

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

A. Aghanians<sup>1</sup>, S. N. Doustimotlagh<sup>\*</sup>

<sup>\*</sup>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](mailto:doustimotlagh@elenoon.ir)

علمی - پژوهشی

شکل تعمیم یافته پروتکل توزیع کلید کوانتومی BB84 با  $n$  پایه قطبش و احتمال های نابرابر

آریس آقانیانس<sup>۱</sup>، سید نصیب اله دوستی مطلق<sup>۲\*</sup>

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 پدیده های مکانیک کوانتومی تضمین می شود، حل می کند. در پیشینه چهار ساله رمزنگاری کوانتومی، پروتکل های توزیع کلید کوانتومی گوناگونی ابداع شده اند که معروف ترین آنها BB84 است و برخی دیگر همچون پروتکل های شش حالت و اردهالی-چائو-لو با اعمال تغییراتی روی آن به وجود آمده اند. در این مقاله، شکل کلی تری از BB84 با به کارگیری  $2n$  حالت قطبش که  $n$  جفت متعامد از حالت های قطبش و  $n$  پایه قطبش را به وجود می آورند، ارائه می شود. افزون بر آن، فرض می شود پایه های قطبش متمایز با احتمال های لزوماً نابرابر انتخاب می شوند. سپس، با مطالعه و تحلیل پروتکل توزیع کلید کوانتومی جدید و دو حالت خاص آن از دیدگاه نظریه احتمال، این پروتکل ها با پروتکل های BB84، شش حالت و اردهالی-چائو-لو مقایسه و سرانجام، با ساخت چهار مثال عددی گوناگون، نتایج به دست آمده از تحلیل ها تأیید می شوند. برتری پروتکل توزیع کلید کوانتومی جدید در مقایسه با پروتکل های BB84، شش حالت و اردهالی-چائو-لو انعطاف پذیری بالای آن در انتخاب تعداد حالت های قطبش و چگونگی تخصیص احتمال روی انتخاب پایه های قطبش است. این برتری سبب می شود 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 بهره مند شد.

کلیدواژه ها: پروتکل BB84، فوتون، پایه قطبش، پروتکل  $2n$  - حالت نایکناخت.

۱- مقدمه

می کنند و حالت های قطبش آنها وظیفه رمزگذاری کیوبیت ها 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 کیوبیت ها توافق می کنند. منظور از چهار حالت قطبش مجاز، دو جفت متشکل از دو حالت قطبش متعامد است که دو قطبش را ایجاد می کنند. برای مثال، حالت های قطبش متعامد افقی و عمودی و حالت های قطبش متعامد  $45^\circ$  درجه و  $135^\circ$  درجه که به ترتیب پایه های قطبش افقی و قطری را به وجود می آورند، چهار حالت قطبش مجاز هستند. آلیس و باب به طور توافقی، یک حالت قطبش از هر پایه قطبش را به مقدار صفر و دیگری را به مقدار یک نسبت می دهند.

برای تبادل کلید خام<sup>۳</sup>، آلیس به هر کیوبیت، فوتونی را که حالت قطبش آن به طور تصادفی از میان چهار حالت قطبش توافق شده انتخاب می شود، نسبت می دهد. در واقع، وی برای هر فوتون، به طور تصادفی یک پایه قطبش موسوم به پایه قطبش گر

توزیع کلید کوانتومی<sup>۱</sup> 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 پدیده های مکانیک کوانتومی تضمین می شود، حل می کند. چارلز هنری بنت و ژیلس براسارد [۱] با الهام از ایده های استیفن ویزنر [۲] در به کارگیری مکانیک کوانتومی برای تولید اسکناس های غیر قابل جعل، نخستین پروتکل توزیع کلید کوانتومی موسوم به BB84 را ابداع کردند. این پروتکل امروزه نیز به شکل گسترده استفاده می شود.

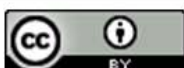
در BB84، طرفین رمزنگاری که در این مقاله آلیس و باب خوانده می شوند، برای تولید و توزیع کلید، تبادل تک فوتون ها را از طریق یک کانال کوانتومی<sup>۲</sup> (فیبر نوری یا فضای آزاد) انجام می دهند. بنابراین فوتون ها نقش حامل های کوانتومی را ایفا

\* رایانامه نویسنده مسئول: Doustimotlagh@Elenoon.Ir

<sup>1</sup> Quantum Key Distribution

<sup>2</sup> Quantum Channel

<sup>3</sup> Raw Key Exchange



طبیعی آن است که میانگین درصد نرخ خطای کلید خام<sup>۲</sup> 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<sup>۳</sup> اجرا شود، آن‌گاه کلیدهای غربال‌شده آلیس و باب یکسان هستند و نیازی به تقطیر کلید<sup>۴</sup> نیست. به بیان دیگر، در چنین شرایطی، نرخ خطای بیت کوانتومی<sup>۵</sup> 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 به‌واقع امن برای رمزنگاری پی‌برند 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، [۴] E91، [۵] B92، 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 ژسین [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<sup>۶</sup> 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  $a \in (0, 1)$

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 به ترتیب 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 به ترتیب فهرست می‌کند.

برای غربال کلید، باب پایه‌های اندازه‌گیر خود را به ترتیب 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<sup>۱</sup> 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 به‌واقع 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  $\frac{1}{2} = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2$  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،

$$P(X = k) = \frac{C(m, k)}{2^m} \quad k = 0, \dots, m \quad (1)$$

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 اطلاعاتی از کلیدهای خام و غربال‌شده ندارند و کلید به‌طور خودکار و هم‌زمان با اجرای پروتکل ساخته شود. بنابراین انتظار

<sup>2</sup> Average Of Raw Key Error Rate Percentage

<sup>3</sup> Eavesdropper

<sup>4</sup> Key Distillation

<sup>5</sup> Quantum Bit Error Rate (Qber)

<sup>6</sup> Six-State Protocol (Ssp)

<sup>1</sup> Sifted Key

در سوی مقابل، چون در پروتکل اردهالی-چائو-لو در مقایسه با BB84، به طور میانگین، کیوبیت های کمتری در مرحله غربال کلید دور ریخته می شوند، پس دستیابی به کلیدی با یک طول از پیش تعیین شده نیازمند تبادل تعداد کمتری فوتون در مرحله تبادل کلید خام است. این امر سبب کاهش زمان اجرای پروتکل می شود و به دنبال آن، از میزان کارکرد و استهلاک تجهیزات و سخت افزارهای کوانتومی مورد استفاده می کاهد. به طور مشابه، چون به طور میانگین، تعداد کیوبیت های دور ریخته شده در مرحله غربال کلید در BB84 در مقایسه با پروتکل شش حالتی کمتر است، پس دستیابی به کلیدی با یک طول از پیش تعیین شده 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 شش حالتی برتری دارد.

این مقاله از چهار قسمت تشکیل شده است: در قسمت یکم، همان گونه که مشاهده شد، سازوکار پروتکل توزیع کلید کوانتومی BB84 (به عنوان اساس این تحقیق) به شکل کوتاهی یادآوری و پیرامون آن و دو شکل تغییر یافته اش موسوم به پروتکل های شش حالتی و اردهالی-چائو-لو بحث می شود؛ در قسمت دوم، روش تحقیق، یعنی طرح مسئله، اهداف، اهمیت و ضرورت، پرسش ها و روش انجام تحقیق بیان می شوند؛ در قسمت سوم، یافته های تحقیق شامل صورت بندی پروتکل  $2n$ -حالتی نایکخواخت، مطالعه و تحلیل آن از دیدگاه نظریه احتمال و بررسی دو حالت خاص آن ارائه می شوند. همچنین، یافته ها با ساخت چهار مثال عددی تأیید می شوند؛ سرانجام، این مقاله با یک نتیجه گیری و جمع بندی در قسمت چهارم به پایان می رسد.

## ۲- روش تحقیق

### ۲-۱- طرح مسئله

پس از مرور کلی پروتکل های BB84، شش حالتی و اردهالی-چائو-لو، یک مسأله مهم این است که ایده های پروتکل های شش حالتی و اردهالی-چائو-لو به طور هم زمان روی BB84 اعمال شوند و در صورت امکان، این ایده ها از آن نیز فراتر روند. سپس، پروتکل توزیع کلید کوانتومی جدید و دو حالتی خاص آن از دیدگاه نظریه احتمال مطالعه و از جنبه های اقتصادی و امنیتی با یکدیگر و با سه پروتکل BB84، شش حالتی و اردهالی-چائو-لو مقایسه شوند.

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

ذکر این نکته ضروری است که در پروتکل شش حالتی، چون آلیس و باب از سه پایه قطبش استفاده می کنند، پس احتمال اینکه باب بتواند پایه اندازه گیر خود را درست انتخاب کند، در مقایسه با BB84 کمتر است، یعنی در پروتکل شش حالتی، به طور میانگین، کیوبیت های بیشتری در مرحله غربال کلید دور ریخته می شوند. اگرچه در نگاه اول، این مسئله شاید امتیازی منفی برای پروتکل شش حالتی 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 می شود که شنودگر اطلاعات کمتری از کلید به دست آورد و دیدگاه منفی اولیه به پروتکل تغییر کند. بنابراین با توجه به میزان امنیت مورد نیاز و برآورد زمان و هزینه، می توان پروتکل توزیع کلید کوانتومی مناسب را از بین BB84 و شش حالتی انتخاب کرد.

از سوی دیگر، همان گونه که در ادامه مقاله ثابت خواهد شد، در پروتکل اردهالی-چائو-لو، یکسان نبودن احتمال انتخاب دو پایه قطبش سبب می شود احتمال اینکه باب بتواند پایه اندازه گیر خود را درست انتخاب کند، در مقایسه با BB84 افزایش یابد. به بیان دیگر، در پروتکل اردهالی-چائو-لو، به طور میانگین، کیوبیت های کمتری در مرحله غربال کلید دور ریخته می شوند. 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 می رود. با وجود این، اگر شنودگر از چگونگی تخصیص احتمال روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر آگاهی داشته باشد، اطلاعات بیشتری از کلید به دست می آورد.

به این ترتیب، اگر شنودگر از حمله ای موسوم به راهبرد برش-بازارسال<sup>۱</sup> استفاده کند (صفحه ۱۵۰ از مرجع [۳] را ببینید)، بیشترین اطلاعات را از کلید در پروتکل اردهالی-چائو-لو به دست می آورد. همچنین، اطلاعات او از کلید در BB84 در مقایسه با پروتکل شش حالتی بیشتر است. بنابراین امنیت پروتکل شش حالتی از دیدگاه به دست 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 شش حالتی به BB84 و BB84 به پروتکل اردهالی-چائو-لو برتری دارد.

<sup>۱</sup> Intercept-Resend Strategy

BB84، شش‌حالتی و اردهالی-چائو-لو را تعمیم می‌دهند. افزون بر آن، پروتکل  $2n$ -حالتی شکل کلی‌تر پروتکل‌های BB84 و شش‌حالتی 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  $2n$ -حالتی نایکنواخت می‌انجامد که افزون بر BB84، پروتکل‌های شش‌حالتی 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، شش‌حالتی 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، شش‌حالتی 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 شش‌حالتی و اردهالی-چائو-لو را به‌طور هم‌زمان روی BB84 اعمال کرد

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 شش‌حالتی 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  $2n$ -حالتی نایکنواخت نامیده می‌شود. سپس، به کمک نظریه احتمال، پروتکل  $2n$ -حالتی نایکنواخت و دو حالت خاص آن به نام‌های پروتکل  $2n$ -حالتی نایکنواخت همگن و پروتکل  $2n$ -حالتی از جنبه‌های اقتصادی و امنیتی با یکدیگر و با پروتکل‌های BB84، شش‌حالتی و اردهالی-چائو-لو مقایسه و در این باره بحث می‌شود. برای دستیابی به این اهداف، مسیر زیر پیموده می‌شود:

- صورت‌بندی پروتکل  $2n$ -حالتی 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  $2n$ -حالتی نایکنواخت به نام پروتکل  $2n$ -حالتی نایکنواخت همگن و مقایسه پروتکل‌های BB84 و اردهالی-چائو-لو از جنبه‌های اقتصادی و امنیتی به کمک آن؛
- صورت‌بندی حالت خاص دوم پروتکل  $2n$ -حالتی نایکنواخت به نام پروتکل  $2n$ -حالتی و تکمیل مقایسه‌ها؛
- ساخت چهار مثال عددی گوناگون برای تأیید یافته‌ها و مقایسه‌های انجام‌شده و اثبات مقایسه‌ناپذیری پروتکل  $2n$ -حالتی نایکنواخت با دو حالت خاص آن از جنبه‌های اقتصادی و امنیتی.

لازم به تأکید است که پروتکل‌های  $2n$ -حالتی نایکنواخت،  $2n$ -حالتی نایکنواخت همگن و  $2n$ -حالتی هر سه پروتکل

متمایز لزوماً برابر نیست و حتی ممکن است از چگونگی تخصیص احتمال روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر در سمت های خود نیز آگاهی نداشته باشند. به این ترتیب، در حالت کلی، فرض می شود تخصیص های احتمال روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر در سمت های آلیس و باب غیر هم شانس و غیر یکسان هستند.

با استناد به اصول مکانیک کوانتومی، روشن است که اگر باب پایه اندازه گیر متناظر به یک فوتون را مشابه پایه قطبش گر از پیش انتخاب شده آلیس برگزیند، آن گاه حالت قطبش آن فوتون و به دنبال آن، مقدار کیوبیتی که حمل می کند، به درستی آشکار می شود. در غیر این صورت، بنابر ذات تصادفی مکانیک کوانتومی، فوتون مورد نظر به طور تصادفی و با احتمال های برابر  $1/2$ ، یکی از حالت های قطبش پایه اندازه گیر باب را به خود می گیرد. در چنین شرایطی، بدیهی است که همه اطلاعات درباره آن فوتون و مقدار کیوبیتی که حمل می کند، از بین می رود.

مراحل تبادل کلید خام و غربال کلید در پروتکل های  $2n$  -حالت نایکناخت و BB84 بسیار شبیه به هم هستند. یگانه تفاوت موجود آن است که در پروتکل  $2n$  -حالت نایکناخت، پایه های قطبش گر و اندازه گیر به جای اینکه با احتمال های برابر از بین دو پایه قطبش موجود انتخاب شوند، با احتمال های لزوماً نابرابر از میان  $n$  پایه قطبش توافق شده انتخاب می شوند. به این ترتیب، گام های اجرای پروتکل  $2n$  -حالت نایکناخت به شرح زیر هستند:

- ۱- برای هر کیوبیت، آلیس فوتونی را که حالت قطبش آن به طور تصادفی از میان  $2n$  حالت قطبش توافق شده انتخاب می شود، نسبت می دهد؛
- ۲- آلیس فوتون را با پایه قطبش مورد نظر موسوم به پایه قطبش گر قطبیده می کند و آن را از طریق یک کانال کوانتومی به باب می فرستد (تبادل کلید خام). انتخاب هر پایه قطبش گر از میان پایه های قطبش موجود با یک احتمال مشخص و مختص به خود صورت می گیرد؛
- ۳- آلیس حالت های قطبش فوتون های ارسالی و پایه های قطبش گر انتخابی خود را به ترتیب در فهرستی یادداشت می کند؛
- ۴- در سوی مقابل، باب هر فوتون دریافتی را با پایه قطبشی موسوم به پایه اندازه گیر که به طور تصادفی از میان  $n$  پایه قطبش انتخاب می شود، اندازه گیری می کند. انتخاب هر پایه اندازه گیر از میان پایه های قطبش موجود با یک احتمال مشخص و مختص به خود صورت می گیرد؛

و به یک پروتکل توزیع کلید کوانتومی جدید دست یافت که دسته ای از پروتکل های توزیع کلید کوانتومی را به طور هم زمان تعمیم می دهد؟»

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

- ۱- چگونه می توان به جای شش حالت قطبش مجاز در پروتکل شش حالتی، از  $2n$  حالت قطبش مجاز ( $n \geq 4$ ) برای رمزگذاری کیوبیت ها استفاده کرد؟
- ۲- هریک از حالت های خاص پروتکل  $2n$  -حالت نایکناخت کدام پروتکل های توزیع کلید کوانتومی را تعمیم می دهند؟
- ۳- از جنبه های اقتصادی و امنیتی، پروتکل  $2n$  -حالت نایکناخت یا دست کم حالت های خاص آن به کدام یک از پروتکل های BB84، شش حالتی یا اردالی-چائو-لو برتری دارند؟

## ۲-۵- روش انجام تحقیق

تحقیق حاضر به روش کتابخانه ای انجام می شود و از نوع بنیادی است. در حقیقت، ابتدا با مراجعه به [۳]، پروتکل های BB84، شش حالتی و اردالی-چائو-لو به همراه تحلیل های مربوط به آنها به طور دقیق مطالعه می شوند که این مطالعه به روش کتابخانه ای انجام می گیرد. سپس، با ایده پردازی و استفاده از نظریه احتمال، پروتکل توزیع کلید کوانتومی جدید و دو حالت خاص آن صورت بندی و تحلیل و مثال های عددی ملموسی برای آنها ارائه می شوند که بیانگر تحقیق از نوع بنیادی هستند.

## ۳- یافته ها

### ۳-۱- صورت بندی پروتکل $2n$ -حالت نایکناخت و مطالعه و تحلیل آن از دیدگاه نظریه احتمال

در این قسمت، با معرفی پروتکل  $2n$  -حالت نایکناخت، به پرسش اصلی تحقیق به شکل مبسوطی پاسخ داده می شود.

پیش از اجرای پروتکل  $2n$  -حالت نایکناخت، آلیس و باب  $2n$  حالت قطبش مجاز ( $n \geq 2$ ) را که از دید آنها قابل قبول هستند، برای رمزگذاری کیوبیت ها توافق می کنند. 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 می کنند. مشابه BB84، آلیس و باب به طور توافقی، یک حالت قطبش از هر پایه قطبش را به مقدار صفر و دیگری را به مقدار یک نسبت می دهند. افزون بر آن، آلیس و باب می دانند که فرایندهای (مستقل و تصادفی) انتخاب پایه های قطبش گر و اندازه گیر به گونه ای هستند که احتمال انتخاب دو پایه قطبش

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  $2n$ -حالت نایک‌نواخت از دیدگاه نظریه احتمال است که مقایسه این پروتکل و حالت‌های خاص آن را با پروتکل‌های BB84، شش‌حالتی 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  $A_1, \dots, A_n$  فضای نمونه‌ای انتخاب پایه قطبش‌گر آلیس را افزاز 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

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

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

$$\sum_{i=1}^n p_i = \sum_{i=1}^n q_i = 1, \quad (4)$$

$$p_i^\gamma \leq p_i, \quad q_i^\gamma \leq q_i, \\ i = 1, \dots, n,$$

پس بنابر نابرابری کوشی-شوارتس<sup>۱</sup> داریم

$$\begin{aligned} &\leq \sum_{i=1}^n p_iq_i \\ &\leq \sqrt{\sum_{i=1}^n p_i^\gamma} \times \sqrt{\sum_{i=1}^n q_i^\gamma} \\ &\leq \sqrt{\sum_{i=1}^n p_i} \times \sqrt{\sum_{i=1}^n q_i} = 1. \end{aligned} \quad (5)$$

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

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  $2n$ -حالتی نایک‌نواخت به‌طور هم‌زمان هر سه پروتکل BB84، شش‌حالتی 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 شش‌حالتی کمتر باشد؛ دو، در مرحله غربال کلید، کیوبیت‌های بیشتری در مقایسه با پروتکل‌های BB84 و شش‌حالتی 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  $2n$ -حالتی نایک‌نواخت وجود ندارد.

اکنون به کمک نظریه احتمال، پروتکل  $2n$ -حالتی 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،

$$p_1, \dots, p_n, q_1, \dots, q_n \in [0, 1],$$

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

<sup>1</sup> Cauchy-Schwarz Inequality

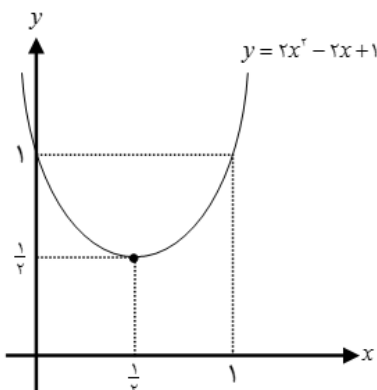
### ۲-۳- حالت خاص یکم: پروتکل 2n-حالته نایکناخت همگن

نخستین حالت خاص پروتکل 2n-حالته نایکناخت هنگامی است که تخصیص های احتمال روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر در سمت های آلیس و باب در حالت کلی، همچنان غیرهم شانس، ولی یکسان هستند، یعنی برای هر  $i = 1, \dots, n$  داریم  $p_i = q_i$ . البته لازم به تأکید است که این برابری هرگز به معنای وابستگی فرایندهای (تصادفی) انتخاب پایه های قطبش گر و اندازه گیر نیست. این حالت خاص به پروتکل 2n-حالته نایکناخت همگن می انجامد. اگر افزون بر فرض انجام شده  $n = 2$  اختیار شود، آن گاه پروتکل چهارحالته نایکناخت همگن به دست خواهد آمد که همان پروتکل اردهالی-چائو-لو است. بنابراین پروتکل 2n-حالته نایکناخت همگن پروتکل اردهالی-چائو-لو را تعمیم می دهد که پاسخی برای دومین پرسش فرعی تحقیق است.

در پروتکل 2n-حالته نایکناخت همگن، با توجه به روابط ریاضی به دست آمده درباره پروتکل 2n-حالته نایکناخت، احتمال یکسان بودن پایه های قطبش گر و اندازه گیر 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 پایه های قطبش گر و اندازه گیر متناظر به یک فوتون در پروتکل اردهالی-چائو-لو در مقایسه با BB84 بیشتر است. بنابراین در پروتکل اردهالی-چائو-لو، کیوبیت های کمتری در مقایسه با BB84 در مرحله غربال کلید دور ریخته می شوند.



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

متناظر به آنها یکسان هستند، آن گاه  $X$  از توزیع دوجمله ای با ثابت  $p = \sum_{i=1}^n p_i q_i$  پیروی می کند و از این رو

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

سرانجام، برای به دست آوردن میانگین درصد نرخ خطای کلید خام دریافتی باب، توجه کنید که اگر پایه های قطبش گر و اندازه گیر متناظر به یک فوتون یکسان باشند، آن گاه حالت قطبش آن فوتون درست آشکار می شود و مقدار کیوبیت مربوطه نیز درست به دست می آید. در غیر این صورت، اگرچه پس از اندازه گیری، حالت قطبش فوتون تغییر می کند، اما بنابر ذات تصادفی مکانیک کوانتومی، به طور میانگین، نیمی از فوتون ها مقدار کیوبیت را درست به دست می دهند. به بیان دیگر، افزون بر کیوبیت هایی که پایه های قطبش گر و اندازه گیر متناظر به فوتون حامل آنها یکسان هستند، در دو حالت زیر، یکسان نبودن این پایه ها سبب بروز خطا در کیوبیت ها نمی شود:

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

بنابراین، به طور میانگین، فقط برای نیمی از کیوبیت هایی که پایه های قطبش گر و اندازه گیر متناظر به فوتون حامل آنها یکسان انتخاب نمی شوند، خطا رخ می دهد. از این رو، میانگین درصد نرخ خطای کلید خام دریافتی باب برابر است با

$$e = \frac{1}{2} (1-p) \times 100 \\ = \frac{1}{2} (1-p) = \left[ \frac{1}{2} \left( 1 - \sum_{i=1}^n p_i q_i \right) \right] \quad (7)$$

که این مقدار با  $p$  رابطه ای معکوس دارد، یعنی با افزایش  $p$  مقدار  $e$  کاهش و با کاهش  $p$  مقدار  $e$  افزایش می یابد.

به این ترتیب، پروتکل 2n-حالته نایکناخت صورت بندی شد و معلوم شد که این پروتکل تعمیم پروتکل های BB84، شش حالت و اردهالی-چائو-لو است. سپس، به کمک نظریه احتمال، رابطه هایی برای محاسبه احتمال یکسان بودن پایه های قطبش گر و اندازه گیر متناظر به یک فوتون و میانگین درصد نرخ خطای کلید خام دریافتی باب به دست آمد. در نتیجه، برای پرسش اصلی تحقیق پاسخی مبسوط ارائه شد.



$$p_1 = \dots = p_n = q_1 = \dots = q_n = \frac{1}{n}. \quad (10)$$

روشن است که این حالت خاص معادل به کارگیری  $2n$  حالت قطبش مجاز به جای چهار یا شش حالت برای رمزگذاری کیوبیت‌هاست که به پروتکل  $2n$ -حالت می‌انجامد. به این ترتیب، نخستین پرسش فرعی تحقیق نیز پاسخ داده می‌شود. به ویژه، اگر  $n=2$ ، آن‌گاه پروتکل  $2n$ -حالت همان BB84 (پروتکل چهارحالت) و اگر  $n=3$ ، آن‌گاه پروتکل  $2n$ -حالت همان پروتکل شش‌حالت است. بنابراین پروتکل  $2n$ -حالت نایک‌نواخت هر دو پروتکل BB84 و شش‌حالت را تعمیم می‌دهد که پاسخ دومین پرسش فرعی تحقیق است.

در پروتکل  $2n$ -حالت، با توجه به روابط ریاضی به دست آمده درباره پروتکل  $2n$ -حالت نایک‌نواخت، احتمال یکسان بودن پایه‌های قطبش‌گر و اندازه‌گیر متناظر به یک فوتون برابر است با

$$p = \sum_{i=1}^n p_i q_i = \sum_{i=1}^n \frac{1}{n^2} = n \times \frac{1}{n^2} = \frac{1}{n}. \quad (11)$$

این رابطه نشان می‌دهد با افزایش جفت حالت‌های قطبش متعادل 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 شش‌حالت به ترتیب برابر  $\frac{1}{4}$  و  $\frac{1}{6}$  است، یعنی در پروتکل شش‌حالت، 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 دو جمله‌ای با ثابت  $p = \frac{1}{n}$  پیروی می‌کند و از این رو

$$\begin{aligned} P(X = k) &= C(m, k) \left(\frac{1}{n}\right)^k \left(1 - \frac{1}{n}\right)^{m-k} \\ &= C(m, k) \frac{(n-1)^{m-k}}{n^m} \quad k = 0, \dots, m. \end{aligned} \quad (12)$$

به ویژه، این احتمال در پروتکل‌های BB84 و شش‌حالت به ترتیب برابر است با

$$\begin{aligned} P(X = k) &= \frac{C(m, k)}{2^m}, \\ P(X = k) &= C(m, k) \frac{2^{m-k}}{3^m}, \end{aligned} \quad (13)$$

$$k = 0, \dots, m.$$

از سوی دیگر، میانگین درصد نرخ خطای کلید خام دریافتی باب برابر  $e = [\Delta \cdot (1 - \sum_{i=1}^n p_i^2)]$  است که میانگین درصد این نرخ را در پروتکل اردهالی-چائو-لو برابر

$$e = [\Delta \cdot (1 - (2a^2 - 2a + 1))] = 1 \cdot a(1-a) \quad (9)$$

به دست می‌دهد. چون مجموع  $a$  و  $1-a$  برابر مقدار ثابت ۱ است، پس  $e$  زمانی بیشترین مقدار ممکن را دارد که  $a = 1-a$ ، یعنی  $a = \frac{1}{2}$ . 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 تعیین شده، 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 به دست می‌آورد. به این ترتیب، سومین پرسش فرعی تحقیق در حالت خاص  $n=2$  پاسخ داده می‌شود.

با توجه به مقایسه‌های انجام شده، انتظار طبیعی آن است که در پروتکل  $2n$ -حالت 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  $2n$ -حالت نایک‌نواخت در قسمت بعدی بحث می‌شود که می‌تواند پاسخ پرسش‌های فرعی تحقیق را به‌طور کامل روشن کند.

### ۳-۳- حالت خاص دوم: پروتکل $2n$ -حالت

برای توصیف و تشریح دیگر حالت خاص پروتکل  $2n$ -حالت نایک‌نواخت که خود حالت خاصی از پروتکل  $2n$ -حالت 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

$$\sigma^2 = \frac{p}{n} - \frac{1}{n^2} \leq \frac{1}{n} - \frac{1}{n^2} = \frac{n-1}{n^2}. \quad (15)$$

چون مخرج کسر سمت راست همواره از صورت آن بیشتر است، پس  $\sigma^2 \in [0, 1)$ . به ویژه، به کمک آزمون مشتق یکم می توان نشان داد  $\sigma^2 \in [0, \frac{1}{4}]$ . بنابراین شرط  $\sum_{i=1}^n p_i = 1$  سبب می شود که  $p_i$  ها نتوانند «زیاد» پراکنده شوند و از این رو، با فرض ثابت بودن  $n$ ، نباید انتظار داشت که تخصیص های احتمال غیرهم شانس و یکسان گوناگون روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر در سمت های آلیس و باب بتوانند مقادیر  $p$  و  $e$  را به طور چشمگیری تغییر دهند.

به هر حال، روشن است که هرچه  $p$  بیشتر باشد، مقدار  $e$  کمتر است و برعکس. بنابراین در پروتکل  $2n$ -حالت که کمترین مقدار ممکن خود را دارد،  $e$  به بیشترین مقدار ممکن خود می رسد. از این رو در پروتکل  $2n$ -حالت نایکناخت همگن، میانگین درصد نرخ خطای کلید خام دریافتی باب در مقایسه با پروتکل  $2n$ -حالت کمتر است.

در نتیجه، با تحلیل ساده یافته ها مشخص می شود که انتظار طبیعی ما بیهوده و غیرمنطقی نبوده است. در واقع، برای هر عدد طبیعی  $n \geq 2$ ، از جنبه اقتصادی، پروتکل  $2n$ -حالت نایکناخت همگن به پروتکل  $2n$ -حالت برتری دارد. به بیان دیگر، برای دستیابی به یک کلید با طول از پیش تعیین شده، پروتکل  $2n$ -حالت نایکناخت همگن نیازمند ارسال فوتون های کمتری در مقایسه با پروتکل  $2n$ -حالت است. بنابراین زمان اجرا و میزان استهلاک تجهیزات و سخت افزارهای کوانتومی مورد استفاده در پروتکل  $2n$ -حالت نایکناخت همگن نیز در مقایسه با پروتکل  $2n$ -حالت کمتر است. با وجود این، از جنبه امنیتی، برتری از آن پروتکل  $2n$ -حالت است چون شنودگر در صورت آگاهی از چگونگی تخصیص احتمال روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر، اطلاعات بیشتری از کلید به دست می آورد. به این ترتیب، سومین پرسش فرعی تحقیق نیز در حالت کلی پاسخ داده می شود.

با وجود این، احتمال یکسان بودن پایه های قطبش گر و اندازه گیر متناظر به یک فوتون در پروتکل  $2n$ -حالت نایکناخت با مقدار این احتمال در دو پروتکل دیگر در حالت کلی قابل مقایسه نیست. در حقیقت، اگر  $p$ ،  $p'$  و  $p''$  به ترتیب نمایانگر این احتمال در پروتکل های  $2n$ -حالت نایکناخت،  $2n$ -حالت

سرانجام، میانگین درصد نرخ خطای کلید خام دریافتی باب برابر  $e = [50 \cdot (1 - \frac{1}{n})]$  است. بنابراین با افزایش جفت حالت های قطبش متعامد، میانگین درصد این نرخ کاهش می یابد. به ویژه، میانگین درصد نرخ خطای کلید خام دریافتی باب در پروتکل های BB84 و شش حالت به ترتیب برابر ۲۵ و ۳۳/۳ درصد است.

اکنون که پروتکل  $2n$ -حالت را به طور کامل شناسایی شد، این پروتکل با پروتکل  $2n$ -حالت نایکناخت همگن مقایسه می شود. مقایسه ای که در اینجا انجام خواهد شد، تعمیم مقایسه پروتکل های BB84 و اردهالی-چائو-لو است که پیشتر صورت گرفت.

ابتدا نشان داده می شود احتمال یکسان بودن پایه های قطبش گر و اندازه گیر متناظر به یک فوتون در پروتکل  $2n$ -حالت کمترین مقدار ممکن را دارد. برای این منظور، فرض کنید  $\bar{p}$  میانگین  $p_1, \dots, p_n$  در پروتکل  $2n$ -حالت نایکناخت همگن است. در این صورت  $\bar{p} = \frac{1}{n} \sum_{i=1}^n p_i = \frac{1}{n}$ . بنابراین واریانس  $p_1, \dots, p_n$  برابر است با

$$\sigma^2 = \frac{1}{n} \sum_{i=1}^n p_i^2 - \bar{p}^2 = \frac{p}{n} - \frac{1}{n^2}. \quad (14)$$

چون  $\sigma^2 \geq 0$ ، محاسبه ای ساده نشان می دهد که  $p \geq \frac{1}{n}$ . از سوی دیگر، چون مقدار واریانس برای  $p = \frac{1}{n}$  برابر صفر است، پس هنگامی کمترین مقدار خود را دارد که  $p_1 = \dots = p_n = \bar{p} = \frac{1}{n}$  یعنی هیچ تخصیص احتمال غیرهم شانس و غیریکسانی روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر در سمت های آلیس و باب نمی تواند  $p$  را کمینه کند. بنابراین، هرچه پراکندگی  $p_i$  ها بیشتر باشد، واریانس آنها و به دنبال آن، احتمال یکسان بودن پایه های قطبش گر و اندازه گیر متناظر به یک فوتون بیشتر خواهد بود. در نتیجه، احتمال یکسان بودن پایه های قطبش گر و اندازه گیر متناظر به یک فوتون در پروتکل  $2n$ -حالت نایکناخت همگن در مقایسه با پروتکل  $2n$ -حالت بیشتر است.

شایان ذکر است که برای  $\sigma^2$  یک کران بالا می توان به دست آورد که شاید البته کوچکترین کران بالای آن نباشد، اما اطلاعات خوبی درباره  $p_i$  ها و به دنبال آن،  $p$  و  $e$  به دست می دهد. در واقع، چون  $p \leq 1$ ، پس

نتایج این تحلیل، سه پروتکل  $2n$ -حالت نایکناخت،  $2n$ -حالت نایکناخت،  $2n$ -حالت نایکناخت همگن و  $2n$ -حالت را با یکدیگر مقایسه می‌کند.

نایکناخت همگن و  $2n$ -حالت باشند، آن‌گاه همواره  $p'' \leq p'$ ، اما هر سه حالت  $p < p'' < p'$ ،  $p < p'' < p'$  و  $p' < p$  ممکن است رخ دهند. جدول (۱) با دسته‌بندی

جدول (۱): مقایسه پروتکل‌های  $2n$ -حالت نایکناخت،  $2n$ -حالت نایکناخت همگن و  $2n$ -حالت

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

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  $e = [\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}]$ . بنابراین همان‌گونه که انتظار می‌رفت، در پروتکل هشت‌حالتی، 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 شش‌حالتی 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

### ۳-۴- مثال‌های عددی

اکنون که پروتکل  $2n$ -حالت نایکناخت و حالت‌های خاص آن به نام‌های پروتکل  $2n$ -حالت نایکناخت همگن و پروتکل  $2n$ -حالت 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 هشت‌حالتی (حالت خاص دوم) به‌دست می‌آید که

$$p = p_1 q_1 + p_2 q_2 = \frac{2}{3} \times \frac{2}{7} + \frac{1}{3} \times \frac{5}{7} = \frac{3}{7} \quad (21)$$

و  $e = [\Delta \cdot (1 - \frac{2}{7})] \square 28$  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 به ترتیب 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  $p = \frac{3}{7}$  پیروی می‌کند و داریم

$$P(X=4) = C(6,4) \left(\frac{3}{7}\right)^4 \left(\frac{4}{7}\right)^2 = \frac{19,440}{117,649} \simeq 0.17. \quad (22)$$

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

سرانجام در مثال چهارم، فرض کنید  $n=6$

$$p_i = \frac{i}{21}, \quad q_i = \frac{i+1}{27} \quad i=1,2,3,4,5,6, \quad (23)$$

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  $\sum_{i=1}^6 p_i = \sum_{i=1}^6 q_i = 1$ ). در این صورت پروتکل دوازده‌حالتی نایک‌نواخت را به‌دست می‌آید که در آن

$$p = \sum_{i=1}^6 p_i q_i = \frac{1}{21} \times \frac{2}{27} + \frac{2}{21} \times \frac{3}{27} + \frac{3}{21} \times \frac{4}{27} + \frac{4}{21} \times \frac{5}{27} + \frac{5}{21} \times \frac{6}{27} + \frac{6}{21} \times \frac{7}{27} = \frac{16}{81} \quad (24)$$

و  $e = [\Delta \cdot (1 - \frac{16}{81})] \square 40$  و  $\gamma$  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،

$$P(X=4) = C(6,4) \left(\frac{1}{4}\right)^4 \left(\frac{3}{4}\right)^2 = \frac{135}{4096} \simeq 0.03. \quad (16)$$

در مثال دوم، فرض کنید  $n=3$  و

$$p_1 = q_1 = \frac{1}{2}, \quad p_2 = q_2 = \frac{1}{3}, \quad p_3 = q_3 = \frac{1}{6}, \quad (17)$$

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  $p_1 + p_2 + p_3 = 1$ ). در این صورت پروتکل شش‌حالتی نایک‌نواخت همگن (حالت خاص یکم) به‌دست می‌آید که در آن

$$p = p_1^2 + p_2^2 + p_3^2 = \frac{1}{4} + \frac{1}{9} + \frac{1}{36} = \frac{7}{18} \quad (18)$$

و  $e = [\Delta \cdot (1 - \frac{7}{18})] \square 30$  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 شش‌حالتی 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  $p = \frac{7}{18}$  پیروی می‌کند و داریم

$$P(X=4) = C(6,4) \left(\frac{7}{18}\right)^4 \left(\frac{11}{18}\right)^2 = \frac{1,452,605}{11,337,408} \simeq 0.13. \quad (19)$$

شایان ذکر است که چون  $\sigma^2 = \frac{1}{\Delta^2}$  پس پراکندگی  $p_1$ ،  $p_2$  و  $p_3$  نسبت به کران بالای  $\frac{1}{\Delta}$  چندان زیاد نیست و مقادیر  $p$  و  $e$  در مقایسه با مقادیر مشابه در پروتکل شش‌حالتی اختلاف چندان ندارند.

در مثال سوم، فرض کنید  $n=2$  و

$$p_1 = 2p_2 = \frac{2}{3}, \quad q_1 = \frac{2}{7}, \quad q_2 = \frac{5}{7}, \quad (20)$$

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  $p_1 + p_2 = q_1 + q_2 = 1$ ). در این صورت پروتکل چهارحالتی نایک‌نواخت به‌دست می‌آید که در آن:

بیشتری از کلید به دست می آورد که از جنبه امنیتی یک اشکال به شمار می رود. در نتیجه، آلیس و باب با بررسی عواملی همچون سطح امنیت و محرمانگی مورد نیاز، میزان حساس بودن اطلاعات محرمانه، زمان و هزینه ی مجاز مصرفی برای اجرا و توان تجهیزات و سخت افزارهای کوانتومی مورد استفاده پروتکل توزیع کلید کوانتومی مناسب خود را انتخاب و بین جنبه های اقتصادی و امنیتی تعادل لازم را برقرار می کنند.

## 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)

آن گاه  $X$  از توزیع دوجمله ای با ثابت  $p = \frac{16}{81}$  پیروی می کند و بنابراین احتمال رخداد آن برابر است با

$$P(X = 4) = C(6, 4) \left(\frac{16}{81}\right)^4 \left(\frac{65}{81}\right)^2 = \frac{1,384,448,000}{94,143,178,827} \approx 0.01. \quad (25)$$

مثال چهارم تخصیص احتمال را روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر در سمت های آلیس و باب در پروتکل  $2n$ -حالت نایکنواخت به خوبی توصیف می کند. افزون بر آن، با اعمال تغییرات جزئی در تخصیص های احتمال این مثال، امکان پذیری هر دو دسته نابرابری های  $p' < p < p''$  و  $p'' < p' < p$  نیز ثابت می شوند. در واقع، اگر برای هر  $i = 1, 2, 3, 4, 5, 6$  قرار دهیم  $p_i = q_i = \frac{i}{21}$ ، آن گاه  $p' = \frac{11}{21}$  و چون  $p = \frac{16}{81}$ ، پس  $p' < p < p''$  از سوی دیگر، اگر برای هر  $i = 1, 2, 3, 4, 5, 6$  قرار دهیم  $p_i = q_i = \frac{i+1}{27}$ ، آن گاه  $p' = \frac{13}{27}$  و باز هم با توجه به مقدار  $p$  خواهیم داشت  $p' < p < p''$ . در نتیجه، در حالت کلی، احتمال یکسان بودن پایه های قطبش گر و اندازه گیر متناظر به یک فوتون در پروتکل  $2n$ -حالت نایکنواخت با مقدار این احتمال در دو پروتکل دیگر قابل مقایسه نیست.

## ۴- نتیجه گیری

در تحقیق حاضر، ابتدا پروتکل  $2n$ -حالت نایکنواخت که تعمیمی از پروتکل های BB84، شش حالت و اردهالی چائو-لو است، صورت بندی و از دیدگاه نظریه احتمال مطالعه و تحلیل شد. در این پروتکل، از  $2n$  حالت قطبش مجاز استفاده می شود که  $n$  پایه قطبش شامل آنها با احتمال های لزوماً نابرابر انتخاب می شوند. به بیان دیگر، به طور میانگین، فراوانی هریک از پایه های قطبش در فهرست های آلیس و باب لزوماً برابر نیست. سپس، با صورت بندی دو حالت خاص پروتکل  $2n$ -حالت نایکنواخت به نام های پروتکل  $2n$ -حالت نایکنواخت همگن و پروتکل  $2n$ -حالت، فاز مقایسه آغاز و مشخص شد اگر پایه های قطبش با احتمال های نابرابر ولی همگن انتخاب شوند، تعداد کیوبیت های کمتری در مرحله غربال کلید دور ریخته می شوند. بنابراین این حالت از جنبه اقتصادی به صرفه تر است چون نیازمند تولید، قطبیده کردن و ارسال تعداد فوتون های کمتری است که به صرف زمان و انرژی کمتری نیاز دارد و تجهیزات و سخت افزارهای کوانتومی مورد استفاده را کمتر مستهلک می کند. با وجود این، شنودگر با آگاهی از چگونگی تخصیص احتمال روی انتخاب پایه های قطبش به عنوان پایه های قطبش گر و اندازه گیر، اطلاعات

---

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

A. Aghanians<sup>1</sup>, S. N. Doustimotlagh<sup>\*</sup>

<sup>\*</sup>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

---

<sup>\*</sup> Corresponding Author Email: [doustimotlagh@elenoon.ir](mailto:doustimotlagh@elenoon.ir)