نشریه علمی «پدافند الکترونیکی و سایبری»
سال هفتم، شماره ۱، بهار ۱۳۹۸؛ ص ۱۱۲-۱۰۵

یک رویکرد جدید محاسبه نرخ ارسال در سامانه‌های تبادل اطلاعات کوانتومی با استفاده از توزیع دوجمله‌ای

سید محمد حسینی[۱]، شهروز جانباز[۲]، مهدی داودی دراره[۳*]، علی زاغیان[۴]

۱- دانشجوی دکتری ریاضی، ۲- استادیار، ۳- استادیار، ۴- دانشیار، دانشکده علوم کاربردی دانشگاه صنعتی مالک اشتر

(دریافت: ۹۶/۱۱/۲۵، پذیرش: ۹۷/۰۳/۰۶)

چکیده

ارزیابی الگوریتم‌های تبادل بیت معمولاً توسط شاخص بازدهی انجام می‌شود، و به نسبت تعداد بیت ارسالی که با موفقیت دریافت شده‌اند به کل تعداد بیت‌های ارسالی اطلاق می شود. هر چند در نظریه اطلاعات کوانتومی هم اغلب تکیه بر همین شاخص است، اما می‌توان بر مبنای آن، عامل ارزیابی دیگری را برای این حوزه از نظریه اطلاعات معرفی کرد که چشم‌اندازی از هزینه‌های الگوریتم را هم در بر دارد. این شاخص تعداد کیوبیت‌های ارسالی مورد نیاز برای دریافت یک دنباله بیتی مطلوب است. با کمک این شاخص جدید می‌توان اطلاعات دقیق‌تری درباره تعداد کیوبیت مورد نیاز برای ارسال، با توجه به طول خروجی مورد انتظار الگوریتم، به‌دست آورد و هزینه‌های پیاده‌سازی الگوریتم را بهتر برآورد کرد. این در حالی است که شاخص بازدهی تنها برای مقایسه نظری الگوریتم‌ها قابل استفاده است. در این مقاله برای توضیح چگونگی محاسبه این شاخص، از ایده‌ای که در صنعت حمل و نقل برای فروش مازاد بلیط استفاده می‌شود بهره می‌بریم. در واقع ابتدا با به‌کار بردن روش فروش مازاد برای آزمایش دو شکاف یانگ، مفاهیم و نمادهای این دو مبحث را یکپارچه کرده و سپس نتایج محاسبات را ارائه داده‌ایم. در نهایت، با استفاده از همین رویکرد، تعداد کیوبیت‌های ارسالی مورد نیاز به‌منظور تولید کلید با طول مطلوب را در پروتکل‌های توزیع کلید کوانتومی BB84 و Six-State، برحسب نرخ خطا محاسبه می‌کنیم.

کلیدواژه‌ها: نرخ ارسال، روش فروش مازاد، آزمایش دو شکاف یانگ، توزیع کلید کوانتومی، نرخ کلید

۱- مقدمه

یکی از مهم‌ترین شاخص‌های ارزیابی روش‌ها و الگوریتم‌ها در نظریه اطلاعات کوانتومی، نرخ خروجی مطلوب است. منظور از نرخ مطلوب، نسبت میزان خروجی قابل استفاده (مطلوب) به میزان ورودی است [۱]. برای مثال، نرخ کلید[۱] در یک پروتکل توزیع کلید کوانتومی (QKD[۲]) نسبت تعداد بیت‌های قابل استفاده به تعداد کیوبیت‌های ارسالی (یا تعداد بیتی که کیوبیت‌ها حمل می‌کنند) است. اگر چه می‌توان این نرخ را احتمال سالم ماندن و سالم رسیدن یک کیوبیت ارسالی و تبدیل آن به یک بیت از کلید توصیف کرد، لیکن ممکن است به‌عنوان یک شاخص عمومی، همواره بیانگر آن‌چه در عمل مورد نیاز است نباشد. مثلاً وقتی در نظر داریم دنباله‌ای از قطعات هم‌اندازه پیام را با رمزنگاری متقارن و با کلیدهای متفاوت رمز کنیم، به کلیدهای سالم با طول ثابت و معین نیاز داریم [۲]. فرض کنیم فرستنده پیام می‌خواهد در صورت فراهم بودن امکانات، این کلیدها را از یک پروتکل QKD به‌دست آورد. بنابراین، باید بداند که برای هر قطعه از پیام، چند کیوبیت باید ارسال شود تا کلیدی به اندازه هر قطعه پیام به‌دست آید. در واقع، باید بتواند کمترین شدت ارسال چشمه ذرات کوانتومی (فوتون، الکترون و...) را برای تضمین طول کلید مورد نیاز هر قطعه از پیام برآورد نماید. در این مقاله، برای محاسبه این کمیت از ایده «فروش مازاد[۳]» در صنعت حمل و نقل بهره می‌گیریم. این روش فروش، تضمین می‌کند که مثلاً یک هواپیما هیچ‌گاه مجبور به پرواز با یک یا چند صندلی خالی نشود.

در این مقاله، ابتدا در بخش ۲، پیشینه علمی مختصری از کاربرد و محاسبه نرخ ارسال کیوبیت بیان و مقدمه‌ای از ایده فروش مازاد را بیان می‌کنیم. سپس در بخش ۳، بر پایه آزمایش دو شکاف یانگ[۴] دارای چشمه نوری کوانتومی تک‌رنگ، ضمن

نویسنده پاسخگو: m.davoudi@mut-es.ac.ir

1- key rate
2- Quantum Key Distribution (QKD)
3- overselling
4- Young's double-slit experiment

تعریف مفاهیم، مساله فروش مازاد را برای محاسبه کمترین تعداد فوتونی که باید ارسال شود تا تعداد مشخصی از آن‌ها در محل مطلوب به پرده برخورد کنند بکار می‌بریم. پس از آن در بخش۴، به بیان و اجرای این ایده روی آزمایش دو شکاف یانگ با چشمه چندرنگ (که به منظور ارسال کوانتومی داده قابل استفاده است[۳]) می‌پردازیم. در بخش۵، بر اساس رویکرد ارائه شده در این مقاله، نرخ ارسال کیوبیت را در چند سامانه QKD محاسبه می‌کنیم تا کمترین تعداد کیوبیت ارسالی مورد نیاز را، برای دست‌یابی به کلیدی امن با طول مشخص، به‌دست آوریم. سپس، نتایج حاصل را با گزارش‌های دیگران مقایسه خواهیم کرد. جمع‌بندی و نتیجه‌گیری در بخش ۶، آورده می‌شود.

۲- معرفی مساله و روش تحقیق

در مطالعه الگوریتم‌های تبادل بیت کوانتومی زمانی که هدف از ارزیابی، مطالعه نظری الگوریتم‌ها و مقایسه کارآیی آن‌هاست، محاسبه نرخ بازدهی الگوریتم‌ها در هر کیوبیت ارسالی، کفایت می‌کند. اما وقتی هدف، پیاده‌سازی یک الگوریتم برای انجام یک هدف خاص باشد، با توجه به هزینه‌های بسیار بالای سامانه‌های تبادل بیت کوانتومی، باید الگوریتم‌ها از نظر هزینه‌های پیاده‌سازی و اجرا هم مقایسه شوند. با عنایت به تنوع زیاد سامانه‌های فیزیکی پیشنهاد شده برای تبادل بیت کوانتومی، درباره هزینه‌های پیاده‌سازی الگوریتم‌ها، تحقیقات بسیاری منتشر شده‌اند [۵-۴]. اما برای برآورد هزینه‌های اجرا، به شاخصی نیاز داریم که بتواند مشخص کند که با توجه به هدف ما، در هر بار اجرای الگوریتم چه مقدار از ذرات کوانتومی حامل اطلاعات باید ارسال شوند تا به خروجی مطلوب دست یابیم. در بین مقالات منتشر شده درباره کارآیی الگوریتم‌های تبادل اطلاعات کوانتومی، به ندرت و برای حالت‌های خاصی از الگوریتم‌ها به محاسبه چنین شاخصی پرداخته شده است [۷-۶]. در این مقاله ما با استفاده از توزیع دوجمله‌ای، روشی را برای محاسبه نرخ ارسال پیشنهاد می‌دهیم که برای هر الگوریتم انتقال بیت کوانتومی قابل استفاده است. ایده این روش، یک برآورد آماری است که مدتی است از آن در سامانه‌های فروش بلیط در سفرهای هوایی استفاده می‌شود. از آنجا که هر بار پرواز یک هواپیما برای شرکت‌های هوایی هزینه سنگینی در بر دارد، برخی از این شرکت‌ها همواره سعی می‌کنند با فروش مازاد بلیط، طوری عمل کنند که هیچ پروازی با صندلی خالی انجام نشود. ایده فروش مازاد عبارت است از برآورد میزان فروش بلیط مازاد بر صندلی موجود، به‌گونه‌ای که از پر شدن همه صندلی‌ها هنگام پرواز اطمینان حاصل شود و از طرفی احتمال مواجهه با مسافری که بلیط خریداری کرده، اما جایی در پرواز ندارد به کمترین میزان برسد.

فرض کنیم احتمال آن که «مسافری که بلیط خریداری کرده، به موقع برای سوار شدن به فرودگاه برسد» برای همه مسافران یکسان و مستقل از دیگران باشد. نماد X_i را به‌عنوان متغیر تصادفی متناظر با این پیشامد در نظر می‌گیریم. فروش بلیط مازاد عبارت است از فروش r بلیط بیش از ظرفیت واقعی هواپیما (یعنی n) به‌گونه‌ای که با وجود عدم حضور (غیبت) تعدادی از مسافران، علاوه بر پر شدن همه صندلی‌ها، شانس «اعتراض مسافر[1]» (یعنی مراجعه تعدادی مسافر که بلیط خریده‌اند اما جای خالی در پرواز برایشان وجود ندارد) از یک آستانه ε کمتر باشد.

فرض کنیم مجموع بلیط‌های فروخته شده $n_S = n + r$ باشد. هر X_i را می‌توان مشابه پرتاب یک سکه نامتوازن درنظر گرفت. از آنجا که متغیرهای تصادفی X_i یکسان هستند، دنباله‌ای از n_S تکرار مستقل آن‌ها مانند $(X_1, X_2, \cdots, X_{n_S})$، یک فرآیند برنولی[2] است. بنابراین، توزیع احتمالِ ظهور n موفقیت در n_S تکرار مستقل، توسط توزیع دوجمله‌ای[3] یا دوجمله‌ای منفی[4] به‌دست می‌آید. عکس این روند هم برقرار است، یعنی با داشتن تعداد موفقیت مورد انتظار n_e، می‌توان با استفاده از این توزیع‌ها کمترین تعداد n_S (یعنی $\tilde{n}_S$) را برای این‌که دست‌کم n_e موفقیت ظاهر شود، به‌دست آورد. در کاربردهای واقعی، مانند حمل و نقل، مقدار $\tilde{n}_S$ به آستانه قابل تحمل تعداد مسافرین معترض یعنی r_0 هم وابسته است. در اینجا این قید را به‌وسیله ε اعمال می‌کنیم که همان احتمال مشاهده تعداد بیش از $n + r_0$ نفر مسافر وقت‌شناس است که بلیط خریداری کرده‌اند.

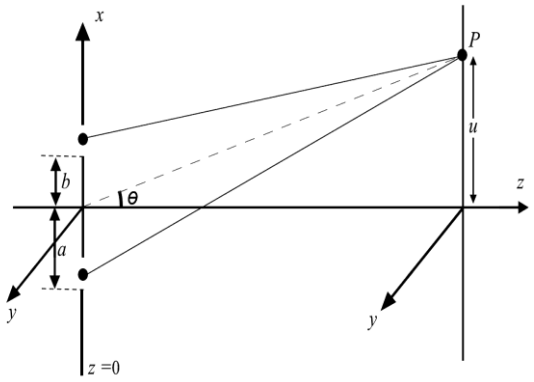
در ادامه این مقاله، تعداد کیوبیت خروجی مورد انتظار هر یک از الگوریتم‌های تبادل بیت کوانتومی مورد بررسی را n_e می‌نامیم و هدف ما محاسبه کمترین تعداد کیوبیت ارسالی مورد نیاز ($\tilde{n}_S$) خواهد بود، به‌گونه‌ای که احتمال دریافت کیوبیت اضافی، از ε بیشتر نشود.

۳- محاسبات برای چشمه نور تک‌رنگ همدوس

برای آزمایش دو شکاف یانگ انواع گوناگونی از آرایش اجزای سامانه پیشنهاد شده است [۸]. در این بخش ساده‌ترین شکل آن

1- plane rage
2- Bernoulli process
3- binomial distribution
4- negative binomial distribution

را برای توضیح ایده خود به‌کار می‌گیریم. صفحه‌ای را با دو شکاف مشابه روی آن در نظر بگیرید که در سمت چپ آن یک چشمه نور تک‌رنگ همدوس با طول موج λ، و در سوی دیگرش یک پرده قرار دارد، به‌گونه‌ای که مکان چشمه، میانه شکاف‌ها و مرکز پرده در یک راستا قرار گرفته‌اند. این راستا را خط مبنا یا خط مرکزها می‌نامیم و میانه شکاف‌ها را مبدأ مختصات در نظر می‌گیریم. فاصله‌های بین خط مبنا تا لبه بیرونی و لبه درونی هر یک از شکاف‌ها را به‌ترتیب با a و b نشان می‌دهیم. فاصله عمودی هر نقطه روی پرده مانند P از خط مبنا را u می‌نامیم و θ زاویه‌ای است که خط گذرا از P و مبدأ با خط مبنا می‌سازد (شکل (۱) را ببینید).



شکل (۱): سامانه آزمایش دو شکاف یانگ (برگرفته از [۳]).

این آزمایش، که برای مشاهده و مطالعه ویژگی‌های کوانتومی و کلاسیک نور طراحی شده، نشان می‌دهد که بر اثر دو پدیده تداخل و پراش، پرتوهای نور روی پرده طرح تداخل را به‌گونه‌ای به‌وجود می‌آورند که یک نوار با بیشترین شدت نور در مرکز پرده $(u,\theta=0)$ و نوارهای تاریک و روشن به طور متقارن در بالا و پایین آن قرار می‌گیرند و شدت نور و تفکیک‌پذیری نوارها با دور شدن از نوار مرکزی (افزایش $|u|$) کاهش می‌یابد. اگر شدت نور در هر نقطه مانند P (واقع در زاویه θ) را با $I(\theta)$ نشان دهیم، که $\theta\in\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$ و I_0 شدت در $\theta=0$ باشد، می‌توان رابطه زیر را برای توزیع شدت طرح تداخلی روی پرده نوشت [۸]:

$$\frac{I(\theta)}{I_0}=\cos^2\left(\frac{\pi b\sin\theta}{\lambda}\right)\cdot\operatorname{sinc}^2\left(\frac{\pi(a-b)\sin\theta}{\lambda}\right), \quad (۱)$$

که در آن، $\operatorname{sinc}(x)=\frac{\sin x}{x}$. انجام آزمایش یانگ در حد چشمه‌های نوری با شدت بسیار کم نشان می‌دهد که حتی وقتی چشمه، تک فوتون ارسال کند، الگوی فرود فوتون‌ها روی پرده همچنان از طرح تداخلی پیروی می‌نماید [۹]. از این رو می‌توان توسط رابطه (۱) و با به‌هنجارسازی آن روی تمام سطح پرده $\left(\theta\in\left[-\frac{\pi}{2},\frac{\pi}{2}\right]\right)$ تابع چگالی احتمال «برخورد به پرده در نقطه P» را برای هر تک فوتونی که از صفحه شکاف‌ها عبور کرده است به‌دست آورد [۱و۴]. همچنین، با انتگرال‌گیری از رابطه (۱) روی بازه زاویه‌ای مفروض $A=\left[\theta_0-c,\ \theta_0+c\right]$ و به‌هنجارسازی، می‌توان احتمال p_A که یک فوتون درون این بازه فرود آید را محاسبه کرد:

$$p_A=\Pr\{\theta\in A\}=\frac{\int_A I(\theta)\,d\theta}{\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} I(\theta)\,d\theta}. \quad (۲)$$

هدف ما در این مرحله پیدا کردن تعداد فوتونی است که بایستی به سوی شکاف‌ها گسیل شود تا از برخورد تعداد مشخصی از آن‌ها به بخش معینی از پرده، اطمینان حاصل شود. از آن‌جا که تابع توزیع احتمال در رابطه (۲) برای هر یک از فوتون‌ها یکسان و مستقل از سایر فوتون‌هاست، ارسال یک کیوبیت را می‌توان متناظر با پرتاب سکه نامتوازن در نظر گرفت. همچنین می‌توان ایده فروش مازاد را برای محاسبه تعداد کیوبیت مورد نیاز به‌کار برد. برای این‌کار، آزمایش ارسال کیوبیت‌ها را یک فرآیند برنولی متناهی در نظر می‌گیریم. بنابراین، تعداد کیوبیت‌ها از توزیع دوجمله‌ای یا توزیع دوجمله‌ای منفی به‌دست می‌آید.

اکنون اگر در آزمایش دو شکاف یانگ، n_s را تعداد فوتون‌های ارسالی توسط چشمه تعریف کنیم، آن‌گاه در بازه زاویه‌ای A نرخ فوتون‌ها یا کیوبیت‌های رسیده به پرده برابر با $n_s\cdot p_A$ است. با این وجود، برای تضمین دریافت دست‌کم n_e کیوبیت و همچنین به حداقل رساندن هزینه‌ها، می‌توان با قبول یک احتمال جزیی ε برای مشاهده بیش از n_e کیوبیت، یک کران بالا برای کمترین تعداد کیوبیت ارسالی به‌دست آورد. برای این کار به تعریف زیر برای توزیع دوجمله‌ای نیاز داریم.

تعریف: فرض کنید X متغیر تصادفی تعداد موفقیت‌های مشاهده شده در دنباله‌ای از y رخداد برنولی مستقل با احتمال موفقیت p_s باشد. در این‌صورت منظور از نماد $X\sim B(y,p_S)$ این است که X از توزیع دوجمله‌ای با پارامترهای y و p_s پیروی می‌کند [۱۰]. از توزیع دوجمله‌ای داریم:

$$\Pr(X=x)=p_s^x\,(1-p_s)^{y-x}\binom{y}{x}, \quad (۳)$$

که در آن، $\binom{y}{x}=\frac{y!}{x!(y-x)!}$. طبق تعریف فوق می‌توان با جایگذاری $x=n_e$ و $p_s=p_A$ در رابطه (۳)، احتمال دریافت موفق n_e فوتون در هر y فوتون ارسال شده از چشمه را به‌دست آورد. در این‌صورت کمترین تعداد فوتون‌های ارسالی ($y \geq n_e$) که به‌ازای آن تعداد موفقیت‌های مشاهده‌شده (مگر با احتمالی کمتر از ε) از n_e تجاوز نکند، یک تخمین برای n_s است یعنی:

$$\tilde{n}_s=\min\left\{y\geq n_e \,\middle|\, \Pr(X<n_e)=0 \;\&\; \Pr(X>n_e)<\varepsilon \;;X\sim B(y,p_A)\right\}. \quad (۴)$$

در جدول (۱)، خلاصه‌ای از نتایج به‌دست‌آمده از این محاسبات، برای پرتو نور تک‌رنگی با $\lambda=۶۰۰nm$، در یک آزمایش دو شکاف با $b=۱\,mm$ و $a-b=۸۰\,\mu m$، به‌ازای بازه‌های زاویه‌ای متقارن و نامتقارن و با $\varepsilon=۰/۰۱$ آورده شده است.

جدول (۱): استفاده از روش فروش مازاد در یک آزمایش دو شکاف یانگ دارای پرتو نور تک‌رنگ، به منظور تخمین تعداد فوتونی که باید چشمه تک‌رنگ ارسال کند ($\tilde{n}_s$) تا با فرض $\varepsilon=۰/۰۱$، برخورد تعداد n_e فوتون به پرده درون بازه A، تضمین شود.

A	p_A	$\tilde{n}_s$		
		$n_e=۱۰^۵$	$n_e=۱۰^۴$	$n_e=۱۰^۳$
$\left[\frac{\pi}{۱۰۰},\frac{\pi}{۵۰}\right]$	۰/۰۰۶۴	۱۵۶۳۳۸۷۵	۱۵۳۶۱۲۰	۱۴۵۲۶۲
$\left[\frac{\pi}{۲۰۰},\frac{\pi}{۱۰۰}\right]$	۰/۰۱۲۴۶	۷۹۶۳۲۷۷	۷۸۲۴۸۲	۷۴۰۰۸
$\left[\frac{\pi}{۲۰۰۰},\frac{\pi}{۱۰۰۰}\right]$	۰/۱۶۲۹	۶۰۹۱۸۴	۵۹۹۴۳	۵۶۹۶
$\left[۰,\frac{\pi}{۲۰۰}\right]$	۰/۴۷۵۱	۲۰۹۲۵۶	۲۰۶۶۱	۱۹۸۵
$\left[۰,\frac{\pi}{۱۰۰۰}\right]$	۰/۳۵۵۴	۲۷۹۵۷۱	۲۷۵۶۵	۲۶۳۶
$\left[-\frac{\pi}{۱۰۰۰},\frac{\pi}{۱۰۰۰}\right]$	۰/۷۱۰۷	۱۴۰۰۸۸	۱۳۸۷۷	۱۳۴۷
$\left[-\frac{\pi}{۱۰۰},\frac{\pi}{۱۰۰}\right]$	۰/۹۷۵۱	۱۰۲۴۲۷	۱۰۲۱۵	۱۰۱۳
$\left[-\frac{\pi}{۱۰},\frac{\pi}{۱۰}\right]$	۰/۹۹۷۷	۱۰۰۱۹۵	۱۰۰۱۲	۱۰۰۰
$\left[-\frac{\pi}{۲},\frac{\pi}{۲}\right]$	۱	۱۰۰۰۰۰	۱۰۰۰۰	۱۰۰۰

۴- محاسبات برای چشمه نور چندرنگ همدوس

در این بخش، محاسبات بخش قبل در یک آزمایش دوشکاف یانگ را این بار برای چشمه نور کاملاً همدوس چندرنگ ارائه می‌دهیم. این کار منجر به پیدا کردن نرخ ارسال برای یک سامانه ارسال داده مبتنی بر ناهنجاری‌های طیفی [۳] می‌شود. طیف یک پرتوی نور چند رنگ همدوس، طیفی گاوسی حول ω_0 و با عرض میانگین (rms) برابر با Γ به‌صورت زیر نوشته می‌شود [۳]:

$$S^{\circ}(\omega)=\exp\left\{-\frac{(\omega-\omega_0)^2}{2\Gamma^2}\right\}. \quad (۵)$$

توزیع طیفی شدت در هر نقطه (u,z) روی پرده و در مقابل شکاف‌ها با رابطه زیر داده می‌شود [۳ و ۱۱]:

$$S(u,z,\omega)=\frac{\omega S^{\circ}(\omega)}{z\,\omega_0}\left|\left(\frac{-S^{\circ}(\omega)i\left(\omega/\omega_0\right)}{z}\right)^{\frac{1}{2}}\times \left\{\int_{-1}^{-\frac{b}{a}}\exp\left[i\,\frac{\pi\left(\omega/\omega_0\right)}{z}\left(x^2-2xu\right)\right]dx+\int_{\frac{b}{a}}^{1}\exp\left[i\,\frac{\pi\left(\omega/\omega_0\right)}{z}\left(x^2-2xu\right)\right]dx\right\}\right|^2, \quad (۶)$$

که در آن، z فاصله مقیاس شده بین مرکز شکاف‌ها و پرده است (در این بخش، به‌منظور سادگی در نمایش و مطابق مرجع [۳]، دو متغیر فاصله یعنی u و z به‌ترتیب با ضرایب ثابت $1/a$ و λ/a^2 مقیاس شده‌اند؛ شکل (۱) را ببینید). اکنون با انتخاب مقداری ثابت برای z و انتگرال‌گیری از رابطه (۶) روی همه فرکانس‌ها، جایگزینی برای $I(\theta)$ در رابطه (۲) به‌دست می‌آوریم. نتیجه، تابعی از u است که می‌توان آن را تابع توزیع احتمال حضور یک فوتون (با هر فرکانسی) در هر نقطه‌ای از پرده همچون P فرض کرد. از جایگزینی این تابع در رابطه (۲) و تغییر متغیر فاصله (u) به زاویه (θ)، نرخ ارسال کیوبیت برای چشمه نور چندرنگ به‌منظور دریافت n_e کیوبیت روی پرده و درون بازه A، به‌دست می‌آید. نتایج برای بازه‌های زاویه‌ای مختلف و با فرض $\varepsilon=۰/۰۱$ در جدول (۲) آمده‌اند.

حال فرض کنیم که می‌خواهیم طبق [۳] از ناهنجاری‌های طیفی در آزمایش دو شکاف یانگ با پرتوی چند رنگ، برای انتقال داده استفاده کنیم. نتایج به‌دست‌آمده نشان می‌دهند که برای $z>۹$، این ناهنجاری‌ها در راستای زاویه‌های انتشار ثابتی

همچون θ_c قابل مشاهده‌اند. به این معنی که در زاویه‌ای اندکی کمتر از آن، طیف همواره متمایل به قرمز، و در زاویه‌ای اندکی بیش از آن، طیف همواره متمایل به آبی است. از این‌رو، مشاهده‌گر باید مثلاً در $\theta \in \left[\frac{\pi}{۱۳}, \frac{\pi}{۱۲}\right]$ قرار داشته باشد تا موفق به مشاهده ناهنجاری‌های طیفی شود و آن‌ها را به درستی به بیت‌های داده تعبیر نماید. بنابراین، احتمال انتقال موفق یک کیوبیت، با احتمال برخورد یک فوتون به پرده در درون این بازه برابر است. در نهایت، با استفاده از این احتمال و از رابطه (۴)، تعداد کیوبیت‌هایی که باید ارسال شوند تا n_e کیوبیت سالم در بازه $\left[\frac{\pi}{۱۳}, \frac{\pi}{۱۲}\right]$ دریافت شود، مطابق سطر آخر جدول (۲) به‌دست می‌آید. این داده‌ها نشان می‌دهند که این روش انتقال داده یک ایده نظری است و اجرای آن در عمل بسیار سخت است.

جدول (۲): استفاده از روش فروش مازاد در یک آزمایش دو شکاف یانگ دارای چشمه نوری چند رنگ، به منظور تخمین تعداد فوتونی که باید چشمه ارسال کند ($\tilde{n}_s$) تا با فرض $\varepsilon = ۰/۰۱$، برخورد تعداد n_e فوتون به پرده درون بازه A، تضمین شود.

A	p_A	$\tilde{n}_s$		
		$n_e = ۱۰^{۵}$	$n_e = ۱۰^{۴}$	$n_e = ۱۰^{۳}$
$\left[-\frac{\pi}{۳}, \frac{\pi}{۳}\right]$	۰/۱۷۷	۵۶۱۵۹۹	۵۵۳۵۵	۵۲۸۸
$\left[-\frac{\pi}{۴}, \frac{\pi}{۴}\right]$	۰/۰۹۷۰	۱۰۲۳۶۳۴	۱۰۰۸۲۷	۹۶۱۱
$\left[۰, \frac{\pi}{۱۰}\right]$	۰/۰۱۳۲	۷۵۳۲۶۶۱	۷۴۱۴۴۲	۷۰۵۱۷
$\left[۰, \frac{\pi}{۱۲}\right]$	۰/۰۱۲۸	۷۷۶۰۲۴۸	۷۶۳۸۴۱	۷۲۶۴۷
$\left[-\frac{\pi}{۱۰۰}, \frac{\pi}{۱۰۰}\right]$	۰/۰۰۶۲	۱۶۰۲۶۰۷۲	۱۵۷۷۳۶۲	۱۴۹۹۹۳
$\left[۰, \frac{\pi}{۵۰}\right]$	۰/۰۰۶۰	۱۶۶۱۲۶۶۰	۱۶۳۵۰۹۴	۱۵۵۴۸۲
$\left[۰, \frac{\pi}{۱۰۰}\right]$	۰/۰۰۳۱	۳۲۰۵۱۷۷۶	۳۱۵۴۶۱۰	۲۹۹۹۵۰
$\left[\frac{\pi}{۱۳}, \frac{\pi}{۱۲}\right]$	$۱/۳۶ \times ۱۰^{-۶}$	۷۲۸۲۰۵۳۳۸۰۷	۷۱۶۶۹۸۶۴۸۱	۶۸۱۴۰۵۱۱۶

۵- تخمین نرخ ارسال برای چند پروتکل QKD

در بخش‌های قبل، روشی جهت یافتن تعداد کیوبیت ارسالی لازم برای دریافت تعداد مشخصی کیوبیت مطلوب شرح داده شد. بر پایه یک آزمایش فیزیکی ساده، عبارت «کیوبیت مطلوب» به کیوبیت‌هایی اطلاق می‌شد که بر محدوده مشخصی از پرده فرود می‌آمدند. اکنون، می‌توانیم این مفهوم را برای پروتکل‌های توزیع کلید به «کیوبیت‌هایی که به‌عنوان کلید قابل استفاده‌اند» تعمیم دهیم. بنابراین، منظور از «تعداد کیوبیت‌های مطلوب مورد نظر»، طول کلید مطلوب خواهد بود.

پروتکل‌های QKD مختلف برای به‌دست آوردن کلید امن شامل مراحل گوناگونی هستند. علاوه بر آن، روش‌های متنوعی برای تصفیه کلید[1] و تقویت محرمانگی[2] هم پیشنهاد شده‌اند که برای افزایش طول کلید، و در صورت نیاز، برای کشف اخلال‌گر[3] قابل استفاده‌اند. از این‌رو، بنا به سطح امنیتی مورد نیاز، می‌توان تعریف کلید مطلوب را به «کلیدی که پس از انجام مجموعه‌ای متشکل از گام‌های پروتکل و تصفیه و اصلاح کلید و تقویت امنیت، برای رمزنگاری قابل استفاده است» تعمیم داد، و سپس ایده فروش مازاد را برای این تعریف جدید اعمال کرد.

پروتکل BB84 به‌عنوان اولین و مشهورترین پروتکل توزیع کلید کوانتومی، در مطالعات و مقالات بسیاری مورد توجه بوده است. برای نمونه، در مرجع [۱۲] تغییرات نرخ کلید آن بر حسب نرخ خطای اندازه‌گیری "مقدار چشم‌داشتی عملگرهای خطا" محاسبه شده است. در همان مرجع این تغییرات برای پروتکل مشهور دیگر یعنی Six-State هم به‌دست آمده است. اما همان‌طور که پیش از این هم اشاره شد، نرخ کلید نشان‌دهنده بازدهی پروتکل به‌ازای هر بیت یا کیوبیتی است که در هر دور از انجام پروتکل ارسال می‌شود. بنابراین، می‌توان آن را معادل احتمال سالم رسیدن یک بیت یا کیوبیت و منتج شدن آن به یک بیت از کلید دانست (که همان احتمال تبدیل شدن به بیت یا کیوبیت مطلوب است). بنابراین، بر اساس داده‌های [۱۲]، می‌توانیم با جایگزینی نرخ کلید به‌جای p_A در رابطه (۴)، رشد تعداد کیوبیت ارسالی برای رسیدن به کلیدی به طول $n_e = ۱۰^{۵}$ بیت را برحسب رشد نرخ خطای اندازه‌گیری در هر دو پروتکل (BB84 و Six-State) به‌دست آوریم. نمودار این رشد برای $\varepsilon = ۰/۰۱$ در شکل (۲) دیده می‌شود.

همچنین می‌توانیم نمودار مشابهی را برای تعمیم BB84 به کیوبیت‌های d- حالته (کیودیت[4]) به‌دست آوریم. اما از آنجا که

1- Key Distillation
2- Privacy Amplification
3- Eavesdropper
4- Qudit

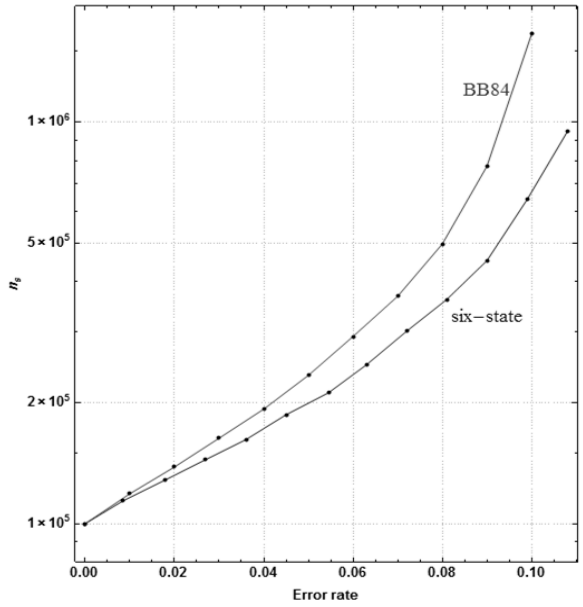
هر کیودیت حامل حداکثر $\log(d)$ بیت داده است، در پروتکل‌های متکی به کیودیت‌ها، نرخ کلید برابر با تعداد بیت‌های مطلوب در ارسال هر یک کیودیت در نظر گرفته می‌شود. لذا، این مقدار می‌تواند بین صفر (۰) و $\log(d)$ و بنابراین، بزرگتر از یک باشد. اکنون برای استفاده از آن به‌جای p_A در رابطه (۴) کافی است مقدار آن را بر $\log(d)$ تقسیم نماییم. به این ترتیب تعداد بیت ارسالی مورد نیاز برای داشتن کلیدی با طول مشخص به‌دست خواهد آمد. در شکل (۳) نتایج برحسب مقادیر مختلف نرخ خطای عملگر، برای $d = ۶, ۸, ۱۰$ و $\varepsilon = ۰/۰۱$ نشان داده شده‌اند. این نمودارها بر پایه داده‌های [۱۲] به‌دست آمده‌اند.

همچنین رشد نمایی تعداد کیوبیت ارسالی (n_s) بر حسب نرخ خطای اندازه‌گیری در نمودارهای شکل‌های (۲ و ۳) دیده می‌شوند. مقایسه این نمودارها با نمودارهای [۱۲] به خوبی نشان می‌دهند که بین n_s و نرخ کلید، به‌عنوان توابعی از نرخ خطای اندازه‌گیری، رابطه معکوس وجود دارد.

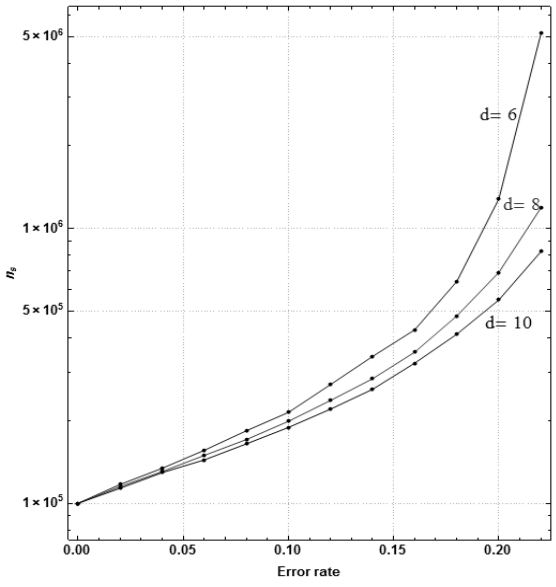
تعداد اندکی از منابع در کنار نرخ کلید (یا به‌جای آن) به بررسی نرخ ارسال پرداخته‌اند. برای مثال، در قسمت پایانی مرجع [۷] تعداد کیوبیت مورد نیاز برای به‌دست آوردن کلید تصفیه شده‌ای با طول مشخص، که در یک پروتکل BB84 با شرط امنیتی ویژه (امنیت کاربسته[1]) صدق کند، محاسبه شده است. طبق قضیه ۱ در [۷]، لازمه برآوردن امنیت کاربسته، آن است که تعداد کیوبیت ارسالی (در نمادگذاری ما n_s) از تابع بتای اویلر[2] تبعیت کند. این امر، به نتایجی که ما بر مبنای توزیع دوجمله‌ای برای این پروتکل به‌دست آورده‌ایم بسیار نزدیک است.

شکل (۴- الف) رشد نمایی n_s را در مقیاس‌های مختلف بر حسب نرخ خطای بیت کوانتومی به‌ازای $\varepsilon = ۰/۰۱$ نشان می‌دهد. البته تفاوت اندک موجود بین این نمودار و نمودار مشابه آن در شکل (۳) از مرجع [۷]، برخاسته از تفاوت در تعریف نرخ بیت مطلوب است، چرا که ما پروتکل را بدون شرط امنیت کاربسته در نظر گرفته‌ایم.

نمودار شکل (۴- ب)، نتایج مشابهی را برای پروتکل Six-State به تصویر کشیده است. این نمودار نشان می‌دهد که در شرایط مشابه از نظر نرخ خطای کوانتومی (در سامانه‌های اندازه‌گیری) و بدون استفاده از روش‌های بهبود امنیت، پروتکل Six-State نرخ ارسال کمتری نسبت به پروتکل BB84 دارد. از این‌رو، در صورتی که زیرساخت لازم برای پیاده‌سازی سامانه‌های مربوط به پروتکل Six-State فراهم باشد، می‌توان با ارسال کیوبیت کمتری به کلیدهای با طول مورد نظر دست یافت.

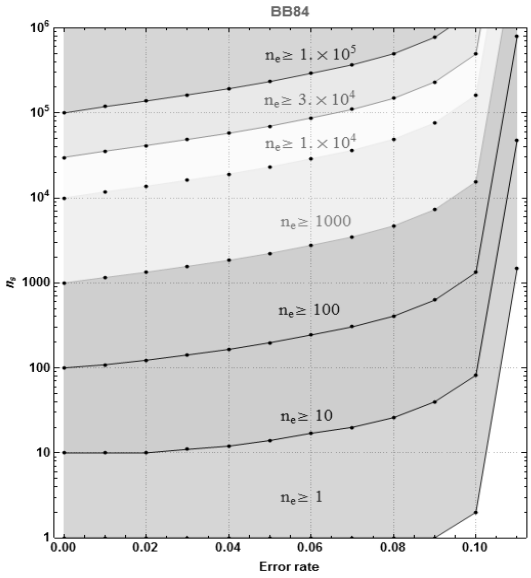


شکل (۲): تغییرات تعداد کیوبیت ارسالی (n_s) لازم برای به‌دست آوردن کلید $۱۰^۵$ بیتی با افزایش نرخ خطا، برای دو پروتکل BB84 (خط بالایی) و Six-State (خط پایینی) به‌ازای $\varepsilon = ۰/۰۱$.

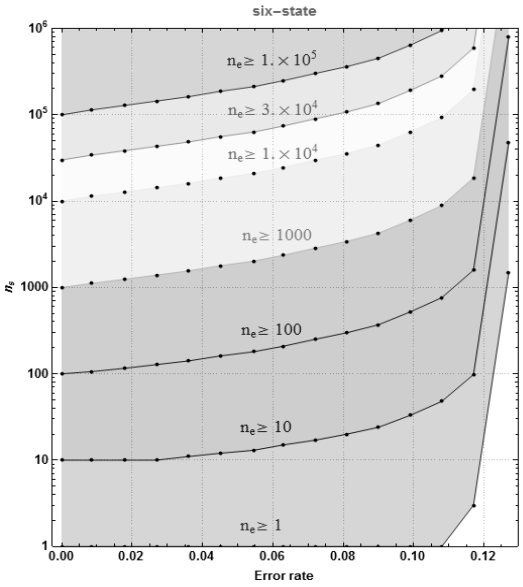


شکل (۳): تغییرات تعداد کیوبیت ارسالی (n_s) لازم برای به‌دست آوردن کلید $۱۰^۵$ بیتی با افزایش نرخ خطا، برای تعمیم BB84 به کیوبیت‌های d-حالته به ازای $d = ۶, ۸, ۱۰$ و $\varepsilon = ۰/۰۱$.

1- pragmatic security
2- regularized incomplete beta function



(الف)



(ب)

شکل (۴): رشد نمایی تعداد کیوبیت ارسالی (n_s) با افزایش نرخ خطای بیت کوانتومی به‌ازای مقادیر مختلف n_e و با $\varepsilon = ۰/۰۱$، **(الف)** برای پروتکل BB84 و **(ب)** برای پروتکل Six-State.

۶- نتیجه‌گیری

در این مقاله، ایده فروش مازاد در صنعت حمل و نقل برای بررسی چگونگی محاسبه تعداد بیت (یا کیوبیت) ارسالی لازم در یک فرآیند تبادل بیت، در نظریه اطلاعات (کوانتومی) و برای دست‌یابی به تعداد مشخصی بیت (یا کیوبیت) مطلوب، به‌کار گرفته شد. با این کار، شاخصی بر پایه کمیت بازدهی، مثلاً نرخ کلید در پروتکل‌های QKD، به‌دست آمد. ایده استفاده شده در این کار بر مبنای فرآیند برنولی است که در آن تعداد موفقیت‌ها در تعداد متناهی رویداد دودویی (دارای فقط دو نتیجه موفقیت یا شکست) از توزیع دوجمله‌ای به‌دست می‌آید. لذا، به عکس می‌توان کمترین تعداد رویداد (n_s) را برای به‌دست آوردن تعداد مشخصی موفقیت (n_e) پیدا کرد. در این مقاله، این ایده ابتدا برای یک سامانه ارسال اطلاعات بر پایه آزمایش دو شکاف یانگ استفاده گردید و بر این اساس، نحوه به‌کار بستن این ایده، برای یک سامانه تبادل بیت کوانتومی شرح داده شد. سپس، بر مبنای این روش، چگونگی محاسبه نرخ ارسال مورد نیاز برای دریافت تعداد معلومی بیت کلید مطلوب در یک پروتکل QKD توضیح داده شد. اغلب، منظور از عبارت «بیت کلید مطلوب» بیت‌های کلیدی است که احتمالاً تصفیه شده و سطح امنیت آن با استفاده از رویکردهای افزایش محرمانگی تقویت شده است. نمودارهای نتایج محاسبات برای دو پروتکل BB84 (و برخی تعمیم‌های آن) و Six-State، به‌دست آمده‌اند. این نتایج رشد نمایی n_s را با افزایش نرخ خطای کیوبیت نشان می‌دهند. مقایسه عددی این نتایج با تعدادی از مقالات اخیر، به ویژه منحنی‌های شکل (۳) در مرجع [۷]، یافته‌های حاصل‌شده در این مقاله را تأیید می‌نماید و نشان می‌دهد که روش جدید ارائه‌شده برای نرخ ارسال، که یک روش عمومی و قابل استفاده برای هر سامانه تبادل کیوبیت است، با دقت مناسبی همان نتایج محاسبه‌شده برای حالت‌های خاص در سایر مقالات را به‌دست می‌آورد.

با توجه به این که در این مقاله فقط از توزیع دوجمله‌ای برای محاسبه نرخ ارسال استفاده شده است، استفاده از توزیع دوجمله‌ای منفی (که توزیع تعداد شکست‌ها در یک فرآیند برنولی، پیش از اولین پیروزی است) و بررسی ویژگی‌های شاخص به‌دست‌آمده از آن را به‌عنوان موضوعی برای ادامه کار این مقاله پیشنهاد می‌کنیم.

۷- منابع

[1] S. Barnett, "Quantum information," Oxford Univ. Press, New York, 2009.

[2] S. A. Oskoueian and N. Bagheri, "Differential cryptanalysis of round-reduced SIMON32 and SIMON48 and SIMON64," Journal of Electronical & Cyber Defence, vol. 5, pp. 1-8, 2017 (In Persian).

[3] J. Pu and S. Chao, "Spectral anomalies in Young's double-slit interference experiment," Optics Express, vol. 12, pp. 5131-5139, 2004.

[4] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Information, vol. 2, 16025, 2016.

[5] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, R. Engle, C. McLaughlin, and G. Baumgartner, "Modeling, simulation, and performance analysis of

decoy state enabled quantum key distribution systems," Applied Sciences, vol. 7, 212, 2017.

[6] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," Physical Review A, vol. 95, 012333, 2017.

[7] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, "Experimental quantum key distribution with finite-key security analysis for noisy channels," Nature Communications, vol. 4, 2363, 2013.

[8] F. L. Pedrotti, L. M. Pedrotti, and L. S. Pedrotti, "Introduction to optics," Pearson Publishing, 3rd Edition, Harlow, 2014.

[9] W. Rueckner and J. Peidle, "Young's double-slit experiment with single photons and quantum eraser," American Journal of Physics, vol. 81, pp. 951-958, 2013.

[10] A. Gaeeni, "An introduction to the probability theory," Imam Hossein Univ. Press, Tehran, 2006 (In Persian).

[11] M. Born, E. Wolf, A. B. Bhatia, P. C. Clemmow, D. Gabor, A. R. Stokes, A. M. Taylor, P. A. Wayman, and W. L. Wilcock, "Principles of optics, electromagnetic theory of propagation, interference and diffraction of light," Cambridge Univ. Press, 7th Edition, 1999.

[12] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution," Nature Communications, vol. 7, 11712, 2016.

Journal of Electronical & Cyber Defence
Vol. 7, No. 1, 2019, Serial No. 25

A New Approach for Estimating the Rate of Emission in Quantum Bit Exchange Systems Using Binomial Distribution

S. M. Hosseini, S. Janbaz, M. Davoudi Darareh*, A. Zaghian

*Malek-Ashtar University of Technology
(Received: 14/02/2018, Accepted: 27/05/2018)

ABSTRACT

Information theoretic bit exchange algorithms are usually evaluated by their efficiency, which is the number of successfully received bits with respect to the number of sent bits. Though, this is also the case in the quantum version of the information theory, another indicator can be derived based on it, to give a view of the costs of the algorithm. This indicator is simply the number of qubits that must be sent to obtain a desired bit string. Depending on the expected length of the output of the algorithm, this indicator reveals more detailed information about the number of qubits that must be emitted, and better estimates the implementation costs, while efficiency is an indicator that can evaluate algorithms only theoretically. We employed the idea of overselling in a transportation ticketing scheme to illustrate how to apply the binomial distribution to calculate the alternative indicator. The scheme is first reworded to fit the concepts and notations of a quantum information encoding system based on the double-slit experiment; typical results are represented. Finally, the scheme is applied to the QKD protocols such as BB84 and Six-State, for calculating the number of qubits necessary to send in order to obtain a key of the desired length, in terms of the error rate.

Keywords: Rate of Emission, Overselling, Double-slit Experiment, Quantum Key Distribution, Key Rate

* Corresponding Author Email: m.davoudi@mut-es.ac.ir