نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۱، بهار ۱۴۰۰، ص ۱۳۶-۱۲۵

علمی – پژوهشی

# شکل تعمیم‌یافته پروتکل توزیع کلید کوانتومی BB84 با $n$ پایه قطبش و احتمال‌های نابرابر

آریس آقانیانس[۱]، سید نصیب‌اله دوستی‌مطلق[۲*]

۱- نخبه وظیفه و ۲- استادیار، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

(دریافت: ۱۳۹۹/۰۲/۱۴، پذیرش: ۱۳۹۹/۰۸/۰۵)

## چکیده

توزیع کلید کوانتومی مسأله تولید و تبادل کلید بین طرفین رمزنگاری را با امنیت نامشروط که با اصول و پدیده‌های مکانیک کوانتومی تضمین می‌شود، حل می‌کند. در پیشینه چهل‌ساله رمزنگاری کوانتومی، پروتکل‌های توزیع کلید کوانتومی گوناگونی ابداع شده‌اند که معروف‌ترین آنها BB84 است و برخی دیگر همچون پروتکل‌های شش‌حالته و اردهالی-چائو-لو با اعمال تغییراتی روی آن به‌وجود آمده‌اند. در این مقاله، شکل کلی‌تری از BB84 با به‌کارگیری $2n$ حالت قطبش که $n$ جفت متعامد از حالت‌های قطبش و $n$ پایه قطبش را به‌وجود می‌آورند، ارائه می‌شود. افزون بر آن، فرض می‌شود پایه‌های قطبش متمایز با احتمال‌های لزوماً نابرابر انتخاب می‌شوند. سپس، با مطالعه و تحلیل پروتکل توزیع کلید کوانتومی جدید و دو حالت خاص آن از دیدگاه نظریه احتمال، این پروتکل‌ها با پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو مقایسه و سرانجام، با ساخت چهار مثال عددی گوناگون، نتایج به‌دست‌آمده از تحلیل‌ها تأیید می‌شوند. برتری پروتکل توزیع کلید کوانتومی جدید در مقایسه با پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو انعطاف‌پذیری بالای آن در انتخاب تعداد حالت‌های قطبش و چگونگی تخصیص احتمال روی انتخاب پایه‌های قطبش است. این برتری سبب می‌شود که با تحلیل پروتکل جدید و دو حالت خاص آن از دیدگاه نظریه احتمال، بتوان با آگاهی بیشتری پروتکل توزیع کلید کوانتومی مناسب را برای تحقق یک هدف مشخص انتخاب کرد و از مزایای آن بهره‌مند شد.

**کلیدواژه‌ها:** پروتکل BB84، فوتون، پایه قطبش، پروتکل $2n$ - حالته نایکنواخت.

## ۱- مقدمه

توزیع کلید کوانتومی[۱] مسأله تولید و تبادل کلید لازم برای اجرای یک الگوریتم رمزنگاری را با حفظ امنیت نامشروط (امنیتی که در آن مهاجم حتی با در اختیار داشتن منابع محاسباتی نامحدود، قادر به شکستن رمز نیست) که با اصول و پدیده‌های مکانیک کوانتومی تضمین می‌شود، حل می‌کند. چارلز هنری بنت و ژیلس براسارد [۱] با الهام از ایده‌های استیفن ویزنر [۲] در به‌کارگیری مکانیک کوانتومی برای تولید اسکناس‌های غیر قابل جعل، نخستین پروتکل توزیع کلید کوانتومی موسوم به BB84 را ابداع کردند. این پروتکل امروزه نیز به شکل گسترده استفاده می‌شود.

در BB84، طرفین رمزنگاری که در این مقاله آلیس و باب خوانده می‌شوند، برای تولید و توزیع کلید، تبادل تک‌فوتون‌ها را از طریق یک کانال کوانتومی[۲] (فیبر نوری یا فضای آزاد) انجام می‌دهند. بنابراین فوتون‌ها نقش حامل‌های کوانتومی را ایفا می‌کنند و حالت‌های قطبش آنها وظیفه رمزگذاری کیوبیت‌ها را بر عهده دارند.

پیش از اجرای BB84، آلیس و باب چهار حالت قطبش مجاز را که از دید آنها قابل قبول هستند، برای رمزگذاری کیوبیت‌ها توافق می‌کنند. منظور از چهار حالت قطبش مجاز، دو جفت متشکل از دو حالت قطبش متعامد است که دو قطبش را ایجاد می‌کنند. برای مثال، حالت‌های قطبش متعامد افقی و عمودی و حالت‌های قطبش متعامد ۴۵ درجه و ۱۳۵ درجه که به‌ترتیب پایه‌های قطبش افقی و قطری را به‌وجود می‌آورند، چهار حالت قطبش مجاز هستند. آلیس و باب به‌طور توافقی، یک حالت قطبش از هر پایه قطبش را به مقدار صفر و دیگری را به مقدار یک نسبت می‌دهند.

برای تبادل کلید خام[۳]، آلیس به هر کیوبیت، فوتونی را که حالت قطبش آن به‌طور تصادفی از میان چهار حالت قطبش توافق‌شده انتخاب می‌شود، نسبت می‌دهد. در واقع، وی برای هر فوتون، به‌طور تصادفی یک پایه قطبش موسوم به پایه قطبش‌گر

* رایانامه نویسنده مسئول: Doustimotlagh@Elenoon.Ir

[1] Quantum Key Distribution
[2] Quantum Channel
[3] Raw Key Exchange

از بین پایه‌های قطبش توافق‌شده انتخاب و پس از قطبیده کرده فوتون، آن را از طریق یک کانال کوانتومی (فیبر نوری یا فضای آزاد) به باب می‌فرستد. آلیس حالت‌های قطبش فوتون‌های ارسالی و پایه‌های قطبش‌گر انتخابی خود را به‌ترتیب در فهرستی یادداشت می‌کند. در سوی مقابل، باب فوتون‌های دریافتی را یکی پس از دیگری از پایه‌های قطبشی موسوم به پایه‌های اندازه‌گیر که باز هم به‌طور تصادفی از بین پایه‌های قطبش توافق‌شده انتخاب می‌شوند، عبور می‌دهد و نتایج آشکارسازی و پایه‌های اندازه‌گیر انتخابی خود را به‌ترتیب فهرست می‌کند.

برای غربال کلید، باب پایه‌های اندازه‌گیر خود را به‌ترتیب از طریق یک کانال کلاسیک (خطوط تلفن یا اینترنت) به آلیس اعلام می‌کند. آلیس پس از مقایسه آنها با فهرست خود، اختلافات موجود را از طریق همان کانال کلاسیک به باب گزارش می‌دهد. سرانجام، آلیس و باب با دور ریختن کیوبیت‌هایی که پایه‌های قطبش‌گر و اندازه‌گیر فوتون حامل آنها یکسان نیستند، به کلید غربال‌شده[1] دست می‌یابند.

لازم به تذکر است که در پیاده‌سازی عملی BB84، انتخاب تصادفی پایه‌های قطبش‌گر و اندازه‌گیر مسأله‌ای بسیار ظریف و حساس است و برای به واقع تصادفی شدن پروتکل، بهتر است پایه‌های قطبش‌گر و اندازه‌گیر با فرایندهایی به‌طور کامل تصادفی و مستقل از هم انتخاب شوند. به این ترتیب، چون انتخاب پایه‌های قطبش‌گر و اندازه‌گیر پیشامدهایی مستقل هستند، پس بنابر قانون احتمال کل، احتمال اینکه پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون یکسان باشند، برابر $(\frac{۱}{۲})^۲+(\frac{۱}{۲})^۲=\frac{۱}{۲}$ است، یعنی به‌طور میانگین، نیمی از کیوبیت‌های ارسالی آلیس در مرحله غربال کلید دور ریخته می‌شوند [۳]. بنابراین، اگر آلیس $m$ فوتون بفرستد و متغیر تصادفی $X$ بیانگر تعداد فوتون‌هایی باشد که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به آنها یکسان هستند، آن‌گاه $X$ از توزیع برنولی پیروی می‌کند و از این‌رو،

$$P(X=k)=\frac{C(m,k)}{۲^m} \quad k=۰,\dots,m \qquad (۱)$$

که در آن، $C(m,k)=\frac{m!}{(m-k)!k!}$ بیانگر انتخاب $k$ شیء از $m$ شیء است.

باید توجه داشت که پیش از اجرای BB84، آلیس و باب هیچ اطلاعی از کلیدهای خام و غربال‌شده ندارند و کلید به‌طور خودکار و هم‌زمان با اجرای پروتکل ساخته شود. بنابراین انتظار طبیعی آن است که میانگین درصد نرخ خطای کلید خام[2] دریافتی باب حدود ۲۵٪ باشد، زیرا در کنار نیمی از فوتون‌ها که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به آنها یکسان هستند، به‌طور میانگین، نیمی از فوتون‌های دیگر نیز پس از اندازه‌گیری با پایه قطبش نادرست، مقدار کیوبیت را درست به‌دست می‌دهند [۳]. از سوی دیگر، اگر کانال کوانتومی مورد استفاده فاقد نویز و اتلاف باشد، دستگاه‌های آلیس و باب خطا نداشته باشند و پروتکل بدون حضور شنودگر[3] اجرا شود، آن‌گاه کلیدهای غربال‌شده آلیس و باب یکسان هستند و نیازی به تقطیر کلید[4] نیست. به بیان دیگر، در چنین شرایطی، نرخ خطای بیت کوانتومی[5] برابر صفر است. البته بدیهی است که در عمل، چنین حالت ایده‌آلی هرگز رخ نمی‌دهد.

پس از ابداع BB84، نویسندگان گوناگونی به قدرت مکانیک کوانتومی در تولید و توزیع کلیدهای به واقع امن برای رمزنگاری پی بردند و به مطالعه و تحقیق در توزیع کلید کوانتومی علاقه‌مند شدند. عده‌ای از آنان نیز تلاش کردند با ایجاد برخی تغییرات در BB84، پروتکل‌های توزیع کلید کوانتومی جدیدی را به‌وجود آورند. از مهم‌ترین این پروتکل‌ها، E91 [۴]، B92 [۵]، پروتکل گولدنبرگ-ویدمن [۶]، پروتکل شش‌حالته [۷ و ۸]، پروتکل اردهالی-چائو-لو [۹]، SARG04 [۱۰]، LM05 [۱۱]، K05 [۱۲]، K08 [۱۳]، S09 [۱۴] و S13 [۱۵] هستند. به تازگی، حسینی و دیگران [۱۶] نیز پژوهش ارزشمندی را در حوزه توزیع کلید کوانتومی انجام داده‌اند.

دو پروتکل زیر به همراه BB84 شالوده اصلی تحقیق حاضر را تشکیل می‌دهند:

در تحقیقاتی جداگانه، بروس [۷] و بچمان-پاسکینوچی و ژیسین [۸] به‌جای چهار حالت قطبش مجاز، شش حالت قطبش مجاز را برای رمزگذاری کیوبیت‌ها به‌کار گرفتند. در واقع، آنان فرض کردند آلیس و باب از سه پایه قطبش که هریک دارای دو حالت قطبش متعامد هستند، برای قطبیده کردن فوتون‌ها و اندازه‌گیری حالت‌های قطبش آنها استفاده می‌کنند. به این ترتیب، آنان پروتکل شش‌حالته[6] را ابداع کردند.

اردهالی، چائو و لو [۹] با همان چهار حالت قطبش مجاز BB84 کار کردند، با این تفاوت که آنان فرض کردند پایه‌های قطبش با احتمال‌های برابر انتخاب نمی‌شوند. در واقع، به بیان ریاضی، اگر احتمال انتخاب یک پایه قطبش برابر $a\in(۰,۱)$

[1] Sifted Key

[2] Average Of Raw Key Error Rate Percentage
[3] Eavesdropper
[4] Key Distillation
[5] Quantum Bit Error Rate (Qber)
[6] Six-State Protocol (Ssp)

باشد، آن‌گاه احتمال انتخاب پایه قطبش دیگر برابر $a-1$ است. به این ترتیب، آنان پروتکل توزیع کلید کوانتومی جدیدی ارائه دادند که در این مقاله پروتکل اردهالی-چائو-لو نامیده می‌شود.

ذکر این نکته ضروری است که در پروتکل شش‌حالته، چون آلیس و باب از سه پایه قطبش استفاده می‌کنند، پس احتمال اینکه باب بتواند پایه اندازه‌گیر خود را درست انتخاب کند، در مقایسه با BB84 کمتر است، یعنی در پروتکل شش‌حالته، به‌طور میانگین، کیوبیت‌های بیشتری در مرحله غربال کلید دور ریخته می‌شوند. اگرچه در نگاه اول، این مسئله شاید امتیازی منفی برای پروتکل شش‌حالته به شمار رود و سبب افزایش میانگین درصد نرخ خطای کلید خام دریافتی باب شود، اما در صورتی که پروتکل در حضور شنودگر اجرا شود، وجود سه پایه قطبش سبب می‌شود که شنودگر اطلاعات کمتری از کلید به‌دست آورد و دیدگاه منفی اولیه به پروتکل تغییر کند. بنابراین با توجه به میزان امنیت مورد نیاز و برآورد زمان و هزینه، می‌توان پروتکل توزیع کلید کوانتومی مناسب را از بین BB84 و شش‌حالته انتخاب کرد.

از سوی دیگر، همان‌گونه که در ادامه مقاله ثابت خواهد شد، در پروتکل اردهالی-چائو-لو، یکسان نبودن احتمال انتخاب دوپایه قطبش سبب می‌شود احتمال اینکه باب بتواند پایه اندازه‌گیر خود را درست انتخاب کند، در مقایسه با BB84 افزایش یابد. به بیان دیگر، در پروتکل اردهالی-چائو-لو، به‌طور میانگین، کیوبیت‌های کمتری در مرحله غربال کلید دور ریخته می‌شوند. به این ترتیب، در پروتکل اردهالی-چائو-لو، میانگین درصد نرخ خطای کلید خام دریافتی باب در مقایسه با BB84 کمتر است که امتیازی مثبت برای آن به شمار می‌رود. با وجود این، اگر شنودگر از چگونگی تخصیص احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر آگاهی داشته باشد، اطلاعات بیشتری از کلید به‌دست می‌آورد.

به این ترتیب، اگر شنودگر از حمله‌ای موسوم به راهبرد برش-بازارسال[1] استفاده کند (صفحه ۱۵۰ از مرجع [۳] را ببینید)، بیشترین اطلاعات را از کلید در پروتکل اردهالی-چائو-لو به‌دست می‌آورد. همچنین، اطلاعات او از کلید در BB84 در مقایسه با پروتکل شش‌حالته بیشتر است. بنابراین امنیت پروتکل شش‌حالته از دیدگاه به‌دست آوردن اطلاعات کلید بیشتر از BB84 و امنیت BB84 نیز از همین دیدگاه بیشتر از پروتکل اردهالی-چائو-لو است. در نتیجه، از جنبه امنیتی، پروتکل شش‌حالته به BB84 و BB84 به پروتکل اردهالی-چائو-لو برتری دارد.

در سوی مقابل، چون در پروتکل اردهالی-چائو-لو در مقایسه با BB84 ، به‌طور میانگین، کیوبیت‌های کمتری در مرحله غربال کلید دور ریخته می‌شوند، پس دست‌یابی به کلیدی با یک طول از پیش تعیین‌شده نیازمند تبادل تعداد کمتری فوتون در مرحله تبادل کلید خام است. این امر سبب کاهش زمان اجرای پروتکل می‌شود و به دنبال آن، از میزان کارکرد و استهلاک تجهیزات و سخت‌افزارهای کوانتومی مورد استفاده می‌کاهد. به‌طور مشابه، چون به‌طور میانگین، تعداد کیوبیت‌های دور ریخته‌شده در مرحله غربال کلید در BB84 در مقایسه با پروتکل شش‌حالته کمتر است، پس دست‌یابی به کلیدی با یک طول از پیش تعیین‌شده نیازمند تبادل تعداد کمتری فوتون در مرحله تبادل کلید خام است. در نتیجه، از جنبه اقتصادی، برتری بر عکس است، یعنی پروتکل اردهالی-چائو-لو به BB84 و BB84 به پروتکل شش‌حالته برتری دارد.

این مقاله از چهار قسمت تشکیل شده است: در قسمت یکم، همان‌گونه که مشاهده شد، سازوکار پروتکل توزیع کلید کوانتومی BB84 (به‌عنوان اساس این تحقیق) به شکل کوتاهی یادآوری و پیرامون آن و دو شکل تغییریافته‌اش موسوم به پروتکل‌های شش‌حالته و اردهالی-چائو-لو بحث می‌شود؛ در قسمت دوم، روش تحقیق، یعنی طرح مسئله، اهداف، اهمیت و ضرورت، پرسش‌ها و روش انجام تحقیق بیان می‌شوند؛ در قسمت سوم، یافته‌های تحقیق شامل صورت‌بندی پروتکل $2n$-حالته نایکنواخت، مطالعه و تحلیل آن از دیدگاه نظریه احتمال و بررسی دو حالت خاص آن ارائه می‌شوند. همچنین، یافته‌ها با ساخت چهار مثال عددی تأیید می‌شوند؛ سرانجام، این مقاله با یک نتیجه‌گیری و جمع‌بندی در قسمت چهارم به پایان می‌رسد.

## ۲- روش تحقیق

### ۲-۱- طرح مسئله

پس از مرور کلی پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو، یک مسأله مهم این است که ایده‌های پروتکل‌های شش‌حالته و اردهالی-چائو-لو به‌طور هم‌زمان روی BB84 اعمال شوند و در صورت امکان، این ایده‌ها از آن نیز فراتر روند. سپس، پروتکل توزیع کلید کوانتومی جدید و دو حالت خاص آن از دیدگاه نظریه احتمال مطالعه و از جنبه‌های اقتصادی و امنیتی با یکدیگر و با سه پروتکل BB84، شش‌حالته و اردهالی-چائو-لو مقایسه شوند.

[1] Intercept-Resend Strategy

بنابراین مسأله‌ای که این مقاله به دنبال حل آن است، صورت‌بندی و تحلیل یک شکل تعمیم‌یافته BB84 با $n$ پایه قطبش است که در آن احتمال انتخاب پایه‌های قطبش به‌عنوان یک پایه قطبش‌گر یا اندازه‌گیر لزوماً یکسان نیستند.

## ۲-۲- اهداف تحقیق

در این تحقیق، ایده‌های کلی‌تری از پروتکل‌های شش‌حالته و اردهالی-چائو-لو به‌طور هم‌زمان روی BB84 اعمال می‌شوند و این ایده‌ها از این سه پروتکل توزیع کلید کوانتومی نیز فراتر می‌روند. به بیان دقیق‌تر، رمزگذاری کیوبیت‌ها با $2n$ حالت قطبش مجاز ($n \geq 2$) انجام می‌شود و افزون بر آن، بر خلاف پروتکل اردهالی-چائو-لو، فرض می‌شود احتمال انتخاب یک پایه قطبش مشخص به‌عنوان پایه قطبش‌گر با احتمال انتخاب همان پایه قطبش به‌عنوان پایه اندازه‌گیر لزوماً برابر نیست. به این ترتیب، پروتکل توزیع کلید کوانتومی جدیدی پدید می‌آید که پروتکل $2n$-حالته نایکنواخت نامیده می‌شود. سپس، به کمک نظریه احتمال، پروتکل $2n$-حالته نایکنواخت و دو حالت خاص آن به نام‌های پروتکل $2n$-حالته نایکنواخت همگن و پروتکل $2n$-حالتِ از جنبه‌های اقتصادی و امنیتی با یکدیگر و با پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو مقایسه و در این باره بحث می‌شود. برای دست‌یابی به این اهداف، مسیر زیر پیموده می‌شود:

- صورت‌بندی پروتکل $2n$-حالته نایکنواخت؛
- به‌دست آوردن احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون و میانگین درصد نرخ خطای کلید خام دریافتی باب به کمک نظریه احتمال و بحث روی یافته‌ها؛
- صورت‌بندی حالت خاص یکم پروتکل $2n$-حالته نایکنواخت به نام پروتکل $2n$-حالته نایکنواخت همگن و مقایسه پروتکل‌های BB84 و اردهالی-چائو-لو از جنبه‌های اقتصادی و امنیتی به کمک آن؛
- صورت‌بندی حالت خاص دوم پروتکل $2n$-حالته نایکنواخت به نام پروتکل $2n$-حالتِ و تکمیل مقایسه‌ها؛
- ساخت چهار مثال عددی گوناگون برای تأیید یافته‌ها و مقایسه‌های انجام‌شده و اثبات مقایسه‌ناپذیری پروتکل $2n$-حالته نایکنواخت با دو حالت خاص آن از جنبه‌های اقتصادی و امنیتی.

لازم به تأکید است که پروتکل‌های $2n$-حالته نایکنواخت، $2n$-حالته نایکنواخت همگن و $2n$-حالتِ هر سه پروتکل BB84، شش‌حالته و اردهالی-چائو-لو را تعمیم می‌دهند. افزون بر آن، پروتکل $2n$-حالتِ شکل کلی‌تر پروتکل‌های BB84 و شش‌حالته نیز هست.

## ۲-۳- اهمیت و ضرورت انجام تحقیق

انجام تحقیق حاضر برای تحقق اهداف گفته‌شده در قسمت گذشته از دو جنبه اهمیت دارد: یکم، جنبه عام؛ و دوم، جنبه خاص. از جنبه عام، چون توزیع کلید کوانتومی امنیت نامشروط را به رمزنگاری کلاسیک هدیه می‌دهد، پس برای ارضای اصل دوم کرکهوفس، تحقیق در این شاخه از اهمیت ویژه‌ای برخوردار است. افزون بر آن، هرچه تعداد پروتکل‌های توزیع کلید کوانتومی ابداع‌شده و شناخته‌شده بیشتر باشد، دستان آلیس و باب برای تولید و توزیع کلید با امنیت نامشروط و به دنبال آن، اجرای امن یک الگوریتم رمزنگاری بازتر خواهد بود.

از جنبه خاص، ایده به‌کاررفته در این تحقیق به شکل جدید و کلی‌تری از پروتکل BB84 به نام پروتکل $2n$-حالته نایکنواخت می‌انجامد که افزون بر BB84، پروتکل‌های شش‌حالته و اردهالی-چائو-لو را نیز تعمیم می‌دهد. بنابراین، با مطالعه پروتکل توزیع کلید کوانتومی جدید از دیدگاه نظریه احتمال، می‌توان به اطلاعات سودمندی پیرامون هر سه پروتکل BB84، شش‌حالته و اردهالی-چائو-لو نیز دست یافت و با آگاهی بیشتری پروتکل توزیع کلید کوانتومی مناسب را از میان انبوهی از پروتکل‌های موجود برای تحقق یک هدف مشخص انتخاب کرد و از مزایای فناورانه آن بهره‌مند شد. گفتنی است که این تحقیق تعدادی از پروتکل‌های توزیع کلید کوانتومی را تحت پوشش خود قرار می‌دهد.

از سوی دیگر، اگر این تحقیق انجام نشود، هرگز نمی‌توان به برتری پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو را از جنبه‌های اقتصادی و امنیتی نسبت به یکدیگر پی برد. این سبب می‌شود که محققان متعددی برای $n$های مختلف و با پیاده‌سازی ایده‌های گوناگون روی BB84، پروتکل‌های توزیع کلید کوانتومی فراوانی را صورت‌بندی کنند بدون آنکه ارتباط و همگرایی میان آنها برقرار شود. بنابراین تحقیق حاضر از این دیدگاه ضرورت دارد که میان تعدادی از پروتکل‌های توزیع کلید کوانتومی ابداع‌شده با الهام از BB84 ارتباط و همگرایی برقراری می‌کند.

## ۲-۴- پرسش‌های تحقیق

پرسش اصلی که این تحقیق قصد پاسخگویی به آن را دارد، به شکل زیر مطرح می‌شود:

*«چگونه می‌توان ایده‌های کلی‌تری از پروتکل‌های شش‌حالته و اردهالی-چائو-لو را به‌طور هم‌زمان روی* BB84 *اعمال کرد*

*و به یک پروتکل توزیع کلید کوانتومی جدید دست یافت که دسته‌ای از پروتکل‌های توزیع کلید کوانتومی را به‌طور هم‌زمان تعمیم می‌دهد؟»*

در کنار پرسش اصلی، این تحقیق در تلاش و تکاپوست که به سه پرسش فرعی زیر نیز پاسخ‌هایی درخور دهد:

۱- چگونه می‌توان به‌جای شش حالت قطبش مجاز در پروتکل شش‌حالته، از $2n$ حالت قطبش مجاز ($n \geq 4$) برای رمزگذاری کیوبیت‌ها استفاده کرد؟

۲- هریک از حالت‌های خاص پروتکل $2n$-حالته نایکنواخت کدام پروتکل‌های توزیع کلید کوانتومی را تعمیم می‌دهند؟

۳- از جنبه‌های اقتصادی و امنیتی، پروتکل $2n$-حالته نایکنواخت یا دست‌کم حالت‌های خاص آن به کدام‌یک از پروتکل‌های BB84، شش‌حالته یا اردهالی-چائو-لو برتری دارند؟

## ۲-۵- روش انجام تحقیق

تحقیق حاضر به روش کتابخانه‌ای انجام می‌شود و از نوع بنیادی است. در حقیقت، ابتدا با مراجعه به [۳]، پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو به همراه تحلیل‌های مربوط به آنها به‌طور دقیق مطالعه می‌شوند که این مطالعه به روش کتابخانه‌ای انجام می‌گیرد. سپس، با ایده‌پردازی و استفاده از نظریه احتمال، پروتکل توزیع کلید کوانتومی جدید و دو حالت خاص آن صورت‌بندی و تحلیل و مثال‌های عددی ملموسی برای آنها ارائه می‌شوند که بیانگر تحقیق از نوع بنیادی هستند.

## ۳- یافته‌ها

### ۳-۱- صورت‌بندی پروتکل $2n$-حالته نایکنواخت و مطالعه و تحلیل آن از دیدگاه نظریه احتمال

در این قسمت، با معرفی پروتکل $2n$-حالته نایکنواخت، به پرسش اصلی تحقیق به شکل مبسوطی پاسخ داده می‌شود.

پیش از اجرای پروتکل $2n$-حالته نایکنواخت، آلیس و باب $2n$ حالت قطبش مجاز ($n \geq 2$) را که از دید آنها قابل قبول هستند، برای رمزگذاری کیوبیت‌ها توافق می‌کنند. بدیهی است که منظور از $2n$ حالت قطبش مجاز، $n$ جفت متشکل از دو حالت قطبش متعامد است که $n$ پایه قطبش متمایز را ایجاد می‌کنند. مشابه BB84، آلیس و باب به‌طور توافقی، یک حالت قطبش از هر پایه قطبش را به مقدار صفر و دیگری را به مقدار یک نسبت می‌دهند. افزون بر آن، آلیس و باب می‌دانند که فرایندهای (مستقل و تصادفی) انتخاب پایه‌های قطبش‌گر و اندازه‌گیر به‌گونه‌ای هستند که احتمال انتخاب دوپایه قطبش متمایز لزوماً برابر نیست و حتی ممکن است از چگونگی تخصیص احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های خود نیز آگاهی نداشته باشند. به این ترتیب، در حالت کلی، فرض می‌شود تخصیص‌های احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب غیرهم‌شانس و غیریکسان هستند.

با استناد به اصول مکانیک کوانتومی، روشن است که اگر باب پایه اندازه‌گیر متناظر به یک فوتون را مشابه پایه قطبش‌گر از پیش انتخاب‌شده آلیس برگزیند، آن‌گاه حالت قطبش آن فوتون و به دنبال آن، مقدار کیوبیتی که حمل می‌کند، به درستی آشکار می‌شود. در غیر این صورت، بنابر ذات تصادفی مکانیک کوانتومی، فوتون مورد نظر به‌طور تصادفی و با احتمال‌های برابر ۵۰٪، یکی از حالت‌های قطبش پایه اندازه‌گیر باب را به خود می‌گیرد. در چنین شرایطی، بدیهی است که همه اطلاعات درباره آن فوتون و مقدار کیوبیتی که حمل می‌کند، از بین می‌رود.

مراحل تبادل کلید خام و غربال کلید در پروتکل‌های $2n$-حالته نایکنواخت و BB84 بسیار شبیه به هم هستند. یگانه تفاوت موجود آن است که در پروتکل $2n$-حالته نایکنواخت، پایه‌های قطبش‌گر و اندازه‌گیر به‌جای اینکه با احتمال‌های برابر از بین دوپایه قطبش موجود انتخاب شوند، با احتمال‌های لزوماً نابرابر از میان $n$ پایه قطبش توافق‌شده انتخاب می‌شوند. به‌این‌ترتیب، گام‌های اجرای پروتکل $2n$-حالته نایکنواخت به شرح زیر هستند:

۱- برای هر کیوبیت، آلیس فوتونی را که حالت قطبش آن به‌طور تصادفی از میان $2n$ حالت قطبش توافق‌شده انتخاب می‌شود، نسبت می‌دهد؛

۲- آلیس فوتون را با پایه قطبش مورد نظر موسوم به پایه قطبش‌گر قطبیده می‌کند و آن را از طریق یک کانال کوانتومی به باب می‌فرستد (تبادل کلید خام). انتخاب هر پایه قطبش‌گر از میان پایه‌های قطبش موجود با یک احتمال مشخص و مختص به خود صورت می‌گیرد؛

۳- آلیس حالت‌های قطبش فوتون‌های ارسالی و پایه‌های قطبش‌گر انتخابی خود را به‌ترتیب در فهرستی یادداشت می‌کند؛

۴- در سوی مقابل، باب هر فوتون دریافتی را با پایه قطبشی موسوم به پایه اندازه‌گیر که به‌طور تصادفی از میان $n$ پایه قطبش انتخاب می‌شود، اندازه‌گیری می‌کند. انتخاب هر پایه اندازه‌گیر از میان پایه‌های قطبش موجود با یک احتمال مشخص و مختص به خود صورت می‌گیرد؛

۵- باب پایه‌های اندازه‌گیر انتخابی و حالت‌های قطبش به‌دست‌آمده از اندازه‌گیری‌های خود را به‌ترتیب در فهرستی یادداشت می‌کند؛

۶- پس از تبادل تعداد زیادی فوتون، باب پایه‌های اندازه‌گیر انتخابی خود را از طریق یک کانال کلاسیک به آلیس اعلام می‌کند، ولی باب هرگز نتایج اندازه‌گیری‌های خود را آشکار نمی‌کند؛

۷- آلیس پایه‌های اندازه‌گیر انتخابی باب را با پایه‌های قطبش‌گر انتخابی خود مقایسه و ناسازگاری‌های موجود را از طریق همان کانال کلاسیک به باب اعلام می‌کند؛

۸- سرانجام، آلیس و باب همه کیوبیت‌هایی را که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به فوتون حامل آنها یکسان نیستند، از فهرست‌های خود دور می‌اندازند (غربال کلید).

پروتکل $2n$-حالته نایکنواخت به‌طور هم‌زمان هر سه پروتکل BB84، شش‌حالته و اردهالی-چائو-لو را تعمیم می‌دهد. همچنین، در حالت کلی انتظار می‌رود: یک، احتمال اینکه باب بتواند پایه اندازه‌گیر خود را درست انتخاب کند، در مقایسه با پروتکل‌های BB84 و شش‌حالته کمتر باشد؛ دو، در مرحله غربال کلید، کیوبیت‌های بیشتری در مقایسه با پروتکل‌های BB84 و شش‌حالته دور ریخته شوند؛ و سه، کلید خام دریافتی باب میانگین درصد نرخ خطای بیشتر از ۲۵٪ داشته باشد. گفتنی است که در حالت کلی، به سبب عدم آگاهی از چگونگی تخصیص احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر، امکان مقایسه این کمیت‌ها در پروتکل‌های اردهالی-چائو-لو و $2n$-حالته نایکنواخت وجود ندارد.

اکنون به کمک نظریه احتمال، پروتکل $2n$-حالته نایکنواخت تحلیل می‌شود تا گام‌هایی در راستای پاسخگویی به پرسش‌های فرعی تحقیق برداشته شوند. برای سهولت در انجام محاسبات ریاضی و بحث‌های مورد نیاز، از اینجا به بعد فرض کنید $n$ پایه قطبش توافق‌شده آلیس و باب با ترتیب دلخواهی چیده شده‌اند و این ترتیب در ادامه مقاله تغییر نمی‌کند. همچنین، فرض کنید برای هر $i=1,\dots,n$، احتمال اینکه آلیس پایه قطبش $i$ام را به‌عنوان پایه قطبش‌گر انتخاب کند، برابر $p_i$ و احتمال این‌که باب پایه قطبش $i$ام را به‌عنوان پایه اندازه‌گیر انتخاب کند، برابر $q_i$ است. بنابراین،

$$p_1,\dots,p_n,q_1,\dots,q_n\in[0,1],$$
$$\sum_{i=1}^{n}p_i=\sum_{i=1}^{n}q_i=1. \qquad (2)$$

لازم به تأکید است که آلیس و باب لزوماً از مقادیر $p_i$ ها و $q_i$ها بی‌خبرند و این مقادیر هیچ نقشی در صورت‌بندی پروتکل ندارند. یگانه هدف از معرفی آنها بررسی پروتکل $2n$-حالته نایکنواخت از دیدگاه نظریه احتمال است که مقایسه این پروتکل و حالت‌های خاص آن را با پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو فراهم می‌سازد.

ابتدا احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون محاسبه می‌شوند. برای این منظور، فرض کنید برای هر $i=1,\dots,n$، $A_i$ پیشامد آن است که آلیس پایه قطبش $i$ام را به‌عنوان پایه قطبش‌گر انتخاب کند و $B_i$ پیشامد آن است که باب پایه قطبش $i$ام را به‌عنوان پایه اندازه‌گیر انتخاب کند. در این صورت پیشامدهای $A_1$، ... و $A_n$ فضای نمونه‌ای انتخاب پایه قطبش‌گر آلیس را افراز می‌کنند و برای هر $i=1,\dots,n$، پیشامدهای $A_i$ و $B_i$ مستقل هستند. بنابراین اگر $E$ پیشامد یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون باشد، آن‌گاه بنابر قانون احتمال کل داریم

$$\begin{aligned}P(E)&=P(A_1)P(E\mid A_1)+\cdots+P(A_n)P(E\mid A_n)\\&=P(A_1)P(B_1\mid A_1)+\cdots+P(A_n)P(B_n\mid A_n)\\&=P(A_1)P(B_1)+\cdots+P(A_n)P(B_n)\\&=p_1q_1+\cdots+p_nq_n\\&=\sum_{i=1}^{n}p_iq_i. \qquad (3)\end{aligned}$$

توجه به این نکته ضروری است که عدد به‌دست‌آمده از رابطه اخیر برای $P(E)$ که برای سادگی با $p$ نشان داده می‌شود، به بازه $[0,1]$ تعلق دارد. در حقیقت، چون

$$\sum_{i=1}^{n}p_i=\sum_{i=1}^{n}q_i=1, \qquad (4)$$
$$p_i^2\le p_i,\ q_i^2\le q_i,$$
$$i=1,\dots,n,$$

پس بنابر نابرابری کوشی-شوارتس[1] داریم

$$\begin{aligned}0&\le\sum_{i=1}^{n}p_iq_i\\&\le\sqrt{\sum_{i=1}^{n}p_i^2}\times\sqrt{\sum_{i=1}^{n}q_i^2}\\&\le\sqrt{\sum_{i=1}^{n}p_i}\times\sqrt{\sum_{i=1}^{n}q_i}=1. \qquad (5)\end{aligned}$$

اکنون اگر آلیس $m$ فوتون بفرستد و متغیر تصادفی $X$ بیانگر تعداد فوتون‌هایی باشد که پایه‌های قطبش‌گر و اندازه‌گیر

[1] Cauchy-Schwarz Inequality

متناظر به آنها یکسان هستند، آن‌گاه $X$ از توزیع دوجمله‌ای با ثابت $p=\Sigma_{i=1}^{n} p_i q_i$ پیروی می‌کند و از این‌رو

$$P(X=k)=C(m,k)\,p^k(1-p)^{m-k} \quad k=0,\ldots,m. \quad (6)$$

سرانجام، برای به‌دست آوردن میانگین درصد نرخ خطای کلید خام دریافتی باب، توجه کنید که اگر پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون یکسان باشند، آن‌گاه حالت قطبش آن فوتون درست آشکار می‌شود و مقدار کیوبیت مربوطه نیز درست به‌دست می‌آید. در غیر این صورت، اگرچه پس از اندازه‌گیری، حالت قطبش فوتون تغییر می‌کند، اما بنابر ذات تصادفی مکانیک کوانتومی، به‌طور میانگین، نیمی از فوتون‌ها مقدار کیوبیت را درست به‌دست می‌دهند. به بیان دیگر، افزون بر کیوبیت‌هایی که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به فوتون حامل آنها یکسان هستند، در دو حالت زیر، یکسان نبودن این پایه‌ها سبب بروز خطا در کیوبیت‌ها نمی‌شود:

۱- فوتون با حالت قطبش متناظر به مقدار صفر که با پایه قطبش $i$ام قطبیده شده است، پس از اندازه‌گیری با پایه قطبش متمایز $j$ ام، حالت قطبشی از آن متناظر به مقدار صفر را پیدا کند؛

۲- فوتون با حالت قطبش متناظر به مقدار یک که با پایه قطبش $i$ام قطبیده شده است، پس از اندازه‌گیری با پایه قطبش متمایز $j$ ام، حالت قطبشی از آن متناظر به مقدار یک را پیدا کند.

بنابراین، به‌طور میانگین، فقط برای نیمی از کیوبیت‌هایی که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به فوتون حامل آنها یکسان انتخاب نمی‌شوند، خطا رخ می‌دهد. از این‌رو، میانگین درصد نرخ خطای کلید خام دریافتی باب برابر است با

$$e=\frac{1}{2}(1-p)\times 100$$

$$=[50\cdot(1-p)]=[50\cdot(1-\sum_{i=1}^{n} p_i q_i)] \quad (7)$$

که این مقدار با $p$ رابطه‌ای معکوس دارد، یعنی با افزایش $p$ مقدار $e$ کاهش و با کاهش $p$ مقدار $e$ افزایش می‌یابد.

به این ترتیب، پروتکل $2n$-حالته نایکنواخت صورت‌بندی شد و معلوم شد که این پروتکل تعمیم پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو است. سپس، به کمک نظریه احتمال، رابطه‌هایی برای محاسبه احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون و میانگین درصد نرخ خطای کلید خام دریافتی باب به‌دست آمد. در نتیجه، برای پرسش اصلی تحقیق پاسخی مبسوط ارائه شد.

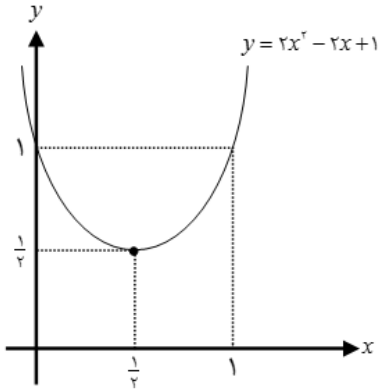
## ۳-۲- حالت خاص یکم: پروتکل $2n$-حالته نایکنواخت همگن

نخستین حالت خاص پروتکل $2n$-حالته نایکنواخت هنگامی است که تخصیص‌های احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب در حالت کلی، همچنان غیرهم‌شانس، ولی یکسان هستند، یعنی برای هر $i=1,\ldots,n$ داریم $p_i=q_i$. البته لازم به تأکید است که این برابری هرگز به معنای وابستگی فرایندهای (تصادفی) انتخاب پایه‌های قطبش‌گر و اندازه‌گیر نیست. این حالت خاص به پروتکل $2n$-حالته نایکنواخت همگن می‌انجامد. اگر افزون بر فرض انجام‌شده $n=2$ اختیار شود، آن‌گاه پروتکل چهارحالته نایکنواخت همگن به‌دست خواهد آمد که همان پروتکل اردهالی-چائو-لو است. بنابراین پروتکل $2n$-حالته نایکنواخت همگن پروتکل اردهالی-چائو-لو را تعمیم می‌دهد که پاسخی برای دومین پرسش فرعی تحقیق است.

در پروتکل $2n$-حالته نایکنواخت همگن، با توجه به روابط ریاضی به‌دست‌آمده درباره پروتکل $2n$-حالته نایکنواخت، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون برابر

$$p=\sum_{i=1}^{n} p_i q_i=\sum_{i=1}^{n} p_i^2 \quad (8)$$

است. به ویژه، این احتمال در پروتکل اردهالی-چائو-لو برابر $p=a^2+(1-a)^2=2a^2-2a+1$ خواهد بود. مطابق شکل (۱)، چون نقطه $(\frac{1}{2},\frac{1}{2})$ رأس سهمی به معادله $y=2x^2-2x+1$ است، پس $p$ در حالت $a=\frac{1}{2}$ کمترین مقدار خود را دارد، یعنی احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون در پروتکل اردهالی-چائو-لو در مقایسه با BB84 بیشتر است. بنابراین در پروتکل اردهالی-چائو-لو، کیوبیت‌های کمتری در مقایسه با BB84 در مرحله غربال کلید دور ریخته می‌شوند.




**شکل (۱):** نمودار سهمی به معادله $y=2x^2-2x+1$

از سوی دیگر، میانگین درصد نرخ خطای کلید خام دریافتی باب برابر $e=[۵۰(۱-\Sigma_{i=۱}^{n}p_i^۲)]$ است که میانگین درصد این نرخ را در پروتکل اردهالی-چائو-لو برابر

$$e=[۵۰(۱-(۲a^۲-۲a+۱))]=۱۰۰a(۱-a) \quad (۹)$$

به‌دست می‌دهد. چون مجموع $a$ و $۱-a$ برابر مقدار ثابت ۱ است، پس $e$ زمانی بیشترین مقدار ممکن را دارد که $a=۱-a$، یعنی $a=\frac{۱}{۲}$. بنابراین در پروتکل اردهالی-چائو-لو، میانگین درصد نرخ خطای کلید خام دریافتی باب در مقایسه با BB84 کمتر است.

در نتیجه، با تحلیل ساده یافته‌ها مشخص می‌شود که از جنبه اقتصادی، یعنی حفظ کیوبیت‌های ارسالی آلیس در مرحله غربال کلید، پروتکل اردهالی-چائو-لو به BB84 برتری دارد. به بیان دیگر، برای دست‌یابی به یک کلید با طول از پیش تعیین‌شده، پروتکل اردهالی-چائو-لو نیازمند ارسال فوتون‌های کمتری در مقایسه با BB84 است. بنابراین زمان اجرای پروتکل و میزان استهلاک تجهیزات و سخت‌افزارهای کوانتومی مورد استفاده نیز در مقایسه با BB84 کمتر است. با وجود این، از جنبه امنیتی، برتری از آن BB84 است چون شنودگر در صورت آگاهی از چگونگی تخصیص احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر، اطلاعات بیشتری از کلید به‌دست می‌آورد. به این ترتیب، سومین پرسش فرعی تحقیق در حالت خاص $n=۲$ پاسخ داده می‌شود.

با توجه به مقایسه‌های انجام‌شده، انتظار طبیعی آن است که در پروتکل $۲n$-حالته نایکنواخت، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون هنگامی کمترین مقدار ممکن را داشته باشد که $p_i$ ها و $q_i$ها همگی با هم برابر باشند. بدیهی است که در چنین شرایطی، میانگین درصد نرخ خطای کلید خام دریافتی باب بیشترین مقدار ممکن را خواهد داشت. این حالت خاص پروتکل $۲n$-حالته نایکنواخت در قسمت بعدی بحث می‌شود که می‌تواند پاسخ پرسش‌های فرعی تحقیق را به‌طور کامل روشن کند.

### ۳-۳- حالت خاص دوم: پروتکل $۲n$-حالتِ

برای توصیف و تشریح دیگر حالت خاص پروتکل $۲n$-حالته نایکنواخت که خود حالت خاصی از پروتکل $۲n$-حالته نایکنواخت همگن نیز هست، فرض کنید تخصیص‌های احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب هم‌شانس و یکسان هستند، یعنی

$$p_۱=\cdots=p_n=q_۱=\cdots=q_n=\frac{۱}{n}. \quad (۱۰)$$

روشن است که این حالت خاص معادل به‌کارگیری $۲n$ حالت قطبش مجاز به‌جای چهار یا شش حالت برای رمزگذاری کیوبیت‌هاست که به پروتکل $۲n$-حالتِ می‌انجامد. به این ترتیب، نخستین پرسش فرعی تحقیق نیز پاسخ داده می‌شود. به ویژه، اگر $n=۲$، آن‌گاه پروتکل $۲n$-حالتِ همان BB84 (پروتکل چهارحالته) و اگر $n=۳$، آن‌گاه پروتکل $۲n$-حالتِ همان پروتکل شش‌حالته است. بنابراین پروتکل $۲n$-حالته نایکنواخت هر دو پروتکل BB84 و شش‌حالته را تعمیم می‌دهد که پاسخ دومین پرسش فرعی تحقیق است.

در پروتکل $۲n$-حالتِ، با توجه به روابط ریاضی به‌دست‌آمده درباره پروتکل $۲n$-حالته نایکنواخت، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون برابر است با

$$p=\sum_{i=۱}^{n}p_iq_i=\sum_{i=۱}^{n}\frac{۱}{n^۲}=n\times\frac{۱}{n^۲}=\frac{۱}{n}. \quad (۱۱)$$

این رابطه نشان می‌دهد با افزایش جفت حالت‌های قطبش متعامد که افزایش پایه‌های قطبش را به دنبال دارد، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون کاهش می‌یابد که البته امری طبیعی است. به ویژه، این احتمال در پروتکل‌های BB84 و شش‌حالته به‌ترتیب برابر $\frac{۱}{۲}$ و $\frac{۱}{۳}$ است، یعنی در پروتکل شش‌حالته، کیوبیت‌های بیشتری در مقایسه با BB84 در مرحله غربال کلید دور ریخته می‌شوند.

از سوی دیگر، اگر آلیس $m$ فوتون بفرستد و متغیر تصادفی $X$ بیانگر تعداد فوتون‌هایی باشد که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به آنها یکسان هستند، آن‌گاه $X$ از توزیع دوجمله‌ای با ثابت $p=\frac{۱}{n}$ پیروی می‌کند و از این‌رو

$$P(X=k)=C(m,k)(\frac{۱}{n})^k(۱-\frac{۱}{n})^{m-k}$$
$$=C(m,k)\frac{(n-۱)^{m-k}}{n^m} \quad k=۰,\ldots,m. \quad (۱۲)$$

به ویژه، این احتمال در پروتکل‌های BB84 و شش‌حالته به‌ترتیب برابر است با

$$P(X=k)=\frac{C(m,k)}{۲^m},$$
$$P(X=k)=C(m,k)\frac{۲^{m-k}}{۳^m}, \quad (۱۳)$$
$$k=۰,\ldots,m.$$

سرانجام، میانگین درصد نرخ خطای کلید خام دریافتی باب برابر $e=[\text{۵۰}(\text{۱}-\frac{\text{۱}}{n})]$ است. بنابراین با افزایش جفت حالت‌های قطبش متعامد، میانگین درصد این نرخ کاهش می‌یابد. به ویژه، میانگین درصد نرخ خطای کلید خام دریافتی باب در پروتکل‌های BB84 و شش‌حالته به‌ترتیب برابر ۲۵ و ۳۳/۳ درصد است.

اکنون که پروتکل $\text{۲}n$-حالتِ را به‌طور کامل شناسایی شد، این پروتکل با پروتکل $\text{۲}n$-حالته نایکنواخت همگن مقایسه می‌شود. مقایسه‌ای که در اینجا انجام خواهد شد، تعمیم مقایسه پروتکل‌های BB84 و اردهالی-چائو-لو است که پیشتر صورت گرفت.

ابتدا نشان داده می‌شود احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون در پروتکل $\text{۲}n$-حالتِ کمترین مقدار ممکن را دارد. برای این منظور، فرض کنید $\overline{p}$ میانگین $p_\text{۱}$، ... و $p_n$ در پروتکل $\text{۲}n$-حالته نایکنواخت همگن است. در این صورت $\overline{p}=\frac{\text{۱}}{n}\Sigma_{i=\text{۱}}^{n}p_i=\frac{\text{۱}}{n}$. بنابراین واریانس $p_\text{۱}$، ... و $p_n$ برابر است با

$$\sigma^\text{۲}=\frac{\text{۱}}{n}\sum_{i=\text{۱}}^{n}p_i^\text{۲}-\overline{p}^\text{۲}=\frac{p}{n}-\frac{\text{۱}}{n^\text{۲}}. \qquad (\text{۱۴})$$

چون $\sigma^\text{۲}\geq\text{۰}$، محاسبه‌ای ساده نشان می‌دهد که $p\geq\frac{\text{۱}}{n}$. از سوی دیگر، چون مقدار واریانس برای $p=\frac{\text{۱}}{n}$ برابر صفر است، پس $p$ هنگامی کمترین مقدار خود را دارد که $p_\text{۱}=\cdots=p_n=\overline{p}=\frac{\text{۱}}{n}$، یعنی هیچ تخصیص احتمال غیرهم‌شانس و غیریکسانی روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب نمی‌تواند $p$ را کمینه کند. بنابراین، هرچه پراکندگی $p_i$ ها بیشتر باشد، واریانس آنها و به دنبال آن، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون بیشتر خواهد بود. در نتیجه، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون در پروتکل $\text{۲}n$-حالته نایکنواخت همگن در مقایسه با پروتکل $\text{۲}n$-حالتِ بیشتر است.

شایان ذکر است که برای $\sigma^\text{۲}$ یک کران بالا می‌توان به‌دست آورد که شاید البته کوچکترین کران بالای آن نباشد، اما اطلاعات خوبی درباره $p_i$ ها و به دنبال آن، $p$ و $e$ به‌دست می‌دهد. در واقع، چون $p\leq\text{۱}$، پس

$$\sigma^\text{۲}=\frac{p}{n}-\frac{\text{۱}}{n^\text{۲}}\leq\frac{\text{۱}}{n}-\frac{\text{۱}}{n^\text{۲}}=\frac{n-\text{۱}}{n^\text{۲}}. \qquad (\text{۱۵})$$

چون مخرج کسر سمت راست همواره از صورت آن بیشتر است، پس $\sigma^\text{۲}\in[\text{۰},\text{۱})$. به ویژه، به کمک آزمون مشتق یکم می‌توان نشان داد $\sigma^\text{۲}\in[\text{۰},\frac{\text{۱}}{\text{۴}}]$. بنابراین شرط $\Sigma_{i=\text{۱}}^{n}p_i=\text{۱}$ سبب می‌شود که $p_i$ ها نتوانند «زیاد» پراکنده شوند و از این‌رو، با فرض ثابت بودن $n$، نباید انتظار داشت که تخصیص‌های احتمال غیرهم‌شانس و یکسان گوناگون روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب بتوانند مقادیر $p$ و $e$ را به‌طور چشمگیری تغییر دهند.

به هر حال، روشن است که هرچه $p$ بیشتر باشد، مقدار $e$ کمتر است و برعکس. بنابراین در پروتکل $\text{۲}n$-حالتِ که $p$ کمترین مقدار ممکن خود را دارد، $e$ به بیشترین مقدار ممکن خود می‌رسد. از این‌رو در پروتکل $\text{۲}n$-حالته نایکنواخت همگن، میانگین درصد نرخ خطای کلید خام دریافتی باب در مقایسه با پروتکل $\text{۲}n$-حالتِ کمتر است.

در نتیجه، با تحلیل ساده یافته‌ها مشخص می‌شود که انتظار طبیعی ما بیهوده و غیرمنطقی نبوده است. در واقع، برای هر عدد طبیعی $n\geq\text{۲}$، از جنبه اقتصادی، پروتکل $\text{۲}n$-حالته نایکنواخت همگن به پروتکل $\text{۲}n$-حالتِ برتری دارد. به بیان دیگر، برای دست‌یابی به یک کلید با طول از پیش تعیین‌شده، پروتکل $\text{۲}n$-حالته نایکنواخت همگن نیازمند ارسال فوتون‌های کمتری در مقایسه با پروتکل $\text{۲}n$-حالتِ است. بنابراین زمان اجرا و میزان استهلاک تجهیزات و سخت‌افزارهای کوانتومی مورد استفاده در پروتکل $\text{۲}n$-حالته نایکنواخت همگن نیز در مقایسه با پروتکل $\text{۲}n$-حالتِ کمتر است. با وجود این، از جنبه امنیتی، برتری از آن پروتکل $\text{۲}n$-حالتِ است چون شنودگر در صورت آگاهی از چگونگی تخصیص احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر، اطلاعات بیشتری از کلید به‌دست می‌آورد. به این ترتیب، سومین پرسش فرعی تحقیق نیز در حالت کلی پاسخ داده می‌شود.

با وجود این، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون در پروتکل $\text{۲}n$-حالته نایکنواخت با مقدار این احتمال در دو پروتکل دیگر در حالت کلی قابل مقایسه نیست. در حقیقت، اگر $p$، $p'$ و $p''$ به‌ترتیب نمایانگر این احتمال در پروتکل‌های $\text{۲}n$-حالته نایکنواخت، $\text{۲}n$-حالته

نایکنواخت همگن و $2n$-حالتِ باشند، آن‌گاه همواره $p'' \le p'$، اما هر سه حالت $p < p'' < p'$، $p' < p < p''$ و $p'' < p' < p$ ممکن است رخ دهند. جدول (۱) با دسته‌بندی نتایج این تحلیل، سه پروتکل $2n$-حالته نایکنواخت، $2n$-حالته نایکنواخت همگن و $2n$-حالتِ را با یکدیگر مقایسه می‌کند.

**جدول (۱):** مقایسه پروتکل‌های $2n$-حالته نایکنواخت، $2n$-حالته نایکنواخت همگن و $2n$-حالتِ

| دیدگاه مقایسه | پروتکل $2n$-حالته نایکنواخت | پروتکل $2n$-حالته نایکنواخت همگن | پروتکل $2n$-حالتِ |
|---|---|---|---|
| **تعداد حالت‌های قطبش فوتون‌ها** | $2n$ | $2n$ | $2n$ |
| **تعداد پایه‌های قطبش‌گر و اندازه‌گیر** | $n$ | $n$ | $n$ |
| **تخصیص احتمال روی انتخاب پایه‌های قطبش** | غیرهم‌شانس و غیریکسان | غیرهم‌شانس و یکسان | هم‌شانس و یکسان |
| **احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون** | $\sum_{i=1}^{n} p_i q_i$ | $\sum_{i=1}^{n} p_i^2$ | $\frac{1}{n}$ |
| **میانگین درصد نرخ خطای کلید خام دریافتی باب** | $50(1-\sum_{i=1}^{n} p_i q_i)$ درصد | $50(1-\sum_{i=1}^{n} p_i^2)$ درصد | $50(1-\frac{1}{n})$ درصد |
| **توزیع متغیر تصادفی بیانگر تعداد فوتون‌ها با فیلترهای یکسان** | دوجمله‌ای با پارامتر $\Sigma_{i=1}^{n} p_i q_i$ | دوجمله‌ای با پارامتر $\Sigma_{i=1}^{n} p_i^2$ | دوجمله‌ای با پارامتر $\frac{1}{n}$ |
| **نوع امنیت** | نامشروط | نامشروط | نامشروط |
| **رتبه از دیدگاه امنیتی** | غیر قابل بحث | ۲ | ۱ |
| **رتبه از دیدگاه اقتصادی** | غیر قابل بحث | ۱ | ۲ |

## ۳-۴- مثال‌های عددی

اکنون که پروتکل $2n$-حالته نایکنواخت و حالت‌های خاص آن به نام‌های پروتکل $2n$-حالته نایکنواخت همگن و پروتکل $2n$-حالتِ شرح داده، از دیدگاه نظریه احتمال مطالعه و تحلیل و برای پرسش‌های تحقیق پاسخ‌هایی درخور ارائه شدند، برای تأیید و تصدیق یافته‌ها، چهار مثال عددی ارائه می‌شوند.

در مثال یکم، فرض کنید $n = 4$ و تخصیص‌های احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب هم‌شانس و یکسان هستند، یعنی برای هر $i = 1,2,3,4$ داریم $p_i = q_i = \frac{1}{4}$. در این صورت پروتکل هشت‌حالته (حالت خاص دوم) به‌دست می‌آید که در آن از هشت حالت قطبش مجاز برای رمزگذاری کیوبیت‌ها استفاده می‌شود. همچنین، با توجه به روابط ریاضی به‌دست‌آمده داریم $p = \frac{1}{4}$ و $e = [50(\frac{1}{4})] \exists 3$. بنابراین همان‌گونه که انتظار می‌رفت، در پروتکل هشت‌حالته، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون و میانگین درصد نرخ خطای کلید خام دریافتی باب در مقایسه با هر دو پروتکل BB84 و شش‌حالته به‌ترتیب کمتر و بیشتر هستند. افزون بر آن، اگر آلیس شش فوتون بفرستد و متغیر تصادفی $X$ بیانگر تعداد فوتون‌هایی باشد که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به آنها یکسان هستند، آن‌گاه $X$ از توزیع دوجمله‌ای با ثابت $p = \frac{1}{4}$ پیروی می‌کند و داریم

$$P(X=۴)=C(۶,۴)(\frac{۱}{۴})^۴(\frac{۳}{۴})^۲=\frac{۱۳۵}{۴۰۹۶}\simeq ۰/۰۳. \quad (۱۶)$$

در مثال دوم، فرض کنید $n=۳$ و

$$p_۱=q_۱=\frac{۱}{۲},\quad p_۲=q_۲=\frac{۱}{۳},\quad p_۳=q_۳=\frac{۱}{۶}, \quad (۱۷)$$

یعنی تخصیص‌های احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب غیرهم‌شانس، ولی یکسان هستند (توجه داشته باشید که $p_۱+p_۲+p_۳=۱$). در این صورت پروتکل شش‌حالته نایکنواخت همگن (حالت خاص یکم) به‌دست می‌آید که در آن

$$p=p_۱^۲+p_۲^۲+p_۳^۲=\frac{۱}{۴}+\frac{۱}{۹}+\frac{۱}{۳۶}=\frac{۷}{۱۸} \quad (۱۸)$$

و $e=[۵۰(۱-\frac{۷}{۱۸})]\%\simeq ۳۰\%$. بنابراین همان‌گونه که انتظار می‌رفت، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون و میانگین درصد نرخ خطای کلید خام دریافتی باب در مقایسه با پروتکل شش‌حالته به‌ترتیب بیشتر و کمتر هستند. افزون بر آن، اگر آلیس شش فوتون بفرستد و متغیر تصادفی $X$ بیانگر تعداد فوتون‌هایی باشد که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به آنها یکسان هستند، آن‌گاه $X$ از توزیع دوجمله‌ای با ثابت $p=\frac{۷}{۱۸}$ پیروی می‌کند و داریم

$$P(X=۴)=C(۶,۴)(\frac{۷}{۱۸})^۴(\frac{۱۱}{۱۸})^۲$$
$$=\frac{۱,۴۵۲,۶۰۵}{۱۱,۳۳۷,۴۰۸}\simeq ۰/۱۳. \quad (۱۹)$$

شایان ذکر است که چون $\sigma^۲=\frac{۱}{۵۴}$، پس پراکندگی $p_۱$، $p_۲$ و $p_۳$ نسبت به کران بالای $\frac{۱}{۴}$ چندان زیاد نیست و مقادیر $p$ و $e$ در مقایسه با مقادیر مشابه در پروتکل شش‌حالته اختلاف چندانی ندارند.

در مثال سوم، فرض کنید $n=۲$ و

$$p_۱=۲p_۲=\frac{۲}{۳},\quad q_۱=\frac{۲}{۷},\quad q_۲=\frac{۵}{۷}, \quad (۲۰)$$

یعنی تخصیص‌های احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب غیرهم‌شانس و غیریکسان هستند (توجه داشته باشید که $p_۱+p_۲=q_۱+q_۲=۱$). در این صورت پروتکل چهارحالته نایکنواخت به‌دست می‌آید که در آن:

$$p=p_۱q_۱+p_۲q_۲=\frac{۲}{۳}\times\frac{۲}{۷}+\frac{۱}{۳}\times\frac{۵}{۷}=\frac{۳}{۷} \quad (۲۱)$$

و $e=[۵۰(۱-\frac{۳}{۷})]\%\simeq ۲۸/۵۷\%$. بنابراین احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون و میانگین درصد نرخ خطای کلید خام دریافتی باب در مقایسه با BB84 به‌ترتیب کمتر و بیشتر هستند. افزون بر آن، اگر آلیس شش فوتون بفرستد و متغیر تصادفی $X$ بیانگر تعداد فوتون‌هایی باشد که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به آنها یکسان هستند، آن‌گاه $X$ از توزیع دوجمله‌ای با ثابت $p=\frac{۳}{۷}$ پیروی می‌کند و داریم

$$P(X=۴)=C(۶,۴)(\frac{۳}{۷})^۴(\frac{۴}{۷})^۲$$
$$=\frac{۱۹,۴۴۰}{۱۱۷,۶۴۹}\simeq ۰/۱۷. \quad (۲۲)$$

این مثال نشان می‌دهد که با نمادگذاری‌های انجام‌شده در پایان قسمت گذشته، نابرابری‌های $p<p''<p'$ امکان‌پذیر هستند.

سرانجام در مثال چهارم، فرض کنید $n=۶$،

$$p_i=\frac{i}{۲۱},\quad q_i=\frac{i+۱}{۲۷}\qquad i=۱,۲,۳,۴,۵,۶, \quad (۲۳)$$

یعنی تخصیص‌های احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب غیرهم‌شانس و غیریکسان هستند (توجه داشته باشید که $\Sigma_{i=۱}^۶ p_i=\Sigma_{i=۱}^۶ q_i=۱$). در این صورت پروتکل دوازده‌حالته نایکنواخت را به‌دست می‌آید که در آن

$$p=\sum_{i=۱}^۶ p_iq_i$$
$$=\frac{۱}{۲۱}\times\frac{۲}{۲۷}+\frac{۲}{۲۱}\times\frac{۳}{۲۷}+\frac{۳}{۲۱}\times\frac{۴}{۲۷}$$
$$+\frac{۴}{۲۱}\times\frac{۵}{۲۷}+\frac{۵}{۲۱}\times\frac{۶}{۲۷}+\frac{۶}{۲۱}\times\frac{۷}{۲۷}$$
$$=\frac{۱۶}{۸۱} \quad (۲۴)$$

و $e=[۵۰(۱-\frac{۱۶}{۸۱})]\%\simeq ۴۰\%$ ۷. افزون بر آن، اگر آلیس شش فوتون بفرستد و متغیر تصادفی $X$ بیانگر تعداد فوتون‌هایی باشد که پایه‌های قطبش‌گر و اندازه‌گیر متناظر به آنها یکسان هستند،

آن‌گاه $X$ از توزیع دوجمله‌ای با ثابت $p=\frac{۱۶}{۸۱}$ پیروی می‌کند و بنابراین احتمال رخداد آن برابر است با

$$P(X=۴)=C(۶,۴)(\frac{۱۶}{۸۱})^{۴}(\frac{۶۵}{۸۱})^{۲}$$
$$=\frac{۱,۳۸۴,۴۴۸,۰۰۰}{۹۴,۱۴۳,۱۷۸,۸۲۷}\simeq ۰/۰۱. \qquad (۲۵)$$

مثال چهارم تخصیص احتمال را روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر در سمت‌های آلیس و باب در پروتکل $۲n$-حالته نایکنواخت به خوبی توصیف می‌کند. افزون بر آن، با اعمال تغییرات جزئی در تخصیص‌های احتمال این مثال، امکان‌پذیری هر دو دسته نابرابری‌های $p''<p<p'$ و $p''<p'<p$ نیز ثابت می‌شوند. در واقع، اگر برای هر $i=۱,۲,۳,۴,۵,۶$ قرار دهیم $p_i=q_i=\frac{i}{۲۱}$، آن‌گاه $p'=\frac{۹۱}{۴۴۱}$ و چون $p=\frac{۱۶}{۸۱}$، پس $p''<p<p'$. از سوی دیگر، اگر برای هر $i=۱,۲,۳,۴,۵,۶$ قرار دهیم $p_i=q_i=\frac{i+۱}{۲۷}$، آن‌گاه $p'=\frac{۱۳۹}{۷۲۹}$ و باز هم با توجه به مقدار $p$ خواهیم داشت $p''<p'<p$. در نتیجه، در حالت کلی، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون در پروتکل $۲n$-حالته نایکنواخت با مقدار این احتمال در دو پروتکل دیگر قابل مقایسه نیست.

## ۴- نتیجه‌گیری

در تحقیق حاضر، ابتدا پروتکل $۲n$-حالته نایکنواخت که تعمیمی از پروتکل‌های BB84، شش‌حالته و اردهالی-چائو-لو است، صورت‌بندی و از دیدگاه نظریه احتمال مطالعه و تحلیل شد. در این پروتکل، از $۲n$ حالت قطبش مجاز استفاده می‌شود که $n$ پایه قطبش شامل آنها با احتمال‌های لزوماً نابرابر انتخاب می‌شوند. به بیان دیگر، به‌طور میانگین، فراوانی هریک از پایه‌های قطبش در فهرست‌های آلیس و باب لزوماً برابر نیست. سپس، با صورت‌بندی دو حالت خاص پروتکل $۲n$-حالته نایکنواخت به نام‌های پروتکل $۲n$-حالته نایکنواخت همگن و پروتکل $۲n$-حالتِ، فاز مقایسه آغاز و مشخص شد اگر پایه‌های قطبش با احتمال‌های نابرابر ولی همگن انتخاب شوند، تعداد کیوبیت‌های کمتری در مرحله غربال کلید دور ریخته می‌شوند. بنابراین این حالت از جنبه اقتصادی به‌صرفه‌تر است چون نیازمند تولید، قطبیده کردن و ارسال تعداد فوتون‌های کمتری است که به صرف زمان و انرژی کمتری نیاز دارد و تجهیزات و سخت‌افزارهای کوانتومی مورد استفاده را کمتر مستهلک می‌کند. با وجود این، شنودگر با آگاهی از چگونگی تخصیص احتمال روی انتخاب پایه‌های قطبش به‌عنوان پایه‌های قطبش‌گر و اندازه‌گیر، اطلاعات بیشتری از کلید به‌دست می‌آورد که از جنبه امنیتی یک اشکال به شمار می‌رود. در نتیجه، آلیس و باب با بررسی عواملی همچون سطح امنیت و محرمانگی مورد نیاز، میزان حساس بودن اطلاعات محرمانه، زمان و هزینه‌ی مجاز مصرفی برای اجرا و توان تجهیزات و سخت‌افزارهای کوانتومی مورد استفاده پروتکل توزیع کلید کوانتومی مناسب خود را انتخاب و بین جنبه‌های اقتصادی و امنیتی تعادل لازم را برقرار می‌کنند.

## ۵- مراجع


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

[2] S. Wiesner, "Conjugate coding," ACM SIGACT News, vol. 15, no. 1, pp. 78-88, 1983.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. of Mod. Phys., vol. 74, no. 1, pp. 145-195, 2002.

[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, no. 6, pp. 661-663, 1991.

[5] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., vol. 68, no. 21, pp. 3121-3124, 1992.

[6] L. Goldenberg and L. Vaidman, "Quantum cryptography based on orthogonal states," Phys. Rev. Lett., vol. 75, no. 7, pp. 1239-1243, 1995.

[7] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett., vol. 81, no. 14, pp. 3018-3021, 1998.

[8] H. Bechmann-Pasquinnuci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," Phys. Rev. A, vol. 59, no. 6, pp. 4238-4248, 1999.

[9] M. Ardehali, H. F. Chau, and H. -K. Lo, "Efficient quantum key distribution," arXiv:quant-ph/9803007v4, 1999.

[10] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett., vol. 92, no. 5, p. 057901, 2004.

[11] M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," Phys. Rev. Lett., vol. 94, no. 14, p. 140501, 2005.

[12] S. V. Kartalopoulos, "Link-layer vulnerabilities of quantum cryptography," Proceedings of the SPIE International Congress on Optics and Optoelectronics, pp. 111-118, 2005.

[13] S. V. Kartalopoulos, "K08: A generalized BB84/B92 protocol in quantum cryptography," Secur. Comm. Networks, vol. 2, pp. 686-693, 2008.

[14] E. E. Hernandez Serna, "Quantum key distribution protocol with private-public key," arXiv:0908.2146v4 [quant-ph], 2012.

[15] E. E. Hernandez Serna, "Quantum key distribution from a random seed," arXiv:1311.1582 [quant-ph], 2013.

[16] S. M. Hosseini, S. Janbaz, M. Davoudi Darareh, and A. Zaghian, "A new approach for estimating the rate of emission in quantum bit exchange systems using binomial distribution," Journal of Electronic & Cyber Defense, vol. 7, no. 1, pp. 105-112, 2019. (In Persian)

Journal of Electronical & Cyber Defence
Vol. 9, No. 1, 2021, Serial No. 33



# Generalized Version of the BB84 QKD Protocol with *n* Polarization Bases and Unequal Probabilities

A. Aghanians1, S. N. Doustimotlagh*

*Supreme National Defense University, Tehran, I. R. Iran

(Received: 04/03/2020, Accepted: 05/08/2020)

**ABSTRACT**

*Quantum key distribution (QKD) solves the problem of key generation and exchange between cryptography parties with unconditional security guaranteed by the principles and phenomena of quantum mechanics. In the 40-year old history of quantum cryptography, several QKD protocols have been invented of which, the BB84 protocol is the most famous one, and some others such as the six-state and Ardehali-Chau-Lo protocols have been created by making some variations of it. In this paper, a more general version of BB84 using 2n polarization states which create n orthogonal pairs of polarization states and n polarization bases is presented. In addition, it is assumed that distinct polarization bases are chosen with necessarily unequal probabilities. Then by studying and analyzing the new QKD protocol and its two special cases using the probability theory, they are compared with the BB84, six-state and Ardehali-Chau-Lo protocols and finally, the results are supported and confirmed by constructing four various numerical examples. The advantage of the new QKD protocol in comparison to the BB84, the six-state and Ardehali-Chau-Lo protocols is its high flexibility in choosing the number of polarization states and the manner of probability allocation on choosing the polarization bases. By analyzing the new protocol and its two special cases using the probability theory, this advantage causes better application of knowledge for a suitable QKD protocol selection in order to realize a certain goal and exploit its technological advantages.*

**Keywords:** BB84 Protocol, Photon, Polarization Basis, Non-uniform 2n-State Protocol

* Corresponding Author Email: doustimotlagh@elenoon.ir