایو m را نتیجه بگیرد درصورتی که بیت s را فرستاده باشد که با استفاده از فرمول زیر قابل محاسبه است.

$$p(s|m) = \frac{p(m|s)}{\sum_{s'} p(m|s')} \tag{۱.۲}$$

کمیت مورد توجه دیگر، احتمال آن است که ایو نتیجه‌ای مشابه با آلیس بدست آورد که **احتمال برخورد**[۹] نام دارد.

$$p_c(s|m) = \sum_{s} p(s|m)^{۲} \tag{۲.۲}$$

چشمداشتیِ احتمال برخورد، روی خروجی های ممکنِ هر اندازه‌گیری ایو به صورت زیر تعریف می‌شود:

$$\langle p_c \rangle = \sum_{m} p(m) p_c(s|m) \tag{۳.۲}$$

برای کیفی کردن مقدار اطلاعات ایو از بیت آلیس می توان از آنتروپی شانون(H)[۱۰] استفاده کرد. از آنجایی که اطلاعات بستگی به نتیجه اندازه‌گیری ایو دارد، نسخه شرطی این آنتروپی مورد استفاده قرار می‌گیرد یعنی $H(S|M)$. آنتروپی شانون به صورت زیر تعریف می‌شود :

$$H(S|M = m) = -\sum_{m} p(s|m) \log p(s|m) \tag{۴.۲}$$

و از آن روی احتمال‌های نتایج ایو میانگین گرفته می‌شود:

$$H(S|M) = \sum_{m} p(m) H(S|M = m) \tag{۵.۲}$$

آنتروپی شانون برآورده کننده‌ی عدم قطعیت یک توزیع احتمال است و در نتیجه اختلاف آنتروپی شانون می‌تواند نشانگر اطلاعات بدست آمده باشد. برای یک توزیع احتمال اولیه‌ی X و توزیع بعدی Y ، اطلاعات بدست آمده به صورت $I = H(X) - H(Y)$ است. این فرمول می‌تواند برای توصیف مقدار اطلاعاتی که ایو از به کار بردن یک حمله مشخص بدست آورده است، مورد استفاده قرار گیرد. معمولاً فرض بر آن است که ایو هیچ اطلاعات اولیه ای درباره کلید رمز ندارد و در نتیجه $H(X) = ۱$ خواهد بود، دلیل این فرض بر این مبنا است که اصولاً آلیس رشته بیت خود را به صورت رندوم انتخاب می‌کند.

[۹] collision probability

[۱۰] shannon entropy

بنابراین مقدار اطلاعات بدست آمده توسط ایو پس از اجرای پروتکل به صورتِ $I = ۱ - H(S|M)$ خواهد بود.

نکته مهم بعدی این است که چه مقدار از کلید باید حذف شود تا اطلاعات ایو از آن کمینه شود. این مقدار را **قسمت حذفی** می‌نامند و مقدار آن با استفاده از چشمداشتی احتمال برخورد بدست می‌آید.

$$\tau = ۱ + \log \langle p_c \rangle^{\frac{۱}{n}} \qquad (۶.۲)$$

با دنبال کردن این معادله یک رشته بیت به طول n باید توسط $n\tau$ بیت حین مرحله تقویت محرمانگی کاهش یابد تا ایو را فقط با حداکثر یک بیت اطلاعات شانون از همه کلید رمز باقی بگذارد[۱۰].

۳.۲ پروتکل BB۸۴

اولین پروتکل برای توزیع کلید کوانتومی توسط بِنِت[۱۱] و براسارد[۱۲] در سال ۱۹۸۴ ارائه شد که با عنوان $BB۸۴$ شناخته شده است[۷]. همانطور که در بخش قبلی توضیح داده شد در این پروتکل مانند بسیاری از پروتکل‌های دیگر معمولاً از فوتون به عنوان ذره سیگنال استفاده می‌شود. قطبش، یکی از ویژگی‌های فوتون است که می‌تواند خواص کیوبیت را در برداشته باشد. به صورت قراردادی دو قطبش راست‌خطی با دو حالت پایه افقی $|۰\rangle$ ، و عمودی $|۱\rangle$ و قطبش قطری با دو حالت پایه $|+\rangle$ و $|-\rangle$ را تعریف می‌کنند به طوری‌که:

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

دو حالت $|۰\rangle$ و $|+\rangle$ در پایه‌های خود بیانگر مقدار بیت ۰ و حالت‌های $|۱\rangle$ و $|-\rangle$ بیانگر مقدار بیت ۱ هستند.

در $BB۸۴$ آلیس دنباله‌ای از تک فوتون‌ها را آماده می‌کند که هر کدام از آن‌ها به صورت کاملا رندوم با احتمال برابر در یکی از چهار حالت قطبش $|۰\rangle$ ، $|۱\rangle$ ، $|+\rangle$ یا $|-\rangle$ انتخاب شده‌اند. او حالت قطبش و مقدار بیت متناظر با هر حالتی که می‌فرستد را برای خود ثبت می‌کند. فوتون‌ها از طریق یک کانال

[۱۱] Bennet
[۱۲] Brassard

کوانتومی مناسب که می‌تواند فضای خلأ یا فیبر نوری باشد به باب منتقل می‌شوند. در طرف دیگر باب به صورت تصادفی و با احتمال برابر یکی از دو پایه راست‌خطی و یا قطری را برای اندازه‌گیری فوتون‌های دریافتی انتخاب می‌کند. پس از اندازه‌گیری، او نیز پایه انتخابی و بیت بدست آمده را برای خود ثبت می‌کند. در اینجا ارتباط کوانتومی پایان می‌یابد و ادامه پروتکل از طریق کانال کلاسیکی ادامه می‌یابد.

مرحله تصفیه در این مرحله باب با استفاده از کانال کلاسیکی (برای مثال هر وسیله ارتباطی مثل تلفن،...) پایه‌هایی را که برای اندازه‌گیری هر بیت انتخاب کرده است را با آلیس در میان می‌گذارد ولی از نتیجه اندازه‌گیری‌هایش حرفی نمی‌زند. آلیس، باب را مطلع می‌کند که در کدام حالت‌ها از پایه‌ی یکسان با او استفاده کرده است. آنها حالتهای با پایه یکسان را نزد خود نگه می‌دارند و سایر حالت‌ها را دور می‌ریزند. حال آنها یک رشته بیت کوتاهتر را بر این اساس در نزد خود دارند. این رشته بیت بدست آمده از مرحله تصفیه را **کلید خام**[۱۳] می‌نامند. اگر کانال کوانتومی بدون نوفه بود و هیچ شنودکننده‌ای در میان نبود کلید خام را می‌توانستند به عنوان کلید رمز نهایی در نظر بگیرند. ولیکن به طور طبیعی نمی‌توان کانال بدون نوفه و عدم حضور شنود کننده را تضمین کرد بنابراین گذراندن سایر مراحل کلاسیکی الزامی‌است[۹].

مرحله اصلاح مرحله اصلاح به دو بخش **تخمین خطا**[۱۴] و **تصحیح خطا** تقسیم می‌شود. در این مرحله هدف آن است که تمام خطاهای رشته بیتِ باب توسط کانال عمومی تصحیح شوند که در پی آن لاجرم باید مقداری از کلید خام اعلام شده و در نتیجه حذف شوند.

تخمین میزان خطا از مهمترین مراحل هر پروتکل است که طی آن بازه خطای[۱۵] کلید خام مشخص می‌شود. در $BB۸۴$ زیر مجموعه کوچک تصادفی از بیت‌های کلید خام به طول r انتخاب می‌شود. این رشته بیت انتخابی توسط آلیس و باب مقایسه می‌شود. تعداد مشخصی خطا،e،به دلیل تفاوت بین بیت‌ها بدست می‌آید. اگر طول رشته انتخابی متناسب با طول رشته کلید خام انتخاب شده باشد، احتمال خطا به صورت $p = \frac{e}{r}$ خواهد بود[۹].

اگر احتمال خطای بدست آمده خیلی زیاد باشد، آنگاه یا استراق سمع از پیام انجام شده و یا کانال

[۱۳] raw key

[۱۴] error estimation

[۱۵] error rate

کوانتومی به صورت غیرمتعارفی نوفه دارد. در این شرایط کلید خام حذف می‌شود و پروتکل باید دوباره شروع شود.

اگر احتمال p از یک مقدار بحرانی کمتر باشد، آنگاه آلیس و باب وارد مرحله‌های بعدی تصحیح خطا و تقویت محرمانگی می‌شوند. میزان این مقدار بحرانی با توجه به مشخصات فیزیکی سیستم بدست می‌آید.

خطاهای باقی مانده با تشکیل زیرمجموعه‌هایی از بیت‌های کلید خام و مقایسه پاریته آنها با استفاده از کانال عمومی برطرف می‌شوند. پاریته یک رشته دودویی (بیت) مثل $\{b_1, b_2, ..., b_n\}$ به صورت $P = b_1 \oplus b_2 \oplus ... \oplus b_n$ تعریف می‌شود که عبارت است از جمع مُد دو مقادیر بیت‌ها. یکی از ساده‌ترین روش‌های تصحیح خطا این است که آلیس به صورت تصادفی چندین جفت بیت از بیت‌های باقی‌مانده از کلید خام را انتخاب می‌کند. سپس جمع مد ۲ آنها را حساب و آن را به باب اعلام می‌کند. باب نیز حاصلجمع مد ۲ همان جفت بیت‌ها را حساب کرده و بررسی می‌کند که آیا مقادیر حاصلجمع خودش و آلیس یکسان است یا خیر. در صورت یکسان بودن آنها بیت اول را نگه داشته و بیت دوم را حذف می‌کنند و اگر یکسان نباشد هر دو بیت را حذف می‌کنند[۲]. در واقعیت الگوریتم‌های بهینه پیچیده‌تری برای تصحیح خطا استفاده می‌شود.

تقویت محرمانگی پس از مرحله تصحیح خطا آلیس و باب یک رشته بیت یکسان در اختیار دارند ولی هنوز ممکن است ایو مقداری اطلاعات از این رشته بیت در دست داشته باشد. بنابراین آلیس و باب باید اطلاعات ایو را از طریق روش‌های تقویت محرمانگی به کمترین مقدار ممکن یعنی صفر برسانند. برای تقویت محرمانگی روش‌های متعدد و پیچیده‌ای وجود دارد که ما در اینجا یکی از ساده‌ترین آنها را شرح می‌دهیم.

آلیس دوباره چندین جفت بیت از رشته بیتِ در دست خود را به صورت تصادفی انتخاب می‌کند و جمع مد ۲ آن را محاسبه می‌کند ولی این بار مقدار آن را اعلام نمی‌کند. او تنها به باب می‌گوید که کدام بیت‌ها انتخاب شده‌اند (برای مثال بیت‌های شماره ۱۰۳ و ۵۳۷) . آلیس و باب جفت بیت‌های انتخابی را حذف و مقدار حاصلجمع مُد دو را جایگزینشان می‌کنند. به این طریق آنها طول کلید را کاهش می‌دهند بدون آنکه خطایی بر جای بگذارند. از آنجاییکه ایو ممکن است تنها اطلاعات جزئی از بیت‌ها داشته باشد، با جایگزینی صورت گرفته توسط آلیس و باب این اطلاعات جزئی کاهش می‌یابد. برای

مثال فرض کنید ایو تنها مقدار بیت اول را می‌داند و از بیت دوم اطلاعی ندارد. بنابراین از حاصلجمع دو بیت نیز چیزی نخواهد دانست. و یا اگر مثلا ایو به احتمال ٪۶۰ از مقدار هر دو بیت اطلاع داشته باشد آنگاه احتمال آنکه او مقدار حاصلجمع مُد دو را درست حدس بزند $(۰/۶)^۲ + (۰/۴)^۲ = ۵۲٪$ است. این فرایند در یک پروتکل باید چندین بار تکرار شود[۳].

الگوریتم‌های تصحیح خطا و تقویت محرمانگی که توضیح داده شد کاملا الگوریتم‌های کلاسیکی هستند و این نشان می‌دهد که رمزنگاری کوانتومی به واقع یک علم میان‌رشته‌ای است. در ادامه چند نمونه از استراتژی‌های حمله که روی این پروتکل پیاده می‌شود را شرح می‌دهیم.

حمله سدسازی و بازارسال ساده

از رایج‌ترین نمونه های حمله مستقل ، حمله سدسازی و بازارسال ($I\&R$) [۱۶]است. هدف اصلی ایو در این نوع حمله آن است که هر فوتون رسیده از طرف آلیس را نزد خود نگه داشته و براساس پایه‌ای که قبلا برای خود مشخص کرده است، اندازه می‌گیرد سپس با توجه به نتیجه‌ای که بدست آمده فوتون‌های جدیدی را تهیه و به سمت باب ارسال می‌کند. برای بیان جزئی‌تر، فرض کنید کیوبیت آلیس در یکی از دو پایه راست‌خطی یا قطری است، یعنی یکی از چهار حالت $|H\rangle$ ، $|V\rangle$ ، $|+\rangle$ یا $|-\rangle$ به طوری که :

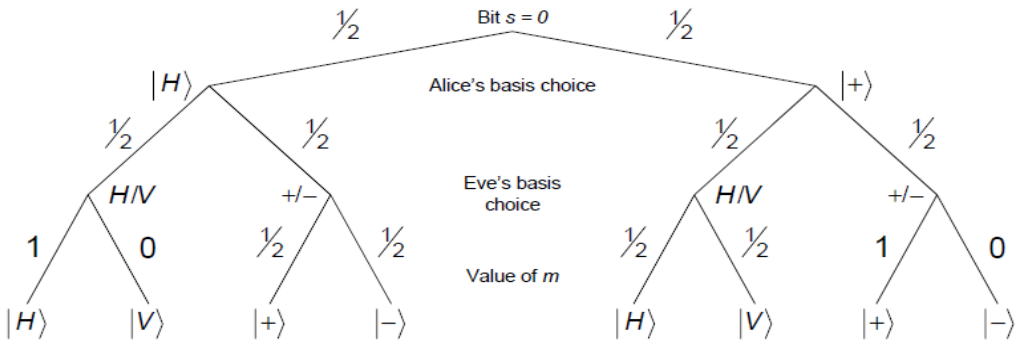
$$|+\rangle = \frac{۱}{\sqrt{۲}}(|H\rangle + |V\rangle)$$

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

اگر آلیس درصدد فرستادن بیت صفر باشد، آن را با احتمال مساوی به صورت $|H\rangle$ و یا $|+\rangle$ کدگذاری می‌کند. ایو بی خبر از نحوه کدگذاری آلیس، به صورت تصادفی یکی از پایه‌های H/V یا $+/-$ را برای اندازه‌گیری انتخاب می‌کند. اگر آلیس $|H\rangle$ را انتخاب کرده باشد و ایو در پایه H/V اندازه بگیرد و یا اگر آلیس $|+\rangle$ را فرستاده و ایو در پایه $+/-$ اندازه گرفته باشد، ایو به نتیجه درست خواهد رسید درغیر این صورت هر ترکیب دیگری، خروجی اندازه‌گیری کاملا تصادفی را در پی خواهد داشت.

فعلا فرض می‌کنیم ایو نمی‌تواند روی مکالمات عمومی بین آلیس و باب شنودی داشته باشد. بنابراین او نمی‌داند در چه شرایطی اندازه‌گیری‌هایش غلط است. احتمالات شرطی$p(m|s)$ برای چهار نتیجه ممکن

[۱۶] Intercept and resend



شکل ۱.۲: حمله $I\&R$ ساده

به صورت زیر است :

$$p(m=|H\rangle\,|s=۰)=p(m=|+\rangle\,|s=۰)=(\frac{۱}{۲})^۳+(\frac{۱}{۲})^۲(۱)=\frac{۳}{۸} \qquad (۷.۲)$$

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

و به همین صورت برای $p(m|s=۱)$ نیز قابل محاسبه است. برای احتمالات شرطی $p(s|m)$ مجموع $\sum_s p(m|s)=\frac{۱}{۲}$ و در نتیجه $p(s|m)=۲p(m|s)$ بدست می‌آید. بنابراین احتمال برخورد در نسخه ساده حمله $I\&R$ به صورت زیر محاسبه می‌شود.

$$p_c(s|m=|H\rangle)=(\frac{۳}{۴})^۲+(\frac{۱}{۴})^۲=\frac{۵}{۸} \qquad (۸.۲)$$

به طور مشابه برای $m=|V\rangle$ و$m=|+\rangle$ و$m=|-\rangle$ قابل محاسبه است که با استفاده از نتایج آن‌ها در میانگین احتمال برخورد، داریم:

$$\langle p_c\rangle=\sum_m \frac{۱}{۴}p_c(s|m)=۴(\frac{۱}{۴})[(\frac{۱}{۴})^۲+(\frac{۳}{۴})^۲]=\frac{۵}{۸} \qquad (۹.۲)$$

با استفاده از احتمال برخورد ، قسمت حذفی می‌تواند به صورت $۱+\log\langle p_c\rangle$ محاسبه شود که در نتیجه $\tau=۰٫۳۲۲$ بدست می‌آید. پس فقط $\frac{۱}{۳}$ از کلید باید حذف شود تا به طور تضمینی ایو به کمتر از یک بیت اطلاعات از کل کلید دسترسی پیدا کند. در محاسبه آنتروپی شانون برای حالت $M=|H\rangle$ داریم:

$$H(S|M=|H\rangle)=-\frac{۳}{۴}\log\frac{۳}{۴}-\frac{۱}{۴}\log\frac{۱}{۴}=۰٫۸۱۱ \qquad (۱۰.۲)$$

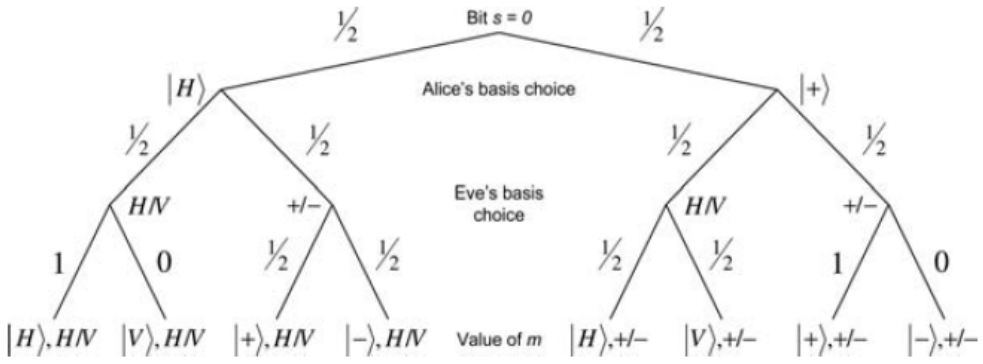
که این نتیجه برای آنتروپی های دیگر $H(S|M=|V\rangle)$ ، $H(S|M=|+\rangle)$ و $H(S|M=|-\rangle)$ برابر است به طوری که

$$H(S|M)=\sum_m \frac{۱}{۴}H(S|M=m) = ۴(\frac{۱}{۴})(-\frac{۳}{۴}\log\frac{۳}{۴}-\frac{۱}{۴}\log\frac{۱}{۴}) = ۰٫۸۱۱ \qquad (۱۱.۲)$$

کل اطلاعاتی که ایو در پایان، به ازای هر بیت خواهد داشت $۱ - H(S|M) \simeq ۰٫۲$ است که نتیجه ضعیفی برای ایو به حساب می‌آید. بنابراین ایو باید استراتژی دیگری را برگزیند تا اطلاعات بیشتری بدست آورد.

حمله سدسازی و بازارسال کامل

در این نوع از حمله $I\&R$ ایو به صورت تصادفی بین پایه‌های H/V و $+/-$ یکی را انتخاب می‌کند تا کیوبیت‌های رسیده از طرف آلیس را اندازه‌گیری کند سپس نتایجی که بدست می‌آورد را به جای کیوبیت‌های آلیس، برای باب می‌فرستد در آخر به شنود مکالمات آلیس و باب در حین مرحله تصفیه می‌پردازد. فرض کنید آلیس بیت ۰ را به صورت $|H\rangle$ کدگذاری کرده باشد و ایو با پایه H/V آن را اندازه بگیرد. ایو حتما حالت $|H\rangle$ را با قطعیت بدست می‌آورد و هیچ خطایی را از خود به جای نخواهد گذاشت. همچنین اگر پایه انتخابی ایو $+/-$ باشد نتیجه اندازه‌گیری او با احتمال مساوی یکی از دو حالت $|+\rangle$ یا $|-\rangle$ خواهد بود.



شکل ۲.۲: حمله $I\&R$ کامل

با مقایسه نمودار شکل ۲.۲ با نمودار شکل حمله $I\&R$ ساده به راحتی قابل مشاهده است که ایو می‌تواند دو پیشامد موجود برای $s=۰$ را حذف کند. به این معنی که احتمال بدست آوردن $|V\rangle$ در

صورتی که آلیس از پایه H/V استفاده کرده باشد و یا بدست آوردن $|-\rangle$ در صورتی که آلیس از پایه $+/-$ استفاده کرده باشد، صفر است. دانستن این احتمال سبب افزایش اطلاعات ایو در مقایسه با حمله $I\&R$ ساده می‌شود. به طور جزیی احتمال‌های شرطی $p(m|s)$ برابرند با:

$$p(m=|H\rangle, H/V|s=۰) = (\tfrac{۱}{۲})^۲ \cdot ۱ = \tfrac{۱}{۴} = p(m=|+\rangle, +/-|s=۰)$$

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

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

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

همچنین مقادیر مشابهی را برای $s=۱$ خواهیم داشت. برای مجموع $\sum_s p(m|s)$ مقدار $\frac{۱}{۴}$ بدست می‌آید به طوری که $p(s|m) = ۴p(m|s)$ است. با استفاده از این نتیجه‌ها، احتمال برخورد در شرایطی که ایو پایه درست را برای اندازه‌گیری هایش انتخاب کند ۱ و اگر پایه‌هایی مخالف با پایه‌های انتخابی آلیس انتخاب کند $\frac{۱}{۲}$ خواهد بود. بنابراین احتمال برخورد میانگین برابراست با:

$$\langle p_c \rangle = \frac{۱}{۴} + ۴\frac{۱}{۱۶} + \frac{۱}{۴} = \frac{۳}{۴}$$

برای آنتروپی شانون در صورتی که ایو پایه مشابه را حدس بزند ۰ و در غیر این صورت $\frac{۱}{۲}$ بدست می‌آید. بنابراین آنتروپی شانون میانگین برابراست با:

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

که ملاحظه می‌شود در این استراتژی حمله، در مقایسه با حالت ساده $I\&R$، ایو اطلاعات بیشتری را بدست می‌آورد.

حمله برپایه درهم‌تنیدگی

نمونه دیگر استراتژی حمله برای ایو استفاده از درهم‌تنیدگی است. در این نمونه ایو یک حالت کمکی را برای هر کیوبیتی که از طرف آلیس بدست او می‌رسد، آماده می‌کند و آن را با کیوبیت آلیس درهم‌تنیده می‌کند. سپس تنها کیوبیت اصلی آلیس را به باب می‌فرستد. بعد از آن ایو قادر است یک اندازه‌گیری و یا هر عملگر کوانتومی دیگری را روی حالت کمکی تحت مالکیت خود اعمال کند تا درباره کیوبیت اصلی اطلاعات بدست آورد.

با در نظر گرفتن پروتکل $BB۸۴$ یک روش ساده حمله برای ایو استفاده از یک زوج درهم‌تنیده مثل حالت‌های بل است.

$$|\phi^{\pm}\rangle = \frac{۱}{\sqrt{۲}}(|۰۰\rangle \pm |۱۱\rangle)$$

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

کافیست ایو یک اندازه‌گیری در پایه بل روی فوتون آمده از طرف آلیس و یکی از فوتون‌های درهم‌تنیده خودش انجام دهد تا به این ترتیب اطلاعات موجود در کیوبیت آلیس را روی فوتون دیگر درهم‌تنیده‌اش انتقال دهد. این عملیات همسان با یک دوربری کوانتومی[۱۷] است که طی آن یک کیوبیت ناشناخته روی حالت کمکی ایو دوربری می‌شود.

$$(\alpha|H\rangle+\beta|V\rangle)\frac{۱}{\sqrt{۲}}(|HH\rangle+|VV\rangle) = \frac{۱}{۲}\left[|\phi^{+}\rangle(\alpha|H\rangle+\beta|V\rangle)+|\phi^{-}\rangle(\alpha|H\rangle-\beta|V\rangle)+\right.$$

$$\left.|\psi^{+}\rangle(\alpha|V\rangle+\beta|H\rangle)+|\psi^{-}\rangle(\alpha|V\rangle-\beta|H\rangle)\right) \quad (۱۲.۲)$$

ایو می‌تواند حالت کمکی خود را تا زمانی که آلیس پایه انتخابی خود را آشکار می‌کند نگه دارد تا آن را در پایه درست اندازه بگیرد و در نتیجه همه اطلاعات را بدست آورد. با در نظر گرفتن احتمال برخورد میانگین و اطلاعات شانونِ ایو درباره‌ی بیت آلیس خواهیم دید که:

$$\langle p_c\rangle = ۱$$

$$۱ - H(S|M) = ۱$$

و این یعنی ایو کل اطلاعات درباره بیت فرستاده شده توسط آلیس را دارد. با این وجود کیوبیتی که ایو به باب می‌فرستد یک زیرسیستم از حالت بل است بنابراین همه اطلاعاتش درباره انتخاب پایه اولیه توسط آلیس را از دست داده است و در یک حالت کاملا مخلوط[۱۸] بسر می‌برد. باب در هر یک از دو پایه H/V یا $+/-$ اندازه‌گیری کند نتیجه‌ای کاملا تصادفی بدست می‌آورد که به سادگی از احتمال برخورد میانگین باب قابل مشاهده است ($\langle p_c\rangle = \frac{۱}{۲}$). در نتیجه آلیس و باب در مرحله تصفیه با میزان خطای زیادی روبه‌رو می‌شوند و متعاقبا از پروتکل خارج می‌شوند.

همانطور که می‌بینیم ایو همه اطلاعات مربوط به بیت آلیس را با استفاده از این استراتژی حمله بدست می‌آورد ولی احتمال برخورد میانگین همچنان مشابه با استراتژی $I\&R$ کامل است. بنابراین ایو

[۱۷] teleportation

[۱۸] mixed state

هیچ اطلاعات اضافی را از به کارگیری این نوع حمله بدست نمی‌آورد.

۴.۲ پروتکل $E۹۱$

در مقابل $BB۸۴$ و پروتکل‌های مشابه آن [۱۴][۱۵] که براساس ارسال تک کیوبیت‌های مستقل هستند، پروتکل‌هایی نیز طراحی شده‌اند که مبنای کارکرد آن‌ها استفاده از ذرات درهم‌تنیده است. درهم‌تنیدگی یک ویژگی منحصربه‌فرد فیزیکی برای سیستم‌های کوانتومی است که در روش‌های ارتباطاتی ابعاد تازه‌ای را بوجود آورده است. امنیت طرح‌ها و پروتکل‌هایی که بر مبنای حالت‌های درهم‌تنیده هستند از این اصل بنیادین نشأت گرفته‌اند که شنودکننده تنها به یک قسمت از سیستم درهم‌تنیده دسترسی خواهد داشت و بنابراین نمی‌تواند نتیجه کلی و دقیقی از کل سیستم داشته باشد[۱۶]. پروتکل پیشگام در این زمینه پروتکل $E۹۱$ است که در سال ۱۹۹۱ توسط آرتور ایکِرت[۱۹] ارائه شد[۱۳]. در این پروتکل ابتدا دو ذرهٔ درهم‌تنیده توسط یک منبع تولید شده و هر کدام از آن‌ها به دست آلیس و باب می‌رسد. مانند گذشته ذرات به کار برده شده را فوتون در نظر می‌گیریم. آلیس و باب با اندازه‌گیری قطبش فوتون‌ها در راستاهای مختلف و اعلام راستای انتخابی خود می‌توانند مشابه پروتکل $BB۸۴$ به نتایج مشخصی برسند. در پروتکل $E۹۱$ آلیس و باب ممکن است قطبش را در زاویه‌های مختلفی اندازه بگیرند. برای مثال ممکن است آلیس در سه جهت ۰°، ۴۵° و ۹۰° اندازه‌گیری کند، درحالی‌که باب سه راستای ۴۵°، ۹۰° و ۱۳۵° را برای اندازه‌گیری انتخاب کرده باشد. زمانی یک بیت به عنوان کلید درنظر گرفته می‌شود که هر دوی آن‌ها در راستای مشابه هم اندازه‌گیری کرده باشند. سپس نتایجی که در آن راستاهای مختلف انتخاب شده باشند به صورت عمومی اعلام شده و با هم مقایسه می‌شوند تا حضور یا عدم حضور ایو در بین مسیر انتقال کیوبیت‌ها برای آن‌ها مشخص شود. برای تشخیص حضور ایو آن‌ها از نامساوی $CHSH$[۲۰] استفاده می‌کنند به این صورت که اگر این نامساوی برقرار نباشد نشان دهنده آن است که درهم‌تنیدگی بین ذرات از بین رفته و درنتیجه حضور ایو مشخص می‌شود.

[۱۹] Artur Ekert

[۲۰] Clauser-Horne-Shimony-Holt

حمله NOT کنترلی

یک استراتژی برای ایو در پروتکل $E۹۱$ آن است که حالت کمکی خود را در حالت $|H\rangle$ آماده کند و یک عملگر NOT کنترلی روی کیوبیت و حالت کمکی خود اعمال کند.

$$CNOT_{۱۲} = |H\rangle\langle H| \otimes I + |V\rangle\langle V| \otimes (|۰\rangle\langle ۱| + |۱\rangle\langle ۰|) \qquad (۱۳.۲)$$

عملگر $CNOT$ یک عملگر کوانتومی است که روی دو کیوبیت (یک کیوبیت به عنوان منبع و دیگری به عنوان هدف) عمل می‌کند. اگر کیوبیت منبع در حالت $|V\rangle$ باشد یک NOT یا بیت برگردان روی کیوبیت هدف انجام می‌شود. اندیس‌ها در معادله ۱۳.۲ نشان دهنده آن است که کدام کیوبیت منبع (اولین اندیس) و کدام کیوبیت هدف (دومین اندیس) است. بکار بردن این اندیس‌ها تنها برای راحتی تشخیص نحوه عملکرد $CNOT$ روی حالتی با بیش از دو کیوبیت است.

ایو پس از دسترسی به کیوبیت ارسالی آلیس عملگر $CNOT$ را روی کیوبیت آلیس و حالت کمکی خود اعمال می‌کند و در پی آن کیوبیت ایو به صورت زیر تغییر می‌کند:

$$CNOT_{۲۳}(|\phi^+\rangle_{۱۲} \otimes |H\rangle_{۳}) = \frac{۱}{\sqrt{۲}}(|HHH\rangle_{۱۲۳} + |VVV\rangle_{۱۲۳}) \qquad (۱۴.۲)$$

حالت بدست آمده یک حالت درهم‌تنیده سه‌تایی GHZ است که دارای ویژگی‌های خاصی است برای مثال اگر یکی از فوتون‌ها اندازه گرفته بشود دو فوتون دیگر، بسته به نتیجه اندازه‌گیری، بلافاصله به یک حالت مشخص ریزش[۲۱] می‌کند. در شرایط معادله ۱۴.۲ اگر آلیس در پایه H/V اندازه‌گیری کند و از طرفی دیگر باب و ایو نیز در پایه مشابه آلیس کیوبیت خود را اندازه‌گیری کنند، نتیجه مشابه با آلیس را بدست می‌آورند. ولی اگر آلیس از پایه $+/-$ استفاده کند نتیجه اندازه‌گیری باب در پایه مشابه او در ۵۰٪ از مواقع با نتیجه آلیس ارتباطی ندارد. بنابراین احتمال برخورد و اطلاعات شانون در حالتی که آلیس و باب پایه H/V را انتخاب کرده باشند به صورت زیر است:

$$\langle p_c\rangle = ۱$$

$$۱ - H(S|M) = ۱$$

در حالیکه برای یک اندازه‌گیری در پایه $+/-$ ، باب نتیجه مشابه با آلیس را با احتمال $\langle p_c\rangle = \frac{۱}{۲}$ بدست می‌آورد. بنابراین کل اطلاعاتی که ایو روی هر بیت رمز بدست می‌آورد $۱ - H(S|M) = ۰/۷۵$ می

[۲۱] collapse

باشد. واضح است که مقدار بدست آمده در مقایسه با استراتژی‌های $I\&R$ بیشتر است. با این وجود یک خطا با احتمال $\frac{1}{4}$ در هر بار استفاده از پایه $+/-$ توسط آلیس و باب وجود دارد. این نامتقارنی در به وجود آمدن خطاها تشخیص وجود ایو برای آلیس و باب را آسان می‌کند[۱۰].

۵.۲ پروتکل Ping-Pong

پروتکل‌هایی که تاکنون معرفی شد و بسیاری دیگر از پروتکل‌های مرسوم در تولید کلید کوانتومی معمولاً پیش‌بینی ناپذیر[۲۲] هستند. به این معنا که اصولاً آلیس یک بیت کلاسیکی را با استفاده از یک سیستم کوانتومی رمزی می‌کند و به باب می‌فرستد ولی او نمی‌تواند پیش بینی کند که دقیقاً کدام یک از بیت‌های انتقالی در آخر به عنوان کلید رمز مورد استفاده قرار خواهند گرفت و کدام یک باید حذف شوند. این نوع ارتباطات پیش‌بینی ناپذیر منجر به اشتراک گذاری یک کلید رمز تصادفی بین آلیس و باب خواهد شد. بعدها آن‌ها می‌توانند از این کلید برای رمزگشایی متون رمزی شده که از طریق کانال کلاسیکی منتقل می‌شود استفاده کنند.

در سال ۲۰۰۲ بیج[۲۳] و همکارانش اولین پروتکل ارتباطی مستقیم[۲۴] را ارائه دادند که در آن طرفین می‌توانند بدون آنکه کلید تصادفی را بین خود تشکیل دهند، با یکدیگر ارتباط برقرار کنند[۱۸]. یعنی آنکه متن اصلی را مستقیماً از طریق کانال کوانتومی در دسترس یکدیگر قرار دهند. پس از آن‌ها بوستروم[۲۵] و فلبینگر[۲۶] پروتکلی را با عنوان $Ping-Pong$ مطرح کردند که علاوه بر پیش‌بینی‌پذیر و مستقیم بودن از ویژگی‌های درهم‌تنیدگی نیز بهره می‌برد. ایده اصلی این پروتکل رمزی کردن اطلاعات از طریق اعمال عملگرهای جایگزیده روی یک زوج EPR (حالت بِل) است.

وقتی دو فوتون در درجه آزادی قطبششان با یکدیگر به صورت بیشینه درهم‌تنیده می‌شوند آنگاه نمی‌توان هرکدام از فوتون‌ها را به صورت منفرد درهم‌تنیده درنظر گرفت. اگر قطبش عمودی را با حالت $|۰\rangle$ و قطبش افقی را با حالت $|۱\rangle$ نمایش دهیم آنگاه حالت‌های بِل $|\psi^{\pm}\rangle$ را می‌توان به صورت زیر

[۲۲] non-determinstic
[۲۳] Beige
[۲۴] Direct communication
[۲۵] Bostrom
[۲۶] Felbinger

نمایش داد:

$$|\psi^{\pm}\rangle = \frac{۱}{\sqrt{۲}}(|۰۱\rangle \pm |۱۰\rangle) \qquad (۱۵.۲)$$

حالت‌های بل حالت‌های درهم‌تنیده بیشینه‌ای هستند که در یک فضای هیلبرت دو ذره‌ای می‌توان آن‌ها را توصیف کرد به طوری‌که فضای هیلبرت آن

$$H = H_A \otimes H_B$$

اندازه‌گیری قطبش یکی از فوتون‌ها، نتیجه‌ای کاملاً تصادفی در پی خواهد داشت. این امر نشأت گرفته از این حقیقت است که ماتریس چگالی کاهش یافته متناظر با هر فوتون نتیجه‌ای کاملاً مخلوط را نشان می‌دهد:

$$\rho_A^{\pm} = Tr_B\{|\psi^{\pm}\rangle\langle\psi^{\pm}|\} = \frac{۱}{۲}(|۰\rangle\langle۰| + |۱\rangle\langle۱|) = \frac{۱}{۲}\mathrm{I}_A \qquad (۱۶.۲)$$

بنابراین هیچ‌کس با دسترسی داشتن به تنها یک کیوبیت از دو جفت کیوبیت درهم‌تنیده قادر به تمایز دو حالت $|\psi^{+}\rangle$ و $|\psi^{-}\rangle$ از یکدیگر نیست. چون حالت‌های $|\psi^{+}\rangle$ و $|\psi^{-}\rangle$ بر یکدیگر عمود هستند تنها با اندازه‌گیری روی هر دوی فوتون‌ها می‌توان آنها را از یکدیگر تشخیص داد. به عبارت دیگر یک بیت اطلاعات می‌تواند در حالت $|\psi^{\pm}\rangle$ رمزگذاری شود به گونه‌ای که برای هرکس که تنها به یکی از فوتون‌ها دسترسی دارد نامشخص باشد.

عملگر یکانی زیر را درنظر بگیرید:

$$\sigma_Z^A \equiv (\sigma_Z \otimes \mathrm{I}) = (|۰\rangle\langle۰| - |۱\rangle\langle۱|) \otimes \mathrm{I} \qquad (۱۷.۲)$$

این عملگر می‌تواند حالت $|\psi^{+}\rangle$ را به $|\psi^{-}\rangle$ (و بالعکس) تبدیل کند. هرچند عملگر σ_Z^A (که درواقع همان عملگر پاولی Z است) تنها روی یک کیوبیت و آن هم به صورت جایگزیده[۲۷] عمل می‌کند ولی اثری غیرجایگزیده[۲۸] بر کل حالت بِل دارد. شخصی که تنها به یک کیوبیت دسترسی داشته باشد می‌تواند یک بیت اطلاعات را روی آن رمزگذاری کند ولی نمی‌تواند آن را رمزگشایی کند زیرا هیچ دسترسی به کیوبیت دیگر ندارد.

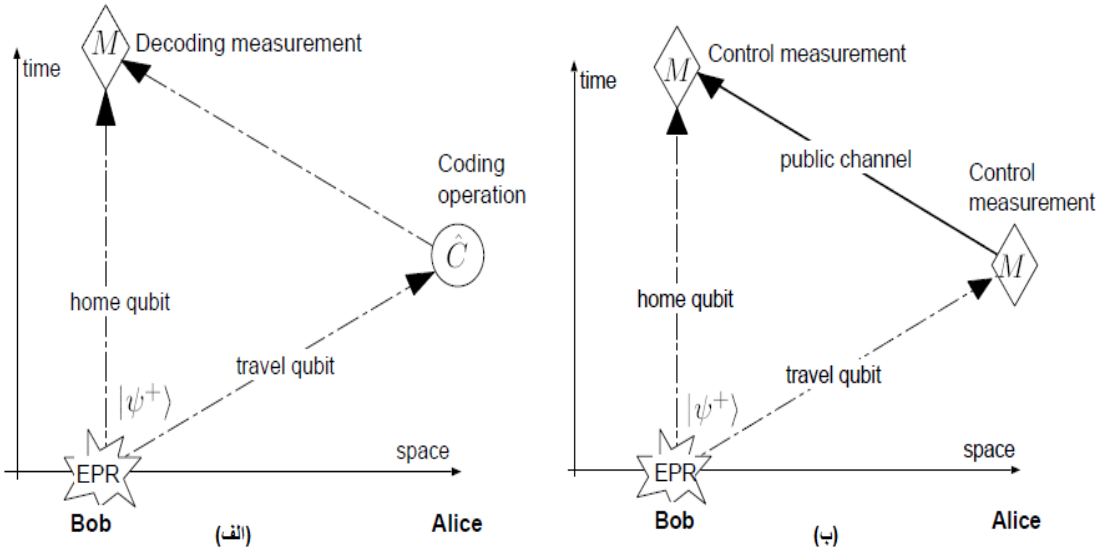
[۲۷] Local

[۲۸] non-local

با توجه به توضیحاتی اولیه‌ای که داده شد روند کار در پروتکل $Ping-Pong$ به این صورت است که ابتدا باب دو فوتون را درحالت $|\psi^+\rangle$ آماده می‌کند. یکی از فوتون‌ها را در نزد خود نگاه داشته و دیگری را برای آلیس می‌فرستد. آلیس بسته به آنکه چه مقدار بیتی را در نظر دارد، تصمیم می‌گیرد که آیا روی کیوبیت دریافتی عملگر σ_Z را اعمال کند یا خیر (عدم اعمال عملگر σ_Z را می‌توان به صورت اعمال عملگر همانی I در نظر گرفت). سپس کیوبیت را به باب بازمی‌فرستد. حال باب دوباره هر دو کیوبیت را در اختیار دارد. او می‌تواند با یک اندازه‌گیری در پایه بِل $|\psi^+\rangle$ یا $|\psi^-\rangle$ را با توجه به آنکه آلیس چه عملگری اعمال کرده است، بدست می‌آورد. بدین ترتیب او می‌تواند یک بیت از اطلاعات را از آلیس دریافت کند. در این پروتکل یک کیوبیت، یک مسیر رفت و برگشتی را طی می‌کند تا یک بیت اطلاعات از آلیس به باب منتقل شود.

در ادامه فلبینگر و بوستروم دو مُد ارتباطی را بین آلیس و باب معرفی می‌کنند؛ مُد پیام و مُد کنترل. به طور پیش فرض آلیس و باب در مُد پیام قرار دارند و به همان صورتی که توضیح داده شد با یکدیگر ارتباط برقرار می‌کنند. امّا در برخی مواقع آلیس پس از دریافت کیوبیت، با احتمال c اعلام می‌کند که مُد کنترل را انتخاب کرده است و به جای آنکه روی کیوبیت دریافتی عملگر اعمال کند، یک اندازه‌گیری در پایه $B_z = \{|۰\rangle, |۱\rangle\}$ انجام می‌دهد. آلیس با استفاده از کانال عمومی نتیجه اندازه‌گیری خود را به باب می‌فرستد. سپس باب نیز وارد مُد کنترل می‌شود و کیوبیت در دست خود را بر پایه B_z اندازه‌گیری می‌کند. باب نتیجه خود را با نتیجه آلیس مقایسه می‌کند؛ اگر نتایج با یکدیگر سازگار نبودند آنگاه پی به حضور شنودکننده خواهند برد و ارتباط را قطع می‌کنند.

نویسندگان در حین بررسی امنیت پروتکل ادعا می‌کنند که پروتکل شبه امن است. به این معنا که شنودکننده می‌تواند مقدار کمی از اطلاعات را قبل از آنکه حضورش آشکار شود بدست می‌آورد. در واقع آن‌ها مُد کنترل را برای تشخیص حضور ایو در نظر گرفته‌اند. هدف ایو برای شنود در این پروتکل تنها کشف عملگر اعمالی آلیس است. از آنجایی که ایو به کیوبیتی که از ابتدا تا انتهای فرایند پروتکل در دست باب باقی می‌ماند دسترسی ندارد، بنابراین همه آنچه که او می‌تواند بدست آورد از کیوبیتِ رفت و برگشتی حاصل می‌شود. آن‌ها در بررسی امنیت پروتکل به حمله‌ای اشاره می‌کنند که طی آن ایو کیوبیتی در حال انتقال از آلیس به باب را با یک کیوبیت از جانب خودش، توسط عملگر یکانی (E) درهم‌تنیده



شکل ۳.۲: الف: نمایی از مُد پیام ؛ ب: نمایی از مُد کنترل

می‌کند:

$$E\left|0\right\rangle\left|\chi\right\rangle=\alpha\left|0\right\rangle\left|\chi_0\right\rangle+\beta\left|1\right\rangle\left|\chi_1\right\rangle \qquad \left|\alpha^2\right|+\left|\beta^2\right|=1$$

$$E\left|1\right\rangle\left|\chi\right\rangle=\alpha'\left|0\right\rangle\left|\chi'_0\right\rangle+\beta'\left|1\right\rangle\left|\chi'_1\right\rangle \qquad \left|\alpha'^2\right|+\left|\beta'^2\right|=1$$

پس از آن ایو اجازه می‌دهد تا سیستم مرکب جدید به دست آلیس برسد. پس از اعمال عملگر توسط آلیس و بازفرستادن آن به سمت باب، ایو در بین راه حالت کمکی خود را اندازه می‌گیرد تا بدین ترتیب اطلاعات رمزگذاری شده توسط آلیس را بدست آورد. بوستروم و فلبینگر با بدست آوردن یک رابطه بین اطلاعات دریافتی ایو و بازه خطای ایجاد شده در مُد کنترل، با استفاده از مرز هولِوُ[۲۹] که کمیتی برای مشخص کردن حداکثر میزان اطلاعات دریافتی است، نشان می‌دهند که اطلاعات دریافتی ایو کاملاً محدود است. همین مسئله را یوشیدا[۳۰] و همکارانش در مقاله‌ای با استفاده از مفهوم رد فاصله[۳۱] به اثبات رسانیده‌اند[۲۰].

پس از ارائه پروتکل $Ping-Pong$ مقالات متعددی در زمینه امنیت این پروتکل در مقابل حمله‌های متعدد بررسی شد[۲۳]،[۲۲]. از طرف دیگر عده‌ای در صدد بهبود بخشیدن و بهینه کردن این پروتکل

[۲۹] Holevo bound

[۳۰] Yoshida

[۳۱] Trace distance

برآمدند. برای مثال کای[۳۲] و لی[۳۳] در مقاله‌ای با عنوان "ارتقا بخشیدن ظرفیت پروتکل بوستروم و فبلینگر" [۲۱]نسخه تعمیم یافته‌ای از پروتکل $Ping-Pong$ را ارائه دادند که در آن به جای انتقال یک بیت اطلاعات کلاسیکی در هر بار اجرای مُد پیام، دو بیت اطلاعات از آلیس به باب منتقل می‌شود. ایده به کار برده شدهٔ آن‌ها استفاده از هر چهار حالت بل و هر چهار ماتریس پاولی در روند کلی انتقال پیام است. همچنین برای بالا بردن امنیت پروتکل آن‌ها در مُد کنترل از دو پایه عمود بر هم $B_x=\{|+\rangle,|-\rangle\}$ و $B_z=\{|0\rangle,|1\rangle\}$ به جای استفاده از یک پایه استفاده کرده‌اند.

یکی دیگر از مقالاتی که در جهت تکمیل پروتکل $Ping-Pong$ ارائه شده است، مقاله اِنگوین[۳۴] با عنوان "مکالمه کوانتومی"[۲۴] است. در این مقاله نویسنده با مطرح کردن ایراداتی بر پروتکل $Ping-Pong$ سعی بر رفع آن ایرادات در مدل اصلاح شده خود دارد. هر چند در برخی مواقع او نیز کاملاً موفق نشده است. برای مثال در مکالمه کوانتومی مطرح می‌شود که در پروتکل $Ping-Pong$ در صورتی که آلیس مُد کنترل را انتخاب کند دیگر کیوبیت ارسالی به سمت باب بازفرستاده نمی‌شود. همین امر سبب می‌شود شنودکننده در هر بار به راحتی تشخیص دهد، آلیس مد کنترل را انتخاب کرده است یا مد پیام. به این ترتیب در هر بار که مد پیام اجرا می‌شود او می‌تواند کیوبیت برگشتی از سمت آلیس را بر پایه $|0\rangle$ و $|1\rangle$ اندازه‌گیری کند و یا با اعمال تصادفی عملگر روی آن سعی بر ایجاد اختلال در انجام پروتکل نماید. این کار سبب می‌شود بدون آنکه کسی متوجه حضورش شود، اطلاعات دریافتی باب کاملاً تصادفی شده و هیچ اطلاعاتی نصیب او نشود. نویسنده برای جلوگیری از چنین حمله‌ای مد کنترل اصلاح شده‌ای را ارائه می‌کند. به این صورت که در کل پروتکل آلیس همیشه کیوبیت دریافتی از باب را پس از اعمال عملگر برای باب بازمی‌فرستد. اما در صورتی که او مد کنترل را انتخاب کرده باشد، عملگری که اعمال کرده است را از طریق کانال عمومی به باب می‌گوید. باب با اندازه‌گیری در پایه بل روی هر دو کیوبیت بررسی می‌کند که آیا عملگری که آلیس اعمال کرده است با تغییراتی که روی حالت بل اتفاق افتاده است همخوانی دارد یا خیر. در صورت عدم همخوانی باب به حضور ایو پی خواهد برد. نکته این اصلاحیه آن است که دیگر ایو قادر به تشخیص مد کنترل از مد پیام نخواهد بود. هر چند در این صورت پروتکل در مقابل حملهٔ ایجاد اختلال محفوظ می‌شود. اما کماکان پروتکل در مقابل حمله‌ی

[۳۲] Cai
[۳۳] Li
[۳۴] Nguyen

سدسازی وبازارسال ($I\&R$) از طرف ایو در خطر است.

حمله ($I\&R$) به این صورت است که در مسیر رفتِ کیوبیت (از باب به آلیس)، ایو کیوبیت را نگه داشته و جفت درهم‌تنیده دیگری را آماده می‌کند و یک کیوبیت آن را برای آلیس می‌فرستد. آلیس به باور آنکه کیوبیت دریافتی همان کیوبیت مدنظر باب است، اقدام به اعمال عملگر مدنظر خود می‌کند و کیوبیت را باز می‌فرستد. در بین راه ایو دوباره کیوبیت را نگه داشته و با کیوبیتی که در نزد خود داشته است اندازه‌گیری بر پایه بل انجام می‌دهد و پی به عملگر اعمالی آلیس می‌برد. سپس ایو همان عملگر را روی ذره‌ای که از باب در دست خود دارد اعمال می‌کند و آن را به او بازمی‌گرداند. بدین ترتیب ایو بدون آنکه خطایی ایجاد کند پی به کل اطلاعات رد و بدل شده بین آلیس و باب می‌برد. نویسنده مقاله ادعا می‌کند که راهی برای جلوگیری از این نوع حمله در پروتکل خود ارائه داده است و آن این است که در هر بار اجرای پروتکل باب قبل از فرستادن کیوبیت خود روی آن یکی از چهار عملگر پاولی را اعمال کند تا بدین ترتیب، اولاً مکالمه حالت دو سویه پیدا کند و ثانیاً از خطر این نوع از حمله سدسازی و بازارسال مصون باقی بمانند.

لازم به ذکر است که ادعای اول (دو سویه شدن پروتکل) نویسنده صحت دارد به‌طوری‌که در مد پیام باب پس از بازپس‌گیری کیوبیت از طرف آلیس نتیجه نهایی را اعلام می‌کند. از آنجایی که به عملگر اعمالی خودش واقف است با توجه به نتیجه نهایی می‌تواند پی به عملگر اعمالی آلیس ببرد. همین امر برای آلیس نیز صادق است و او نیز متوجه عملگر اعمالی باب خواهد شد. بنابراین یک مکالمه بین طرفین ارتباط، شکل می‌گیرد.

اما ادعای دوم (مصون ماندن از حمله نگه داشتن و دوباره فرستادن ایو) نمی‌تواند درست باشد زیرا تغییر حالت بل کیوبیت ارسالی باب تاثیری در حمله ایو ندارد بلکه هدف ایو تنها پی بردن به عملگر آلیس است که با همان روشی که توضیح داده شد، وی همچنان قادر خواهد بود عملگر آلیس را بدون آنکه اثری از خود به جای بگذارد کشف کند[۲۵].

در انتهای فصل به معرفی چند نوع دیگر از استراتژی‌های حمله مرسوم در بین پروتکل‌های توزیع کلید کوانتومی می‌پردازیم:

۶.۲ استراتژی‌های حمله در محیط واقعی

پروتکل‌ها و حمله‌هایی که پیشتر توضیح داده شد بر مبنای حضور در یک محیط ایده‌آل بوده است. محیطی که در آن منابع ساطع کننده فوتون تنها سیگنال‌های تک فوتون گسیل می‌کنند و آشکارسازها ٪۱۰۰ بهینه هستند. اما با استفاده از تکنولوژی امروز دسترسی به چنین شرایطی غیر ممکن است. آشکارسازها به شدت حساس‌اند و اغلب حتی با وجود اینکه فوتونی فرستاده نشده است، کلیک می‌کنند (به این پدیده شمارش تاریک[۳۵] می‌گویند). این اتفاق در حین مراحل تصحیح خطا و تقویت محرمانگی مشخص می‌شود.

از طرفی هیچ منبع ساطع کننده تک فوتون وجود ندارد بلکه یک پالس سیگنال معمولی، اغلب شامل تعداد زیادی فوتون است. برای حل این مشکل از پالس‌های همدوس ضعیف[۳۶] (WCP) در دستگاه‌های واقعی رمزنگاری کوانتومی استفاده می‌شود. WCPها به صورت زیر توصیف می‌شوند:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \qquad (۱۸.۲)$$

که بر هم‌نهی از حالت‌هایی با تعداد فوتون از صفر تا n هستند[۳۷]. چنین پالس‌هایی میانگین تعداد فوتون (μ) کمتری دارند به طوریکه احتمال کشف بیش از یک فوتون در هر پالس از توزیع پوآسون زیر تبعیت می‌کند:

$$P(n,\mu) = \frac{\mu^n}{n!} e^{-\mu} \qquad (۱۹.۲)$$

میانگین تعداد فوتون (μ) را نمی‌توان به صورت دلخواه کاهش داد زیرا این کار سبب کاهش بازده پروتکل می‌شود. در این بخش برخی استراتژی‌های حمله ارائه شده است که در آن از چنین گریزراه‌هایی[۳۸] که به علت محدودیت‌های فیزیکی به وجود آمده‌اند، استفاده شده است.

[۳۵] dark count
[۳۶] weak coherent pulses
[۳۷] Fock states
[۳۸] loopholes

۱.۶.۲ حمله PNS

حمله تقسیم تعداد فوتون[۳۹] یا PNS اولین بار توسط هاتنِر[۴۰] و همکارانش معرفی شد و پس از آن توسط سایر متخصصان علم رمزنگاری کوانتومی مانند براسارد[۴۱] مورد بحث و بررسی قرار گرفت. این نوع حمله از قدرتمندترین حملات مستقل است.

PNS روی چشمه‌های فوتونی گسیل کننده پالس‌های ضعیف همدوس (WCP) به کار برده می‌شود. چشمه‌هایی که فوتون‌های منفرد را تنها با یک احتمال مشخص تولید می‌کنند و با یک احتمال بسیار کوچک نیز پالس‌هایی شامل دو یا چند فوتون با قطبش یکسان ساطع می‌کنند.

استراتژی حمله برای ایو این است که پالس‌های حاوی چندین فوتونِ فرستاده شده توسط آلیس را نگه داشته، یک فوتون از بین آنها را برداشته و در حافظه کوانتومی خود ذخیره می‌کند. سپس اجازه می‌دهد باقی فوتون‌ها به باب برسد. پس از آن ایو صبر می‌کند تا آلیس و باب پایه‌های اندازه‌گیری خود را از کانال عمومی مقایسه کنند حال او می‌تواند فوتونی که برداشته است را در پایه صحیح اندازه‌گیری کند.

به طور دقیق تر حمله PNS کمی پیچیده‌تر از فرایندی که توضیح داده شد، است. با توجه به فرمول ۱۹.۲ احتمال آنکه چشمه آلیس پالس خالی از فوتون[۴۲] گسیل کند، بالاست و احتمال گسیل یک پالس تک فوتون در حدود ٪۱۰ است. همچنین احتمال گسیل یک پالس حاوی چند فوتون بسیار پایین است (در حدود ٪۵). به همین دلیل ایو نمی‌تواند برای همه پالس‌هایی که از آلیس به او می‌رسد این حمله را اجرا کند بلکه او باید تنها پالس‌های حاوی چند فوتون را بررسی کند. در نتیجه او باید عملگری را به کار ببندد که طی آن در هر بار بتواند یک اندازه‌گیری غیر مخرب[۴۳] انجام دهد تا یک فوتون را جدا کرده و پالس را به یک حالت با تعداد ثابتی از فوتون‌ها فرو بریزد[۴۴]. او با استفاده از چنین عملگری می‌تواند تمام اطلاعات را از سیگنال‌های حاوی چند فوتون بدست آورد.

به طور کلی برنامه‌ی ایو نسبت به هر سیگنال آمده از طرف آلیس به این صورت است: او از

[۳۹] photon number splitting
[۴۰] Huttner
[۴۱] Brassard
[۴۲] vacum pulse
[۴۳] non-demolition measurement
[۴۴] collapse

همه سیگنال‌های بدون فوتون چشم پوشی می‌کند تا جایی که همه شمارش‌های تاریک متوقف می‌شوند. همه سیگنال‌های حاوی چند فوتون را با استفاده از استراتژی PNS مورد حمله قرار می‌دهد و همه اطلاعات درباره بیت رمز را از این سیگنال‌ها بدست می‌آورد بدون آنکه خطایی برجا بگذارد. قسمتی از سیگنال‌های تک فوتون را متوقف می‌کند و به قسمت دیگری از آنها با استراتژی $I\&R$ حمله می‌کند. ایو تعداد سیگنال‌های حذف شده را طوری انتخاب می‌کند که با احتمال آشکارسازی کلی باب سازگار باشد. با فرض بی نقص بودن کانال کوانتومی و آشکارسازها همه خطاهای ناشی از این برنامه توسط حمله $I\&R$ ایجاد می‌شوند ولی باب قادر نخواهد بود که این خطاها را از آنچه که او نسبت به شمارش‌های تاریک انتظار دارد تمییز دهد. در این شرایط ارتباط به طور کلی نا امن است.

تا کنون راه‌حل‌های متعددی برای این مشکل ارائه شده است ولی یکی از قابل اطمینان‌ترین آن‌ها استفاده از روش حالت‌های تله‌ای[۴۵] است. در مقاله[۲۶] نشان داده شده است که توزیع پوآسون تعداد فوتون‌ها در مواجهه با حمله PNS تا وقتی که شدت سیگنال‌ها مقدار مشخصی هستند، ثابت است. در روش حالت‌های تله‌ای آلیس با استناد به این نتیجه، به صورت تصادفی برخی پالس‌ها را با تعداد میانگین فوتونی کمتر می‌فرستد یعنی شدت را کاهش می‌دهد و همین سبب می‌شود که حمله PNS تشخیص داده شود.

۲.۶.۲ حمله اسب تروژان

تا به حال استراتژی‌های حمله به این صورت بوده‌اند که ایو درصدد کشف بیشترین میزان اطلاعات ممکن از کیوبیت‌های تبادلی بین آلیس و باب بوده است. ولی ایو می‌تواند استراتژی کاملا متفاوتی را نیز در نظر بگیرد. این نوع حمله که باز هم بر اساس شرایط واقعیِ دستگاه‌ها شکل می‌گیرد حمله اسب تروژان[۴۶] یا حمله تزریق نور[۴۷] نام دارد. در این روش ایو پالس‌هایی(فوتون‌هایی) را به سمت دستگاه‌های آلیس و باب می‌فرستد سپس پالس بازگشتی را مورد تجزیه و تحلیل قرار می‌دهد. پالس بازگشتی می‌تواند حامل اطلاعاتی درباره آشکارسازها باشد و یا اینکه کشف کند آلیس چه پایه‌ای را برای آماده‌سازی فوتون درنظرگرفته است. اگر ایو بتواند قبل از آنکه فوتونِ آلیس به باب برسد پایه را کشف کند، با یک حمله

[۴۵] decoy state

[۴۶] trojan-horse attack

[۴۷] light injection attack

$I\&R$ ساده همه اطلاعات رشته بیت را به دست خواهد آورد.

اقدام متقابل در مواجهه با این نوع استراتژی حمله نیز با تغییر دادن شدت نور میسر می‌شود. آلیس و باب می‌توانند با ردوبدل کردن فوتون‌هایی با شدت مشخص دستگاه‌های خود را کالیبره کنند. همچنین برای شرایطی که ارتباط آنها منحصرا یک طرفه است می‌توانند با افزودن دستگاههای جدیدی در سیستم‌های خود مانع وارد شدن پالس‌های تزریقی ایو شوند. برای مثال فوتون‌هایی که قرار است از چشمه آلیس خارج شوند کافیست از یک عایق اپتیکی[۴۸] و یک فیلتر عبور کنند. این عایق اپتیکی با جلوگیری از ورود سیگنال‌ها به سیستم آزمایشگاهی آلیس مانع اجرا شدن چنین حمله‌ای می‌شود.

[۴۸] optical isolator

فصل ۳

پروتکل توزیع کلید کوانتومی به روش $N۰۹$

۱.۳ مقدمه

مکانیک کوانتومی از آغاز شکل گیری‌اش در حدود یک قرن پیش تا به امروز دستاوردهای شگرفی داشته است. هرچند مفاهیم نظری آن معمولاً محل بحث و بررسی فراوان بوده است. به هرحال پدیده‌های جدیدِ متعددی برپایه مکانیک کوانتومی پیش بینی و مشاهده شده‌اند که در حوزه فیزیک کلاسیک غیر قابل توضیح هستند. وجود بسیاری از زمینه‌های علمیِ امروز مدیون مکانیک کوانتومی هستند یکی از این زمینه‌ها ارتباطات کوانتومی است. در این فصل یک پروتکل توزیع کوانتومی معرفی خواهیم کرد که در کمال تعجب اطلاعات زمانی در آن منتقل می‌شوند که هیچ ذره‌ی فیزیکی کوانتومی بین فرستنده و گیرنده ردوبدل نشده باشد. این پروتکل توزیع کلید کوانتومی بر اساس مفهومی تحت عنوان "**اندازه‌گیری بدون برهم‌کنش**" بنا شده است. این مفهوم که در رمزنگاری و همچنین رایانش کوانتومی مورد استفاده قرار گرفته است، از این حقیقت ناشی می‌شود که حضور یک جسمِ مانع به عنوان ابزاری برای اندازه‌گیری در یک تداخل‌سنج سبب می‌شود تا تداخل به هم بریزد، حتی اگر هیچ ذره‌ای توسط جسم جذب نشده باشد. بنابراین لازم است قبل از آنکه به معرفی پروتکل مورد نظر بپردازیم ابتدا درباره این مفهوم توضیحات بیشتری داده شود.

۲.۳ اندازه‌گیری بدون برهم‌کنش

غیر جایگزیدگی[۱] یکی از جنبه‌های رمزآلود مکانیک کوانتومی است که همواره مورد مناقشاتی در بین دانشمندان بوده است. بعد از مباحثات متعدد پیرامون نظریه EPR، در نهایت نامساوی بل نشان داد که غیرجایگزیدگی می‌تواند وجود داشته باشد[۲۸]. پس از آن به صورت آزمایشگاهی و تجربی نیز این امر اثبات گردید[۲۹]. با استفاده از مفهوم غیرجایگزیدگی می‌توان نوعی از اندازه‌گیری را توصیف کرد که قادر است حضور یک جسم در یک محدوده از فضا را بدون آنکه ذره یا نوری آن جسم را لمس کند مشخص کند. این نوع از اندازه‌گیری، اندازه‌گیری بدون برهمکنش[۲] یا اندازه‌گیری خلاف واقع[۳] نامیده می‌شود که هیچ مشابه کلاسیکی برای آن وجود ندارد. ابتدا اندازه‌گیری غیرجایگزیده را به صورت مختصر

[۱] non-locality

[۲] interaction-free measurement

[۳] counterfactual measurement

تبیین می‌کنیم.

اگر یک جسم باردار و یا جسمی که دارای یک تکانه الکتریکی(مغناطیسی) باشد را در محدوده‌ی مشخصی از فضا قرار دهیم می‌توان با اندازه‌گیری میدان الکتریکی(مغناطیسی) که اطراف جسم ایجاد شده است بدون آنکه ذره‌ای را با خود جسم برهم‌کنش دهیم، پی به حضور آن در محل موردنظر ببریم. مکانیک کوانتومی اجازه می‌دهد تا وجود یک جسم را به روشی غیرجایگزیده، با استفاده از اثر آهارانو-بوم[۴] تشخیص داد[۳۰] این اثر را حتی اگر جسم هیچ میدان الکترومغناطیسی در اطراف محدوده فضایی خود ایجاد نکرده باشد نیز می‌توان مشاهده کرد زیرا تنها مشخص بودن پتانسیل الکتریکی جسم در یک نقطه از فضا می‌تواند حضور آن را بدون آنکه ذره‌ای از آن عبور کند، مشخص کند.

همچنین اگر جسم هیچ تغییر قابل مشاهده‌ای را در یک فاصله ایجاد نکند یعنی با دنیای خارجی خود تنها به صورت جایگزیده[۵] برهم‌کنش داشته باشد نیز می‌توان تحت شرایطی موقعیتش را با اندازه‌گیری بدون برهم‌کنشِ غیرجایگزیده‌ای پیدا کرد. برای مثال فرض کنید یک جسم در یکی از دو جعبه وجود دارد، اگر داخل یکی از دو جعبه را مشاهده کنیم و جسم مورد نظر را نیابیم خواهیم دانست که حتماً جسم در جعبه دیگر است. یک مثال پیچیده‌تر از کسب اطلاعات به روش اندازه‌گیری بدون برهم‌کنش، اندازه‌گیری روی یک سیستم آماده شده در یکی از حالت بِل است. اگر دو جسم در یک ویژه حالتِ مکان، با هم درهم‌تنیده شده باشند، اندازه‌گیری مکان یک جسم مکان جسم دیگر را مشخص می‌کند.

در دو مثالی که توضیح داده شد عاملی که سبب تشخیص موقعیت یک جسم بدون برهم‌کنش با آن می‌شد، اطلاعات اولیه‌ای است که از جسم، قبل از انجام اندازه‌گیری داده شده است. در مثال اول مشخص شده بود که جسم حتما در یکی از دو جعبه قرار دارد و در مثال دوم ارتباط بین مکان دو جسم مشخص بود. ولیکن در صدد آن هستیم نوعی از اندازه‌گیری بدون برهم‌کنش را معرفی کنیم که بدون داشتن هیچ اطلاعات اولیه از جسم، بتواند حضور آن را در محدوده‌ای از فضا مشخص کند.

[۴] Aharonov-Bohm

[۵] local

۳.۳ آزمایش نتیجه منفی رنینگر

یکی از اولین آزمایشات ذهنی از این نوع اندازه‌گیری در بیش از نیم قرن پیش توسط رنینگر[۶] ارائه شد[۳۱].همه آزمایشاتی که به عنوان اندازه‌گیری بدون برهم‌کنش طراحی شده‌اند نسخه کامل شده و پیچیده تر این آزمایش هستند. آزمایش نتیجه منفی رنینگر[۷] را می‌توان به صورت شکل ۱.۳ در نظر

شکل ۱.۳: آزمایش نتیجه منفی رنینگر[۳۲]

گرفت. وقتی یک فوتون که حالت آن را می‌توان به صورت$|\psi\rangle$ در نظرگرفت، توسط یک چشمه گسیل تک فوتون ساطع شده و وارد یک شکافنده پرتو با ضریب انتقال[۸] $\frac{۱}{۲}$ شود تبدیل به برهم‌نهی از دو حالت $|\psi_۱\rangle$ و $|\psi_۲\rangle$ با احتمال یکسان $\frac{۱}{۲}$ می‌شود به طوریکه:

$$|\psi\rangle = \frac{۱}{\sqrt{۲}}(|\psi_۱\rangle + |\psi_۲\rangle)$$

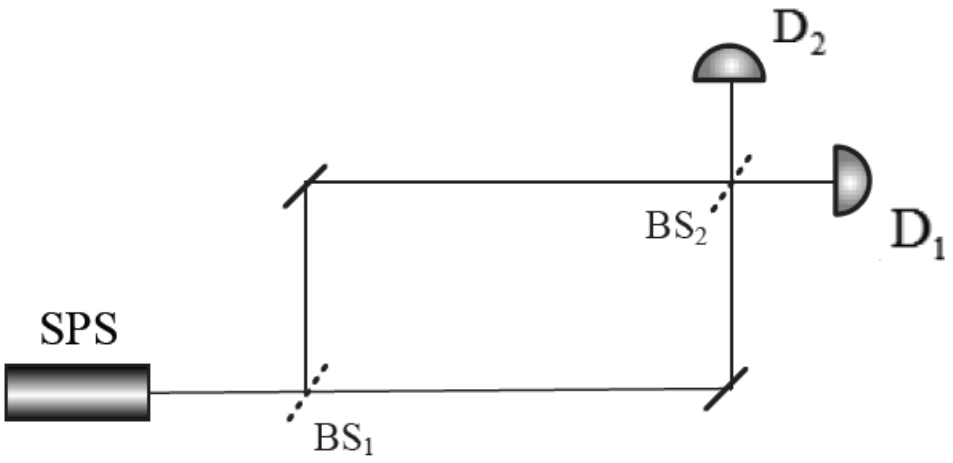
پس از عبور فوتون از شکافنده پرتو[۹] ،$|\psi_۱\rangle$بازتاب شده و مسیر کوتاه‌تری را برای رسیدن به آشکار ساز $D_۱$ پیش رو دارد یعنی بعد از طی کردن یک بازه زمانی $\Delta t_۱$ به $D_۱$ می‌رسد و حالت $|\psi_۲\rangle$ مسیر بلندتری را برای رسیدن به آشکارساز $D_۲$ پیش‌رو دارد و مدت زمان $\Delta t_۲$ را برای رسیدن به $D_۲$ احتیاج دارد. به عنوان نتیجه، ٪۵۰ از فوتون‌ها باید توسط $D_۱$ آشکار شده و ٪۵۰ دیگر به آشکارساز $D_۲$ برسند(در این آزمایش آشکارسازها ٪۱۰۰ بهینه درنظر گرفته شده‌اند). در چنین شرایطی واضح است که اگر یک آشکارسازی توسط $D_۱$ انجام شود، آنگاه می‌دانیم که مطمئناً هیچ ذره‌ای به $D_۲$ نخواهد

[۶] Renninger
[۷] Renninger's negative-result experiment
[۸] transmission efficiency
[۹] beam splitter

رسید. به طور معکوس اگر D_1 بعد از طی زمان Δt_1 هیچ آشکارسازی انجام ندهد، آنگاه می‌دانیم که فوتون با طی کردن زمان طولانی‌تر Δt_2 به آشکارساز D_2 خواهد رسید. بنابراین در این آزمایش طبق اصول مکانیک کوانتومی می‌دانیم در حالت اول که اندازه‌گیری توسط D_1 انجام می‌شود برهم نهی $|\psi\rangle = \frac{1}{\sqrt{2}}(|\psi_1\rangle + |\psi_2\rangle)$ به $|\psi_1\rangle$ ریزش کرده و یک نتیجه مثبت از این آشکارسازی بدست می‌آید. ولی در حالت دوم گرفتن نتیجه منفی(یا نتیجه نگرفتن) از آشکارساز D_1 سبب می‌شود که برهم‌نهی حالت‌های فوتون به حالت $|\psi_2\rangle$ ریزش کند و آشکارسازی توسط D_2 صورت پذیرد. به همین دلیل این آزمایش با عنوانِ اندازه‌گیری منفی نامیده می‌شود[۳۲]. آزمایشی که رنینگر ارائه داده است مدل پیچیده‌تر از آنچه که توضیح داده شد است. در واقع نکته اصلی آزمایش رنینگر این است که ممکن است یک آشکارساز چیزی را آشکار نکند(اندازه نگیرد) اما با این وجود در سرنوشت اندازه‌گیری یک سیستم تاثیرگذار باشد.

۴.۳ اندازه‌گیری بدون برهم‌کنش الیتزور و وایدمن

اندازه‌گیری بدون برهم‌کنشی که الیتزور[۱۰] و وایدمن[۱۱] درسال ۱۹۹۳ ارائه داده‌اند براساس استفاده از یک تداخل‌سنج ماخ-زندر[۱۲] است که در اپتیک کلاسیکی نیز کاربرد دارد.



شکل ۲.۳: تداخل سنج ماخ-زندر

[۱۰] Elitzur
[۱۱] vaidman
[۱۲] Mach-Zehnder

شکل ۲.۳ نمایی از این تداخل سنج را نشان می‌دهد. طرز کار تداخل‌سنج به این صورت است که فوتون(یا هر نوع ذره دیگری) پس از ورود به دستگاه به اولین شکافنده پرتو($BS_۱$) با ضریب انتقال $\frac{۱}{۲}$می‌رسد. پس از آن حالت فوتون تبدیل به برهم‌نهی از دو حالت عبوری و بازتابی با احتمال برابر$\frac{۱}{۲}$ می‌شود. حالت‌های فوتون به گونه‌ای توسط آینه‌ها بازتاب می‌شوند که در نهایت، اگر در مسیرهای تداخل‌سنج خللی وجود نداشته باشد دو حالت پس از رسیدن به شکافنده نور دوم دوباره جمع‌آوری شده و به حالت اولیه برمی‌گردند. دو آشکارساز $D_۱$ و $D_۲$ برای آشکارسازی فوتون‌ها پس از شکافنده پرتو دوم تعبیه شده اند. در این شکل موقعیت آینه‌ها و شکافنده‌های پرتو به گونه‌ای طراحی شده است که پس از عبور از $BS_۲$ بدلیل تداخل ویرانگر هیچ ذره‌ای به آشکارساز $D_۲$ نمی‌رسد بلکه هر ذره ورودی در انتهای مسیر تداخل سنج توسط $D_۱$ آشکارسازی می‌شود. ولی اگر بدون تغییر موقعیت آینه‌ها و آشکارسازها، یکی از دو مسیر تداخل‌سنج را مسدود کنیم، ذراتی که موفق به عبور از تداخل‌سنج می‌شوند با احتمال مساوی توسط یکی از دو آشکارساز $D_۱$ یا $D_۲$ آشکار می‌شوند. بنابراین آشکارساز $D_۲$ تنها در شرایطی ذرات را آشکار می‌کند که چیزی مانع مسیر ذرات در یکی از بازوهای تداخل‌سنج شده باشد.

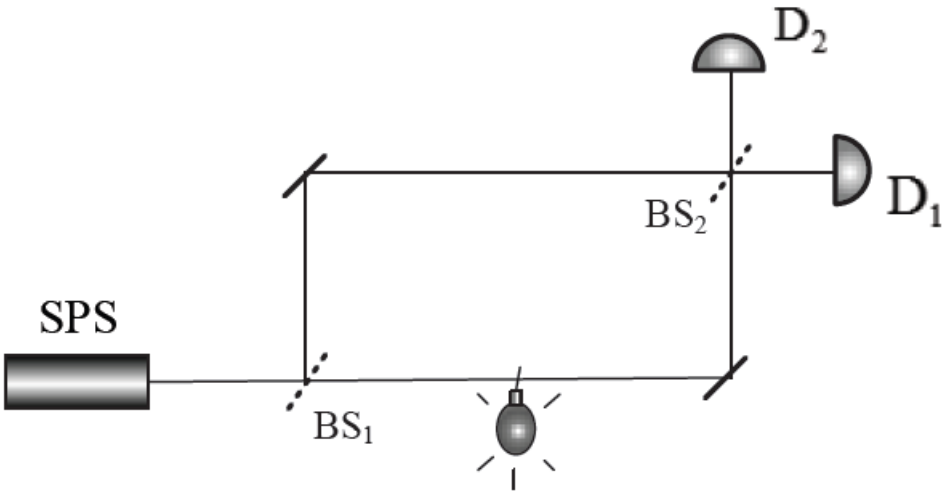
با توجه به توضیحات داده شده دستورالعمل الیتزور و وایدمن برای پیدا کردن وجود یک جسم در یک محدوده مشخص، بدون آنکه ذره‌ای از جسم عبور داده شود به صورت زیر است:

یک تداخل‌سنج فوتونی به صورتی که در بالا توضیح داده شد آماده می‌شود و مسیرهای عبور فوتون، به صورتی قرار می‌گیرد که یکی از بازوهای تداخل‌سنج از محدوده فضایی که قصد تشخیص جسم در آن ناحیه را داریم بگذرد.

حال اگر یک تک‌فوتون وارد سیستم شود سه نتیجه برای این اندازه‌گیری امکان خواهد داشت:

- هیچ آشکارسازی کلیک نکند.
- آشکارساز $D_۱$ کلیک کند.
- آشکارساز $D_۲$ کلیک کند.

در نتیجه اول فوتون توسط جسم جذب و یا پراکنده شده است و هیچ‌گاه به آشکارسازها نمی‌رسد. احتمال وقوع این نتیجه $\frac{۱}{۲}$ است. نتیجه دوم که با احتمال $\frac{۱}{۴}$ رخ می‌دهد نتیجه موردنظر الیتزور و وایدمن نیست زیرا احتمال دارد فوتون چه در شرایطی که جسم در مسیر عبوری فوتون در تداخل سنج باشد و چه در این



شکل ۳.۳: اندازه‌گیری بدون برهم‌کنش الیتزور و وایدمن

شرایط نباشد، به آشکارساز D_1 برسد بنابراین از آن نتیجه‌ای نمی‌توان گرفت. نتیجه سوم همان نتیجه مد نظر است؛ این نتیجه که با احتمال $\frac{1}{4}$ رخ می‌دهد دربردارنده این اطلاعات است که حتما جسمی در بین راه فوتون وجود داشته است ولی فوتون توسط جسم پراکنده و یا جذب نشده است. درواقع این آزمایش یک اندازه‌گیری بدون برهم‌کنش با جسم است زیرا تنها یک فوتون وارد تداخل‌سنج شده و اگر با جسم برهم‌کنش می‌کرد نمی‌توانست به آشکارساز D_2 برسد.

مکانیک کوانتومی می‌تواند این آزمایش را به طور ساده‌ای توصیف کند: فرض کنید حالت فوتونی که به سمت راست حرکت می‌کند $|1\rangle$ و حالت فوتون وقتی به سمت بالا می‌رود $|2\rangle$ باشد. همچنین می‌دانیم که فاز (تابع موج) یک فوتون پس از بازتاب شدن به اندازه $\frac{\pi}{2}$ تغییر می‌کند. بنابراین اثر صفحه نیمه نقره اندود (شکافنده پرتو) روی حالت فوتون به صورت زیر است:

$$\begin{aligned} |1\rangle &\to \tfrac{1}{\sqrt{2}}(|1\rangle + i\,|2\rangle) \\ |2\rangle &\to \tfrac{1}{\sqrt{2}}(|2\rangle + i\,|1\rangle) \end{aligned} \qquad (۱.۳)$$

و اگر آینه‌ها کاملاً نقره اندود باشند به صورت زیر توصیف می‌شوند:

$$\begin{aligned} |1\rangle &\to i\,|2\rangle \\ |2\rangle &\to i\,|1\rangle \end{aligned} \qquad (۲.۳)$$

در عدم حضور جسم یعنی اگر یک تداخل‌سنج استاندارد باشد تحول حالت فوتون به شرطی که از سمت

راست وارد تداخل‌سنج شده باشد، از اولین مرحله تا آخر به صورت زیر خواهد بود:

(۳.۳)

$$|۱\rangle \rightarrow \frac{۱}{\sqrt{۲}}(|۱\rangle + i\,|۲\rangle) \rightarrow \frac{۱}{\sqrt{۲}}(i\,|۲\rangle - |۱\rangle) \rightarrow \frac{۱}{۲}(i\,|۲\rangle - |۱\rangle) - \frac{۱}{۲}(|۱\rangle + i\,|۲\rangle) = -\,|۱\rangle$$

در نتیجه فوتون تداخل‌سنج را در حالی ترک می‌کند که به سمت آشکارساز $D_۱$ می‌رود. ولی در شرایطی که جسم در یکی از مسیرها حضور دارد تحولات به صورت زیر فرمول بندی می‌شوند:

(۴.۳)

$$|۱\rangle \rightarrow \frac{۱}{\sqrt{۲}}(|۱\rangle + i\,|۲\rangle) \rightarrow \frac{۱}{\sqrt{۲}}(i\,|۲\rangle + i\,|scattered\rangle) \rightarrow \frac{۱}{۲}(i\,|۲\rangle - |۱\rangle) + \frac{۱}{\sqrt{۲}} i\,|scattered\rangle$$

$|scattered\rangle$ بیانگر حالت فوتون پراکنده شده توسط جسم است. با توجه به خواص اندازه‌گیری کوانتومی، آشکارسازها عامل ریزش حالت‌های کوانتومی هستند.

(۵.۳)

$$\frac{۱}{۲}(i\,|۲\rangle - |۱\rangle) + \frac{i}{\sqrt{۲}}\,|scattered\rangle \rightarrow \begin{cases} |۲\rangle \;\Rightarrow\; D_۲ clicks\;,\; probability \frac{۱}{۴} \\ |۱\rangle \;\Rightarrow\; D_۱ clicks\;,\; probability \frac{۱}{۴} \\ |scattered\rangle \;\Rightarrow\; no-clicks\;,\; probability \frac{۱}{۲} \end{cases}$$

بنابراین آشکارسازی $D_۲$ اطلاعاتی را درباره حضور یک جسم در مسیر تداخل‌سنج می‌دهد، بدون آنکه با ذره برهم‌کنشی داشته باشیم. مشاهده می‌شود که تنها وقتی جسم حضور دارد آشکارساز $D_۲$ می‌تواند فوتون را آشکار کند. بنابراین آشکارسازی $D_۲$ دربردارنده این اطلاعات است که حتماً جسم در قسمتی از بازوهای تداخل‌سنج قرار داده شده است [۳۲]،[۳۳]،[۳۴].

در ادامه به توصیف اولین پروتکل توزیع کلید کوانتومی ارائه شده برپایه اندازه‌گیری پادواقعی یا اندازه‌گیری بدون برهم‌کنش می‌پردازیم.

۵.۳ پروتکل $N09$

توزیع کلید کوانتومی ورای جذابیت‌های اقتصادی و امنیتی که دارد، بستر مناسبی برای تبلور ایده‌ها و مفاهیم جدید نظریه اطلاعات کوانتومی و مطالعات مکانیک کوانتومی را پدید آورده است. پیرو همین امر در سال ۲۰۰۹ نُه[۱۳] پروتکل جدید و جالبی را ارائه کرد که با عبارت $N09$ شناخته شده است. در این پروتکل اطلاعات به صورت امن بین آلیس و باب توزیع می‌شود حتی در زمانی که هیچ ذره‌ی حامل اطلاعاتی بین آنها منتقل نشده باشد. درواقع در این پروتکل یک **اندازه‌گیری خلاف واقع** یا به عبارت دیگر یک **اندازه‌گیری بدون برهم‌کنش** به‌کار بسته شده است و به همین دلیل به عنوان توزیع کلید کوانتومی خلاف واقع($CQKD$)[۱۴] از آن یاد می‌شود. اندازه‌گیری بدون برهم‌کنش برپایه ویژگی‌های بنیادین مکانیک کوانتومی این اجازه را می‌دهد تا بدون ایجاد برهم‌کنشی بین جسم مورد نظر و وسیله اندازه‌گیری حضور آن جسم آشکار شود. همان طور که در بخش قبل توضیح داده شد یکی از مشهور ترین این نوع از اندازه‌گیری‌ها آزمایش ذهنی مربوط به الیتزور و وایدمن است.

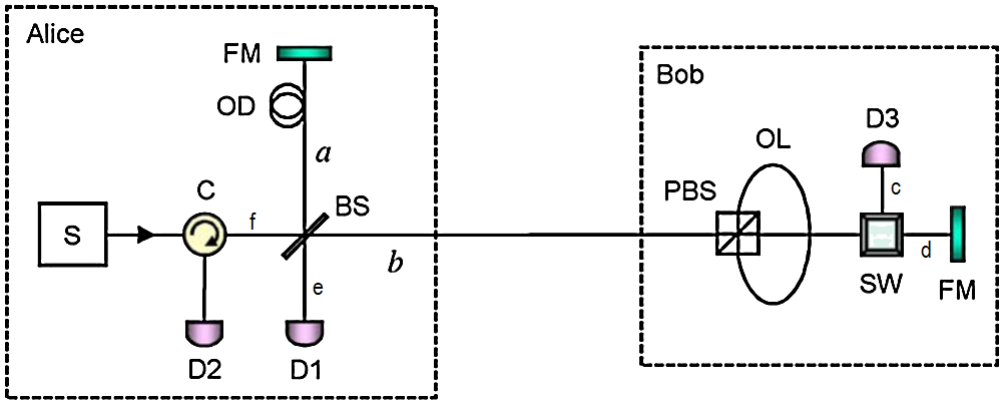
$CQKD$ پروتکل‌های مرسوم قبلی که برپایه انتقال موثر ذرات حامل اطلاعات بین طرفینِ ایجاد ارتباط بودند را به چالش کشیده است.در نتیجه یک پیشرفت نظری مهمی در این زمینه اتفاق افتاد و سبب شد مطالعات و پیشنهادات بیشتری در این نوع از پروتکل‌ها ارائه شود[۳۷]،[۳۸]،[۳۹]. برای شروع توضیحات درباره پروتکل $N09$ ابتدا مراحل انجام پروتکل را با توجه به شکل ۴.۳ توضیح می‌دهیم.

ابتدا آلیس به صورت تصادفی یک تک فوتون ساطع شده از چشمه S را به یکی از دو حالت قطبش عمود برهم $|H\rangle$ یا $|V\rangle$ رمزگذاری می‌کند تا بدین وسیله مقدار بیت مورد نظر خود را در قالب یک فوتون رمزگذاری کند. حالت قطبش افقی، $|H\rangle$، بیانگر بیت ۰ و حالت قطبش عمودی $|V\rangle$، بیانگر مقدار بیت ۱ است.تک فوتون رمزگذاری شده پس از عبور از یک گردان اپتیکی[۱۵] (C) وارد یک شکافنده پرتو (BS) می‌شود. با عبور تک فوتون از شکافنده پرتو، حالت فوتون به دو حالت در هر دو مسیر a و b شکافته می‌شود. این دو حالت شکافته شده را با توجه به بیت انتخابی آلیس می‌توان به صورت زیر در

[۱۳] Noh

[۱۴] Counterfactual Quantum Key Distribution

[۱۵] optical circulator



شکل ۴.۳: نمای پروتکل $N۰۹$

نظر گرفت:

$$|\varphi_۰\rangle = \sqrt{T}|۰\rangle_a|H\rangle_b + i\sqrt{R}|H\rangle_a|۰\rangle_b$$
$$|\varphi_۱\rangle = \sqrt{T}|۰\rangle_a|V\rangle_b + i\sqrt{R}|V\rangle_a|۰\rangle_b \qquad (۶.۳)$$

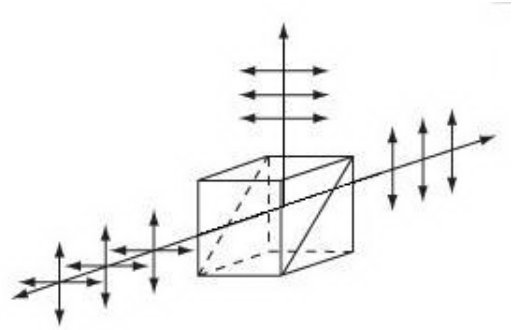
با توجه به شکل مسیر a بیانگر مسیر به سمت آینه فارادی (FM) و b بیانگر مسیر به سمت قسمت باب است. $|۰\rangle_k$ $(k = a, b)$ حالت خلأ مسیرها را مشخص می‌کند. R و $T = ۱ - R$ نیز به ترتیب ضریب بازتابندگی و ضریب عبور از BS را نشان می‌دهد. در مسیر a فوتون توسط یک آینه فارادی بازتاب می‌شود و همیشه در ناحیه امنیتی آلیس باقی می‌ماند. در مسیر b، فوتون از قسمت آلیس به قسمت باب حرکت می‌کند.

باب نیز مانند آلیس یکی از دو قطبش H یا V که نشان دهنده مقدار بیت مورد نظرش است را به صورت تصادفی انتخاب می‌کند. اگر قطبش فوتون ورودی با قطبشی که باب در نظر گرفته است یکسان باشد، سیستم برای باب به گونه‌ای طراحی شده است که سبب می‌شود فوتون به سمت آشکارساز $D_۳$ هدایت شده و در نتیجه مسیر اپتیکی b یک طرفه می‌گردد. بستن مسیر اپتیکی با استفاده از سازوکار دستگاه‌های قسمت باب صورت می‌گیرد (شکل ۴.۳)؛ اگر پالس اپتیکی ورودی به قسمت باب، به صورت افقی پلاریزه شده باشد از شکافنده پرتو قطبشی[۱۶] (PBS) عبور می‌کند و مستقیماً به سمت کلید اپتیکی با سرعت بالا[۱۷] (SW) می‌رود و اگر فوتون به صورت عمودی قطبیده شده باشد، ابتدا از

[۱۶] polarizing beam splitter

[۱۷] high speed optical switch

شکافنده پرتو قطبشی بازتاب شده سپس وارد حلقه اپتیکی[۱۸] می‌شود و پس از آن به سمت کلید اپتیکی می‌رود.عملکرد PBS در شکل زیر تبیین شده است.



شکل ۵.۳: نحوه عملکرد یک شکافنده پرتو قطبشی

بنابراین باب با کنترل اختلاف زمانی ایجاد شده می‌تواند به صورت مؤثری حالت قطبشی انتخاب شده‌اش را به سمت آشکارساز $D_۳$ هدایت کند.

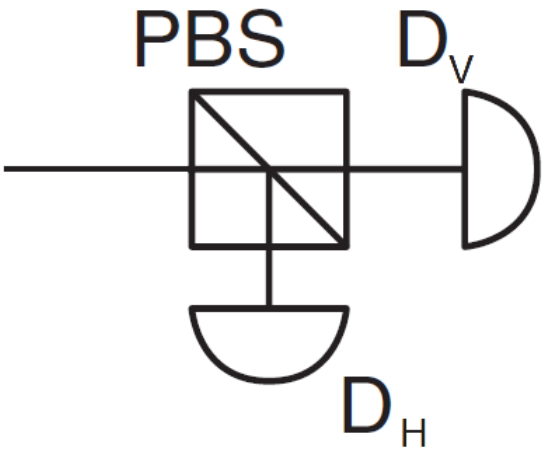
حال اگر قطبش انتخابی باب با مقدار بیتی که آلیس برای فوتون درنظر گرفته است متفاوت باشد، مسیر b برای حالت فوتون شکافته شدهٔ ورودی دیگر بسته نخواهد بود یعنی دیگر فوتون تحت تأثیر کلید اپتیکی SW نخواهد بود بلکه با عبور از کلید توسط آینه فارادی واقع در قسمت باب بازتاب شده و به BS اولی باز می‌گردد. در این شرایط که فوتون قرار است بازتاب شود، مسیر b به گونه‌ای طراحی شده است که طول آنها برای هر دوحالت قطبش $|H\rangle$ و $|V\rangle$ یکسان باشد. هرچند که ممکن است حالت‌ها مسیرهای متفاوتی را در قسمت باب طی کرده باشند اما بازه زمانی یکسانی را برای رسیدن دوباره به BS طی می‌کنند.

عملکرد دو آینه فارادی این است که فاز حالت قطبش را به اندازه $\frac{\pi}{۲}$ تغییر می‌دهد تا به صورت خودکار اثرات ناشی از دوشکستی[۱۹] را در مسیر اپتیکی جبران کند. همچنین فرض شده است که آشکارسازهای نشان داده شده در شکل ۴.۳ قادر به تشخیص قطبش فوتون‌هایی که آشکار می‌شوند، هستند. این نوع از آشکارسازها به راحتی با ترکیبی از یک شکافنده پرتو قطبشی و دو آشکارساز قابل تهیه هستند (شکل ۶.۳).

قبل از آنکه به بررسی نتایج ممکن برای عبور فوتون از چشمه تا رسیدن به یکی از آشکارسازها

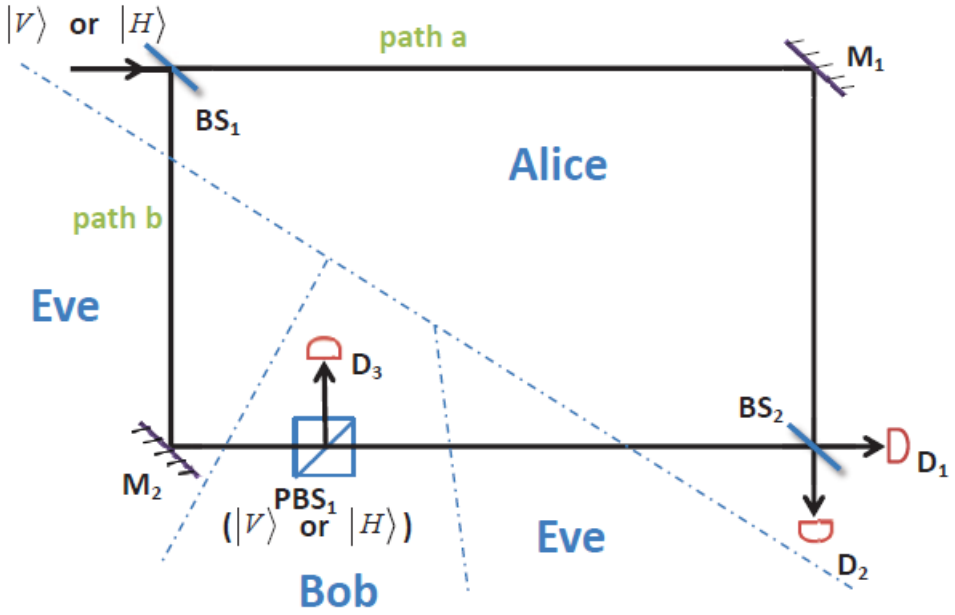
[۱۸] optical loop

[۱۹] birefringence



شکل ۶.۳: نحوه عملکرد آشکارساز قطبشی

بپردازیم، مسیر حرکتی فوتون را به صورت دیگری نیز تبیین می‌کنیم تا درک بهتری از آن بدست آید. یان بینگ لی[۲۰] و همکاران در مقاله [۳۶] تصویر ساده‌تری برای پروتکل $N۰۹$ ارائه کرده‌اند. شکل



شکل ۷.۳: نمایش دیگری از پروتکل $N۰۹$

۷.۳ نمایش الگوواری را از توزیع کلید کوانتومی خلاف‌واقعی نشان می‌دهد که بسیار شبیه به تداخل‌سنج ماخ-زندر و آزمایش الیتزور و وایدمن است. کل فضا توسط خطوط نقطه چین به سه زیرفضا تقسیم

[۲۰] Yan-Bing Li

می‌شود؛ مشابه آنچه توضیح داده شد آلیس از سمت خود یک فوتون را در یکی از دو حالت $|H\rangle$ یا $|V\rangle$ به سمت BS_1 می‌فرستد سپس فوتون به دو مسیر a و b وارد می‌شود. مسیرa مسیری است که همواره در محدوده امنیتی آلیس قرار دارد ولی مسیر b از یک فضای عمومی می‌گذرد و وارد زیرفضای باب می‌شود. باب به صورت تصادفی شکافنده پرتو قطبشی خود را روی یکی از دو حالت قطبش $|H\rangle$ یا $|V\rangle$ تنظیم می‌کند تا بدین ترتیب حالت قطبش فوتون در مسیر b را در صورت یکسان بودن با قطبش انتخابی خود مسدود کند. و اگر قطبش‌ها متفاوت بودند اجازه دهد تا فوتون مسیر را ادامه دهد تا به BS_2 برسد. از طرفی دیگر حالت فوتون در مسیر a نیز با هدایت آینه M_1 وارد BS_2 می‌شود و تداخل با حالت فوتون در مسیر b سبب ایجاد یک تداخل مخرب خواهد شد که توسط آشکارساز D_1 تشخیص داده می‌شود.

برای بررسی دقیق‌تر همه حالاتی که ممکن است اتفاق بیفتد، دوباره به مدل اصلی پروتکل یعنی شکل ۴.۳ برمی‌گردیم؛ به طور خلاصه تا اینجا فوتون پس از عبور از BS در دو مسیر a و b حضور خواهد داشت. در مسیر a مانعی بر سر راه خود ندارد و فوتون پس از یک بازتاب از آینه دوباره به سمت BS باز می‌گردد،ولی در مسیر b اگر قطبش انتخابی باب با آلیس یکسان باشد، فوتون به سمت آشکارساز D_3 هدایت می‌شود. یعنی سیستم کوانتومی به صورت زیر تغییر می‌کند:

$$\begin{aligned} |\varphi_s\rangle &= \sqrt{T}|0\rangle_a|\psi\rangle_b + i\sqrt{R}(\sqrt{T}|\psi\rangle_e|0\rangle_f + i\sqrt{R}|0\rangle_e|\psi\rangle_f) \\ &= \sqrt{T}|0\rangle_a|\psi\rangle_b + i\sqrt{RT}|\psi\rangle_e|0\rangle_f - R|0\rangle_e|\psi\rangle_f \end{aligned} \tag{۷.۳}$$

($\psi = \{H, V\}$) بنابراین سه سرنوشت برای فوتون می‌توان در نظر گرفت:

- فوتون از مسیر a می‌گذرد و با احتمال RT توسط آشکارساز D_1 آشکار می‌گردد.
- فوتون ازمسیر a می‌گذرد و با احتمالR^2 توسط آشکارساز D_2 آشکار می‌گردد.
- فوتون در مسیر b به سمت آشکارساز D_3 رفته و با احتمال T آشکار می‌شود.

اگر فوتون به سمت D_3 هدایت نشود یعنی قطبش انتخابی آلیس و باب یکی نبوده است و همان‌طور که توضیح داده شد، حالت فوتون در مسیر b پس از برخورد به آینه فارادی دوباره به BS برمی‌گردد. در این

صورت تغییرات سیستم به صورت زیر خواهد بود:

(۸.۳)

$$|\varphi_d\rangle = -\sqrt{T}(\sqrt{T}|۰\rangle_e|\psi\rangle_f + i\sqrt{R}|\psi\rangle_e|۰\rangle_f) + i\sqrt{R}(\sqrt{T}|\psi\rangle_e|۰\rangle_f + i\sqrt{R}|۰\rangle_e|\psi\rangle_f)$$
$$= -|۰\rangle_e|\psi\rangle_f$$

واضح است که در این شرایط تنها یک اتفاق برای فوتون میسر است و آن آشکار شدن توسط آشکارساز $D_۲$ است.

پس از کامل شدن فرآیند آشکارسازی فوتون‌ها،آلیس و باب یکدیگر را نسبت به فعالیت هر کدام از آشکارسازهایشان آگاه می‌کنند. اگر $D_۲$ یا $D_۳$ آشکارسازی را انجام داده باشند، آنها حالت قطبش اولیهٔ انتخابی خود و نیز آنچه که آشکار شده است را اعلام می‌کنند. اعلام این نتایج صرفاً برای رصد کردن حضور ایو در حین اجرای پروتکل است. اگر $D_۱$ آشکارسازی را انجام داده باشد، آلیس حالت قطبش آشکار شده را با حالت قطبش اولیه‌ای که انتخاب کرده بود، مقایسه می‌کند. اگر هر دوی آن‌ها با هم سازگار باشند او هیچ اطلاعاتی از قطبش فوتون را بروز نمی‌دهد، در غیر این صورت او نیز نتایج اندازه‌گیری خود را اعلام می‌کند.

به این ترتیب آلیس و باب می‌توانند با در نظر گرفتن رویدادهایی که برای آشکارساز $D_۱$ اتفاق می‌افتد (یعنی آن دسته از رویدادهایی که قطبش آشکار شده در $D_۱$با قطبش اولیه سازگار است) را به عنوان کلید خام درنظر بگیرند. غیر از آنچه عنوان شد، سایر رویدادهایی که ممکن است اتفاق بیفتند نادیده گرفته می‌شوند. همچنین رویدادهایی نظیر آشکارسازی همزمان چند آشکارساز و یا عدم آشکارسازی هیچ کدام از آشکارسازها نیز ممکن است بدلیل کامل نبودن دستگاه‌ها و یا حضور شنودکننده اتفاق بیفتند که آنها نیز برای افزایش امنیت پروتکل مورد بررسی قرار می‌گیرند.

بازده کلی ساخت یک بیت از کلید خام $\frac{RT}{۲}$ است. این مقدار دربیشترین حالت خود در صورت آنکه $R = T = ۰/۵$ باشد به حدود ۱۲/۵٪ می‌رسد[۳۷]. در این پروتکل آلیس تنها اعلام می‌کند که آشکارساز $D_۱$ آشکارسازی را درست انجام داده است یا خیر و اطلاعات دیگری را بروز نمی‌دهد. بنابراین برای ایو اطلاعات بیت آشکار نخواهد شد. مشابه با سایر پروتکل‌ها این بار نیز آلیس و باب می‌توانند با استفاده از بخش کوچکی از کلید خامِ بدست آمده اقدام به تعیین بازه خطا کنند و ایجاد اختلال ایو را از این طریق تخمین بزنند سپس بعد از طی کردن سایر مراحل کلاسیکی یک رشته بیت کوتاهتر به عنوان کلید امن نهایی بدست خواهد آمد.

با توجه به آنچه که توضیح داده شد نتیجه می‌گیریم یک بیت از کلید خام تنها زمانی شکل می‌گیرد که آشکارساز D_1 تک فوتونی را آشکار کند. بنابراین در شرایط ایده‌آل فوتون‌هایی که برای ساخت کلید استفاده می‌شوند مسیرb را طی نکرده‌اند بلکه فقط مسیر a را گذرانده‌اند. زیرا اگر از مسیر b گذر کرده بودند باید توسط D_3 آشکار می‌شدند. در نتیجه فرایند توزیع کلید کوانتومی، بدون آنکه فوتون‌های حامل اطلاعات از کانال کوانتومی(مسیر b) بگذرند صورت می‌گیرد و ایو هرگز به فوتون حامل اطلاعات دسترسی نخواهد داشت. در واقع وقتی مقادیر انتخابی بیت آلیس و باب یکسان باشند به دلیل اندازه‌گیری و یا عدم اندازه‌گیری باب، حالت اولیه $|\phi_0\rangle$ ($|\phi_1\rangle$) به یکی از دو حالت $|H\rangle_a|0\rangle_b$ ($|V\rangle_a|0\rangle_b$) یا $|0\rangle_a|H\rangle_b$ ($|0\rangle_a|V\rangle_b$) ریزش می‌کند.این در حالی است که حالت‌های مهم برای ساخت کلید دو حالت $|H\rangle_a|0\rangle_b$ و $|V\rangle_a|0\rangle_b$ در میان چهار حالت ریزش شده هستند.بنابراین باب کلید رمز را از رویدادهای آشکار نکرده‌اش بدست می‌آورد[۳۵]،[۳۶]،[۳۷].

۶.۳ بررسی امنیت پروتکل$N09$

امنیت پروتکل پیشنهادی Noh با استفاده از اصل عدم کپی برداری برای حالت‌های عمود برهم در یک سیستم مخلوط متشکل از دو زیرسیستم قابل بررسی است. همانطور که در فصل اول نیز توضیح داده شد، امکان ندارد که حالت‌های عمود برهم در صورت دسترسی به تنها یکی از زیر سیستم‌ها کپی شوند. یک نکته مهم در پروتکل حاضر این است که ایو تنها به یک زیرسیستم (مسیر b) دسترسی دارد در حالیکه او هرگز نمی‌تواند به زیر سیستم دیگر (مسیر a) دسترسی پیدا کند. به همین منظور Noh یک تعبیر جدید از اصل عدم کپی برداری را برای حالت‌های عمود برهم ارائه کرده است: اگر ماتریس‌های چگالی کاهشی یک زیرسیستم در دسترس نسبت به هم غیر عمود باشند و اجازه دسترسی به زیرسیستم دیگر وجود نداشته باشد، تشخیص دو حالت کوانتومی عمود برهم بدون تخریب آن‌ها غیرممکن است. فرض کنید $|\psi_0\rangle$ و $|\psi_1\rangle$ دو حالت خالصِ بهنجار شده از سیستم کوانتومی AB که مرکب از دو زیر سیستم A و B است، باشد. با توجه به بسط اشمیت خواهیم داشت:

$$|\psi_0\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$
$$|\psi_1\rangle = \sum_j \lambda_j |j_A\rangle |j_B\rangle \qquad (۹.۳)$$

λ_i و λ_j ضرایب اشمیت و $|i_A\rangle$ و $|j_A\rangle$ حالت‌های عمود برهم بهنجارشده برای زیرسیستم A هستند. به طور مشابه حالت‌های $|i_B\rangle$ و $|j_B\rangle$ برای زیرسیستم B هستند. همچنین فرض می‌شود که اپراتور یکانی[۲۱] U تنها روی دو فضای زیرسیستم B و دستگاه اندازه‌گیری ایو که به صورت یک حالت بهنجار شدهٔ اولیه $|m\rangle$ درنظر گرفته می‌شود، عمل می‌کند. برای پنهان نگه داشتن مداخله ایو، حالت‌های $|\psi_۰\rangle$ و $|\psi_۱\rangle$ باید بعد از تحول یکانی تخریب نشده[۲۲] باقی بماند؛

$$\begin{aligned} U(|\psi_۰\rangle\,|m\rangle) &= |\psi_۰\rangle\,|m_۰\rangle \\ U(|\psi_۱\rangle\,|m\rangle) &= |\psi_۱\rangle\,|m_۱\rangle \end{aligned} \tag{۱۰.۳}$$

در اینجا $|m_۰\rangle$ و $|m_۱\rangle$ حالت‌های نهایی دستگاه اندازه‌گیری ایو هستند. از آنجایی که U روی زیرسیستم A عمل نمی‌کند معادله ۱۰.۳ را می‌توان به صورت زیر نوشت:

$$\begin{aligned} U(|i_B\rangle\,|m\rangle) &= |i_B\rangle\,|m_۰\rangle \\ U(|j_B\rangle\,|m\rangle) &= |j_B\rangle\,|m_۱\rangle \end{aligned} \tag{۱۱.۳}$$

با ضرب داخلی مختلط معادله دوم روابط ۱۱.۳ در معادله اول آن و همچنین با توجه به خاصیت اپراتورهای یکانی ($UU^\dagger = ۱$) خواهیم داشت:

$$\langle i_B\,|j_B\rangle = \langle i_B\,|j_B\rangle\,\langle m_۰\,|m_۱\rangle \tag{۱۲.۳}$$

دو شرط را می‌توان برای برقراری رابطه ۱۲.۳ در نظر گرفت.

۱. $|m_۰\rangle = |m_۱\rangle$ باشد.

۲. یا $\langle i_B\,|j_B\rangle = ۰$ به ازای همه i و j ها برقرار باشد.

شرط دوم بیانگر آن است که ماتریس‌های چگالی کاهش یافته زیر سیستم B، ($\rho_s(B) = Tr_A[|\psi_s\rangle\,\langle\psi_s|]$) بر هم عمود هستند. یعنی باید رابطه $Tr[\rho_۰(B)\rho_۱(B)] = ۰$ برای دو حالت $|\psi_۰\rangle$ و $|\psi_۱\rangle$ برقرار باشد:

(۱۳.۳)

$$\rho_۰(B) = Tr_A(|\psi_۰\rangle\,\langle\psi_۰|) = Tr_A(\sum_i |\lambda_i|^۲\,|i_A\rangle\,\langle i_A| \otimes |i_B\rangle\,\langle i_B|) = \sum_i |\lambda_i|^۲\,|i_B\rangle\,\langle i_B|$$

$$\rho_۱(B) = Tr_A(|\psi_۱\rangle\,\langle\psi_۱|) = Tr_A(\sum_j |\lambda_j|^۲\,|j_A\rangle\,\langle j_A| \otimes |j_B\rangle\,\langle j_B|) = \sum_j |\lambda_j|^۲\,|j_B\rangle\,\langle j_B|$$

[۲۱] unitary

[۲۲] undisturbed

که با توجه به روابط بالا مشخص است که این رابطه برقرار است.

حال اگر طبق فرض، ماتریس‌های چگالی کاهش یافته زیر سیستم در دسترس B غیر عمود باشند ($Tr[\rho_0(B)\rho_1(B)] \neq 0$) آنگاه ایو بدون به ریختن حالت‌های $|\psi_0\rangle$ و $|\psi_1\rangle$ هیچ اطلاعاتی بدست نمی‌آورد حتی اگر حالت‌های $|\psi_0\rangle$ و $|\psi_1\rangle$ برهم عمود باشند.

این امر را می‌توان با توجه به معادلات ۶.۳ نشان داد. اگرچه حالت‌های $|\phi_0\rangle$ و $|\phi_1\rangle$ برهم عمود هستند اما ماتریس‌های چگالی کاهش یافته زیر سیستمِ در دسترس (مسیر b) در پروتکل $N09$ برهم غیر عمود هستند زیرا:

(۱۴.۳)

$$\begin{aligned}
\rho_0(path\ b) &= Tr_{(path\,a)}(|\varphi_0\rangle\langle\varphi_0|) \\
&= Tr_{(path\,a)}[(\sqrt{T}|0\rangle_a|H\rangle_b + i\sqrt{R}|H\rangle_a|0\rangle_b)(\sqrt{T}_a\langle 0|_b\langle H| - i\sqrt{R}_a\langle H|_b\langle 0|)] \\
&= Tr_{(path\,a)}[T(|0\rangle_{aa}\langle 0|\otimes|H\rangle_{bb}\langle H|) - i\sqrt{RT}(|0\rangle_{aa}\langle H|\otimes|H\rangle_{bb}\langle 0|) \\
&\qquad +i\sqrt{RT}(|H\rangle_{aa}\langle 0|\otimes|0\rangle_{bb}\langle H|) + R(|H\rangle_{aa}\langle H|\otimes|0\rangle_{bb}\langle 0|)] \\
&= T|H\rangle_{bb}\langle H| + R|0\rangle_{bb}\langle 0|
\end{aligned}$$

به همین ترتیب برای $\rho_1(pathb)$ داریم:

$$\rho_1(path\ b) = T|V\rangle_{bb}\langle V| + R|0\rangle_{bb}\langle 0|$$

بنابراین:

$$Tr[\rho_0(path\,b)\rho_1(path\,b)] = R^2 \neq 0 \qquad (۱۵.۳)$$

اگرچه برای $R = 0$، حالت‌های $|\phi_0\rangle$ و $|\phi_1\rangle$ می‌توانند بدون تخریب تشخیص داده شوند که در این صورت نیز با دریافت ما سازگار است.

در پروتکل‌های مرسوم توزیع کلید کوانتومی که برپایه انتقال ذرات حامل اطلاعات هستند، ایو می‌تواند به روش‌های مستقل یا جمعی دسترسی کامل به ذرات سیگنال عبوری از کانال کوانتومی داشته باشد. در پروتکل $N09$، ایو تنها می‌تواند به بخشی از سیستم کوانتومی یک ذره حامل اطلاعات دسترسی پیدا کند و نه تمام سیستم کوانتومی آن. این ویژگی مشابه با ویژگی پروتکل $ping-pong$ است. در پروتکل $ping-pong$ نیز شنودکننده تنها می‌توانست به یکی از دو فوتون آماده شده در حالت‌های بل

دسترسی پیدا کند. این ویژگی ممتاز طبیعتاً منجر به امنیت عملی پروتکل در شرایط گوناگون می‌شود. Noh در ضمیمه مقاله خود [۴۰] به بررسی امنیت پروتکل در مقابل حمله $I\&R$ ساده و مسئله تشخیص کانال کوانتومی پرداخته است.

۱.۶.۳ امنیت در مقابل حمله$I\&R$ ساده

همانطور که در فصل قبل توضیح داده شد، حمله $I\&R$ ساده در پروتکل‌های توزیع کلید کوانتومی مرسوم (که بر پایه انتقال ذره حامل اطلاعات هستند) به این صورت است که ایو همیشه می‌تواند ذره را نگه داشته، اندازه‌گیری مانند آنچه باب ممکن است انجام دهد را روی آن اعمال کند و سپس یک فوتون تقلبی سازگار با نتیجه اندازه‌گیری خودش به باب بفرستد.

پروتکل $N۰۹$ دارای این ویژگی است که ایو ممکن است بعضی از مواقع موفق به نگه داشتن فوتون نشود، زیرا در طی تلاشی که ایو ممکن است برای نگه داشتن ذره کوانتومی انجام دهد موجب شود که ذره تنها در مسیر a قرار بگیرد، یعنی مسیری که ایو به آن دسترسی ندارد. در این شرایط فرض می‌کنیم او دیگر فوتونی برای باب نمی‌فرستد یا می‌توان این گونه درنظر گرفت که حالت خلأ را برای باب می‌فرستد. همچنین فرض می‌کنیم ایو نیز مانند باب برای خود قطبشی را در نظر می‌گیرد بنابراین اگر پالس اپتیکی ورودی به دستگاه ایو دارای قطبش عمود بر قطبش انتخابی او باشد، بدون آنکه تخریبی در حالت به وجود آید از دستگاه ایو عبور می‌کند. همچنین اگر ایو موفق به آشکارسازی یک فوتون شود او باید یک فوتون تقلبی با قطبشی مشابه با قطبش آشکار شده، برای باب بفرستد تا به این طریق تغییر احتمالات آشکارسازیِ آشکارسازهای $D_۱$ ، $D_۲$ و $D_۳$ را به حداقل برساند.

با به کارگیری استراتژی حمله $I\&R$ ساده ایو ممکن است به نتایج زیر دست یابد.

نتیجه اول اگر قطبش‌های آلیس و باب با هم برابر باشند، احتمالات آشکارسازی $D_۱$،$D_۲$ و $D_۳$ مانند حالتی که ایو حضور ندارد بدون تغییر می‌ماند. این گزاره بدون توجه به انتخاب قطبش ایو همواره درست است. زیرا اگر قطبش ایو و آلیس مخالف هم باشند، فوتون از دستگاه ایو بدون تخریب می‌گذرد و ادامه پروتکل مشابه حالت بدون حضور او توسط آلیس و باب طی خواهد شد. همچنین اگر قطبش ایو و آلیس مشابه باشند این بار ایو جای باب را در پروتکل می‌گیرد یعنی یا می‌تواند فوتون را آشکار

کند که در این صورت فوتونی مشابه آنچه آلیس بدست آورده است را برای باب می‌فرستد و باب حتماً آن را آشکار خواهد کرد و یا ایو نمی‌تواند فوتون را آشکار کند که در این صورت حالت فوتون در مسیر a ریزش می‌کند و احتمال کشف آن توسط D_1 تغییری نمی‌کند. بنابراین در این شرایط آلیس و باب متوجه حضور ایو نمی‌شوند همچنین ایو نیز هیچ اطلاعاتی درباره مقدار بیت بدست نمی‌آورد حتی اگر فوتون توسط D_1 آشکار شود.

نتیجه دوم اگر قطبش آلیس و باب برهم عمود باشند.در این جا دو امکان وجود دارد:

۱. قطبش ایو عمود بر قطبش آلیس باشد.

۲. قطبش ایو مشابه با قطبش آلیس باشد.

در امکان ۱ تداخل باقی می‌ماند و فوتون بدون آنکه اختلالی برایش بوجود آید از دستگاه ایو می‌گذرد و وارد قسمت باب می‌شود. باتوجه به سازوکار اصلی پروتکل بدلیل مخالف بودن قطبش آلیس و باب، فوتون توسط آینه فارادی قسمت باب بازتاب می‌گردد و بدلیل باقی ماندن تداخل حالت‌های فوتون در دو مسیر a وb فوتون با قطعیت توسط آشکارساز D_2 آشکار می‌شود. آلیس و باب چنین نتایج حاصل از آشکارساز D_2 را طبق اصول پروتکل حذف می‌کنند. در نتیجه مداخله ایو اطلاعاتی را برای او در پی نخواهد داشت و آلیس و باب متوجه حضور او نخواهند شد. در امکان ۲ تداخل از بین می‌رود و احتمال آشکارسازی‌ها به صورت قابل توجهی در مقایسه با شرایطی که ایو وجود ندارد تغییر می‌کند. این تغییرات به شرح زیر می‌توانند باشند:

- ایو پس از تلاش برای اندازه‌گیری حالت فوتون، سبب فروریزش آن به مسیر a شود و آشکارساز D_1 فوتون را آشکار کند. در این شرایط آلیس و باب خطای بیتی را با احتمال RT تجربه خواهند کرد زیرا بنابر آن بوده است که در صورت عدم حضور ایو آشکارساز D_2 فوتون را آشکار کند ولی به جای آن مشابه رابطه ۷.۳ به احتمال RT باز هم D_1 فوتون را آشکار می‌کند. لازم به ذکر است که در این شرایط ایو هیچ اطلاعاتی را بدست نخواهد آورد.

- اگر فوتون پس از عبور از مسیر a توسط D_2 آشکار شود، آلیس و باب چنین وقایعی را حذف می‌کنند در نتیجه متوجه حضور او نخواهند شد و ایو هیچ اطلاعاتی بدست نمی‌آورد.

- اگر فوتون با احتمال T از مسیر b بگذرد توسط ایو آشکار می‌شود. به همین دلیل ایو متوجه می‌شود که قطبشی مشابه با قطبش آلیس انتخاب کرده است. سپس ایو یک فوتون تقلبی با همان حالت قطبش را به باب می‌فرستد. بدلیل مخالف بودن قطبش آلیس (و ایو) با باب، فوتون از دستگاه باب بازمی‌گردد. ایو دوباره فوتون را آشکار می‌کند(در این مرحله است که ایو متوجه عمود بودن قطبش باب نسبت به قطبش خودش می‌شود) سپس او باید یک فوتون را به سمت آلیس باز بفرستد. در غیر این صورت حضور او بدلیل از بین بردن یک فوتون آشکار می‌شود؛ در آخر اگر فوتون توسط $D_۱$ آشکار شود، آلیس و باب با یک خطای بیت روبه رو خواهند شد که با احتمال RT رخ می‌دهد. اگر فوتون در آشکارساز $D_۲$ آشکار شود، آلیس وباب این وقایع را حذف می‌کنند و در نتیجه متوجه مداخله ایو نمی‌شوند. بنابراین باز هم ایو هیچ اطلاعاتی بدست نخواهد آورد.

به طور کلی در این نوع از حمله $I\&R$ احتمال اینکه فوتون توسط $D_۱$ آشکار شود دو برابر می‌شود. این نتیجه به دلیل وقوع حالت‌هایی است که به خاطر حضور ایو سبب می‌شد $D_۱$ به احتمال RT آشکارسازی فوتون را انجام دهد در حالیکه قطبش آلیس و باب باهم مخالف بودند. بنابراین نیمی از این وقایع خطا هستند به این معنی که یک بازه خطای ۵۰ درصدی در کلید خامِ توزیع شده وجود دارد. بنابراین کلید خام کاملاً تحت تاثیر حمله قرار گرفته است. مضافاً اینکه ایو هیچ شانسی برای بدست آوردن اطلاعات از مقدار بیت ندارد به این معنی که اطلاعات ایو ٪۰ است.

به جهت آنکه ایو بخواهد اطلاعاتی بدست آورد، باید استراتژی حمله خود را به قیمت نا امن‌تر شدن حضورش اصلاح کند : بدین منظور او باید قبل از فرستادن فوتون برای باب حالت قطبش را به حالت عمود برآن تبدیل کند. با انجام این‌کار ضمن اینکه از قطبش انتخابی آلیس و باب باخبر می‌شود سبب می‌شود آلیس و باب نسبت به فهمیدن قطبش یکدیگر نیز گمراه شوند. در نتیجه این بار آلیس و باب با یک خطای ۲۵ درصدی مواجه می‌شوند درحالی‌که ایو نیز دارای ٪۲۵ اطلاعات از کلید خام خواهد بود. ولیکن این اصلاحیه سبب ایجاد افزایش خطای آشکارسازی در $D_۳$ می‌شود. به این ترتیب که فوتون تقلبی با حالت قطبش تغییر یافته ممکن است با وجود عمود بودن قطبش‌های آلیس و باب، در آشکارساز $D_۳$ آشکار شود. احتمال کلی اتفاق افتادن این خطا $\frac{T}{۴}$ است. بنابراین مداخله ایو در این نسخه اصلاح شدهٔ حمله $I\&R$ راحت‌تر آشکار می‌شود.

این نتایج را می‌توان با پروتکل $BB84$ مقایسه کرد. در پروتکل $BB84$ اگر ایو از یک استراتژی حمله $I\&R$ استفاده کند بازه خطایی که در یک کلید خام تولید می‌کند ۲۵٪ و مقدار اطلاعات دریافتی او ۵۰٪ است. بنابراین پروتکل $N09$ نسبت به حمله $I\&R$ قوی‌تر است. آلیس و باب به راحتی می‌توانند حضور ایو را تنها با بررسی بازه تولید کلید خام بدست آورند بدون آنکه نیازی به تلاش بیشتر برای محاسبه بازه خطا داشته باشند.

به طور ایده‌آل یک کلید خام تنها وقتی تولید می‌شود که یک فوتون حامل اطلاعات در محدوده امن آلیس باقی بماند یعنی فوتون مسیر a را طی کند و در آخر توسط D_1 آشکار شود. برخلاف سایر پروتکل‌های مرسوم ، ایو نمی‌تواند فرایند استفاده از حمله $I\&R$ را اصلاح کند(مانند حمله $I\&R$ کامل)زیرا او نمی‌تواند فوتون حامل اطلاعات را نگه دارد. تاثیر یک حمله $I\&R$ تنها در اضافه کردن یک خطای بیت ساختگی مشخص می‌شود. به همین دلیل است که بازه کلید خام تولیدی در اثر وجود حمله $I\&R$ دو برابر می‌شود[۴۰].

۲.۶.۳ تشخیص کانال کوانتومی

Noh در بررسی فواید امنیتی پروتکل ارائه شده‌اش مسئله تشخیص کانال کوانتومی[۲۳](QCI) را نیز مطرح می‌کند. تعریف او از این مسئله این است که در یک شبکه کوانتومی ممکن است کانالهای کوانتومی متعددی به وسیله فضا–زمان و یا در قالب طول موجشان از هم جدا شده و در دسترس باشند اما این گونه فرض می‌شود که آلیس و باب تنها یکی از آنها را برای توزیع کلید استفاده می‌کنند، بدون آنکه آن را به صورت عمومی افشا کنند. بنابراین سوال این است که آنگاه ایو چگونه می‌تواند بدون آنکه حضورش مشخص شود کانال کوانتومی درست را تشخیص دهد؟ درواقع مسئله تشخیص کانال کوانتومی دارای اهمیت کاربردی است زیرا یک پیش شرط لازم برای هر حملهٔ شنودکننده است. برای مثال وقتی ایو بخواهد از حمله اسب تروژان استفاده کند، در آن لازم است پالس‌های نور را از طریق یک کانال کوانتومی به قسمت باب و آلیس بفرستد و نور برگشتی را مورد بررسی قرار دهد تا تحلیلی از دستگاه‌های آلیس و باب داشته باشد. حال اگر ایو کانال کوانتومی صحیح را قبل از به کار بستن چنین حمله‌هایی تشخیص ندهد ممکن است به راحتی حضورش با احتمال بالایی آشکار شود. این کار به وسیله

[۲۳] quantum channel identification

آشکارسازهای کمکی که برای تحلیل نورهای ورودی به کانال‌های کوانتومی تله‌ای درنظر گرفته شده‌اند، اتفاق می‌افتد.

مسئله تشخیص کانال کوانتومی در پروتکل‌های توزیع کلید کوانتومی مرسوم که بر پایه انتقال ذره حامل اطلاعات هستند، به راحتی امکان پذیر است. می‌دانیم که حالتهای کوانتومی ذرات انتقالی بر حالت خلأ عمود هستند، بنابراین ایو می‌تواند کانال کوانتومی صحیح را بدون به همریختن حالت کوانتومی ذره تشخیص دهد. در مقابل در پروتکل $N۰۹$ اگر ایو تلاش کند تا کانال کوانتومی صحیح را به وسیله ردیابی ذره در حال انتقال تشخیص دهد ممکن است سبب ایجاد خطای بیت با احتمال غیر صفر شود. همچنین این پروتکل به خودی خود قابلیت مخفی کردن کانال کوانتومی را دارد. این ویژگی‌ها در ادامه توضیح داده می‌شوند:

۱. ابتدا شرایطی در نظر گرفته می‌شود که قطبش آلیس و باب یکسان هستند. دراین شرایط از آنجا که مسیر اپتیکی b توسط باب مسدود می‌شود ، تداخل از بین می‌رود. این امر از دید ایو غیر قابل تشخیص است.

فرض کنید که ایو با رصد کردن ذره در حال انتقال، تشخیص دهد ذره درکدام مسیر است. حتی اگر ایو حالت داخلی فوتون را از بین نبرد(برای مثال ایو تنها فوتون را نگه دارد بدون آنکه اندازه‌گیری کند) باز هم سبب از بین رفتن تداخل حالت‌های فوتون در دو مسیر a و b می‌شود. بنابراین آلیس و باب نمی‌توانند پی به حضور او ببرند. در نتیجه زمانی که فوتون در اولین مواجهه با شکافنده پرتو (BS) با احتمال T از آن عبور می‌کند ایو ممکن است در تشخیص کانال کوانتومی موفق باشد. اما وقتی فوتون در اولین مواجهه با شکافنده با احتمال R از آن بازتاب شود، ایو در تشخیص کانال کوانتومی موفق نخواهد بود. بنابراین او کانال صحیح را از کانال موهومی تشخیص نداده و چیزی جز حالت خلأ بدست نمی‌آورد.

۲. این بار شرایطی را در نظر بگیرید که قطبش‌های آلیس و باب بر یکدیگر عمود باشند.همانطور که پیشتر نیز توضیح داده شد اگر تداخل باقی بماند، فوتون همیشه در آشکارساز $D_۲$ آشکار می‌شود. از آنجایی که عمل ایو سبب به هم ریخته شدن تداخل می‌شود نتایج زیر ممکن خواهند بود:

(آ) فوتون در اولین مواجهه با BS بازتاب شده و در ایستگاه آلیس باقی می ماند. در این شرایط ایو تنها حالت خلأ را بدست می‌آورد و در تشخیص کانال کوانتومی ناموفق خواهد

بود. زمانی که فوتون در مواجهه دوم با BS نیز بازتاب شود و توسط D_2 با احتمال R^2 آشکار شود، آلیس و باب پی به حضور ایو نمی‌برند اما وقتی فوتون در مواجهه دوم با BS از آن عبور کند و D_1 آشکارسازی را انجام دهد، یک خطای بیت رخ خواهد داد و آلیس و باب در اصل می‌توانند حضور ایو را با چک کردن خطای بیت آشکار کنند.

(ب) اگر فوتون در مواجهه اول با BS از آن بگذردو به سمت ایستگاه باب برود؛ در این شرایط ایو با رصد کردن ذره انتقالی در تشخیص کانال کوانتومی موفق خواهد بود. با توجه به اینکه ایو حالت داخلی فوتون را از بین نبرده است. فوتون ممکن است به ایستگاه آلیس بازگردد. بنابراین اگر فوتون در مواجهه دوم با BS باز هم از آن عبور کند و آشکارساز D_2 با احتمال T^2 آن را آشکار کند، حضور ایو مشخص نمی‌شود. اما وقتی فوتون در دومین مواجهه با BS از آن بازتاب شود، D_1 با احتمال TR آن را آشکار می‌کند و یک خطای بیت رخ می‌دهد. در نتیجه عمل ایو در اصل قابل ردیابی است.

از مطالبی که در بالا آورده شد می‌توان اینطور برداشت کرد که ایو با چهار امکان در یک تلاش خود برای تشخیص کانال کوانتومی مواجه خواهد شد:

۱. ایو در تشخیص کانال کوانتومی موفق است و حضور او مشخص نمی‌شود. این امکان با احتمال $p_1 = \frac{T}{2} + \frac{T^2}{2}$ رخ می‌دهد.

۲. ایو در تشخیص کانال کوانتومی موفق می‌شود ولی خطای بیت ایجاد می‌کند. این امکان با احتمال $p_2 = \frac{RT}{2}$ رخ می‌دهد.

۳. ایو در تشخیص کانال کوانتومی موفق نیست و حضورش مشخص نمی‌شود. این امکان با احتمال $p_3 = \frac{R^2}{2} + \frac{R}{2}$ رخ می‌دهد.

۴. ایو در تشخیص کانال کوانتومی موفق نیست و حضورش خطای بیت ایجاد می‌کند. این امکان با احتمال $p_4 = \frac{RT}{2}$ رخ می‌دهد.

طبیعتاً احتمال p_1 را می‌توان به عنوان بازدهی[۲۴] تشخیص کانال کوانتومی در نظر گرفت. برای آنکه ایو به بهترین نتیجه‌گیری ممکن یعنی p_1 برسد باید ضریب انتقال BS به سمت ۱ میل کند($T \to 1$). تنها

[۲۴] efficiency

در چنین شرایط حدی ایو می‌تواند به صورت کاملاً امن، کانال کوانتومی صحیح را مانند سایر پروتکل‌های مرسوم با قطعیت تشخیص دهد. عموماً برای $(T < ۱)$، $p_۱$ کمتر از ۱ خواهد بود. در حقیقت بازدهی تشخیص کانال کوانتومی می‌تواند تا حد $p_۱ = ۰$ کاهش یابدبااین شرط که ضریب انتقال دهندگی BS به سمت صفر میل کند$(T \to ۰)$. در شرایطی که احتمال تولید کلید کوانتومی بیشینه باشد $(R = T = \frac{۱}{۲})$، بازدهی برابر با $p_۱ = \frac{۳}{۸}$ خواهد بود.

اگر به صورت دقیق‌تر به امکان ۴ توجه کنیم. با پدیدهٔ جالبی مواجه می‌شویم که در آن ایو در تشخیص کانال کوانتومی ناموفق است زیرا او چیزی جز خلأ مشاهده نکرده است اما حالت کوانتومی داخلی فوتون را به هم‌ریخته است ولی با این وجود باز هم آلیس و باب می‌توانند به احتمال غیر صفر به حضور او پی ببرند. این پدیده را می‌توان **تشخیص خلاف واقع**[۲۵] یک شنودکننده نامید. تنها امکانی که در آن ایو می‌تواند به تشخیص کانال کوانتومی موفق شود، برای تشخیص حضور او کافی است. اما حتی اگر ایو موفق به این عمل هم نشود باز هم ممکن است حضورش آشکار شود. همین پدیده در حمله $I\&R$ که توضیح داده شد نیز کاربرد دارد.[۴۰]

۳.۶.۳ امنیت در مقابل سایر حمله ها

در عمل برای اجرای پروتکل‌های توزیع کلید کوانتومی بدلیل نبود چشمه ایده‌آلی که ساطع کننده تک فوتون باشد از پالس‌های ضعیف همدوس[۲۶] استفاده می‌شود که در آن احتمال حضور پالسی با بیش از یک فوتون وجود دارد. پروتکل $N۰۹$ در مقابل چنین حمله‌هایی که ممکن است ناشی از استفاده این گونه پالس‌ها باشد مزایای امنیتی شفافی دارد: اولاً ایو نمی‌تواند تعداد فوتون‌های موجود در هر پالس را تشخیص دهد زیرا او به مسیر a دسترسی ندارد. گذشته از آن، شمارش تعداد فوتون‌های عبوری از مسیر کوانتومی (مسیرb) با وجود اینکه حالت‌های آنها را به هم نمی ریزد برای ایو غیر ممکن است. ایو اطلاعات راجع به اینکه ذره در کدام مسیر بوده است را از طریق اندازه‌گیری تعداد فوتون در مسیرb بدست می‌آورد و سبب نابودی تداخل می‌شود. بنابراین ایو باعث ایجاد خطای در آشکارسازی می‌شود و تنها با اندازه‌گیری تعداد فوتون‌ها موجب آشکار شدن حضورش در بین راه می‌شود. درنتیجه پروتکل $N۰۹$ ذاتاً در مقابل حمله PNS (شکافت تعداد فوتون‌ها) مقاوم است.

[۲۵] counterfactual detection

[۲۶] weak coherence pulses

ثانیاً در حالیکه همه فوتون‌ها در طول مسیر a عبور می‌کنند،ایو نمی‌تواند یک فوتون را جدا کند . به این صورت است که اگر همه فوتون‌ها پس از عبور از از مسیر a در D_1 آشکار شوند، حتی اگر در زمانی که یک پالس حاوی چند فوتون به کار برود، اطلاعات بیت برای ایو فاش نمی‌شود.

نهایتاً ایو نمی‌تواند یک کپی از حالت کوانتومی اولیه بدست آورد حتی اگر در جدا کردن یک فوتون موفق شده باشد. بلکه ایو در هر بار متوجه داشتن یک فوتون نزد خودش بشود چیزی جز یک حالت ریزش شده بدست نیاورده است زیرا او همچنان توسط اصل $no-cloning$ محدود شده است.[۳۵]

فصل ۴

نتیجه‌گیری

در این پایان نامه ابتدا پیشینه‌ی مختصری از رمزنگاری کلاسیکی و انواع اصلی آن مطرح شد. با توجه به نقایص موجود در رمزنگاری کلاسیکی و همچنین افزایش سریع احتمال استفاده از کامپیوترهای کوانتومی، این نوع از رمزنگاری کلاسیکی دیگر قادر به تأمین امنیت ارتباطاتی در دنیای امروز و آینده نیست. درنتیجه باید توجهات ویژه‌ای به نمونه جایگزین آن یعنی رمزنگاری کوانتومی شود. برای ورود به زمینه رمزنگاری کوانتومی لازم دیده شد تا ضمن ارائه‌ی مقدمه‌ای کوتاه درباره‌ی نظریه اطلاعات کوانتومی و بیان تفاوت‌های آن با نمونه کلاسیکی به بررسی چند مورد از پروتکل‌های مهم رمزنگاری کوانتومی یا به عبارت دیگر پروتکل‌های توزیع کلید کوانتومی بپردازیم. در فصل دو سعی بر آن شده است که انواع متفاوتی از پروتکل‌ها توضیح داده شود. برای مثال پروتکل یک طرفه برمبنای انتقال کیوبیت‌های مستقل مانند $BB۸۴$ ، پروتکل یک طرفه برمبنای درهمتنیدگی کوانتومی مانند $E۹۱$، و همچنین پروتکل دوطرفه برمبنای درهمتنیدگی کوانتومی مانند $Ping-pong$. همپنین در خلال بررسی این پروتکل‌ها استراتژی‌های حمله‌ی مختلف از سوی شنودکننده مورد بحث و بررسی قرار داده شده است.

پروتکل‌های توصیف شده و همچنین بسیاری از پروتکل‌های دیگر اصولاً برپایه انتقال ذرات کوانتومی به عنوان سیگنال برای برقراری ارتباط و توزیع کلید هستند. اما در فصل سوم پروتکلی توصیف شد که در آن با استفاده از مفهوم **اندازه‌گیری بدون برهم‌کنش** توانسته است بدون انتقال ذره حامل اطلاعات، کلید رمز تصادفی را تولید کند. مفهوم اندازه‌گیری بدون برهم‌کنش از این حقیقت ناشی می‌شود که حضور یک جسمِ مانع به عنوان ابزار اندازه‌گیری در یک تداخل‌سنج سبب می‌شود تداخل موجود به هم بریزد حتی اگر آن جسم موفق به اندازه‌گیری نشود. با استفاده از همین ایده نُه (Noh) در پروتکل پیشنهادی خود ($N۰۹$) آن دسته از رویدادها را به عنوان کلید انتخاب می‌کند که طی آن باب به دلیل عدم موفقیتش در اندازه‌گیری ذره سبب می‌شود که تداخل از بین برود و ذره حامل اطلاعات تنها در مسیر در دسترس آلیس باقی بماند. بنابراین ذره‌ای بین آنها تبادل نمی‌شود تا ایو بتواند با رصد آن به اطلاعات پی ببرد.

برای بررسی امنیت پروتکل $N۰۹$، Noh تعبیر جدیدی از اصل عدم کپی برداری را ارائه و از طریق آن امنیت پروتکل را اثبات کرده است. همچنین امنیت پروتکل در مقابل استراتژی‌های حمله دیگر نظیر $I\&R$ ساده، PNS و همچنین تشخیص کانال کوانتومی از طرف ایو به صورت مبسوط مورد بررسی قرار گرفته است. این بررسی‌ها نشان می‌دهد که پروتکل $N۰۹$ دارای امنیت بسیار بالایی در مقایسه با سایر پروتکل‌ها است ولیکن بازده تولید کلید آن نسبتاً مقدار کمی است (حدود ٪۱۲٫۵).به هر حال $N۰۹$ سبب پیشگامی نسل جدیدی از پروتکل‌های توزیع کلید کوانتومی شد که امروزه نمونه‌های زیادی

برمبنای آن شکل گرفته‌اند.

در ادامه به عنوان پیشنهاد می‌توان به بررسی پروتکل‌های مشابه $N۰۹$ پرداخت که در آن‌ها ضمن ارتقا بخشیدن به مسئله امنیتی آن در مقابل حمله‌های ناشی از ناکارآمدی دستگاه‌ها، به مسئله بهبود بازده تولید کلید آن نیز پرداخته شده است.

مراجع

[1] S. M. Barnett, (2009), *"Quantum Information"*, Oxford university press.

[2] G.Benenti,G.Casati,G.Strini, (2007), *"principle of quantum computation and information"*, Volume I , world scientific.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden,(2002),*"Quantum cryptography"*, Rev. Mod. Phys. 74 145.

[4] R. Rivest, A. Shamir, and L. Adleman, (1978), *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, 21(2):120.

[5] Xiongfeng Ma, (2008), *Quantum cryptography: from theory to practice*,Doctor of Philosophy Thesis, University of Toronto.

[6] Michael A. Nielsen Isaac L. Chuang, (2010), *Quantum Computation and Quantum Information*,10th Anniversary edition published ,Cambridge University Press.

[7] C. H. Bennett and G. Brassard, (1984), *"Quantum cryptography : Public key distribution and coin tossing"* , In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179 .

[8] Kollmitzer C., Pivk M. (Eds.), (2010), *"Applied Quantum Cryptography"*, Lect. Notes Phys. 797 (Springer, Berlin Heidelberg), DOI 10.1007/978-3-642-04831-9

[9] M.Pivk,(2010), *"Quantum Key Distribution"*, Lect. Notes Phys. 797, 23–47 DOI 10.1007/978-3-642-04831-9 3

[10] S.Schauer, (2010), *"Attack Strategies on QKD Protocols"*, Lect. Notes Phys. 797, 71–95 DOI 10.1007/978-3-642-04831-9 5

[11] McMahon.D, (2008), *Quantum computing explained*, by John Wiley Sons, Inc.

[12] Wootters,W.K., Zurek,W.H, (1982), *A single quantum cannot be cloned*. Nature 299(5886), 802–803 . DOI 10.1038/299802a0

[13] Ekert, A.K., N. D. Mermain, (1991), *"Quantum cryptography based on Bell's theorem"*,Phys. Rev. Lett. 67, 661-663.

[14] Bennett, Ch.H., (1992), *"Quantum cryptography using any two nonorthogonal states"*,Phys. Rev. Lett. 68, 3121-3124.

[15] Bennett, Ch.H., G. Brassard and Mermin N.D.,(1992), *"Quantum cryptography without Bell's theorem"*,Phys. Rev. Lett. 68, 557-559.

[16] Piotr Zawadzki ,(2015), *An improved control mode for the ping-pong protocol operation in imperfect quantum channels*,Quantum Inf Process 14:2589–2598,DOI 10.1007/s11128-015-0989-x

[17] A.Cabello, (2000), *"Quantum key distribution without alternative measurements"*, Phys. Rev. A 61(5), 052,312.

[18] A. Beige, B.-G. Englert, C. Kurtsiefer, H.Weinfurter., (2002), *Secure communication with a publicly known key* Acta Phys. Pol. A 101, 357

[19] K. Bostrom, T. Felbinger,(2002),*Deterministic Secure Direct Communication Using Entanglement* Phys. Rev. Lett. 89 187902.

[20] Masakazu Yoshida, Takayuki Miyadera, Hideki Imai. , (2013), *On the Security of Quantum Key Distribution Ping-Pong Protocol*,Journal of Quantum Information Science 3, 16-19

[21] Q.y Cai , B.w Li,(2004) ,*Improving the capacity of the Boström-Felbinger protocol* Phys. Rev. A 69, 054301

[22] A. Wójcik, (2003),*Eavesdropping on the ''Ping-Pong'' Quantum Communication Protocol*,Phys. Rev. Lett. 90, 157901

[23] Qing-yu Cai, (2003),*Eavesdropping on the two-way quantum communication protocols with invisible photons*, Phys. Rev. Lett. 91, 109801.

[24] Ba An Nguyen, (2004), *Quantum dialogue*, Physics Letters A 328 6–10

[25] Xiaojun Wen , Yun Liu , Nanrun Zhou, (2007), *Secure quantum telephone*,Optics Communications 275, 278–282

[26] L¨utkenhaus, N., Jahma, M., (2002), *Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack*, New J. Phys. 4, 44.1–44.9

[27] G.Jaeger, (2006), *"Quantum Information;An Overview"*, Springer.

[28] J. Bell,(1964), Physics 1, 195

[29] A. Aspect, J. Dalibard, and G. Roger,(1982), Phys. Rev. Lett. 49, 1804

[30] Y. Aharonov and D. Bohm,(1959), Phys. Rev. 115, 1804

[31] M. Renninger,(1960), Z. Phys. 158, 417

[32] A. Cardoso, J. L. Cordovil and J. R. Croca,(2015),*Interaction-Free Measurements: A Complex Nonlinear Explanation*,Journal of Advanced Physics, Vol. 4, pp. 1-5

[33] A. C. Elitzur, L. Vaidman,(1993),*Quantum mechanical interaction-free measurements*, Found. Phys. 23, 987-997

[34] L.Vaidman,(2001),*The Meaning of the Interaction-Free Measurements*,arXiv:quant-ph/0103081v1

[35] T.-G. Noh,(2009), *Counterfactual Quantum Cryptography*, Phys. Rev. Lett. 103, 230501

[36] Yan-Bing Li, Qiao-yan Wen, Zi-Chen Li,(2014)*Security flaw of counterfactual quantum cryptography in practical setting*,arXiv:1312.1436v5 .

[37] Ying Sun and Qiao-Yan Wen,(2010),*Counterfactual quantum key distribution with high efficiency*,PhysRevA.82.052318

[38] H. Salih, Z.H. Li, M. Al-Amri, and M.S. Zubairy,(2013), *Protocol for Direct Counterfactual Quantum Communication*, Phys.Rev. Lett. 110, 170502

[39] Akshata Shenoy H., R. Srikanth, T. SrinivaAkshata Shenoy H., R. Srikanth,T. Sriniva, (2011), *Counterfactual quantum certicate authorization*,arXiv:1402.2250v2

[40] T.-G. Noh, arXiv:0809.3979v2

Abstract

Quantum cryptography has attracted widespread attention as it is ultimately secure by using physics's laws and does not require computational and mathematical complexity unlike its classical counterparts. Quantum key distribution (QKD) is one of the most important applications of quantum cryptography.

In QKD, two distant people (like Alice & Bob) can share a secret key with each other to use it further as a key of a classical cyphertext. From the first QKD protocol (BB84) to recent protocols which presented in last few years, all of them were based on transmitting signal particles through a quantum channel.

In 2009 Tae Gon Noh presented a novel QKD protocol by using the idea of "Interaction free measurement" (N09). In fact his protocol is entirely different from all previous QKD protocols, because the sifted key in N09 is just created by selecting the events which the photons have not actually traveled through the quantum channel. Thus the eavesdropper could not access those photons. Due to this advantage, N09 is very attractive from the security aspect. However the efficiency of the N09 is not satisfying.

In this thesis, first the history of classical cryptography is mentioned. Then, after an introduction about Quantum information theory, the processes of QKD protocols is indicated. we have also mentioned three important QKD protocols and study their security. At the end we have investigated verify N09 protocol and its security in details.

Keywords: cryptography, quantum key distribution, Intercept and resend attack, security, interaction free measurement.

University of Shahrood

Faculty Of Physics Sciences

Studying the approach and security of quantum key distribution in N09 protocol

Masomeh Golara

Supervisor

Dr. M. Annabestani

Feb 2016