نشریه علمی «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال اول، شماره ۱، بهار ۱۴۰۰؛ ص ۶۵-۵۷

علمی – تخصصی

بررسی برخی کاربردها، شبیه‌سازی و تحلیل امنیتی پروتکل رمزنگاری کوانتومی BB۸۴

حامد شجاعی یاس[1*]، علی هادی پور[2]

۱ و۲- کارشناسی ارشد دانشگاه صنعتی مالک اشتر

(دریافت: ۹۹/۰۷/۰۷، پذیرش: ۱۴۰۰/۰۴/۰۹)

چکیده

رمزنگاری کوانتومی و یا توزیع کلید کوانتومی (QKD[1]) روشی است که اجازه می‌دهد با محافظت از توزیع یک رشته بیت، از آن به‌عنوان کلید در پروتکل‌های رمزنگاری استفاده شود. وقتی مشاهده شد که رایانه‌های کوانتومی می‌توانند رمزنگاری کلید عمومی را براساس نظریه اعداد بشکنند، مطالعات گسترده‌ای در زمینه QKD آغاز شد. استفاده از رمزنگاری کوانتومی، یک امنیت تضمینی و محرمانگی کاملی ارائه می‌دهد و با حملات عمده‌ای به‌منظور رمزگشایی، شکست ناپذیری خود را اثبات کرده است. اگرچه به‌صورت ریاضی امنیت پروتکل‌های رمزنگاری کوانتومی به اثبات رسیده است، اما این نکته باید مورد تاکید قرار بگیرد که پیاده سازی آن در دنیای واقعی از محدودیت دستگاه‌های فیزیکی رنج می‌برد که این موضوع خود می‌تواند باعث آسیب پذیری برای سوء استفاده قرار گرفتن توسط یک استراق سمع‌کننده شود. نتیجه این تحقیقات ارائه اولین پروتکل توزیع کلید کوانتومی به نام پروتکل BB۸٤ بود. حال بر این اساس، هدف این مقاله، بررسی برخی کاربردها، توضیح و بررسی ساختار پروتکل، پیاده‌سازی و تجزیه و تحلیل امنیتی پروتکل رمزنگاری کوانتومی BB۸٤ است.

کلید واژه‌ها: رمزنگاری کوانتومی، پروتکل توزیع کلید کوانتومی، QKD، BB۸۴.

۱- مقدمه

در سند نقشه جامع علمی کشور [۱] که در بردارنده دورنما و اولویت‌های راهبردی توسعه علم در کشور می‌باشد، علم رمزنگاری و کدگذاری در بین اولویت‌های سطح الف (بالاترین اهمیت) قرار دارد. از طرف دیگر علم محاسبات و پردازش اطلاعات کوانتومی در سطح (ب) قرار گرفته است. این اولویت‌گذاری نشان‌دهنده جایگاه این مهم در توسعه و پیشبرد علمی کشور می‌باشد. با توجه به اهمیت موضوع بر آن شدیم تا در این مقاله به معرفی مباحث پیشرفته رمزنگاری کوانتومی و به‌صورت تخصصی‌تر الگوریتم توزیع کلید کوانتومی BB۸٤ بپردازیم.

رمزنگاری، دانشی است که به بررسی و شناخت اصول و روش‌های انتقال یا ذخیره اطلاعات به‌صورت امن (حتی اگر مسیر انتقال اطلاعات و کانال‌های ارتباطی یا محل ذخیره اطلاعات ناامن باشند) می‌پردازد.

رمزنگاری، استفاده از روش‌های ریاضی، برای برقراری امنیت اطلاعات است. در اصل، رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است. به‌صورتی که تنها شخصی که از کلید و الگوریتم آگاه است می‌تواند اطلاعات اصلی از اطلاعات رمزگذاری، استخراج کند و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد نمی‌تواند به اطلاعات دسترسی پیدا کند [۲]. در رمزنگاری کلاسیک، یک کلید برای رمزگذاری و رمزگشایی اطلاعات به‌کار می‌رود. یک استراق سمع‌کننده زمانی قادر به رمزگشایی داده‌های رمز شده خواهد بود که کلید متناظر را بداند. بدین‌گونه مسئله اصلی در رمزنگاری، بنا نهادن یک کلید قوی بین دو طرف مجاز می‌باشد که به‌عنوان مسئله توزیع کلید مطرح می‌شود. هدف از توزیع کلید کوانتومی محرمانه، برقراری ارتباط ایمن بین آلیس و باب در حضور یک استراق سمع‌کننده می‌باشد. ایمنی توزیع کلید کوانتومی توسط اصول نظریه کوانتومی تضمین می‌شود. در سال ۱۹۸۴ بنت و براساد پروتکل رمزنگاری کوانتومی چهارحالته را پیشنهاد کردند [۳]. اولین اثبات امن بودن بی‌قید و شرط این پروتکل که بسیار پیچیده بود، توسط مایرز در سال ۲۰۱۰ ارائه شد [۴]. در سال ۱۹۹۹ توسط چاو و لو اثبات ساده‌ای ارائه شد اما متاسفانه برای اجرا نیاز به کامپیوتر کوانتومی داشت [۵]، تا اینکه بعداً شور[2] و پرسکیل[3] [۶] اثبات ساده‌ای از ایمنی پروتکل چهار حالته با ترکیب و تعمیم دیدگاه‌های مایرز و لو و چاو پیشنهاد کردند. آن‌ها امنیت پروتکل توزیع کلید کوانتومی چهارحالته مبتنی بر خالص‌سازی درهم تنیدگی را اثبات کردند. در اثبات آن‌ها نشان داده شده است که آلیس باید کیوبیت‌ها را

* رایانامه نویسنده مسئول: Hamed.shojaeeyas@gmail.com

[1] Quantum Key Distribution

[2] Shor

[3] Preskill

به‌وسیله یک جایگشت تصادفی قبل از ارسال به باب در هم ادغام کند (یعنی آلیس به‌جای آنکه یک جفت EPR[1] تهیه کند برای باب ارسال کند، یک حالت کوانتومی رمزگذاری شده همراه با کد تصحیح خطای کوانتومی برای باب ارسال کند) که این ادغام باعث افزایش نرخ خطای قابل تحمل پروتکل چهار حالته از حدود ۷ درصد (که توسط مایرز به‌دست آمده) به حدود ۱۱درصد می‌شود. همچنین شور و پرسکیل نشان دادند که در پروتکل چهارحالته، خطاهای وارونه سازی بیت و وارونه سازی فاز مجزا هستند، یعنی علائم خطای وارونه سازی بیت، اطلاعاتی به دو کاربر در مورد خطای فاز نمی‌دهد. همچنین شور و پرسکیل ایده مشاهده‌پذیرهای کامیوت‌کننده مربوط به‌ویژه حالت‌های همزمان پایه‌های بل با N بزرگ (N تعداد جفت کیوبیت‌ها است)، که به وسیله نمونه‌گیری تصادفی به‌کار بردند و تنها ورودی‌های قطری ماتریس چگالی که به میانگین ماتریس چگالی وابسته بود را در نظر گرفتند. ماتریس چگالی Diag (ماتریس قطری) عبارت است از:

$$\mathrm{Diag}(a, b, c, d) \quad (۱)$$

شور و پرسکیل پایه‌های بل را که پایه‌های متعامد برای حالات کوانتومی دو کیوبیتی می‌باشند، به شکل زیر در نظر گرفتند:

$$\Phi^{\pm} = \frac{1}{\sqrt{2}}(|01> + |10>)$$
$$\Phi^{\pm} = \frac{1}{\sqrt{2}}(|00> + |11>) \quad (۲)$$

که چهار ورودی ماتریس چگالی (عناصر قطر اصلی) به‌صورت زیر تفسیر می‌شوند:

(a) یکی از پایه‌های بل، بدون خطاست، (b) اگر بیت پایه بل وارونه شود، بدون آن‌که فاز آن وارونه شود، (c) اگر فاز پایهٔ بل وارونه شود، بدون آن‌که بیت آن وارونه شود، (d) اگر فاز و بیت پایهٔ بل هر دو وارونه شوند.

تبدیل هادامارد (H) که به‌صورت رابطه (۳) است، روی این ماتریس چگالی اعمال می‌شود و ماتریس را به شکل رابطه (۴) در می‌آورد.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (۳)$$

$$H = \mathrm{Diag}(a, b, c, d) \quad (۴)$$

با فرض

$$e = \big((b + c)\big)/2 \quad (۵)$$

متوسط این ماتریس چگالی برابر است با:

$$\mathrm{Diag}(a, b, c, d) = \mathrm{Diag}\big(a, ((b + c)), ((b + c))/2, d\big)$$

در نمونه‌گیری تصادفی پروتکل چهار حالته، نرخ خطای بیت برابر e+d است که در اثبات شور و پرسکیل، d مهم نیست و در نظر گرفته نشده است. به این معنی که آلیس و باب نمی‌توانند هیچ شناختی از ارتباط بین خطاهای وارونه سازی فاز و وارونه سازی بیت داشته باشند [۷].

بخش‌های بعدی نوشتار به این ترتیب که در بخش (۲)، به توضیح و بررسی پروتکل رمزنگاری کوانتومی BB۸٤ پرداخته می‌شود. در بخش (۳)، کاربردها و موارد استفاده از این پروتکل و نیز پیاده سازی آن بیان خواهد شد. در بخش (۴)، تجزیه و تحلیل امنیت پروتکل BB۸٤ بررسی و انواع حملات علیه آن مورد توجه قرار خواهد گرفت. بخش (۵)، نتیجه‌گیری کلی از مقاله تشریح می‌گردد.

۲- توضیح و بررسی پروتکل رمزنگاری کوانتومی BB۸٤

در این پروتکل حالت‌های کوانتومی توسط "آلیس" تهیه شده و متناظر با هر کدام از حالت‌های موجود پایه اندازه‌گیری در نظر گرفته می‌شود. در کنار این برای هر حالت هم یک بیت متناظر در نظر گرفته می‌شود. در این پروتکل ارسال‌کننده و دریافت کننده اطلاعات از دو کانال ارتباطی استفاده می‌کنند.

۱- یک کانال ارتباطی کوانتومی یک طرفه که اطلاعات از طریق آن ارسال می‌شود [۳].

۲- یک کانال ارتباطی کلاسیک دو طرفه که مقایسه پایه‌های اندازه‌گیری و استخراج کلید رمز اطلاعات از طریق آن انجام می‌شود [۳].

مراحل پروتکل به شرح زیر می‌باشد:

بیت	0	1	0	1	1
پایه	+	×	×	+	×
فوتون	↔	⤡	⤢	↕	⤡

شکل (۱): بیت‌های ارسالی توسط آلیس [۴]

۱- در مرحله اول "آلیس" فوتون‌های درهم‌تنیده منفرد را تحت زوایای ۰، π/۴، ۲π/۴، ۳π/۴ به‌صورت تصادفی به ترتیب در چهار حالت کوانتومی $|0>, |\bar{0}>, |1>, |\bar{1}>$ فراهم می‌کند.

[1] Einstein-Podolsky-Rosen

۲- "باب" پس از اینکه حالت‌های ارسالی توسط "آلیس" را دریافت کرد با پایه‌های کاملاً تصادفی متناظر با محورهای xz اقدام به اندازه‌گیری این حالت‌ها می‌کند. البته نتیجه اندازه‌گیری او روی هر کدام از چهار حالت همواره $< 0|$ یا $< 1|$ است [۴].

فوتون	↔	↘	↗	↕	↘
پایه تصادفی	+	+	×	+	×
بیت حاصل	0	0	0	1	1

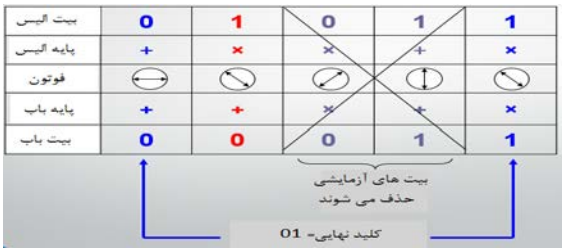
شکل (۲): بیت های دریافتی توسط باب [۴]

۳- سپس باب برای اینکه از حضور و یا عدم حضور "عامل سوم، استراق سمع" مطمئن شود، از طریق یک کانال کلاسیکی با آلیس ارتباط (مثلاً تلفنی) برقرار می‌کند. زیرا از این طریق میزان خطای باب در دریافت اطلاعات صحیح، سنجیده می‌شود و با استفاده از بحث فوق، حضور "عامل نفوذی" آشکار می‌گردد. در این ارتباط تلفنی در ابتدا "باب" به "آلیس" اعلام می‌کند که در اندازه‌گیری هر حالت کوانتومی از کدام پایه اختیاری استفاده کرده است، در این صورت "آلیس" درست و یا غلط بودن پایه انتخابی را به "باب" اعلام می‌کند [۴].

بیت آلیس	0	1	0	1	1
پایه آلیس	+	×	×	+	×
فوتون	↔	↘	↗	↕	↘
پایه باب	+	+	×	+	×
بیت باب	0	0	0	1	1

شکل (۳): ارسال پایه توسط باب [۴]

۴- بیت‌های ناشی از اندازه‌گیری‌ها با پایه‌های نامناسب توسط "باب" حذف می‌شوند و به این ترتیب آلیس و باب به یک دسته مشترک از بیت‌های صحیح بین خود می‌رسند [۴]



شکل (۴): مقایسه بیت‌ها [۴]

۵- در صورتی بیت‌های باقیمانده بین آلیس و باب با هم در توافق نباشند، کسر α از داده‌های ارسالی به سرقت رفته است و در این صورت احتمال آنکه بیت‌های باقیمانده بین آلیس و باب در توافق نباشند، برابر $\alpha/4$ است. در صورت کشف مزاحم و یا سرقت کننده اطلاعات آلیس و باب به مرحله اول برگشته و از اول به ارسال اطلاعات می‌پردازند [۷].

۳- پیاده‌سازی و کاربردهای پروتکل BB۸٤

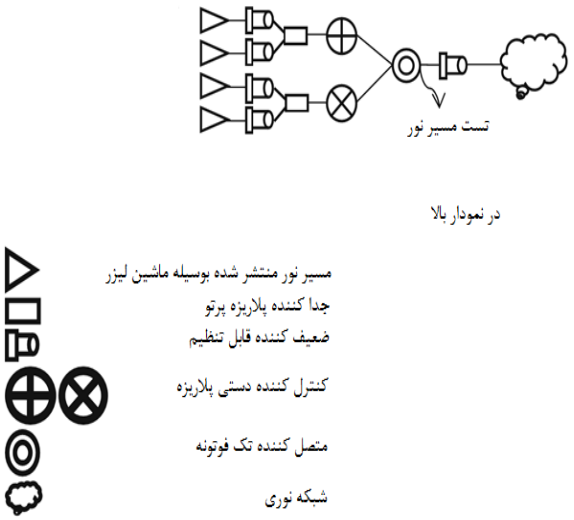
بعد از ورود رمزنگاری کوانتومی از آزمایشگاه‌های تحقیقاتی به بازارهای تجاری، کاربرد QKD صورت واقعی به خود گرفته است. اگر چه بعضی از چالش‌ها هنوز وجود دارد، ولی رمزنگاری کوانتومی کمبودهای رمزنگاری متعارف را هدف گرفته است. انگلیس، آلمان و فرانسه به‌عنوان نوید بخش‌ترین بازارها برای محصولات توزیع کلید کوانتومی در اروپا ذکر شده است. در حال حاضر محصولات تجاری QKD به‌صورت انبوه به‌وسیله شرکت‌های "ID Quanique" سوئیس و فناوری‌های MagiQ ایالات متحده آمریکا تولید می‌شود. یکی دیگر از فعالیت‌ها، پروژه SECOQC اروپا می‌باشد که توسط ۴۱ سازمان انجام می‌شود [۷].

۳-۱- پیاده سازی پروتکل BB۸٤

پیاده سازی پروتکل و سامانه[1] توزیع کلید کوانتومی وابسته به تکنولوژی طراحی در تولید و آماده‌سازی، انتقال و تشخیص کیوبیت‌ها می‌باشد. به‌دلیل اینکه سیگنال لیزر در انتقال توسط فیبر بسیار عالی است و تک فوتون قابل جدا شدن نیست، پس تک فوتون بهترین حمل‌کننده سیگنال کوانتومی می‌باشد [۸].

۳-۱-۱- انتقال سیگنال‌های کوانتومی

براساس پروتکل BB۸٤ چهار سیگنال فوتون توسط سیگنال کوانتومی تولید شده، که توسط شکل زیر نشان داده می‌شود.



شکل (۵): نمودار شماتیک انتقال سیگنال کوانتومی [۸]

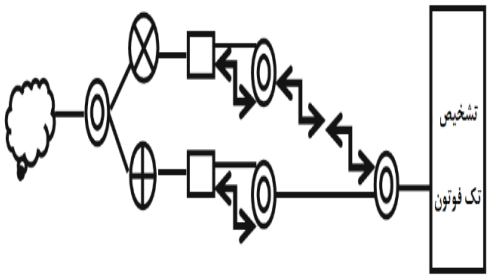
[1] System

بعد از انتشار نور در چهار مسیر، اولین تضعیف حدود ۵۰dB می‌باشد و تضعیف مرحله بعدی حدود ۴۶ dB و خطا حدوداً ۱dB می‌باشد. مسیر نور آزمایشی در نمودار به‌منظور کالیبره کردن جهت درهم‌تنیدن MPC استفاده می‌شود [۸].

۳-۱-۲- تشخیص کیوبیت

گیرنده کیوبیت باید سامانه تشخیص فوتوالکتریک باشد که می‌تواند سیگنال‌های کوانتومی خیلی ضعیف را تشخیص دهد و کلید کوانتومی که با سیگنال کوانتومی حمل می‌شود را شناسایی کند. در این سامانه تنها تشخیص‌دهنده تک فوتون با استفاده از اثر بهمن برای کشف فوتون‌ها تنظیم شده است.

نماد[1]، نماد یک جامپر ۲ متری می‌باشد. از جامپر با چندین SMC برای ساختن خط فوتون چهارحالته به شکل اشعه برای تشخیص تک فوتون استفاده می‌شود. در شکل زیر تابع اصلی PBS برای جداکردن نور درهم‌تنیده شده در دو حالت عمودی می‌باشد. برای تشخیص چهار حالت نور درهم‌تنیده، دریافت‌کننده لیزری به ۲، ۴ و یا ۶ جامپر افزیش پیدا می‌کند.

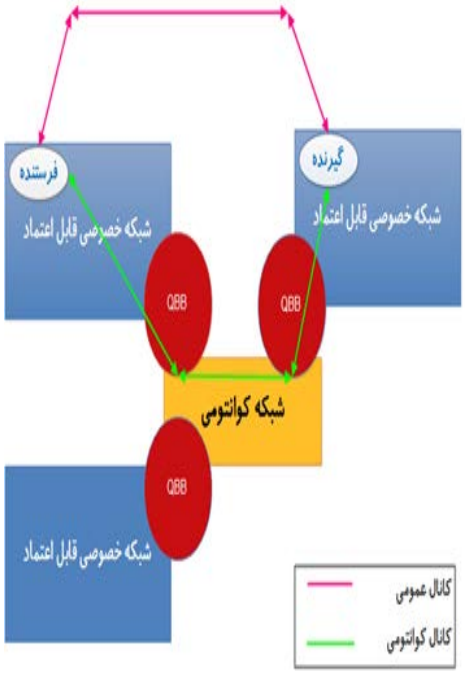


شکل (۶): نمودار شماتیک واقعیت بخشی [۸]

۳-۲- معماری شبکه SECOQC

رمزنگاری کوانتومی که بعضاً به توزیع کلید کوانتومی شناخته می شود، امنیت فوق العاده‌ای را فراهم می‌کند. اما در عین حال بعضی محدودیت‌ها را هم به دنبال دارد. یکی دنبال نکردن نظریه No-cloning است که QKD ها تنها اتصالات یک به یک را فراهم و پشتیبانی می‌کنند. بنابراین تعداد لینک‌ها می‌تواند به تعداد ۲ / N(N- ۱) که N بیانگر تعداد گره‌ها می‌باشد، افزایش پیدا کند. حال اگر یک گره بخواهد در در داخل شبکه QKD شرکت کند، همین امر باعث بعضی به‌وجود آمدن بعضی از مسائل و مشکلات همانند احداث خطوط ارتباط کوانتومی می‌شود. برای برطرف کردن این مسائل، SECOQC شروع شد.

معماری شبکه SECOQC می‌تواند به دو قسمت تقسیم شود. شبکه خصوصی مطمئن و شبکه کوانتومی تشکیل شده از اسکلت کوانتومی که به اختصار QBBs نامیده می‌شود. شبکه خصوصی، یک شبکه معمولی با گره پایانی و یک QBB است [۹].



شکل (۷): معماری شبکه SECOQC [۹]

QBB یک کانال ارتباطی کوانتومی بین QBBs ها فراهم می‌کند. QBB از تعدادی دستگاه‌های QKD تشکیل شده که توسط ارتباطات یک به یک به دیگر دستگاه‌های QKD متصل شده‌اند.

از این طریق، SECOQC می‌تواند اتصال راحت‌تری را برای پیوستن یک گره پایانی جدید به شبکه QKD و همچنین بازیابی سریع از تهدید لینک کانال کوانتومی را فراهم کند. SECOQC مبنایی را برای ارتباطات بسیار امن از راه دور در یک نظام شبکه‌ای فراهم خواهد کرد که ترکیبی از تکنولوژی کاملاً جدید از توزیع کلید کوانتومی با راه‌حل‌هایی از علوم کامپیوتر کلاسیک، طراحی شبکه و رمزنگاری است [۹].

۳-۳- پیاده سازی پروتکل BB۸٤ روی ۸۰۲/۱۱

توزیع کلید در پروتکل در دو مرحله اتفاق می‌افتد. در قسمت اول دو مرحله اول الگوریتم انجام شده و باقیمانده مراحل در قسمت دوم می‌باشد. در قسمت اول از کانال کوانتومی استفاده شده و در قسمت دوم از کانال عمومی استفاده می‌شود [۱۰]. آلیس فرستنده اطلاعات و باب گیرنده اطلاعات فرض شده است. در جدول (۱)، مراحل پیاده‌سازی پروتکل BB۸٤ روی ۸۰۲/۱۱ آورده شده است.

[1] Polarization Beam Splitter

جدول (۱): مراحل پیاده‌سازی پروتکل BB۸٤ روی ۸۰۲/۱۱

قسمت اول	قسمت دوم
آلیس اطلاعات را با درهم‌تنیدگی تصادفی می‌فرستد.	آلیس از کانال عمومی برای فرستادن درهم‌تنیدگی استفاده می‌کند.
باب فوتون‌ها را دریافت می‌کند.	باب درهم‌تنیدگی دریافتی را با درهم‌تنیدگی تولیدی خودش مقایسه می‌کند.

اجتماع لیست‌ها به عنوان کلید خام مورد استفاده قرار می‌گیرد.

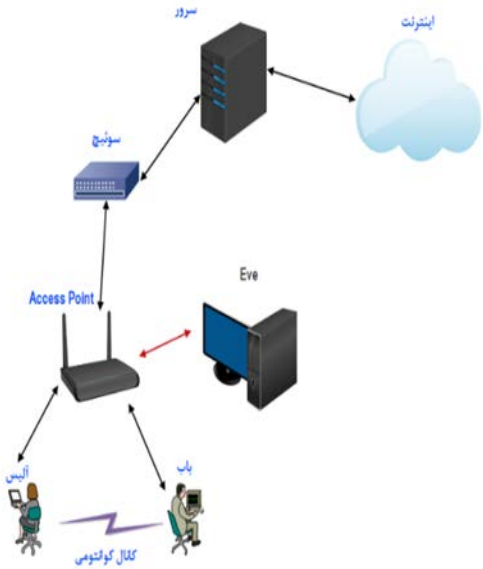
۳-۳-۱- ساختار نرم‌افزاری پیاده سازی پروتکل

برای پیاده سازی این پروتکل از زبان برنامه نویسی جاوا استفاده شده است. این نرم‌افزار در دو کانال کار می‌کند: کانال کوانتومی و کانال عمومی.

آلیس، باب و ایو هر کدام در ماشین جداگانه‌ای اجرا می‌شوند. برای پیاده سازی پروتکل از ۵ شیء آلیس، باب، ایو، کانال کوانتومی و کانال عمومی استفاده می‌شود.

۳-۳-۲- ساختار سخت افزاری پروتکل

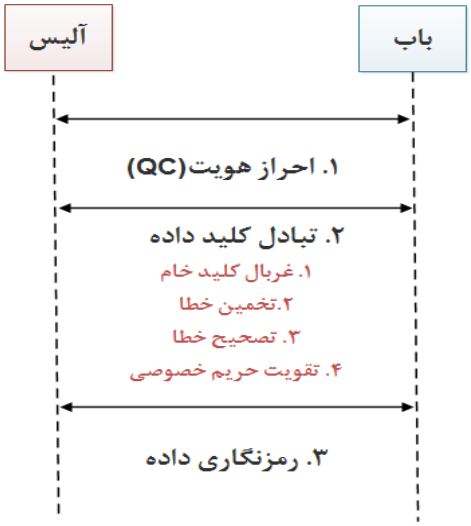
ساختار سخت افزاری پیاده سازی مطابق شکل (۸) می‌باشد.



شکل (۸): ساختار سخت افزاری پروتکل BB۸۴ [۱۰]

همه دستگاه‌ها در یک حالت مشابه می‌باشند. از سوئیچ به منظور متصل کردن همه دستگاه‌ها و نقطه دسترسی استفاده شده است. از آدرس IP ایستا به‌منظور مطمئن شدن از ارتباط همه ایستگاه‌های کاری استفاده شده است [۱۰].

قالب طراحی پروتکل در شکل (۹) نشان داده شده است. مطابق با این شکل، در فرآیند توزیع کلید کوانتومی آلیس و باب وظیفه خود را انجام می‌دهند [۱۰].



شکل (۹): پروتکل دو قسمته در QKD [۱۰]

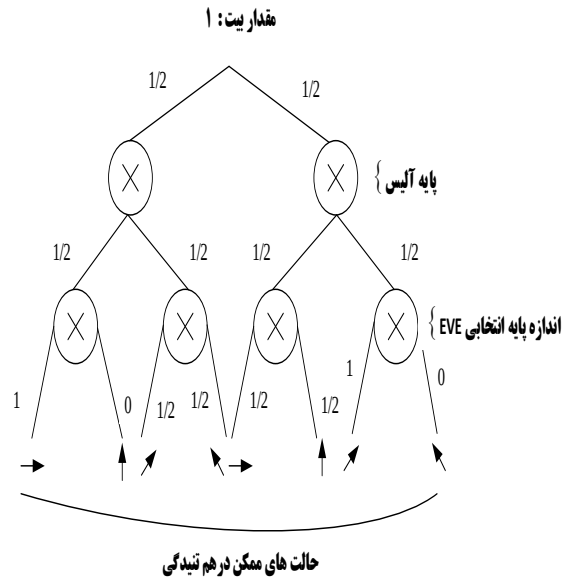
۴- تحلیل امنیتی پروتکل BB۸٤

حملات مختلفی تاکنون بر علیه پروتکل BB۸٤ صورت گرفته و مورد بررسی پژوهشگران در این عرصه بوده است که در این بخش به بررسی چند مورد از آن حملات پرداخته خواهد شد.

۴-۱- حمله ارسال و دریافت[1]

این حمله در یک محیط ایده آل پیاده سازی شده است. در این نوع حمله، مهاجم فوتون‌های نوری را از آلیس دریافت کرده و با پایه تصادفی خود تفسیر می‌کند، به‌دلیل عدم نویز در محیط ایده آل، کل فوتون‌ها را دریافت می‌کند. مهاجم حالتی مثل شکل (۱۰) را می‌پیماید. در شکل (۱۰)، فرستنده بیت 0 را می‌فرستد. سپس مهاجم فوتون جایگزین را با قطبیت مشخص به باب می‌فرستد. شدت پالس مهاجم باید طوری باشد که باب این فوتون را با نرخ یکسان دریافت کند. در واقع در این حالت یک شخص سوم در وسط دو نفر نشسته است و اطلاعات را بین آن دو رد و بدل می‌کند. تلاش ایو ارزشمند خواهد بود اگر اطلاعات به‌دست آمده $1/\sqrt{2}$ برابر اطلاعات آلیس باشد. فرض می‌کنیم در مرحله تصحیح خطا و تقویت امنیت پروتک BB۸٤، T بیت خطا کشف شده است. اگر فرض کنیم در ارتباط آلیس و باب کمتر از ۱e بیت در معرض حمله دریافت و فرستادن هستند، اطلاعات به دست آمده توسط ایو بیشتر از $e1/\sqrt{2}$ نمی‌باشد. جدول (۲) نمونه حمله دریافت و فرستادن را نشان می‌دهد.

[1] Intercept and Resend



شکل (۱۰): نحوه دریافت توسط مهاجم [۱۱]

فرض بر این است که در حالت معمولی ایو به کانال عمومی گوش نمی‌دهد، مانند فاز به‌دست آوردن کلید در پروتکل BB۸٤.

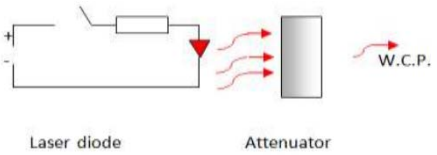
اطلاعاتی که می‌توان به‌دست آورد همان ۰/۲ کل بیت‌ها می‌باشد که خیلی کم است [۱۱].

جدول (۲): نمونه ارسال و دریافت آلیس و باب [۱۱]

Alice random bits	0	1	1	0	1	0	0	1
Alice sending Basis	+	×	+	×	×	+	×	+
Alice polarization	→	↖	↑	↗	↖	→	↗	↑
Eve basis measurement	+	+	×	×	+	×	×	+
Polarization Eve measures and sends	→	→	↗	↗	↑	↗	↗	↑
Bob basis measurement	+	×	×	×	+	×	+	+
Polarization Bob measures	→	↗	↗	↗	↑	↗	→	↑
Shared secret key	0	0	-	0	-	-	-	1
Error generated	√	x		√				√

۴-۲- حمله PNS[1]

در محیط واقعی تولید یک دستگاهی که منبع تک فوتون باشد بسیار مشکل است و پالس سیگنال واقعی حاوی تعداد زیادی فوتون می‌باشد. پالس‌های منسجم ضعیف در ابزارهای واقعی رمزنگاری استفاده می‌شود. شکل (۱۱) یک منبع تولید فوتون را نشان می‌دهد. WCP یک پالس فوتون است که متوسط تعداد فوتون‌هایش کم می‌باشد.

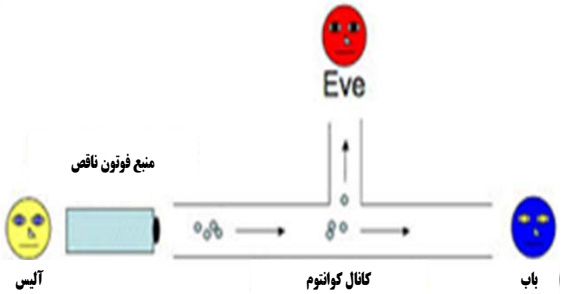


شکل (۱۱): تولید کننده پالس منسجم ضعیف [۱۲]

حمله PNS از این ویژگی منبع‌ها برای حمله استفاده می‌کند. این حمله به منبع‌های تولید فوتون تمرکز دارد. استراتژی این حمله این است که ایو قسمتی از فوتون‌ها را برداشته و بقیه را برای باب می‌فرستد، حال باید ایو منتظر بماند تا در مرحله دوم آلیس قطبیت‌های استفاده شده را برای باب بفرستد و در نتیجه ایو می‌تواند قطبیت درست هر فوتون را به‌دست آورد [۱۱].

۴-۳- حمله تزریق فوتون

نام دیگر این حمله، حمله اسب تروجان[2] می‌باشد. در این نوع حمله ایو تمرکز خود را روی ایستگاه‌هایی که آلیس و باب استفاده می‌کنند می‌گذارد، سپس برخلاف حمله قبلی که روی فوتون‌های ارسال شده توسط آلیس و باب تمرکز می‌کرد، در این نوع حمله پالس‌های نوری را به‌سمت فرستنده و گیرنده می‌فرستد، سپس پالس‌های نوری برگشته شده را توسط عامل تشخیص که در اختیار ایو است تشخیص می‌دهد. ایو می‌تواند از این سیگنال‌های نوری برگشته شده استفاده کرده و قطبیت استفاده شده توسط آلیس را بیابد. حال اگر ایو بتواند زودتر از باب اطلاعات را دریافت کرده و به باب بفرستد می‌تواند حمله دریافت و ارسال را انجام داده و رشته مخفی را به‌دست آورد. از اینرو ایو می‌تواند اطلاعاتی را بدون فهمیدن طرفین به‌دست آورد [۱۳].



شکل (۱۲): حمله PNS [۱۲]

[1] Photon Number Splitting

[2] Trojan Horse

۴-۴- حمله مرد میانی[1]

این حمله برای همه بسیار مشخص می‌باشد. دلیل این حمله در این پروتکل، عدم احراز اصالت یا نشناختن طرفین ارتباط است که در این قسمت فقط راه‌حل‌های این حمله بررسی می‌شوند.

۱- استفاده از گواهی دیجیتال یا ویژگی‌های دیگری از ساختار کلید عمومی.

۲- با یک ساختار، دو طرف یک کلید مشترک داشته باشند تا کد احراز اصالت را رمز کنند.

۳- آلیس جفت EPR خود را در داخل کیوبیت‌های مرحله اول بفرستد. پس باب می‌تواند همبستگی آن را بفهمد.

۴- در قسمت آخر آلیس و باب می‌توانند قسمتی از کد را برای مطمئن شدن از عدم وجود شنودگر از طریق ایمیل یا تلفن به هم بگویند.

۵- در قسمت آخر الگوریتم یک قسمت از کد را به‌صورت آشکار به یکدیگر بفرستند تا مطمئن شوند هر دو طرف اطلاعات همدیگر را به‌صورت درست به‌دست می‌آورند.

در کل با توجه به [۱۴]، نتیجه‌ای که گرفته می‌شود این است که برای جلوگیری از این حمله روی پروتکل، باید با رمزنگاری کلاسیک آمیخته شود [۱۴].

۴-۵- حمله حالت ساختگی

نوع جدیدی از حمله است که روی جمع‌آوری اطلاعات و به‌دست آوردن ضعف‌های گیرنده (باب) می‌باشد. یک شکل تخصصی‌تری از حمله ارسال و دریافت می‌باشد که به‌جای دوباره درست کردن سیگنال، ایو کل سیگنال که از خودش مشتق شده را با در دست گرفتن کل ارتباط، می‌فرستد.

یکی از پایه‌های اصلی این حمله عدم‌تطابق بازده آشکارساز می‌باشد. سیگنالی که ایو به باب بعد از دریافت سیگنال‌های آلیس می‌فرستد دارای یک فاصله زمانی می‌باشد که اگر باب پایه‌ای به جزء آنکه ایو انتخاب کرده انتخاب کند، ایو از لو رفتن در امان می‌ماند.

گام‌های این حمله در پروتکل BB۸٤ به‌صورت زیر می‌باشد:

۱- ایو کانال را گوش می‌دهد و یک حمله ساده دریافت و عمل فرستادن را انجام می‌دهد و براساس پایه انتخابی خود، بیت‌ها را محاسبه می‌کند.

۲- او سیگنال‌هایی را به باب می‌فرستد که هم ارزش بیت مخالف و هم حالت مخالف دارند. با این کار تاخیر زمانی تنظیم خواهد شد و اگر باب با قطبیت مشابه ایو اندازه‌گیری کند، سیگنال را دریافت خواهد کرد، در غیر این‌صورت نمی‌تواند سیگنال را اندازه‌گیری کند.

۳- اکنون اگر ایو بتواند با مبنای آلیس اطلاعات را دریافت کند، باب نیز همین کار را خواهدکرد. در غیر این‌صورت هم ایو و هم باب با مبنای مخالف آلیس دریافت خواهند نمود.

۴- از این‌رو، ایو به باب دسترسی کامل دارد.

استراتژی این حمله توسعه حمله ارسال و دریافت بوده و مؤثرتر از آن می‌باشد. اما مشکل کوچک آن وابستگی شدیدش به همزمان‌سازی و کارایی تشخیص دهنده ایو می‌باشد. به‌طورکلی این یک استراتژی متفاوتی از بقیه حمله‌ها می‌باشد [۹].

۵- نتیجه گیری

در این مقاله به تفصیل به پروتکل توزیع کلید کوانتومی BB۸٤ پرداخته شد. برخی از کاربردها، نحوه شبیه‌سازی و تحلیل امنیتی مرتبط با این پروتکل مورد بررسی دقیق قرار گرفت. درحقیقت اگرچه پروتکل BB۸٤ از لحاظ ریاضی امن بوده، ولی به‌منظور پیاده سازی در فضای واقعی از منظر دستگاه‌های سخت افزاری محدودیت داشت. همان‌طور که بیان شد، این پروتکل با توجه به عدم وابستگی به کامپیوترهای کوانتومی می‌تواند به سامانه‌های کلاسیک موجود اضافه شود. در این حالت تنها با گذاشتن یک کانال کلاسیک و یک کانال کوانتومی حتی ناامن، می‌توان کلید مخفی را برای ارسال پیام‌های رمز شده به‌صورت کاملاً امن و بدون هیچ‌گونه پیش‌فرضی در مورد توانایی استراق سمع‌کننده بین فرستنده و گیرنده به اشتراک گذاشت.

۶- مراجع

[1] S. C. F. C. Revolution, “Comprehensive scientific map of the Iran(InPersian),”2012,Available: https://irimc.org/Portals/0/PDF/ScientificMap.pdf.

[2] J. Kaltz and Y. Lindell, “Introduction to modern cryptography: principles and protocols,” ed: Chapman and Hall, 2008.

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” arXiv preprint arXiv:.06557, 2020.

[4] D.Mayers,“Unconditional-security-in-quantum Journal of the ACM, vol. 48, No. 3, pp. 351-406, 2010.

[5] H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” science, vol. 283, no. 5410, pp. 2050-2056, 1999.

[1] Man-In-The-Middle

```
    {
        plus  = "+ ";
        plus_ = "+";
        X     = "X ";
        X_    = "X";

        if (basis.equals(plus) ||
basis.equals(plus_))
        {
            double polarization_num =
qubit.randomGenerator();
            if (polarization_num < 0.5)
            {
                polarization = "|";
            }
            else
            {
                polarization = "H";
            }
        }
        else if (basis.equals(X))
        {
            double polarization_num =
qubit.randomGenerator();
            if (polarization_num < 0.5)
            {
                polarization = "/";
            }
            else
            {
                polarization = "\\";
            }
        }
        return polarization;
    }
    public int generateBit(String
polarization)
    {
        if
(polarization.equals("|"))  return 1;
        else if
(polarization.equals("/"))  return 1;
        else if
(polarization.equals("H"))  return 0;
        else if
(polarization.equals("\\")) return 0;
        else return H99;
    }

    public int measureQubit(Qubit
myqubit, String basis_)
    {
        int bit;
        if
(myqubit.basis.equals(basis_))
        {
            bit =
generateBit(myqubit.polarization);
            myqubit = null;
        }
        else
        {
            myqubit.basis        =
basis_;
            myqubit.polarization =
```


[6] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Physical review letters, vol. 85, no. 2, p. 441, 2000.

[7] A. Laucht and et al., "Roadmap on quantum nano technologies," Nanotechnology, vol. 32, no. 16, p. 162003, 2021.

[8] S.-s. Jiang, R.-n. Chi, X.-j. Wen, and J. Fang, "An Implementation Scheme of BB84-Protocol-Based Quantum Key Distribution System," in Advanced Technologies, Embedded and Multimedia for Human-centric Computing: Springer, pp. 973-978, 2014.

[9] T. Rubya, N. P. Latha, and B. Sangeetha, "A survey on recent security trends using quantum cryptography," JCSE, vol. 2, No. 9, pp. 3038-3042, 2015.

[10] N. H. K. Aizan, Z. A. Zukarnain, and H. Zainuddin, " Implementation of BB84 Protocol on 802.11 i," in 2016 Second International Conference on Network Applications, Protocols and Services, , pp. 130-134. 2016

[11] R. Aggarwal, H. Sharma, and D. Gupta, "Analysis of various attacks over bb84 quantum key distribution protocol," International Journal of Computer Applications, vol. 20, no. 8, pp. 28-31, 2017.

[12] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," Journal of modern optics, vol. 48, no. 13, pp. 2023-2038, 2013.

[13] H.-K. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," arXiv preprint quant-ph/0102138, 2001.

[14] Y. Wang, H. Wang, Z. Li, and J. Huang, "Man-in-the-middle attack on BB84 protocol and its defence," in 2015 2nd IEEE International Conference on Computer Science and Information Technology, pp. 438-439, 2015.

پیوست:

کد پیاده سازی پروتکل BB۸٤ در ذیل آورده شده است:

```
public class Qubit {
    private String polarization, basis;
    public Qubit(String polarization,
String basis)
    {
        this.polarization =
polarization;
        this.basis = basis;
    }

    public String generateBasis()
    {
        double basis_num =
qubit.randomGenerator();
        if (basis_num < 0.5) basis =
"+";
        else basis = "X";
        return basis;
    }

    public String
generatePolarization(String basis)
```

```
myqubit.generatePolarization(basis_);

            bit =
generateBit(myqubit.polarization);
            myqubit = null;
        }
        return bit;
    }

}
```

در کد فوق، کلاس Qubit که منطق پروتکل BB۸٤ می‌باشد پیاده‌سازی شده است، تابع generateBasis() پایه درهم‌تنیدگی را مشخص می‌کند، تابع generatePolarization() درهم‌تنیدگی قطب‌ها را مشخص کرده و تابع generateBit() تولید بیت‌ها را بیان می‌کند. در نهایت با توجه به پایه و جهت درهم‌تنیدگی، بیت‌های ارسالی از طرف آلیس به باب مشخص خواهد شد.