کاربرد QRNG در سامانه های رمزنگاری کوانتومی

علی نخعی امرودی [1,*]، رامین نصیری [۲]

۱- استادیار دانشکده رایانه، شبکه و ارتباطات، دانشگاه جامع امام حسین (ع)

۲- استادیار دانشکده علوم پایه، دانشگاه جامع امام حسین (ع)

چکیده

ضرورت استفاده از اعداد تصادفی در رمزنگاری کوانتومی به دلیل ایجاد امنیت غیرقابل شنود است. ادعای غیرقابل هک بودن رمزنگاری کوانتومی، در صورتی صحیح است که اعداد تصادفی واقعی و ذاتاً تصادفی وجود داشته باشد. به عبارتی برای داشتن کلید رمزنگاری کوانتومی نیاز به یک مولد اعداد تصادفی واقعی است که رشته بیت اعداد واقعاً تصادفی ایجاد نماید و سپس الگوریتم‌های رمزنگاری با این رشته تصادفی شروع به کار کنند. در این مقاله، با بررسی پروتکل رمزنگاری کوانتومی BB84 به بررسی مهم‌ترین کاربردهای QRNG در سامانه‌های رمزنگاری کوانتومی خواهیم پرداخت.

کلمات کلیدی: رمزنگاری کوانتومی، مولد اعداد تصادفی کوانتومی، پروتکل BB84

۱. رمزنگاری کوانتومی و ضرورت استفاده از QRNG در آن

رمزنگاری کوانتومی در مقایسه با سایر فناوری‌های کوانتومی، گسترش تجربی بیش‌تری داشته و توانسته است در ابعاد تجاری و صنعتی هم دستاوردهای مهمی داشته باشد [۷،۱]. رمزنگاری کوانتومی استفاده ازمکانیک کوانتومی برای کشف حضور اخلال‌گر[1] (شنود کننده) احتمالی به هنگام انتقال اطلاعات محرمانه بین دو پایگاه است و یک روش ایمن و قابل اعتماد برای انتقال کلیدهای خصوصی از طریق کانال‌های عمومی را فراهم می‌آورد. این امر به‌عنوان یکی از اقدامات پدافند غیرعامل، به منظور حفاظت از اطلاعات حساس و طبقه‌بندی شده‌ی فردی، امنیتی، نظامی، صنعتی، تجاری و دولتی بسیار ضروری است [۸،۲]. به همین دلیل در سال‌های اخیر، رمزنگاری کوانتومی به‌طور قابل توجهی مورد علاقه‌ی محققین و گروه‌های علمی در سراسر دنیا قرار گرفته است. رمزنگاری کلید یک‌بار مصرف (OTP)[2] تنها روش در رمزنگاری کلاسیک است که دارای امنیت اثبات شده می‌باشد. مشکل اصلی در پیاده‌سازی این روش، طول بسیار زیاد و یک‌بار مصرف بودن کلید است. این نقطه ضعف توسط پروتکل‌هایی بر پایه‌ی دانش فیزیک کوانتومی، برای تولید و توزیع کلید تصادفی با طول

* **Corresponding author: Email: kpnakhaei@ihu.ac.ir**
[1] Eavesdropper
[2] One Time Pad

دلخواه در شرایط کاملاً امن برطرف می‌شود. این رویکرد با نام توزیع کلید کوانتومی (QKD)[1] شناخته می‌شود. در واقع، QKD پرکاربردترین زمینه‌ی کاری رمزنگاری کوانتومی است. سامانه‌های QKD، سامانه‌های پیچیده‌ای متشکل از سخت‌افزار (مؤلفه‌های الکتریکی، اپتیکی و الکترواپتیکی) و نرم‌افزار (پروتکل‌ها و روش‌های مرسوم پس پردازش کلاسیک به منظور تولید کلید امن) هستند. طراحی و تحلیل سامانه‌های رمزنگاری کوانتومی نیاز به مهارت در زمینه‌های متفاوتی همچون فیزیک کوانتومی، اپتیک، نظریه‌ی اطلاعات، ریاضی، آمار و مهندسی برق دارد.

پروتکل BB84 نخستین و مهم‌ترین پروتکل QKD است که در سال ۱۹۸۴ توسط بِنِت[2] و براسارد[3] پیشنهاد شد [۱]. به‌طور خلاصه، در پروتکل BB84 استاندارد، فرستنده‌ی پیام، آلیس[4]، هر بیت از یک کلید محرمانه را با یک سامانه‌ی کوانتومی دوترازی (بیت کوانتومی یا کیوبیت) کدگذاری می‌کند. کیوبیت از طریق یک کانال کوانتومی برای گیرنده‌ی پیام، باب[5]، فرستاده می‌شود. همواره فرض می‌شود که یک اخلال‌گر، به نام ایو[6]، می‌تواند به کانال کوانتومی دسترسی داشته باشد و هرگونه اندازه‌گیری مجاز از نقطه نظر قوانین مکانیک کوانتومی را بر روی کیوبیت انجام دهد. برای جلوگیری از استراق‌سمع، ضروری است که آلیس با استفاده از یک QRNG، کیوبیت‌ها را به صورت کاتوره‌ای در یکی از دو پایه‌ی غیرمتعامد آماده کند.

ایو پایه‌های انتخابی آلیس را که برای انجام یک اندازه‌گیری درست (یعنی با نتیجه‌ی دقیق) موردنیاز است، نمی‌داند. بدون داشتن این اطلاعات، ایو در تعدادی از دفعات، اندازه‌گیری نادرست انجام می‌دهد و به‌طور غیرقابل اجتناب تابع موج یا بردار حالت کیوبیت را منحرف می‌کند. چنین انحرافاتی، منجر به افزایش نرخ خطا در اطلاعات دریافتی توسط باب می‌شود که این امر، حضور ایو را آشکار می‌کند.

بدون توجه به نوع پروتکل مورد استفاده، در حالت کلی می‌بایست فرضیه‌هایی در مورد تجهیزات به کار رفته در بخش‌های آلیس و باب انجام داد تا از وجود امنیت در سامانه‌ی QKD اطمینان حاصل کرد. از جمله‌ی این فرضیه‌ها می‌توان به موارد زیر اشاره کرد:

- کاملاً کاتوره‌ای بودن عملکرد تولید کننده‌ی اعداد تصادفی (RNG)؛
- تک‌فوتونی بودن منبع نوری؛
- تصادفی بودن فاز پالس‌ها؛
- همدوس بودن حالت‌های کوانتومی؛
- یکسان بودن بازدهی آشکارسازها؛
- تک مد بودن پالس‌های تک‌فوتونی؛
- هم‌زمانی کامل ارسال و دریافت بیت‌های متناظر.

با وجود این فرضیه‌ها، ایو قادر نخواهد بود اندازه‌گیری‌هایی انجام دهد که منجر به استحصال اطلاعات از حالت کوانتومی سامانه، بدون ایجاد تغییر غیرقابل اجتناب روی آن حالت‌ها شود. با این کار، در انتقال کیوبیت‌ها و در نتیجه، به اشتراک‌گذاری بیت‌ها خطا وارد شده و بنابراین حضور اخلال‌گر شناسایی می‌شود. در این حالت، کلید غربال شده، به طور حتم و بدون قید و شرط امن خواهد بود. بدون قید و شرط بودن امنیت بدین معنا است که هیچ محدودیت نظری و تجربی به‌جز مقید بودن به اصول فیزیک کوانتوم برای ایو در نظر گرفته نمی‌شود.

[1] Quantum Key Distribution
[1] Bennett
[2] Brassard
[3] Alice
[4] Bob
[5] Eve

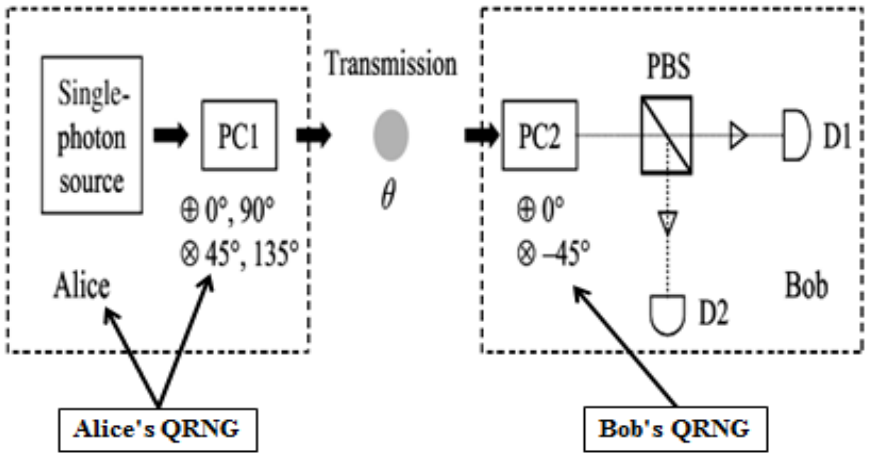
در پیاده‌سازی‌های تجربی رمزنگاری کوانتومی، آن‌چه به‌عنوان حامل اطلاعات انتخاب می‌شود، اغلب اوقات منحصراً فوتون است. تحت شرایط معین، تابع موج فوتون در برابر نویزهای محیطی بسیار قوی عمل می‌کند و یک فوتون می‌تواند از طریق کانال کوانتومی تار نوری یا فضای آزاد تا چندین کیلومتر فرستاده شود. روش‌های به‌کار رفته در این دو نوع از رمزنگاری کوانتومی با هم متفاوت است. در رمزنگاری کوانتومی فضای آزاد، فوتون‌های آلیس، از طریق هوای آزاد به دستگاه گیرنده‌ی باب می‌رسند. در رمزنگاری کوانتومی تار نوری، آلیس فوتون‌های مورد نظر خود را به داخل یک تار نوری می‌فرستد و باب آن‌ها را پس از انتشار از میان کانال کوانتومی، دریافت می‌کند. این سامانه‌ها متداول‌تر و پرکاربردتر از همتاهای فضای آزاد خود هستند، زیرا در آن‌ها از قطعات ارتباطی استاندارد استفاده می‌شود. در حالت کلی می‌توان گفت که برای کدگذاری و انتقال اطلاعات در هوای آزاد بهتر است از کدگذاری روی قطبش استفاده شود، ولی در رمزنگاری مبتنی بر تار نوری، استفاده از کدگذاری روی فاز فوتون‌ها مناسب‌تر و مرسوم‌تر است.

۲. چگونگی کاربرد QRNG در سامانه های QKD

همان‌طور که پیش از این گفته شد، تقریباً همه پروتکل‌های رمزگذاری کوانتومی به منبعی از اعداد تصادفی نیاز دارند. برای درک ضرورت استفاده از QRNG در سامانه‌های QKD، به تشریح جزییات اجرای پروتکل BB84، در دو حالت: (۱) استفاده از قطبش و (۲) استفاده از فاز تک فوتون‌ها می‌پردازیم.

۲-۱ اجرای پروتکل BB84، در حالت استفاده از قطبش تک فوتون ها

مطابق شکل ، در ساده‌ترین حالت از پروتکل BB84، داده‌ها به وسیله‌ی حالت‌های قطبش تک‌فوتون‌ها کد می‌شوند و عددهای دودویی 0 و 1 توسط حالت‌های قطبش عمود بر هم بیان می‌شوند.
در این پروتکل، از دو دسته حالت قطبشی غیر متعامد که پایه‌های $\oplus$ و $\otimes$ نامیده می‌شوند استفاده می‌شود. دو حالت قطبش برای پایه‌ی $\oplus$ را می‌توان در نمادگذاری دیراک[1] به صورت $|\uparrow\rangle$ و $|\rightarrow\rangle$ نشان داد، درحالی‌که دو حالت پایه‌ی $\otimes$ به ترتیب به صورت $|\nearrow\rangle$ و $|\nwarrow\rangle$ نشان داده می‌شوند. این نمادگذاری‌ها در جدول خلاصه شده است. در این‌جا، θ زاویه‌ی قطبش فوتون نسبت به محور عمودی است.



[1] Dirac notation

شکل ۱. شمای برپایی یک سامانه‌ی QKD فضای آزاد، با استفاده از پروتکل BB84 استاندارد قطبشی [۲].

مطابق جدول ، به طور کلی در اجرای پروتکل BB84 استاندارد قطبشی، گام‌های زیر انجام می‌گیرد:

۱- آلیس ابتدا رشته بیتی را که از طریق یک QRNG در اختیار گرفته است، طبق جدول ، با انتخاب تصادفی پایه‌های $\oplus$ و $\otimes$ کد می‌کند. سپس فوتون‌ها را با فواصل زمانی منظم، از طریق کانال کوانتومی هوای آزاد یا تار نوری برای باب ارسال می‌کند (سطرهای اول، دوم و سوم از شکل).

۲- باب فوتون‌ها را دریافت و نتایج را با استفاده از انتخاب تصادفی یکی از پایه‌های $\oplus$ و $\otimes$ توسط QRNG خود ثبت می‌کند (سطرهای چهارم و پنجم از شکل). مجموع این دو گام را انتقال کوانتومی می‌نامند و نتیجه‌ی آن، یک مجموعه بیت به نام کلید خام[1] می‌باشد.

۳- باب از طریق یک کانال عمومی (مانند خط تلفن)، بدون این‌که نتایج خود را آشکار کند، به آلیس خبر می‌دهد که به ترتیب چه پایه‌های آشکارسازی را انتخاب کرده است.

٤- آلیس پایه‌های باب را با پایه‌های خود مقایسه می‌کند، سپس بیت‌های متناظر با پایه‌های مشابه را حفظ و نامشابه‌ها را حذف می‌کند. در ادامه، از طریق کانال عمومی پایه‌های انتخابی خود را به باب اطلاع می‌دهد، تا باب نیز بیت‌های متناظر با پایه‌های غیریکسان را کنار بگذارد. در پایان این مرحله، درصورتی‌که هیچ گونه خطای ناشی از ناکاملی قطعات، اتلاف و هم‌چنین مداخله‌ی ایو در میان نباشد، آلیس و باب به یک رشته‌ی مشابه از بیت‌ها به نام کلید غربال شده می‌رسند (سطرهای ششم و هفتم از شکل).

٥- آلیس از طریق کانال عمومی، بخشی از بیت‌های تأیید شده‌اش را برای باب می‌فرستد. باب با مقایسه‌ی این بیت‌ها با نتایج خود، میزان خطای پیش آمده در انتقال بیت‌ها را تعیین می‌کند (سطر هشتم شکل). اگر نرخ خطای محاسبه شده کم‌تر از یک مقدار مشخص از پیش تعیین شده باشد، آلیس و باب می‌توانند بیت‌های باقی‌مانده را به‌عنوان یک کلید خصوصی نزد خود نگه دارند (سطر هشتم شکل).

جدول ۱. نمایش داده‌ها در پروتکل BB84 برای انتخاب پایه‌های قطبش [۲].

Basis	Binary 1	Binary 0
$\oplus$	$\|\uparrow\rangle$ $\theta = 0^\circ$	$\|\rightarrow\rangle$ $\theta = 90^\circ$
$\otimes$	$\|\nearrow\rangle$ $\theta = 45^\circ$	$\|\nwarrow\rangle$ $\theta = 135^\circ$

شکل نمونه‌ای از اجرای این پنج گام را نشان می‌دهد. سطر چهارم، انتخاب تصادفی پایه‌های آشکارسازی توسط QRNG باب را نشان می‌دهد. این انتخاب به طور میانگین در نیمی از موارد با انتخاب‌های آلیس یکسان خواهد بود. در این موارد، باب نتیجه‌ی درست را ثبت خواهد کرد. برای نصف دیگر بیت‌ها، باب تنها با احتمال ۵۰٪ به نتیجه‌ی درست خواهد رسید. البته این موضوع اهمیت چندانی ندارد، زیرا این داده‌ها اصلاً در تولید کلید به‌کار نمی‌روند.

[1] Raw key

Alice's QRNG →	A's data	1	0	0	1	1	1	0	0	1	0	0	1
	A's basis	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊗	⊕	⊗	⊗	⊕
	θ (°)	0	135	90	45	45	0	90	135	0	135	135	0
Bob's QRNG →	B's basis	⊗	⊗	⊕	⊕	⊗	⊕	⊗	⊕	⊕	⊗	⊕	⊗
	B's result	1	0	0	0	1	1	0	1	1	0	1	1
	Same basis ?	n	y	y	n	y	y	n	n	y	y	n	n
	Sifted bits		0	0		1	1			1	0		
	Data check ?		y	n		y	n			y	n		
	Private key			0			1				0		

شکل ۲. یک بخش گزینش شده از اجرای پروتکل BB84 استاندارد قطبشی[۲].

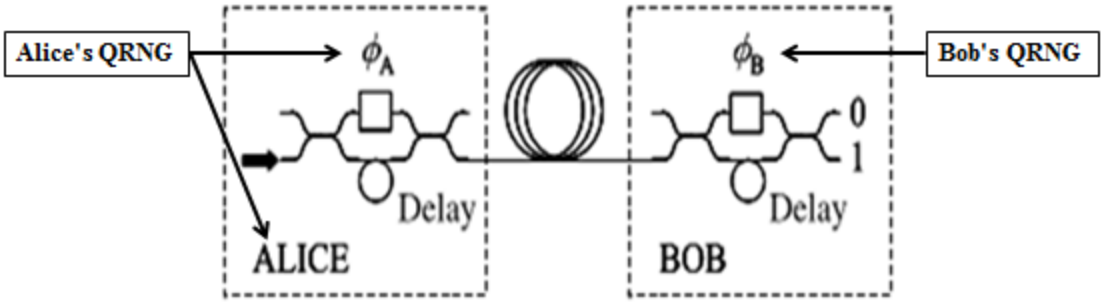
۲-۲ اجرای پروتکل BB84، در حالت استفاده از فاز تک فوتون ها

در اغلب سامانه‌های QKD مبتنی بر کانال کوانتومی فیبر نوری، از تاخیر فازهای ایجاد شده توسط تداخل‌سنج‌های ماخ-زنر (MZI) برای رمز کردن اطلاعات در حالت‌های کوانتومی (کیوبیت‌ها) استفاده می‌شود. در پروتکل‌های مبتنی بر فاز، آلیس می‌تواند از طریق کنترل فاز پالس‌های تک‌فوتون عبوری از یک MZI نامتوازن، که در یکی از بازوهای آن از یک مدولاتور الکترواپتیکی[1] (EOM) استفاده شده است، یک حالت کوانتومی خاص را آماده و ارسال کند. برای استفاده از EOM به عنوان مدولاتور فاز، باید از نوری استفاده کرد که دارای قطبش خطی در راستای محور اپتیکی بلور باشد و ولتاژ مناسب برای تغییر فاز به اندازه‌ی دلخواه را به بلور اعمال کرد.

مطابق شکل ، یک فوتون پس از عبور از یک MZI نامتوازن با بازوی کوتاه s و بلند l، در یک حالت برهم نهی از دو زمان متفاوت s یا l خواهد بود. بنابراین اگر مدولاتور فاز در بازوی کوتاه تداخل‌سنج آلیس، فاز $\emptyset_A$ را به فوتون اعمال کند، حالت کوانتومی در انتهای تداخل‌سنج را می‌توان به صورت

$$|l\rangle + e^{i\emptyset_A}|s\rangle \qquad (۱)$$

نشان داد.



شکل ۳. اجرای QKD فیبر نوری مبتنی بر فاز اپتیکی، با کمک دو تداخل‌سنج ماخ- زنر نامتوازن (با طول بازوهای متفاوت) [۳ و ۴].

[1] Electro-Optical Modulator (EOM)

سیگنال کوانتومی در بخش باب نیز از یک تداخل‌سنج نامتوازن مشابه با تداخل‌سنج آلیس عبور می‌کند و به باب این امکان را می‌دهد که با کمک یک EOM، پایه‌های اندازه‌گیری ویژه‌ای را با کمک یک QRNG انتخاب و فاز $\emptyset_B$ را در بازوی کوتاه خود به فوتون اعمال کند. اگر اختلاف بازوهای کوتاه و بلند تداخل‌سنج‌های آلیس و باب به ترتیب Δl_A و Δl_B باشد، در حالت ایده‌آل باید

$$\delta l = \Delta l_A - \Delta l_B = 0 \text{ و } l_A = l_B \text{ ،} s_A = s_B \quad (۲)$$

بنابراین حالت برهم نهی در انتهای تداخل‌سنج باب به صورت زیر خواهد بود:

$$|\psi\rangle = e^{i\emptyset_A}|s_A l_B\rangle + e^{i\emptyset_B}|l_A s_B\rangle \propto |s_A l_B\rangle + e^{i(\emptyset_B - \emptyset_A)}|l_A s_B\rangle \quad (۳)$$

طرح شماتیک اجرای پروتکل BB84 در یک سامانه‌ی تمام فیبری و بر اساس تداخل‌سنج ماخ-زنر در شکل ارائه شده است. مطابق این شکل، آلیس با توجه به پایه‌ی اندازه‌گیری تصادفی خود، به صورت تصادفی یکی از اختلاف فازهای $(0, \pi, \frac{\pi}{2}, -\frac{\pi}{2})$ را انتخاب کرده و باب نیز به صورت تصادفی یکی از اختلاف فازهای $(0, \frac{\pi}{2})$ را به فوتون اعمال می‌کند. اگر اختلاف فاز بین دو بازو $\phi_A - \phi_B = 0, \pi$ شود، آن‌ها نتایج مناسب را به‌دست آورده و این نتایج را حفظ می‌کنند؛ اما اگر $\phi_A - \phi_B = \pm\frac{\pi}{2}$ شود، نتایج تصادفی بوده و بنابراین چنین فوتون‌هایی به طور کلی کنار گذاشته می‌شوند. در حالت اوّل، اندازه‌گیری در D_1 را با بیت "0" و آشکارسازی در D_2 را با بیت "1" نمایش می‌دهیم و به این ترتیب به مجموعه‌ای از کدهای مشخص دست پیدا می‌کنیم. احتمال آن‌که فوتون عبور کرده از تداخل‌سنج، در آشکارساز D_1 یا D_2 اندازه‌گیری شود برابر است با:

$$\frac{1}{2}[1 \pm \cos(\phi_A - \phi_B)] \quad (۴)$$

در این‌جا ϕ_A و ϕ_B اختلاف فاز اعمال شده توسط مدولاتورهای فاز آلیس و باب بوده و علامت مثبت و منفی به ترتیب مربوط به احتمال آشکارسازی در D_1 و D_2 است. با توجه به این‌که:

$$\cos\alpha + cos\beta = 2cos\frac{\alpha+\beta}{2}cos\frac{\alpha-\beta}{2} \quad (۵)$$

و

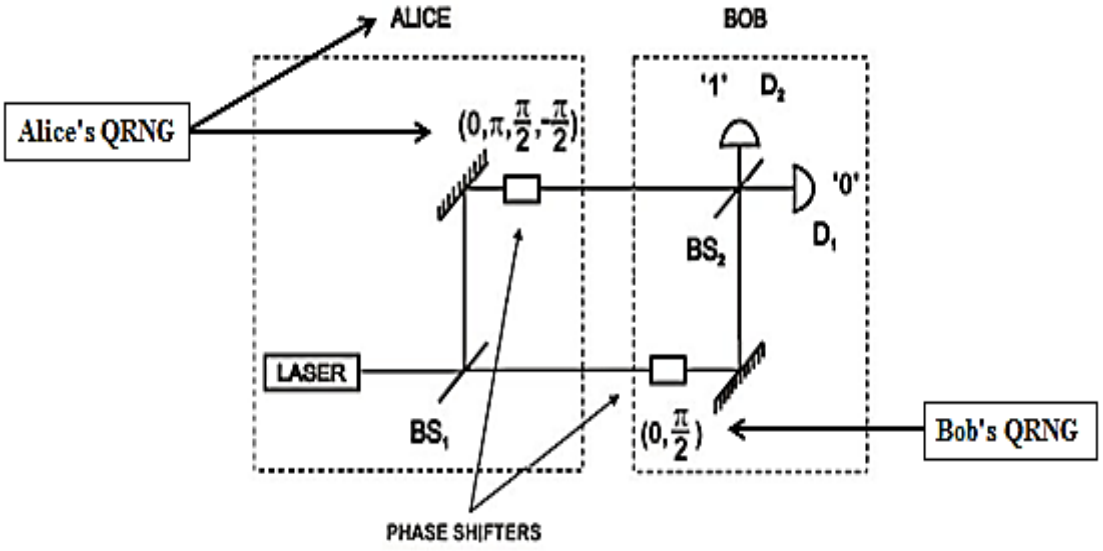
$$cos\alpha - cos\beta = -2sin\frac{\alpha+\beta}{2}\,sin\frac{\alpha-\beta}{2}$$

بنابراین می توان احتمال آشکارسازی فوتون در D_1 را به صورت زیر بدست آورد:

$$P(D_1) = \frac{1}{2}(1 + \cos(\phi_A - \phi_B)) = cos^2\left(\frac{\phi_A - \phi_B}{2}\right) \quad (۶)$$

و به طریق مشابه، احتمال آشکارسازی فوتون در D_2 برابر است با:

$$P(D_2) = \frac{1}{2}(1 - \cos(\phi_A - \phi_B)) = sin^2\left(\frac{\phi_A - \phi_B}{2}\right) \quad (۷)$$



شکل ۴. شمای اجرای پروتکل BB84 فازی، با استفاده از یک تداخل‌سنج ماخ- زنر متوازن [۵].

براساس آن‌چه گفته شد، می‌توان قراردادهای مربوط به انتخاب پایه‌های اندازه‌گیری توسط آلیس و باب، انتخاب فاز، تعریف بیت‌های "0" و "1" با توجه به آشکارسازی فوتون‌ها در D_1 یا D_2 و نحوه‌ی تولید کلید خصوصی در پروتکل BB84، در حالت کدگذاری روی فاز فوتون‌ها را در جدولی به‌صورت زیر خلاصه کرد:

جدول ۲. قراردادهای بین آلیس و باب در پروتکل BB84 و در حالت کدگذاری روی فاز فوتون‌ها [۵].

قراردادهای آشکارسازی			قراردادهای باب		قراردادهای آلیس		
Detectors	Bits	Phase Differences ($\Delta\phi$)	Bob's Bases	Bob's Phases (ϕ_B)	Encoded Bits / Alice's Bases	0	1
D_1	"0"	0	0	0	0	0	π
D_2	"1"	π	1	$\pi/2$	1	$\pi/2$	$3\pi/2$

اکنون می‌توان اجرای پروتکل BB84 مبتنی بر فاز و تولید یک کلید کوانتومی خصوصی با کمک آن‌را با توجه به قراردادهای بیان شده بین آلیس و باب، به‌صورت زیر توضیح داد [۵]:

وقتی تغییر فاز نسبی اعمال شده توسط تداخل‌سنج‌ها 0 یا π است، فوتون در بازوی مشخص و معینی از جفت کننده‌ی فیبری[1] (FC) باب دیده خواهد شد؛ زیرا این تغییر فازها با همان فریزهای کلاسیک تاریک و روشن در پدیده‌های تداخل‌سنجی مطابقت دارند. اما برای تغییر فازهای نسبی $\pi/2$ یا $3\pi/2$، فوتون می‌تواند با احتمال ۵۰:۵۰ وارد هر یک از بازوهای FC شود و بنابراین اندازه‌گیری‌های باب می‌تواند مقادیر 0 یا 1 را با احتمال یکسان بدست آورد. این حالت معادل فوتونی است که با زاویه‌ی قطبش $45°$ وارد یک PBS می‌شود و می‌تواند به هرکدام از آشکارسازها برسد.

نمونه‌ای از اجرای پروتکل BB84 در حالت کدگذاری روی فاز اپتیکی در شکل ۱ آورده شده است. داده‌های ستون اول این جدول به‌وسیله‌ی یک QRNG ایجاد و در اختیار آلیس قرار می‌گیرد. داده‌های ستون‌های دوم و پنجم (به ترتیب

[1] Fiber Coupler (FC)

گام‌های دوم و چهارم) نیز توسط دو QRNG تولید و بطور جداگانه در اختیار آلیس و باب قرار می‌گیرند. فازهای انتخاب شده در ستون سوم، با توجه به داده‌های ستون‌های اول و دوم و با مراجعه به جدول انتخاب می‌شوند. ستون ششم هم با توجه به اختلاف فازهای اعمال شده توسط آلیس و باب برای هر یک از فوتون‌ها نوشته می‌شود. در نهایت، داده‌های ستون هفتم که بخشی از بیت‌های کلید را تشکیل می‌دهند با توجه به آشکارسازی در D_1 یا D_2 تعیین می‌شوند.

Alice			Bob		Detection	
Encoded Bit	Base	ϕ_A	ϕ_B	Base	$\Delta\phi$	Decoded Bit
Step1	Step2	Step3	Step5	Step4	Step6	Step7
1	0	π	0	0	π	1
0	1	$\pi/2$	$\pi/2$	1	0	0
0	1	$\pi/2$	0	0	$\pi/2$	1 or 0
1	0	π	0	0	π	1
0	0	0	$\pi/2$	1	$\pi/2$	1 or 0
1	1	$3\pi/2$	$\pi/2$	1	π	1
1	1	$3\pi/2$	0	0	$3\pi/2$	1 or 0
0	0	0	$\pi/2$	1	$\pi/2$	1 or 0

Alice's QRNG

Bob's QRNG

شکل ۱. اجرای پروتکل BB84 در حالت کد گذاری روی فاز فوتون‌ها. اعداد پررنگ متمایز شده در گام‌های ۲ و ۴ به مفهوم انتخاب پایه‌های یکسان توسط آلیس و باب هستند [۶].

۳.بحث و نتیجه گیری

به طور خلاصه موارد زیر را در خصوص کاربرد مولدهای تصادفی کوانتومی در سامانه‌های رمزنگاری کوانتومی بیان می‌شود:

۱- در سامانه های رمزنگاری کوانتومی (از جمله سامانه های QKD)، به هنگام انتقال پیام های محرمانه، از اعداد تصادفی به عنوان هسته برای تولید کلید استفاده می شود. قدرت این کلیدها به تصادفی بودن هسته ی ورودی بستگی دارد.

۲- در حال حاضر، عمدتاً از مولد اعداد شبه تصادفی (PRNG) استفاده می‌شود که اساساً یک الگوریتم مبتنی بر نرم‌افزار است که از یک عدد هسته شروع کرده، مقادیر تصادفی بعدی را از این عدد تولید و سپس به اعداد تصادفی تبدیل می‌کند. هسته ی نرم افزار می تواند تاریخ، دما، فشار یا هر ورودی قطعی (معین و غیراحتمالاتی) دیگر باشد که به یک الگوریتم داده می‌شود و این الگوریتم، ورودی معین را با کمک یک فرمول ریاضیاتی، تصادفی می کند. اعداد شبه تصادفی همانطور که از نامشان پیداست، تنها دارای تقریبی از تصادفیت هستند. اگر یک مهاجم، الگوریتم مورد استفاده برای تولید آن ها را بداند، می تواند آنها را مهندسی معکوس کند.

۳- در مقابل PRNG، مولد اعداد تصادفی واقعی (TRNG) وجود دارد که از ورودی‌های مبتنی بر سخت‌افزار برای ایجاد مقادیر تصادفی استفاده می‌کند. TRNG ها خود به دو دسته کلاسیک و کوانتومی تقسیم می شوند. در TRNG های

کلاسیک، از ورودی هایی که عموماً فرآیندهای فیزیک کلاسیک مانند نویز بهمنی، نویز حرارتی یا نویز اتمسفر هستند برای تولید اعداد تصادفی استفاده می شود. این نویزها ابتدا به سیگنال‌های الکترونیکی و سپس به سیگنال‌های دیجیتال تبدیل می‌شوند و در نهایت بیت‌های تصادفی را به وجود می‌آورند. اما این فرآیندها نیز در واقع کاملاً تصادفی نیستند. اگر مهاجم بداند که از کدام پدیده طبیعی استفاده شده و برخی از الگوهای زیربنایی مربوط به آن پدیده را نیز درک کند، می‌تواند به کمک هوش مصنوعی رمزگذاری انجام شده با این اعداد تصادفی را بشکند. این آسیب‌پذیری می‌تواند هم اکنون، حتی بدون اینکه مهاجم نیازی به استفاده از یک کامپیوتر کوانتومی داشته باشد، مورد سوء استفاده قرار گیرد. بسیاری از کارشناسان حدس می‌زنند که فقدان تصادفی بودن واقعی ممکن است یکی از راه‌هایی باشد که آژانس امنیت ملی[1] (NSA) وزارت دفاع ایالات متحده آمریکا، بر اساس افشاگری های ادوارد اسنودن[2]، رمزگذاری بسیاری از ارتباطات دیجیتال را شکسته است.

۴- بنابراین PRNG و TRNG های کلاسیک به دلیل قابل پیش بینی بودن آسیب پذیر هستند. برای مقابله با این مشکل، از TRNG های کوانتومی (QRNG) استفاده می‌شود. این مولدها با استفاده از ویژگی‌های ذاتی فیزیک کوانتومی - مانند مشاهده اسپین یک ذره زیر اتمی که در یک حالت کوانتومی قرار دارد- در تولید آنتروپی، اعداد کاملاً تصادفی در اختیار کاربر قرار می‌دهند که غیرقابل پیش‌بینی هستند. به عنوان نمونه، در مثال استفاده از اسپین، هیچ راهی برای پیش‌بینی اسپین ذره، قبل از لحظه‌ای که ذره در آن مشاهده می‌شود وجود ندارد.

۱۲. مراجع

[1] G. Brassard, **Quantum cryptography: public key distribution and coin tossing,** in: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (1984) 175–179.

[2] M. Fox, **Quantum Optics An Introduction**, first edidition, Oxford University Press, (2006).

[3] P.D. Townsend, J.G. Rarity, and P.R. Tapster, **Single Photon Interference in 10 km Long Optical Fibre Interferometer,** Electronics Letters 29 (1993) 634-635.

[4] C. Marand and P.D. Townsend, **Quantum key distribution over distances as long as 30 km,** Optics Letters 20 (1995) 1695-1697.

[5] M. Hendrych, **Experimental Quantum Cryptography,** Doctoral Thesis, Palack'y University, Olomouc, Czech Republic (2002).

[6] L.L. Huang, **Long-Distance Quantum Key Distribution over Telecom Fiber,** Master of Applied Science, Graduate Department of Electrical & Computer Engineering, University of Toronto (2006).

[7] V. Kalaivani, **Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications.** *Personal and Ubiquitous Computing* 27.3 (2023): 875.

[8] S. Fauzia, **Quantum Cryptography**. *Evolution and Applications of Quantum Computing* (2023): 233-248.

[1] National Security Agency (NSA)
[2] Edward Snowden