Scientific Journal of Electronic & Cyber Defense
Vol. 12, No. 2, Summer 2024, Serial No. 46
ISSN: 2322-4347 , E-ISSN: 2980-8979

DAS system performance improvement algorithm based on quantum technology

A. Soleimani[1], A. Naseri[2]*
Associate Professor, Imam Hossein ،University, Tehran, Iran.

(Received: 2024/04/27, Revised: 2024/07/08, Accepted: 2024/08/03, Published: 2024/08/31)
DOR:

ABSTRACT

Fiber optic eavesdropping has always been and will be the focus of various sectors of electronic and cyber warfare in the defense and security sector. So far, many efforts have been made at the global level to monitor the performance of the fiber optic communication link, the results of which can be expressed in the form of DAS and OTDR technologies. Unfortunately, both methods are unable to distinguish the listening systems from the fiberoptics in front of the advanced fever and listening techniques.In this article, the properties of quantum technology in the field of quantum key distribution are used to improve the performance of DAS, and an algorithm is proposed that is capable of detecting the fiber listening system with high accuracy in addition to monitoring the losses in the optical fiber communication link. specifies The results of the proposed algorithm indicate that this algorithm is able to detect the presence of a listening device with 98% accuracy, detect people within a radius of 2 meters with an accuracy of over 70%, and detect a motorcycle within a radius of 20 meters with an accuracy of over 72%. More than 75% of light vehicle detection in a radius of 120 meters and more than 76% accuracy of heavy vehicle detection in a radius of 180 meters of optical fiber.

Keywords: Tapping , DAS, OTDR, VOTDR, ,Quantum key, QKD DV, QKD CV.

*Corresponding Author Email: parmis2159@gmail.com

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۲، تابستان ۱۴۰۳، ص ۹۷-۸۵

علمی – پژوهشی

روش پیشنهادی برای بهبود عملکرد سامانه DAS مبتنی بر فناوری کوانتومی

سید علی سلیمانی [۱]، علی ناصری [۲*]

۱- دانشجوی دکتری ، دانشگاه صنعتی مالک‌اشتر، تهران، ایران. ۲- دانشیار، دانشگاه امام حسین (ع)، تهران، ایران.

(دریافت: ۱۴۰۳/۰۲/۰۸، بازنگری: ۱۴۰۳/۰۴/۱۸، پذیرش: ۱۴۰۳/۰۵/۱۳، انتشار: ۱۴۰۳/۰۶/۱۰)

DOR:

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

تب زنی باانگیزه شنود از فیبر نوری همواره مورد توجه بخش‌های مختلف جنگ الکترونیک و سایبری بخش دفاعی و امنیتی بوده و خواهد بود. تلاش‌های زیادی تاکنون در سطح جهانی برای مانیتورینگ عملکرد لینک ارتباط فیبر نوری انجام شده است که حاصل آنها را می‌توان در قالب فناوری‌های DAS و OTDR بیان نمود. متأسفانه هر دو روش در مقابل تکنیک‌های پیشرفته تب زنی و شنود، ناتوان می‌باشند به عبارتی قادر به تشخیص سامانه‌های شنود از فیبر نوری نیستند. در این مقاله از خواص فناوری کوانتوم در حوزه توزیع کلید کوانتومی برای بهبود عملکرد DAS بهره گرفته می‌شود و الگوریتمی پیشنهاد می‌گردد که قادر است علاوه بر مانیتورینگ تلفات در مسیر لینک ارتباط فیبر نوری، سامانه شنود از فیبر را بادقت بالایی شناسایی و محل آن را مشخص می‌نماید. نتایج حاصل از الگوریتم پیشنهادی حاکی از این است که این الگوریتم قادر است بادقت ۹۸ درصد وجود سامانه شنود را تشخیص، بادقت بالای ۷۰ درصد تشخیص نفر در شعاع ۲ متری، بادقت بالای ۷۲ درصد تشخیص موتورسیکلت در شعاع ۲۰ متری، بادقت بالای ۷۵ درصد تشخیص خودرو سبک در شعاع ۱۲۰ متری و بادقت بالای ۷۶ درصد تشخیص خودرو سنگین در شعاع ۱۸۰ متری فیبر نوری را انجام دهد.

کلیدواژه‌ها: تب زنی، VOTDR،OTDR،DAS، کلید کوانتومی، QKD CV،QKD DV

۱- مقدمه

ارتباطات، مهم‌ترین رکن پشتیبانی صحنه نبرد محسوب می‌شود. این موضوع به حدی اهمیت یافته که ارتباطات را رکن عملیات آینده بر می‌شمارند و سناریوهای عملیاتی را مبتنی بر توانمندی و قابلیت‌های ارتباطی تدوین می‌نمایند. امروزه ضرورت تبادل اطلاعات اعم از صوت، تصویر و ویدئو در همه سطوح واضح و روشن است. موفقیت صحنه نبرد کاملاً به کار آیی امن شبکه و سامانه فرماندهی و کنترل وابسته است. به همان میزان که ارتباطات در موفقیت صحنه عملیات مؤثرتر می‌گردد به همان میزان هم انگیزه طرف مقابل برای شنود، فریب، اختلال و تخریب ارتباطات بیشتر می‌شود.

از طرفی در صحنه عملیات طرفی که توانایی و قدرت دسترسی و دستیابی به اطلاعات طرف مقابل را داشته باشد، احتمال پیروزی آن چندین برابر می‌گردد.

همگرایی و فرماندهی مناسب بر صحنه عملیات مستلزم بهره‌گیری مناسب از فناوری‌های روز ارتباطی، اطلاعاتی و امنیتی و حفاظت و حراست از زیرساخت‌های مهم ارتباطی است.

زیرساخت‌های ارتباطی نظیر فیبر نوری یکی از مهم‌ترین و پرکاربردترین زیرساخت‌هاست. تب زنی این روزها به دلیل توسعه آشکارسازها و روش‌های استخراج سیگنال به‌شدت توسعه پیدا کرده است. این موضوع امنیت فیبر نوری را با چالش جدی مواجه نموده است. امروزه یکی از بزرگ‌ترین چالش‌های فنی ارتباطات فیبر نوری، محافظت فیبر نوری در مواجهه با تلاش‌های دشمن برای دسترسی و دستیابی به فیبر و محتوی آن است. در حال حاضر محافظت از فیبر نوری توسط سامانه‌های مرسوم نظیر OTDR[۲] و DAS[۳] می‌باشد. این سامانه‌ها قادر به تشخیص تب‌های غیرمجاز و به‌تبع آن شنود ناشی از آن نیستند. این مقاله با بهره‌گیری مناسب از خواص فناوری کوانتومی به رفع این موضوع می‌پردازد.

در سال‌های اخیر تحول شگرفی در توسعه فناوری‌های کوانتومی رخ‌داده است. نهادهای مطرح جهانی که آینده‌نگاری حوزه فناوری را انجام می‌دهد من‌جمله مرکز DCDC[۴] بریتانیا و آزمایشگاه لینکلن دانشگاه MIT[۵] بهره‌گیری از فناوری کوانتوم در

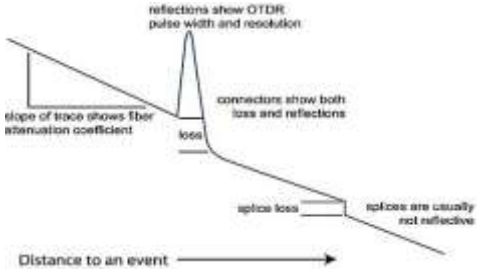
* رایانامه نویسنده مسئول: parmis2159@gmail.com

[2] Optical Time Domain Reflectometer
[3] Distributed Acoustic Sensing
[4] Development, Concepts and Doctrine Centre
[5]. Massachusetts Institute of Technology

عرصه‌های مختلف جامعه را پیش‌بینی نموده‌اند. از مهم‌ترین فناوری‌های حوزه کوانتوم، ارتباطات و توزیع کلید کوانتومی است که بسیار حائز اهمیت بوده و تحولی شگرف در حوزه ارتباطات امن به دنبال خواهد داشت. خواص کوانتومی می‌تواند در پایش فیبر نوری و تشخیص دقیق‌تر قطع‌شدگی و تلفات فیبر تأثیرگذار باشد.

۲- روش‌های مراقبت از فیبر نوری

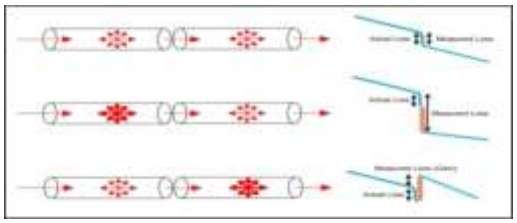
بزرگ‌ترین عامل اتلاف فیبر نوری پراکندگی می‌باشد. در فیبر، نور در تمام جهات پراکنده می‌شود که شامل بعضی از پراکندگی‌ها به سمت منبع نیز می‌باشد. سامانه OTDR[1] یا بازتاب‌سنج نوری بر پایه محدوده زمانی کار می‌کند. این سامانه نور را در فیبر ارسال نموده و با دریافتی نور برگشتی از فیبر میزان تضعیف فیبر و محل آن را شناسایی می‌نماید به عبارتی متناسب با نمودار میزان تضعیف نسبت به طول فیبر، محل قطع‌شدگی‌ها و نقاط دارای تلفات را در فیبر مشخص می‌کند. شکل ۱ یک نمونه نمودار سامانه OTDR را نشان می‌دهد.



شکل (۱): نمونه نمودار سامانه **OTDR** [۱]

OTDR شامل یک فرستنده لیزری با توان بالا می‌باشد که یک پالس نور را به درون فیبر ارسال می‌کند. نور پراکنده شده به عقب و نور منعکس شده، از طریق فیبر به سمت سامانه OTDR بر می‌گردد و در پایان از طریق یک متصل‌کننده OTDR به سمت یک گیرنده حساس هدایت شده می‌شود. در هر لحظه از زمان، نوری که OTDR دریافت می‌کند، نور پراکنده شده از عبور پالس از ناحیه‌ای از فیبر می‌باشد؛ بنابراین می‌تواند نمایشی از وضعیت فیبر در طول مسیر ارائه کند؛ لذا مقدار نور پراکنده برگشتی به OTDR متناسب با پراکندگی فیبر، وابسته به حداکثر قدرت پالس تست OTDR و طول پالس ارسال شده می‌باشد.

اتصالات و جوش‌ها در اصطلاحات OTDR حوادث نامیده می‌شوند که هر دو باید اتلاف را نشان بدهند. کانکتورها و جوش‌های مکانیکی یک نقطه اوج از بازتاب را نشان خواهند داد. ارتفاع این نقطه اوج مقدار بازتاب را در حوادث نشان می‌دهد. مگر اینکه آن آن‌قدر بزرگ باشد که گیرنده OTDR را اشباع کند و قادر به نمایش آن نباشد در این حالت در نقطه اوج ممکن است یک سطح صاف و ادامه‌دار تا انتها داشته باشد که نشان می‌دهد گیرنده overload شده است. گاهی اوقات اتلاف یک جوش فیوژن خوب، آن‌قدر کوچک است که قابل‌دیدن با OTDR نمی‌باشد که ممکن است اپراتور را گیج کند. در OTDR خیلی مهم است که طول تمام کابل‌های شبکه را بدانید. با این کار eventها را می‌توان فهمید که در کجا بایستی مشاهده کرد. پالس‌های انعکاسی نشانگر دقت OTDR می‌باشد. عملکرد OTDR جهت اندازه‌گیری تضعیف روی فیبر در شکل ۲ نشان‌داده‌شده است[۱].



شکل (۲): عملکرد **OTDR** جهت اندازه‌گیری تضعیف روی فیبر[۱]

۲- ۳- سامانه DAS

حفاظت فیزیکی از زیرساخت‌های کشورها همواره مورد توجه بوده و خواهد بود. در بین این زیرساخت‌ها یکی از مهم‌ترین آن‌ها زیرساخت‌های ارتباطی و فناوری اطلاعات می‌باشند؛ زیرا حاوی اطلاعات بوده که حفظ آنها از اهمیت بالایی برخوردار است. حسگر تمام توزیع شده فیبر نوری لرزش و صوت، یک حسگر حفاظت فیزیکی است که با استفاده از سیگنال‌های نوری و با استفاده از فیبر نوری به حفظ حریم‌ها می‌پردازد. این حسگرها، کاربردهای بسیاری از جمله موارد زیر را دارند:

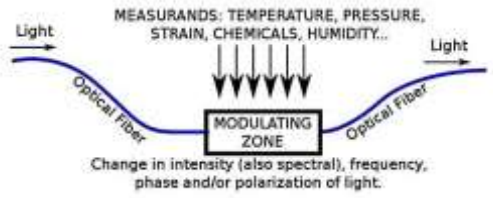
- ❖ حفاظت فیزیکی خطوط انتقال
- ❖ حفاظت فیزیکی فیبر نوری و فناوری آنتی تپ حفاظت فیزیکی خطوط انتقال
- ❖ مرزبانی برای مسافت‌های بسیار طولانی
- ❖ حسگرهای صوت

وقتی که لرزش در جایی از فیبر نوری به فیبر اعمال شود، طبیعتاً ضریب شکست خیلی کم تغییر می‌کند که منجر به تغییر فاز در پالس ارسال شده خواهد شد. سامانه حسگر صوتی توزیع‌شده (DAS) از بازتاب سنجی دامنه نوری حساس به فاز برای شناسایی و یافتن وقایع حتی لرزش‌های ضعیف استفاده می‌کند. این سامانه از یک لیزر پالسی همدوس استفاده می‌کند. لرزش باعث تغییر فاز می‌شود و تغییر سیگنال تداخلی را موجب می‌شود. با تغییر شدت سیگنال رایلی در زمان‌ها و مکان‌های متفاوت، امکان آشکارسازی لرزش و مکان لرزش در جای‌جای فیبر فراهم می‌شود.

اساس کار سامانه حسگر توزیع شده صوت و لرزش در شکل ۳

[1] .Optical Time-domain Reflectometer

نشان داده شده است [۲].

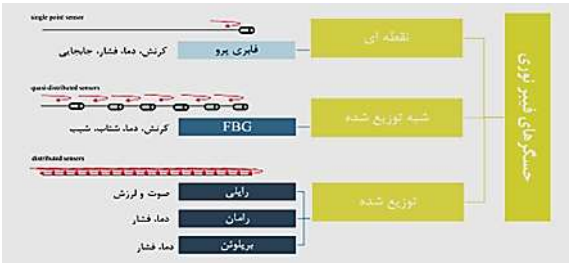


شکل (۳): اساس کار سامانه **DAS** [۲]

طرح کارکردی حسگرهای فیبر نوری در شکل ۴ آمده است [۲].

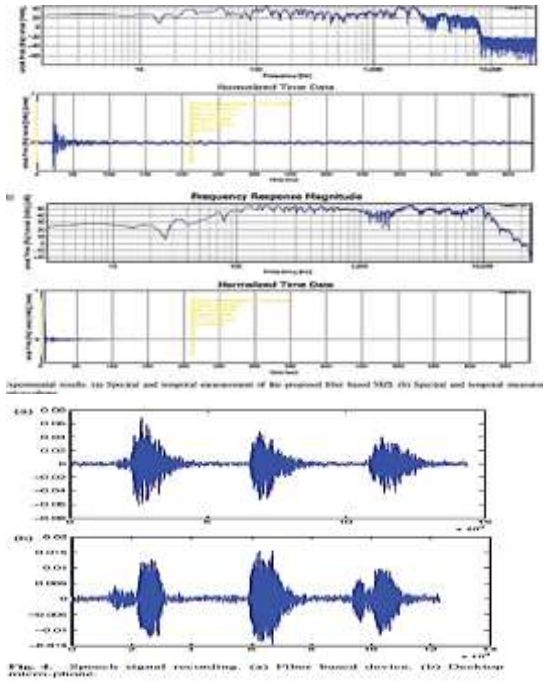
این سامانه‌ها بردی معادل ۵۰ تا ۱۵۰ کیلومتر و دقت مکان یابی زیر ۱۰ متر دارند.

نمونه‌ای از آشکارساز بلوک دیاگرام جمع‌آوری و پردازش صوت پیرامونی فیبر نوری در شکل ۴ به نمایش درآمده است[۲].

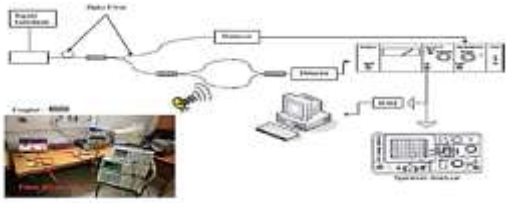


شکل (۴): نمونه‌ای از آشکارساز بلوک دیاگرام جمع‌آوری و پردازش صوت پیرامونی فیبر نوری [۲]

نمودار نتایج تست‌های انجام شده در شکل ۵ و نمونه‌ای از صوت جمع‌آوری شده و پردازش پیرامونی در شکل ۶ نشان‌داده‌شده است[۲].



شکل (۵): نمودار نتایج تست‌های انجام شده[۲]



شکل (۶): نمونه‌ای از صوت جمع‌آوری شده و پردازش پیرامونی [۲]

از قابلیت سامانه حسگر صوتی توزیع‌شده می‌توان به موارد زیر اشاره نمود:

- ✓ حساسیت بالا
- ✓ ابعاد کوچک و وزن سبک
- ✓ پهنای باند بزرگ
- ✓ عملکرد در دمای بالا
- ✓ توانایی سنجش توزیع‌شده
- ✓ ایمنی در برابر تداخل الکترومغناطیسی

نتایجی که از این ویژگی در سامانه حسگر توزیع‌شده صوت و لرزش (DAS) حاصل می‌شود عبارت‌اند از:

- ✓ تشخیص هم‌زمان چند نقطه هدف و اعلام زنگ هشدار برای تمام نقاط تشخیص‌داده‌شده
- ✓ شناسایی هوشمند انواع رویداد برای کاربردهای مختلف
- ✓ نظارت بر نشت
- ✓ نظارت بر نفوذ شخص متجاوز
- ✓ نظارت بر عوارض زمین‌شناسی مانند رانش زمین و تشخیص اولیه لرزش زمین

۳- ۴- تپ زنی

یکی از چالش‌های جدی امنیت فیبر نوری، تلاش دشمن برای بهره‌برداری از روش‌های تب زنی و دسترسی به محتوای داده‌های روی فیبر است. سازمان‌ها با رمزنگاری تلاش می‌نمایند دستیابی به اطلاعات فیبر نوری را برای دشمن غیرممکن یا زمان‌بر نمایند. اما این امر مانع از نزدیکی دشمن به فیزیک فیبر نوری، تغییر در محتوای داده‌های روی فیبر و یا تزریق و تحکم و کنترل روی داده‌های فیبر نوری نمی‌شود.

روش‌های مرسوم استفاده از OTDR و سامانه‌های ONMS[1] نیز برای تشخیص افت ناشی از دسترسی‌های غیرمجاز به فیبر نوری کفایت از حل مشکلات ناشی از چالش‌های فوق نیست.

باتوجه‌به روش‌های تپ زنی در حال حاضر، تپ زنی بدون ایجاد ارتعاش یا بدون لمس کابل فیبر نوری، غیرممکن است؛ لذا سیستم‌های تپ زن باید بتوانند به کابل فیبر نوری دسترسی پیدا کنند. تپ زنی امروزه یکی از تهدیدات بزرگ زیرساخت‌های ارتباطی نظیر فیبر نوری است که مخاطرات ناشی از آن می‌تواند هر سازمانی را با چالش‌های جدی و شکست‌های بزرگ روبرو

[1] Optical Network Management System

نماید. استراتژی برخورد با تپ به سه بخش تقسیم می‌گردد.[۲]

- ✓ پیشگیری از تپ زنی‌های آتی
- ✓ پیداکردن تپ‌های موجود روی خطوط
- ✓ تضمین امنیت خط

برای آشکارسازی تپ‌های موجود روش‌های استفاده از OTDRهای دقیق موسوم به VOTDR[1] توصیه شده است. متأسفانه به دلیل شرایط خطوط فیبر نوری این روش، نقاط خطای بسیار بالایی دارد که استفاده از این سیستم‌ها را با سختی مواجه می‌کند. در نتیجه استفاده از سیستم‌های بر خط VOTDR به‌صورت کمکی در کنار تکنیک پیشنهادی توصیه می‌گردد. در مرجع [۳]موضوع امن‌سازی ارتباط با هشدارهای کوانتوم مفصل بحث شده.

۴- ۵- توزیع کلید کوانتومی

در رمزنگاری کلاسیک هنگامی که یک کلید برای رمزگذاری و رمزگشایی وجود دارد به آن رمزنگاری متقارن گفته می‌شود. با استفاده از علم ریاضیات و کمک رایانه‌ها، می‌توان کلیدهایی تولید کرد که بسیار بزرگ‌تر باشد و حدس‌زدن آن بسیار سخت‌تر باشد. اما مسئله بالقوه دیگر این است که این امکان وجود دارد که این کلیدها توسط یک فرد غیرمجاز خوانده شود. پس در زمینه رمزنگاری متقارن دو چالش عمده وجود دارد. یکی آن که کلیدی که انتخاب می‌شود باید از پیچیدگی لازم برخوردار باشد. دوم آن که کلید انتخابی باید به طور امن بین دو طرف تبادل گردد، طور یکه هیچ‌کس قادر به کشف یا شنود آن نباشد[۴]. رمزنگاری با کلید عمومی که با نام رمزنگاری نامتقارن نیز شناخته می‌شود، راه‌حلی دقیق برای حل چالش‌های فوق دارد. این روش رمزنگاری اجازه می‌دهد تا هر فرد در یک مکالمه دو کلید عمومی و خصوصی ایجاد کند. اگر پیامی را با استفاده از کلید عمومی شخص گیرنده رمزگذاری شود، گیرنده می‌تواند آن را با استفاده از کلید خصوصی منطبق خود رمزگشایی کند.

رمزنگاری کلید عمومی این مزیت را دارد که شما نیازی به انتقال مخفیانه کلید رمزگشایی به گیرنده پیام مخفی خود را نداشته باشید؛ زیرا آن شخص قبلاً کلید رمزگشایی را دارد. کلید رمزگشایی کلید خصوصی آنهاست؛ بنابراین، تنها چیزی که برای ارسال پیام نیاز است کلید رمزگذاری عمومی و منطبق با گیرنده است. شما می‌توانید کلید عمومی گیرنده را به‌راحتی به دست آورید، زیرا گیرنده می‌تواند کلید عمومی خود را با هر کسی به اشتراک بگذارد، زیرا کلیدهای عمومی فقط برای رمزگذاری پیام‌ها استفاده می‌شوند نه رمزگشایی آنها؛ بنابراین بر خلاف رمزنگاری متقارن، در رمزنگاری نامتقارن نیازی به تعویض کلید قبل از برقراری ارتباط نیست و این مزیت مهمی قلمداد می‌شود. معمولاً مرحله تبادل کلید رمزنگاری متقارن نیز با استفاده از طرح تبادل کلید عمومی انجام می‌شود.

با ظهور رایانه‌های کوانتومی، این امکان وجود دارد که روش‌های رمزنگاری نامتقارن نیز امنیت کنونی خود را از دست بدهند و تبادل کلید عمومی و متعاقباً رمزگذاری کلید خصوصی نیز با چالش جدی مواجه شود. امنیت رمزنگاری کلید عمومی بر فرض اثبات نشده دشواری در انجام برخی مسائل پیچیده ریاضی استوار است که در زمان معقولی با استفاده از رایانه‌های کلاسیک قابل‌حل نیستند. اما الگوریتم شُر نشان داد که پروتکل‌های رمزنگاری کلاسیک نظیر RSA[2] که مبتنی بر اعداد اول هستند به طور بالقوه در برابر رایانه‌های کوانتومی آسیب‌پذیر هستند[۵]. در واقع، رایانه‌های کوانتومی این پتانسیل را دارند که بتوانند چنین مسائل پیچیده ریاضی را در زمان کوتاهی بر روی رایانه‌های کوانتومی حل کنند[۵]. در نتیجه ظهور رایانه‌های کوانتومی، سیستم‌های رمزنگاری کلاسیک مانند DES[3]، RAS، DLP[4] و IEF[5] را منسوخ و توزیع کلید کنونی را غیر امن می‌کنند. پد یکبار مصرف یا OTP[6] نوعی رمزگذاری متقارن است که اگر به‌درستی پیاده‌سازی شود، از امنیت زیادی برخوردار بوده و خطر رایانه‌های کوانتومی را نیز برطرف می‌سازد. این روش می‌تواند چالش اول که حفظ پیچیدگی لازم است را با افزایش تعداد بیت‌ها برطرف سازد. از طرف دیگر به دلیل اینکه کلید فقط یک‌بار استفاده می‌شود به طور قابل اثباتی امن است. اما چالش دوم همچنان پابرجا است و توزیع خود کلید خصوصی از طریق یک کانال بالقوه ناامن یک چالش جدی قلمداد می‌شود.

تولید تک فوتون‌های کوانتومی از طریق تضعیف فوتون‌ها انجام می‌شود و یکی از بیشترین کاربردهای تبادل تک فوتون‌های کوانتومی استفاده در توزیع کلید کوانتومی یا QKD است.QKD این پتانسیل را ارائه می‌دهد که برای اولین‌بار در تاریخ بشر کانال‌های ارتباطی امن بین طرفین دور در لینک ارتباطی ایجاد شود. کانال‌های کوانتومی را می‌توان با فیبرهای نوری استاندارد مخابراتی یا با کانال‌های نوری فضای آزاد دارای دید مستقیم، تا حدودی تحقق بخشید.

برای چالش توزیع کلید خصوصی از طریق یک کانال بالقوه ناامن برای اولین‌بار آقای استفان ویزنر در سال ۱۹۷۰ ایده رمزنگاری کوانتومی را مطرح کرد و نشان داد که از ویژگی‌های منحصربه‌فرد ذرات کوانتومی می‌توان برای حل مشکل انتقال امن کلیدهای رمزنگاری استفاده کرد.

[1]The High Refresh Rate of The Instrumen Optical Time Domain Reflectometer

[2] Rivest–Shamir–Adleman
[3] Data Encryption Standard
[4] Data Loss Prevention
[5] International Energy Forum
[6] One Time Pad

۵- ۶- پروتکل‌های کوانتومی

پروتکل‌های کوانتومی مختلفی تاکنون ارائه شده است که در ادامه به طور اجمال توضیح هر کدام خواهد آمد[۵].

❖چرخاندن سکه کوانتومی

چرخاندن سکه کوانتومی یا QCF[1] پروتکلی است که برای برقراری ارتباط بین دو طرفی که به یکدیگر اعتماد ندارند استفاده می‌شود. مشابه توزیع کلید کوانتومی، شرکت‌کنندگان از طریق یک کانال کوانتومی ارتباط برقرار می‌کنند و از طریق انتقال کیوبیت‌ها اطلاعات را مبادله می‌کنند. بازیکن پذیرنده تا زمانی که اندازه‌گیری را انجام ندهد، اطلاعات موجود در کیوبیت را نمی‌داند. اطلاعات مربوط به هر کیوبیت روی یک فوتون ذخیره شده و توسط آن حمل می‌شود. اگرچه ورق‌زدن سکه کوانتومی وسیله‌ای امن برای برقراری ارتباط در تئوری است، اما به دلیل نیاز به حافظه‌های کوانتومی، منابع تک فوتون و آشکارسازهای تک فوتون، انجام آن دشوار است و سطح آمادگی فناوری بالایی ندارد.

❖امضای دیجیتال کوانتومی

امضای دیجیتال کوانتومی یا QDS[2] روشی برای حفاظت از رمزهای کلید عمومی در مقابل حملات کامپیوترهای کوانتومی است. امضای دیجیتال کلاسیک که در حال حاضر مورداستفاده قرار می‌گیرد قابلیت جعل دارد، ولی امضای دیجیتال کوانتومی در حالت ایده‌آل در برابر قدرتمندترین کامپیوترهای کلاسیک و کوانتومی مقاوم خواهد بود. سخت‌افزار موردنیاز برای پیاده‌سازی QDS مشابه سیستم‌های موردنیاز برای QKD است و ممکن است هر دو طرح QDS و QKD بتوانند به طور موازی در امتداد فیبرهای نوری مشابه با استفاده از سخت‌افزار ارسال و دریافت یکسان عمل کنند.

❖اشتراک‌گذاری راز کوانتومی

به‌اشتراک‌گذاری راز، یکی از مأموریت‌های ارتباطی اساسی در رمزنگاری کلاسیک است. هدف آن این است که یک پیام را به چند قسمت تقسیم کند به‌گونه‌ای که هیچ زیر مجموعه غیرمجاز برای بازسازی پیام اصلی کافی نباشد[۷].

ازآنجایی‌که در فعالیت‌های مشترک امن نقش دارد، اشتراک‌گذاری راز، یک مأموریت رمزنگاری اصلی برای ارتباطات چندجانبه، از جمله کنترل موشک‌ها را تشکیل می‌دهد[۸].

طرح‌های کلاسیک به‌اشتراک‌گذاری راز را می‌توان تنها بر اساس پیچیدگی ریاضی پیاده‌سازی کرد؛ بنابراین، با ظهور کامپیوترهای کوانتومی، اشتراک‌گذاری راز نیز مجبور می‌شود با قوانین مکانیک کوانتومی وارد عصر امن اطلاعاتی شود که به آن اشتراک‌گذاری راز کوانتومی یا QSS[3] اطلاق می‌شود. اولین پروتکل اشتراک‌گذاری مخفی کوانتومی در سال ۱۹۹۹ با استفاده از حالت درهم‌تنیده سه فوتون برای سه شرکت‌کننده پیشنهاد شد[۹].

بااین‌وجود، مشکلات در آماده‌سازی و انتقال حالت‌های درهم‌تنیده، نرخ کلید مخفی و فاصله انتقال QSS را محدود می‌کند و پیاده‌سازی عملی آن را با چالش جدی QSS مواجه کرده است. بر خلاف QKD، این روش در مقابل حملات اسب تروآ مقاوم است برای ارتباطات کوانتومی چندجانبه که یکی از سنگ بناهای اینترنت کوانتومی آینده است، ضروری است[۱۰].

در واقع QSS روشی برای به اشتراک گذاشتن پیام‌های مخفی بین اعضای یک گروه با حفظ کامل امنیت اطلاعات است. بااین‌حال، محدودیت‌های نرخ - فاصله به‌شدت نرخ کلید امن و فاصله انتقال QSS را محدود می‌کند.

❖پروتکل BB84[4]

در سال ۱۹۸۴، چارلز بنت و ژیل براسارد اولین پروتکل رمزنگاری کوانتومی که امروزه با نام BB84 شناخته می‌شود را معرفی کردند[۱۱].

پروتکل BB84 یکی از روش‌های توزیع کلید کوانتومی است و به طور قابل اثباتی امن است. در این پروتکل وجود یک کانال کوانتومی برای انتقال کلید کوانتومی و یک کانال کلاسیک معتبر برای انتقال داده الزامی است. معمولاً از فوتون‌های قطبش یافته برای انتقال اطلاعات از طریق کانال کوانتومی استفاده می‌شود، جایی که فرستنده به طور تصادفی حالت‌های قطبش را با استفاده از مولد اعداد تصادفی ایجاد می‌کند. معمولاً به‌عنوان روشی برای برقراری ارتباط امن کلید خصوصی ازیک‌طرف به‌طرف دیگر برای استفاده در رمزگذاری پد یکبار مصرف استفاده می‌شود. این روش هنوز هم یکی از پروتکل‌های مهم توزیع کلید کوانتومی به شمار می‌رود. در علم رمزنگاری، پد یکبار مصرف یک تکنیک رمزگذاری است که در آن از یک کلید یکبار مصرف استفاده می‌شود. طول این کلید کوچک‌تر از پیام ارسال شده نیست و بایستی از قبل به اشتراک گذاشته شده باشد. در این تکنیک، اطلاعات رمزگذاری نشده با یک کلید مخفی تصادفی یا همان پد یکبار مصرف جفت می‌شود، سپس با استفاده از ترکیب هر بیت یا کاراکتر اطلاعات رمزگذاری نشده با بیت یا کاراکتر مربوطه از پد یکبار مصرف به روش هم‌نهشتی اطلاعات رمزگذاری می‌شود. در حالت ایده‌آل،

[1] Qualifications and Credit Framework
[2] Quantom Digital Signature
[3] Quick Security Setup
[4] Charles Bennett and Gilles Brassard in 1984

پروتکل BB84 در برابر حملات آسیب‌ناپذیر است. اما در عمل، عوامل مختلفی مانند فقدان منابع و آشکارسازهای تک فوتون ایده‌آل و همچنین پیدایش تکنیک‌های استراق سمع پیشرفته پیاده‌سازی عملیاتی این پروتکل را با چالش مواجه کرده است.

❖ پروتکل T12

در پروتکل T12 به‌جای استفاده از منبع تک فوتون، فرض می‌شود که فرستنده دارای یک منبع با فاز تصادفی از حالت‌های همدوس است[۱۲]. پالس‌های نوری هم در شدت و هم در درجه آزادی دیگری مدوله می‌شوند که برای رمزگذاری اطلاعات کوانتومی استفاده می‌شود. این درجه آزادی می‌تواند قطبش یا فاز نسبی یک تداخل‌سنج ماخ زندر نامتقارن باشد. برای مدولاسیون شدت، فرستنده به طور تصادفی از بین سه مقدار ممکن انتخاب می‌کند. همچنین برای رمزگذاری، فرستنده به طور تصادفی یکی از چهار حالت ممکن را انتخاب می‌کند، درست مانند پروتکل استاندارد BB84. شدت‌ها و حالت‌ها به طور مستقل از هم توسط فرستنده انتخاب می‌شوند، به‌طوری‌که امکان جفت‌کردن هر حالت با شدت متفاوت وجود دارد. این امکان اجرای ساده‌تر را فراهم می‌کند و از همبستگی اتفاقی بین شدت و رمزگذاری اطلاعات جلوگیری می‌کند. علاوه بر این، می‌توان بیت‌های کلید را از هر دوپایه انتخاب کرد و در نتیجه مدل استاندارد BB84 را به‌عنوان یک مورد خاص زمانی به دست آورد. این سازگاری در عمل مفید است، زیرا نسبت بهینه بین پایه‌ها می‌تواند به ویژگی‌های کانال کوانتومی بستگی داشته باشد.

❖ پروتکل Decoy state

پروتکل حالت فریب به‌عنوان یکی از مهم‌ترین روش‌ها برای محافظت از امنیت توزیع کلید کوانتومی با استفاده از یک منبع همدوس تضعیف شده در نظر گرفته شده است. این پروتکل که در سال ۲۰۰۵ پیشنهاد شد در واقع روشی استاندارد برای بهبود پروتکل‌های توزیع کلید ارائه کرد[۱۳]. برای تولید حالت‌های فریب با شدت‌های مختلف معمولاً از مدولاسیون جریان پمپ در لیزرهای نیمه‌هادی و یا مدولاسیون خارجی توسط مدولاتورهای نوری استفاده می‌شود. استفاده از پروتکل BB84 همراه با روش حالت فریب در حال حاضر کاربردی‌ترین پروتکل توزیع کلید کوانتومی است که در رژیم کلید محدود در برابر حملات عمومی امن شده است. دلایل این موضوع عبارت‌اند از:

- ✓ در شرایطی که کانال کوانتومی تلفات بالایی داشته باشد، این پروتکل عملکرد مناسبی از خود نشان می‌دهد.
- ✓ تحقق آن با منابع نوری ارزان‌قیمت امکان‌پذیر است. گروه‌های تحقیقاتی متعددی نشان داده‌اند که در شرایط دنیای واقعی این روش انتقال کلید امکان‌پذیر است و از امنیت بالایی نیز برخوردار است. در حال حاضر، دستیابی به نرخ تولید کلید مخفی بالاتر و فاصله انتقال امن طولانی‌تر از مهم‌ترین روندهایی است که در گروه‌های تحقیقاتی و شرکت‌های فعال در این حوزه دنبال می‌شود.

❖ پروتکل SARG04[1]

این پروتکل در سال ۲۰۰۴ پیشنهاد شد. این یک پروتکل ساده است که از چهار حالت غیرمتعامد استفاده می‌کند. فرستنده به طور تصادفی یکی از چهار حالت ممکن را انتخاب می‌کند و رشته فوتون‌ها را برای گیرنده می‌فرستد. سپس گیرنده σx یا σz را اندازه‌گیری می‌کند.

بنابراین، در سطح کوانتومی مشابه BB84 است. اما تغییری در فرآیند غربال‌کردن کلاسیک وجود دارد. در این پروتکل، میانگین تعداد فوتون‌ها در هر پالس باید بزرگ‌تر در نظر گرفته شود. در جبران آن، این پروتکل سپر بهتری در برابر حمله تقسیم تعداد فوتون یا PNS در QBER=0 فراهم می‌کند[۱۴].

❖ پروتکل SSP[2]

پروتکل شش‌حالته یا به‌اختصار SSP در سال ۱۹۹۹ پیشنهاد شد. [۱۵]همان‌طور که از نام آن مشخص است، این پروتکل از شش حالت قطبش ممکن استفاده می‌کند؛ بنابراین در مجموع سه‌پایه به‌جای دوپایه در پروتکل BB84 وجود دارد. فرستنده به طور تصادفی از بین این شش حالت یک حالت را انتخاب می‌کند و آن را برای گیرنده می‌فرستد. گیرنده آن را در پایهx ، yیا z به طور تصادفی اندازه‌گیری می‌کند. در اینجا احتمال اینکه گیرنده و فرستنده یک‌پایه را انتخاب کنند به یک‌سوم کاهش می‌یابد، به این معنی که آنها باید به طور متوسط دو سوم بیت‌های ارسال شده را برای ایجاد یک کلید امن کنار بگذارند. اما به دلیل وجود حالت‌های احتمالی بیشتر از BB84، میزان خطای ناشی از اندازه‌گیری شنودگر افزایش خواهد یافت؛ بنابراین، حداکثر اطلاعات شنودگر کمتر از اطلاعات شنودگر در پروتکلBB84 خواهد بود. به‌این‌ترتیب، این پروتکل در برابر استراق سمع تک کیوبیت‌ها نسبت به طرح BB84 امن‌تر است.

❖ پروتکل E91

در این پروتکل که در سال ۱۹۹۹۱ پیشنهاد شد[۱۶]. از جفت فوتون‌های درهم‌تنیده برای توزیع کلید استفاده می‌شود. این جفت فوتون‌ها می‌تواند توسط فرستنده، گیرنده، و یا توسط منبعی جدا از هر دو ایجاد شود. فوتون‌ها به‌گونه‌ای توزیع

1.Valerio Scarani, Antonio Acin, Gregoire Ribordy, and Nicolas Gisin
2.State Scholarship Portal

می‌شوند که گیرنده و فرستنده هر کدام یک فوتون از هر جفت را داشته باشند. این پروتکل بر دو ویژگی درهم‌تنیدگی متکی است.
الف: حالت‌های درهم‌تنیده کاملاً همبستگی دارند به این معنا که اگر گیرنده و فرستنده هر دو اندازه‌گیری کنند که آیا ذرات آنها قطبش عمودی یا افقی دارند، همیشه یک پاسخ را با احتمال ۱۰۰ درصد دریافت می‌کنند. اگر هر دو جفت پلاریزاسیون مکمل (متعامد) دیگری را اندازه‌گیری کنند، همین امر صادق است.
ب: هر گونه تلاش برای استراق سمع توسط شنودگر، این همبستگی‌ها را به‌گونه‌ای از بین می‌برد که گیرنده و فرستنده می‌توانند تشخیص دهند. مشابهBB84 ، این پروتکل شامل یک پروتکل اندازه‌گیری خصوصی قبل از تشخیص حضور شنودگر است. برای تشخیص استراق سمع، گیرنده و فرستنده می‌توانند با پیاده‌سازی آزمایش‌های تست بل، نقض قضیه بل به واسطه شنود را مشاهده کنند. به‌طورکلی، پیاده‌سازی پروتکل‌های مبتنی بر درهم‌تنیدگی کوانتومی مثل E91 از پیاده‌سازی پروتکل‌های آماده‌سازی و اندازه‌گیری مثل BB84 دشوارتر است، به این دلیل که کانال کوانتومی درهم‌تنیدگی را در فواصل طولانی از بین می‌برد. بااین‌حال، هر دو نوع پروتکل در میان یک لینک ۱۰۰۰ کیلومتری با استفاده از ماهواره مدار پایین زمین آزمایش شده‌اند.

❖ پروتکل B92

این پروتکل در سال ۱۹۹۲ پیشنهاد شد.[۱۷]تفاوت اصلی B92 با BB84 در این است که فقط دو حالت قطبش به‌جای چهار حالت قطبش ممکن در BB84 ضرورت دارد. نتایج به‌دست‌آمده از یک تحقیق نشان می‌دهد که پروتکل BB84 عملکرد بهتری نسبت به B92 در توزیع امن کلید در فواصل طولانی از خود نشان می‌دهد، طور یکه برای یک نرخ تکرار ۱۰ مگاهرتز در ارتفاع مداری ۱۰۰ کیلومتر، نرخ بیت ارتباط امن برای پروتکل BB84 حدود ۲۸۰ کیلوهرتز و برای پروتکل B92 حدود ۷۰ کیلوهرتز ارزیابی شده است[۱۸].

❖ پروتکل BBM92

پروتکل BBM92 یک پروتکل توزیع کلید کوانتومی است که شامل جفت فوتون‌های درهم‌تنیده است و می‌تواند به‌عنوان یک نسخه مبتنی بر درهم‌تنیدگی از پروتکل BB84 در نظر گرفته شود. این پروتکل برای اولین‌بار در سال ۱۹۹۲ پیشنهاد شد[۱۹]. درحالی‌که پروتکل BB84 بر اساس آماده‌سازی و اندازه‌گیری حالت قطبش فوتون‌ها کار می‌کند، در پروتکل BBM92 یک تصادفی بودن ذاتی ناشی از اندازه‌گیری جفت فوتون‌های درهم‌تنیده وجود دارد. در این پروتکل، یک فرستنده مشترک اقدام یک جفت فوتون درهم‌تنیده تولید می‌کند و آنها را از طریق یک کانال کوانتومی برای هر دو طرف فرستنده و گیرنده کلید می‌فرستد. کانال‌های کوانتومی می‌توانند فضای آزاد، آب یا فیبر نوری باشند. گیرنده و فرستنده به طور مستقل اندازه‌گیری‌های خود را به‌صورت تصادفی انجام می‌دهند. هنگامی که اندازه‌گیری انجام شد، هر دو انتخاب‌های پایه خود را از طریق کانال عمومی اعلام می‌کنند. تنها آن اندازه‌گیری‌هایی که فرستنده و گیرنده پایه یکسانی را برای آن انتخاب کرده‌اند برای تولید کلید مورداستفاده قرار می‌گیرند و بقیه اندازه‌گیری‌ها ارزشی ندارند و کنار گذاشته می‌شوند. به کلیدی که پس از این فرآیند ساخته می‌شود، کلید غربال شده گفته می‌شود. علاوه بر این، برای دستیابی به یک کلید امن عملیات تصحیح خطا و تقویت حریم خصوصی بر روی کلید غربال شده انجام می‌شود. لازم به ذکر است که پروتکل‌های توزیع کلید مبتنی بر درهم‌تنیدگی یا به‌اختصار EBQKD[1] برای ارتباطات کوانتومی از راه دور مانند ماهواره به زمین ایده‌آل است، زیرا می‌تواند بین دو ایستگاه زمینی دور از هم یک ارتباط امن برقرار کند. همچنین، صرف‌نظر از اینکه ماهواره توزیع‌کننده جفت فوتون‌های درهم‌تنیده قابل‌اعتماد است یا خیر، امنیت به خطر نمی‌افتد. لازم به ذکر است که EBQKD ماهواره به زمین قبلاً انجام شده است[۲۰]. محدودیت فعلی استفاده از EBQKD نرخ تولید کلید پایین آن است، زیرا جفت فوتون‌های درهم‌تنیده معمولاً توسط فرآیند تبدیل پایین پارامتری خود به خودی SPDC تولید می‌شود که راندمان بسیار پایینی دارد. یکی از عوامل اصلی که نرخ تولید کلید را محدود می‌سازد، راندمان پایین تولید جفت فوتون‌های درهم‌تنیده و جذب و اتلاف فوتون‌ها در کانال ارتباطی است.

راندمان پایین را می‌توان با استفاده از منابع تولید جفت فوتون با درخشندگی و فیدلیتی بالا جبران کرد. انتخاب طول‌موج مناسب برای فوتون‌های درهم‌تنیده یکی از راه‌های کاهش اثر کانال بر نرخ تولید کلید امن است.

❖ پروتکل MSZ96

پروتکلMSZ96 یک پروتکل توزیع کلید کوانتومی است که بر اساس نور چلانده کار می‌کند، طور یکه بدون استفاده از قطبش فوتون مشابه آنچه در پروتکل BB84 داریم و یا استفاده از فوتون‌های درهم‌تنیده مشابه آنچه در پروتکل E91 داریم، اقدام به توزیع امن کلید می‌کند. این پروتکل برای اولین‌بار در سال ۱۹۹۶ پیشنهاد شد[۲۱]. این پروتکل بر اساس پرتوهای نور ضعیف کار می‌کند و نیازی به منبع تک فوتون ندارد. در شرایطی که تلفات فوتون‌ها در کانال کوانتومی زیاد است این پروتکل کارایی بالایی دارد. دلیل آن این است که گیرنده می‌تواند تمام بیت‌هایی را که معیار غربال‌گری را برآورده نمی‌کنند دور بیندازد

1 .Entanglement Based Quantum Key Distribution

و آنهایی را که معیار غربالگری را برآورده می‌کنند نگه دارد. مزیت دیگر این پروتکل این است که اگر تلفات کانال بسیار زیاد باشد، فرستنده می‌تواند سیگنال ارسالی خود را کمی قوی‌تر کند. این افزایش اندک در توان سیگنال ارسالی تأثیر شدیدی بر کاهش امنیت توزیع کلید نخواهد داشت.

❖ پروتکل COW

پروتکل همدوس یک‌طرفه COW برای اولین‌بار در سال ۲۰۰۵ پیشنهاد شد[۲۲]. این یک پروتکل ساده برای مبارزه با حمله تقسیم عدد فوتون PNS است. در این پروتکل، در سمت فرستنده اطلاعات به‌صورت همدوس بین پالس‌های لیزری مختلف رمزگذاری می‌شود و در سمت گیرنده بررسی می‌شود که آیا چنین همدوسی حفظ شده است یا خیر. حمله PNS این همدوسی را می‌شکند، بنابراین پروتکل COW می‌تواند آن را شناسایی کند. توزیع کلید کوانتومی در فواصل طولانی با استفاده از این روش پیاده‌سازی شده است و حتی محصولات تجاری بر اساس این پروتکل نیز روانه بازار شده‌اند. در ترکیب با آشکارسازهای کم‌نویز، پروتکل COW مخصوصاً برای فیبرهای بلند یا پرتلفات کاربرد دارد. علی‌رغم محبوبیت زیاد این پروتکل، COW در برابر انواع دیگر حملات قوی نیست.

❖ پروتکل DPS[1]

پروتکل تغییر فاز تفاضلی یاDPS یک پروتکل توزیع کلید کوانتومی است که برای اولین‌بار در سال ۲۰۰۲ پیشنهاد شد[۲۳]. در این پروتکل رمزنگاری ابتدا یک فوتون منفرد در یک حالت برهم‌نهی خطی از سه حالت پایه آماده می‌شود و در قالب سه پالس متوالی از سمت فرستنده تولید شده و به گیرنده فرستاده می‌شود. در این پروتکل اختلاف‌فاز بین دو پالس متوالی اطلاعات بیت کوانتومی را حمل می‌کند. گیرنده با استفاده از یک سیستم تشخیص فاز تفاضلی غیرفعال اقدام به اندازه‌گیری اطلاعات کوانتومی می‌کند. این طرح برای پیاده‌سازی در بستر فیبر نوری مناسب است و کارایی ایجاد کلید با راندمان بالاتر از BB84 مبتنی بر فیبر معمولی را ارائه می‌دهد. طرح DPS در برابر حمله تقسیم پرتو برای نور همدوس تضعیف شده بهتر از BB84عمل می‌کند.

❖ پروتکل KMB09

پروتکل KMB09 یک پروتکل توزیع کلید کوانتومی است که در آن گیرنده و فرستنده از دوپایه بایاس نشده استفاده می‌کنند که یکی از آنها کد "۰ "و دیگری "۱ "را کد می‌کند. امنیت این پروتکل به دلیل افزایش نرخ خطای انتقال شاخص ITER و نرخ خطای بیت کوانتومی QBER است که توسط یک استراق سمع ایجاد می‌شود.

❖ پروتکل HD

توزیع کلید کوانتومی با ابعاد بالا، امکان نرخ بالای کلید امن با بازده اطلاعات فوتونی بالا را ارائه می‌دهد. این پروتکل که می‌تواند بر اساس درهم‌تنیدگی زمان - انرژی پیاده‌سازی شود، در برابر حملات جمعی امن است. نرخ پایین تولید کلید امن از مهم‌ترین معایب این پروتکل به شمار می‌رود.

❖ پروتکل CV^{2}

پیاده‌سازی پروتکل توزیع کلید کوانتومی متغیر پیوسته برای رمزنگاری کوانتومی امن به‌خوبی امکان‌پذیر است. این پروتکل بر فناوری استاندارد مخابراتی موجود قابلیت پیاده‌سازی دارد و نرخ کلید مخفی بالاتری را در هر پالس در فاصله نسبتاً کوتاهی به دلیل امکان رمزگذاری بیش از یک بیت در هر پالس نشان می‌دهد. اصطلاح "متغیر پیوسته" به این دلیل برای این پروتکل استفاده می‌شود که به‌جای استفاده از آشکارساز تک فوتون که در BB84و بسیاری دیگر از پروتکل‌ها استفاده می‌شود، از آشکارساز همودین استفاده می‌شود.

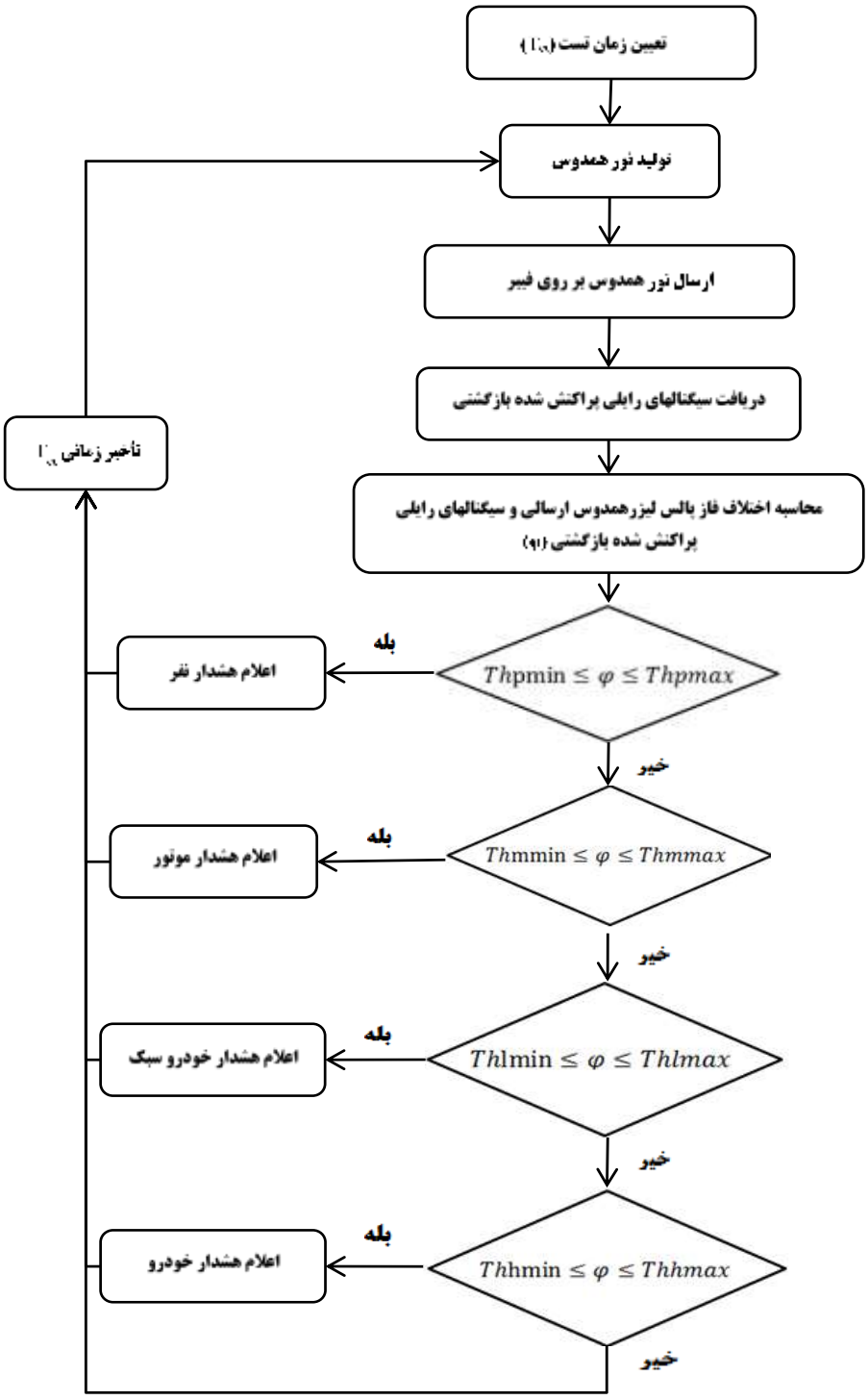
۵- روش پیشنهادی

به‌کارگیری سامانه‌های فعلی حسگر صوتی توزیع شده صوت و لرزش DAS پاسخگوی رفع چالش‌های بزرگ سازمان‌ها برای جلوگیری از دسترسی دشمن به محتوای داده‌های روی فیبر، جلوگیری از نزدیکی دشمن به فیزیک فیبر نوری، تغییر در محتوای داده‌های روی فیبر و یا تزریق و تحکم و کنترل روی داده‌های فیبر نوری با روش‌های مختلف نظیر انواع روش‌های تپ زنی نیست. هنوز مشکلاتی در تشخیص برد، مسافت، تلورانس محل دقیق تشخیص فیبر نوری ناشی از دست‌پیچ داخل حوضچه‌ها و همچنین میزان دقت در نتایج سامانه‌ها وجود دارد. ضمن آن که اگر روی فیبر نوری سیستم‌های شنود قرار گرفته باشد با سامانه‌های DAS نیز قابل‌تشخیص نمی‌باشد؛ لذا این موضوع ما را بر آن داشت برای رفع چالش‌های فوق، اقدام به ارائه پیشنهاد بهینه‌سازی سامانه حسگر توزیع شده صوت و لرزش DAS نماییم.

بلوک دیاگرام روش فعلی عملکرد سامانه حسگر توزیع‌شده صوت و لرزش DAS در شکل شماره ۷ نمایش داده شده است.

1.Differential-Phase-Shift

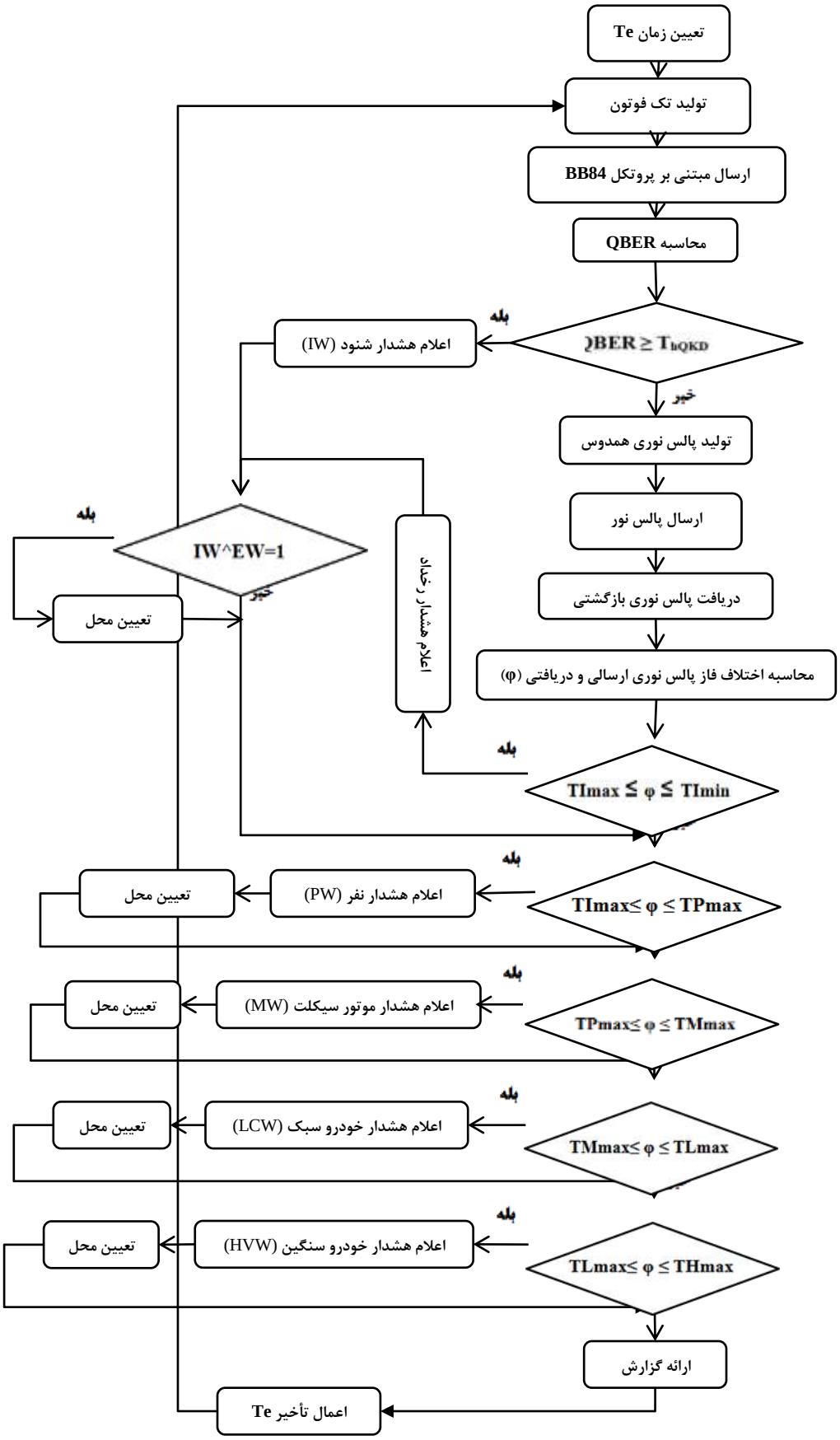
2.Continuous-Variable



شکل (۷): الگوریتم عملکرد DAS

پیشنهاد ما در این مقاله روش بهینه‌سازی عملکرد سامانه DAS وش ارسال تک فوتون‌های کوانتومی و توزیع کلید کوانتومی است. این روش با تکنیک استفاده از روش‌های توزیع کلید کوانتومی پیوسته QKD-CV[1] و روش‌های توزیع کلید کوانتومی گسسته QKD-DV[2] امکان‌پذیر است. این تکنیک می‌تواند خط را در صورت عدم آشکارسازی تپ هم امن نماید. الگوریتم روش پیشنهادی که از خواص کوانتومی برای بهبود عملکرد DAS در شناسایی تب و شنود غیرمجاز بهره می‌گیرد در شکل ۸ آمده است.

[1] Quantum Key Distribution Continuse-Variable
[2] Quantum Key Distribution Discrete-Variable



شکل (۸): الگوریتم روش پیشنهادی

۶- همان‌طور که در شکل ۸ آمده است ابتدا فاصله زمانی بین دو ارزیابی (Te) را تعیین می‌شود. سپس تولید تک فوتون نموده و با پروتکل توزیع کلید کوانتومیBB84 نسبت به ارسال آن و محاسبه نرخ خطای بیت کوانتومی (QBER) اقدام می‌گردد. درصورتیکه QBER از مقدار مرسوم آن در توزیع کلید کوانتومی بیشتر باشد شنود از فیبر تشخیص داده و اعلام هشدار شنود (IW) صادر می‌گردد. علت این موضوع جذب تک فوتون‌ها توسط سیستم شنود است که در حالت غیر تک فوتون این موضوع ممکن نیست. در ادامه تولید پالس نوری همدوس نموده در لینک فیبر نوری ارسال شده و سپس با مقایسه پالس نوری رفت و برگشت مقدار اختلاف فاز (φ) محاسبه می‌گردد [۲۴].

۷- درصورتی‌که میزان اختلاف‌فاز $TImin \leq \varphi \leq TImax$ باشد اعلام هشدار رخداد (EW) صادر می‌شود در صورت هشدار توأمان EW و IW تعیین محل شنود انجام می‌شود. درصورتی‌که اختلاف‌فاز در این بازه نباشد با تحلیل آن به شرح زیر نسبت شناخت نوع رویداد و تعیین محل آن اقدام می‌گردد.

- درصورتی‌که میزان اختلاف‌فاز $TImax \leq \varphi \leq TPmax$ باشد اعلام هشدار رخداد تشخیص نفر صادر می‌شود.
- درصورتی‌که میزان اختلاف‌فاز $TPmax \leq \varphi \leq TMmax$ باشد اعلام هشدار رخداد تشخیص موتورسیکلت صادر می‌شود.
- درصورتی‌که میزان اختلاف‌فاز $TMmax \leq \varphi \leq TLmax$ باشد اعلام هشدار رخداد تشخیص خودرو سبک صادر می‌شود.
- درصورتی‌که میزان اختلاف‌فاز $TLmax \leq \varphi \leq THmax$ باشد اعلام هشدار رخداد تشخیص خودرو سنگین صادر می‌شود.

تعیین محل از اختلاف زمان رفت‌وبرگشت نور به طور دقیق محاسبه می‌شود. بدین صورت که از حاصل‌ضرب سرعت در زمان رفت‌وبرگشت تقسیم بر دو، فاصله از مبدأ دقیقاً محاسبه شده و تعیین محل صورت می‌گیرد.

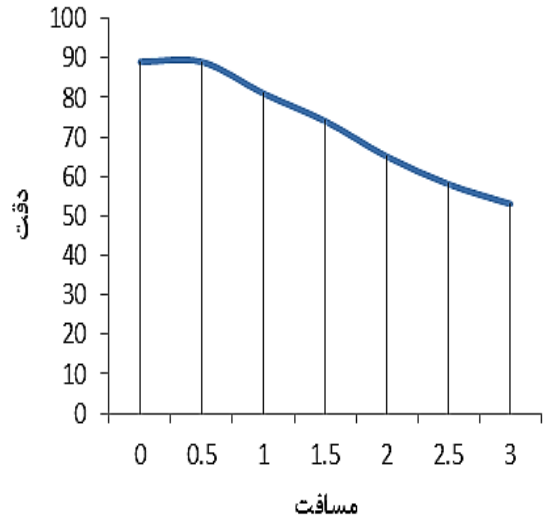
در انتها پس از تعیین محل رخدادها نسبت به ارائه گزارش وضعیت رویدادهای طول مسیر فیبر اقدام می‌شود و پس از تأخیر Te مجدداً فرایند ارزیابی صورت می‌پذیرد.

۸- ۷- ارزیابی و نتیجه گیری

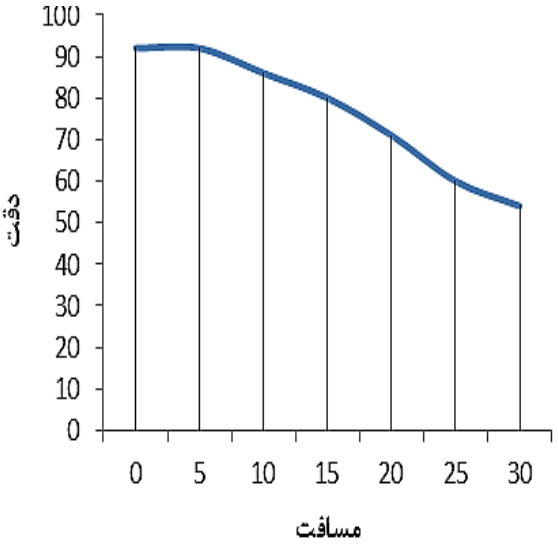
همان‌طور که در بند قبل بیان شد روش پیشنهادی بهبودیافته سیستم حسگر صوتی (DAS)می‌باشد که با بهره‌گیری از خواص فناوری کوانتومی علاوه بر تشخیص رویدادهای مرسوم قادر به تشخیص تب‌ها و سامانه شنود از فیبر می‌باشد. به عبارتی می‌توان گفت الگوریتم پیشنهادی دارای قابلیت‌های زیر است:

- ✓ تشخیص انواع تب‌ها
- ✓ تشخیص سامانه‌های شنود
- ✓ تشخیص نفوذ و تجاوز افراد به حریم فیبر
- ✓ تشخیص نفوذ و تجاوز موتورسیکلت به حریم فیبر
- ✓ تشخیص نفوذ و تجاوز خودرو سبک به حریم فیبر
- ✓ تشخیص نفوذ و تجاوز خودرو سنگین به حریم فیبر

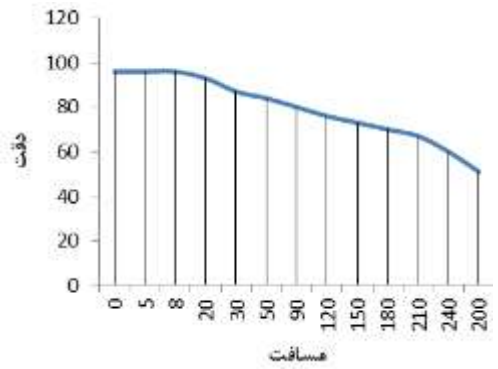
نتایج حاصله از ارزیابی الگوریتم پیشنهادی با داده‌های جمع‌آوری‌شده برای دقت تشخیص نسبت به مسافت نفر، موتورسیکلت، خودرو سبک و خودرو سنگین به ترتیب در شکل‌های ۹، ۱۰، ۱۱ و ۱۲ آمده است.



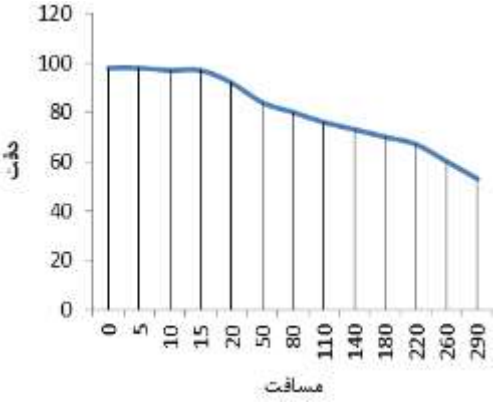
شکل (۹): دقت روش پیشنهادی در تشخیص" نفر"



شکل (۱۰): دقت روش پیشنهادی در تشخیص" موتورسیکلت"

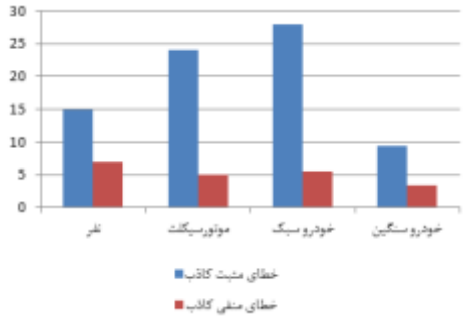


شکل (۱۱): دقت روش پیشنهادی در تشخیص" خودرو سبک"



شکل (۱۲): دقت روش پیشنهادی در تشخیص" خودرو سنگین"

میانگین خطای مثبت کاذب و خطای منفی کاذب در مسافت‌های مختلف برای تشخیص عامل‌های مختلف در شکل ۱۳ آمده است.



شکل (۱۳): خطای مثبت کاذب و خطای منفی کاذب روش پیشنهادی

مطابق ارزیابی‌های صورت‌گرفته روش پیشنهادی بادقت ۹۸ درصد وجود سامانه شنود از فیبر را تشخیص داده و مطابق شکل‌های فوق الذکر بادقت بالای ۷۰ درصد قادر به تشخیص نفر در شعاع ۲ متری و بادقت بالای ۷۲ درصد قادر به تشخیص موتورسیکلت در شعاع ۲۰ متری و بادقت بالای ۷۵ درصد قادر به تشخیص خودرو سبک در شعاع ۱۲۰ متری و بادقت بالای ۷۶ درصد قادر به تشخیص خودرو سنگین در شعاع ۱۸۰ متری می‌باشد.

۶- مراجع

[1]"Electical & Computer Technical Website", http://microrf.ir, 2023.

[۲]گزارشات پروژه " حسگر توزیع شده صوت و لرزش"، دانشگاه صنعتی شریف، مرکز فوتونیک و کوانتوم، ابوالفضل بهرام‌پور، ۱۳۹۸.

[3] Y. Gong1, R. Kumar2, A. Wonfor, "Secure optical communication using a quantum alarm", Official journal of the CIOMP 2047-7538 , pp 180-192, 2020.

[۴ گزارش اول پروژه " مقایسه عملکرد پروتکل‌های توزیع کلید کوانتومی گسسته"، دانشگاه صنعتی شریف، مرکز فوتونیک و کوانتوم، مرتضی نیک‌آیین،۱۳۹۸.

[۵]گزارشات پروژه " نقشه راه ورود به حوزه ارتباطات و رمزنگاری کوانتومی"، سند سیاسی تفصیلی مرکز اندیشه‌ای کوثر، حسین طالب،۱۴۰۰.

[6] Bruss, D., Erdelyti, G., Meyer, T., Riege, T., Rothe, J., "Quantum Cryptography: A Survey", ACM Computing Surveys, Vol. 39, No. 2, Article 6, 2007.

[7] A. Shamir, Communications of the ACM 22, 612, 1979.

[8] G. J. Simmons, in Workshop on the Theory and Application of of Cryptographic Techniques pp. 436–467, 1989.

[9] M. Hillery, V. Bu˘zek, and A. Berthiaume," Quantum secret sharin", Physical Review. A 59, 1829 , 1999.

[10] Jie Gu, Xiao-Yu Cao, Hua-Lei Yin, Zeng-Bing Chen, "Differential phase shift quantum secret sharing using twin field", Opt. Express 29, 9165, 2021.

[11] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York,,1984.

[12] 2 M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoystate quantum key distribution with quantified security", Opt. Express 21, 24550-24565,2013.

[13] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, "Decoy State Quantum Key Distribution" Physical Review Letters. 94, 230504, 2005.

[14] Scarani, Valerio & Acín, Antonio & Ribordy, Grégoire & Gisin, Nicolas. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". Physical review letters. 92. 057901. 2004.

[15] Bruss, Dagmar "Optimal Eavesdropping in Quantum Cryptography with Six States", Physical Review Letters, 81. 10.1103/PhysRevLett.81.3018 (1998).

[16] A. K. Ekert, "Quantum cryptography based on bell's theorem", Physical Review Letters. 67, pp. 661–663, 1991.

[17] C. Bennett, "Quantum cryptography using any two nonorthoganol states", Physical Review Letters. 68, pp. 3121-3124,1992.

[18] R. Etengu, F. M. Abbou, H. Y. Wong, A. Abid, N. Nortiza, A.Setharaman," Performance Comparison of BB84 and B92 Satellite-Based Free Space Quantum Optical Communication Systems in the Presence of Channel Effects" Journal of Optical Communications, Volume 32, Issue 1, pp.37-47, 2011.

[19] C. H. Bennet, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem", Physical Review Letters. 68, pp. 557-559, 1992.

[20] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang,, … J.-W. Pan, "Satellite-Relayed Intercontinental Quantum Network", Physical Review Letters, 120(3), 2018.

[21] Mu, Yi; Seberry, Jennifer; Zheng, Yuliang, "Shared cryptographic bits via quantized quadrature phase amplitudes of light" Optics Communications. pp. 344–352,1996.

[22] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden: "Fast and simple one-way quantum key distribution" Applied Physics Letters. 87(19); 194108, 2005.

[23] K. Noue, E.Waks, & Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution" Physical Review Letters, 89(3), 2002.

[24] A. Fichtner, A. Bogris, T. Nikas, Theory of phase transmission fibre-optic deformation sensing, Geophysical Journal International, Volume 231, Issue 2, Pages 1031–1039, 2022.

[25] Project No. 2 "Performance Comparison of Discrete Quantum Key Distribution Protocols", Sharif University of Technology, Photonics and Quantum Center, Morteza Nik Ayin, 2018.

[26] Project reports "Reviewing the Principles and Basics of Quantum Communication Technology", Imam Hossein University (AS), Faculty and Research Institute of Fawa, Communication and Network Science and Technology Center, Ali Naseri, 2018.

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۲، تابستان ۱۴۰۳، ص ۹۷-۸۵

علمی – پژوهشی

روش پیشنهادی برای بهبود عملکرد سامانه DAS مبتنی بر فناوری کوانتومی

سید علی سلیمانی [۱]، علی ناصری [۲*]

۱- دانشجوی دکتری ، دانشگاه صنعتی مالک‌اشتر، تهران، ایران. ۲- دانشیار، دانشگاه امام حسین (ع)، تهران، ایران.

(دریافت: ۱۴۰۳/۰۲/۰۸، بازنگری: ۱۴۰۳/۰۴/۱۸، پذیرش: ۱۴۰۳/۰۵/۱۳، انتشار: ۱۴۰۳/۰۶/۱۰)

DOR:

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

تب زنی باانگیزه شنود از فیبر نوری همواره مورد توجه بخش‌های مختلف جنگ الکترونیک و سایبری بخش دفاعی و امنیتی بوده و خواهد بود. تلاش‌های زیادی تاکنون در سطح جهانی برای مانیتورینگ عملکرد لینک ارتباط فیبر نوری انجام شده است که حاصل آنها را می‌توان در قالب فناوری‌های DAS و OTDR بیان نمود. متأسفانه هر دو روش در مقابل تکنیک‌های پیشرفته تب زنی و شنود، ناتوان می‌باشند به عبارتی قادر به تشخیص سامانه‌های شنود از فیبر نوری نیستند. در این مقاله از خواص فناوری کوانتوم در حوزه توزیع کلید کوانتومی برای بهبود عملکرد DAS بهره گرفته می‌شود و الگوریتمی پیشنهاد می‌گردد که قادر است علاوه بر مانیتورینگ تلفات در مسیر لینک ارتباط فیبر نوری، سامانه شنود از فیبر را بادقت بالایی شناسایی و محل آن را مشخص می‌نماید. نتایج حاصل از الگوریتم پیشنهادی حاکی از این است که این الگوریتم قادر است بادقت ۹۸ درصد وجود سامانه شنود را تشخیص، بادقت بالای ۷۰ درصد تشخیص نفر در شعاع ۲ متری، بادقت بالای ۷۲ درصد تشخیص موتورسیکلت در شعاع ۲۰ متری، بادقت بالای ۷۵ درصد تشخیص خودرو سبک در شعاع ۱۲۰ متری و بادقت بالای ۷۶ درصد تشخیص خودرو سنگین در شعاع ۱۸۰ متری فیبر نوری را انجام دهد.

کلیدواژه‌ها: تب زنی، VOTDR،OTDR،DAS، کلید کوانتومی، QKD CV،QKD DV

۱- مقدمه

ارتباطات، مهم‌ترین رکن پشتیبانی صحنه نبرد محسوب می‌شود. این موضوع به حدی اهمیت یافته که ارتباطات را رکن عملیات آینده بر می‌شمارند و سناریوهای عملیاتی را مبتنی بر توانمندی و قابلیت‌های ارتباطی تدوین می‌نمایند. امروزه ضرورت تبادل اطلاعات اعم از صوت، تصویر و ویدئو در همه سطوح واضح و روشن است. موفقیت صحنه نبرد کاملاً به کار آیی امن شبکه و سامانه فرماندهی و کنترل وابسته است. به همان میزان که ارتباطات در موفقیت صحنه عملیات مؤثرتر می‌گردد به همان میزان هم انگیزه طرف مقابل برای شنود، فریب، اختلال و تخریب ارتباطات بیشتر می‌شود.

از طرفی در صحنه عملیات طرفی که توانایی و قدرت دسترسی و دستیابی به اطلاعات طرف مقابل را داشته باشد، احتمال پیروزی آن چندین برابر می‌گردد.

همگرایی و فرماندهی مناسب بر صحنه عملیات مستلزم بهره‌گیری مناسب از فناوری‌های روز ارتباطی، اطلاعاتی و امنیتی و حفاظت و حراست از زیرساخت‌های مهم ارتباطی است.

زیرساخت‌های ارتباطی نظیر فیبر نوری یکی از مهم‌ترین و پرکاربردترین زیرساخت‌هاست. تب زنی این روزها به دلیل توسعه آشکارسازها و روش‌های استخراج سیگنال به‌شدت توسعه پیدا کرده است. این موضوع امنیت فیبر نوری را با چالش جدی مواجه نموده است. امروزه یکی از بزرگ‌ترین چالش‌های فنی ارتباطات فیبر نوری، محافظت فیبر نوری در مواجهه با تلاش‌های دشمن برای دسترسی و دستیابی به فیبر و محتوی آن است. در حال حاضر محافظت از فیبر نوری توسط سامانه‌های مرسوم نظیر OTDR[۲] و DAS[۳] می‌باشد. این سامانه‌ها قادر به تشخیص تب‌های غیرمجاز و به‌تبع آن شنود ناشی از آن نیستند. این مقاله با بهره‌گیری مناسب از خواص فناوری کوانتومی به رفع این موضوع می‌پردازد.

در سال‌های اخیر تحول شگرفی در توسعه فناوری‌های کوانتومی رخ‌داده است. نهادهای مطرح جهانی که آینده‌نگاری حوزه فناوری را انجام می‌دهد من‌جمله مرکز DCDC[۴] بریتانیا و آزمایشگاه لینکلن دانشگاه MIT[۵] بهره‌گیری از فناوری کوانتوم در

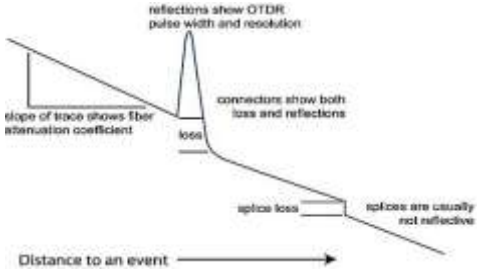
* رایانامه نویسنده مسئول: parmis2159@gmail.com

[2] Optical Time Domain Reflectometer
[3] Distributed Acoustic Sensing
[4] Development, Concepts and Doctrine Centre
[5]. Massachusetts Institute of Technology

عرصه‌های مختلف جامعه را پیش‌بینی نموده‌اند. از مهم‌ترین فناوری‌های حوزه کوانتوم، ارتباطات و توزیع کلید کوانتومی است که بسیار حائز اهمیت بوده و تحولی شگرف در حوزه ارتباطات امن به دنبال خواهد داشت. خواص کوانتومی می‌تواند در پایش فیبر نوری و تشخیص دقیق‌تر قطع‌شدگی و تلفات فیبر تأثیرگذار باشد.

۲- روش‌های مراقبت از فیبر نوری

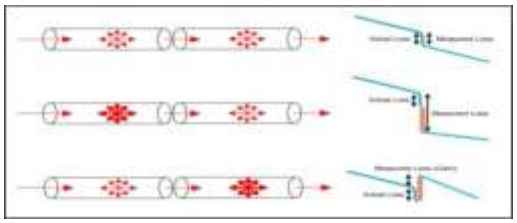
بزرگ‌ترین عامل اتلاف فیبر نوری پراکندگی می‌باشد. در فیبر، نور در تمام جهات پراکنده می‌شود که شامل بعضی از پراکندگی‌ها به سمت منبع نیز می‌باشد. سامانه OTDR[1] یا بازتاب‌سنج نوری بر پایه محدوده زمانی کار می‌کند. این سامانه نور را در فیبر ارسال نموده و با دریافتی نور برگشتی از فیبر میزان تضعیف فیبر و محل آن را شناسایی می‌نماید به عبارتی متناسب با نمودار میزان تضعیف نسبت به طول فیبر، محل قطع‌شدگی‌ها و نقاط دارای تلفات را در فیبر مشخص می‌کند. شکل ۱ یک نمونه نمودار سامانه OTDR را نشان می‌دهد.



شکل (۱): نمونه نمودار سامانه **OTDR** [۱]

OTDR شامل یک فرستنده لیزری با توان بالا می‌باشد که یک پالس نور را به درون فیبر ارسال می‌کند. نور پراکنده شده به عقب و نور منعکس شده، از طریق فیبر به سمت سامانه OTDR بر می‌گردد و در پایان از طریق یک متصل‌کننده OTDR به سمت یک گیرنده حساس هدایت شده می‌شود. در هر لحظه از زمان، نوری که OTDR دریافت می‌کند، نور پراکنده شده از عبور پالس از ناحیه‌ای از فیبر می‌باشد؛ بنابراین می‌تواند نمایشی از وضعیت فیبر در طول مسیر ارائه کند؛ لذا مقدار نور پراکنده برگشتی به OTDR متناسب با پراکندگی فیبر، وابسته به حداکثر قدرت پالس تست OTDR و طول پالس ارسال شده می‌باشد.

اتصالات و جوش‌ها در اصطلاحات OTDR حوادث نامیده می‌شوند که هر دو باید اتلاف را نشان بدهند. کانکتورها و جوش‌های مکانیکی یک نقطه اوج از بازتاب را نشان خواهند داد. ارتفاع این نقطه اوج مقدار بازتاب را در حوادث نشان می‌دهد. مگر اینکه آن آن‌قدر بزرگ باشد که گیرنده OTDR را اشباع کند و قادر به نمایش آن نباشد در این حالت در نقطه اوج ممکن است یک سطح صاف و ادامه‌دار تا انتها داشته باشد که نشان می‌دهد گیرنده overload شده است. گاهی اوقات اتلاف یک جوش فیوژن خوب، آن‌قدر کوچک است که قابل‌دیدن با OTDR نمی‌باشد که ممکن است اپراتور را گیج کند. در OTDR خیلی مهم است که طول تمام کابل‌های شبکه را بدانید. با این کار eventها را می‌توان فهمید که در کجا بایستی مشاهده کرد. پالس‌های انعکاسی نشانگر دقت OTDR می‌باشد. عملکرد OTDR جهت اندازه‌گیری تضعیف روی فیبر در شکل ۲ نشان‌داده‌شده است[۱].



شکل (۲): عملکرد **OTDR** جهت اندازه‌گیری تضعیف روی فیبر[۱]

۲- ۳- سامانه DAS

حفاظت فیزیکی از زیرساخت‌های کشورها همواره مورد توجه بوده و خواهد بود. در بین این زیرساخت‌ها یکی از مهم‌ترین آن‌ها زیرساخت‌های ارتباطی و فناوری اطلاعات می‌باشند؛ زیرا حاوی اطلاعات بوده که حفظ آنها از اهمیت بالایی برخوردار است. حسگر تمام توزیع شده فیبر نوری لرزش و صوت، یک حسگر حفاظت فیزیکی است که با استفاده از سیگنال‌های نوری و با استفاده از فیبر نوری به حفظ حریم‌ها می‌پردازد. این حسگرها، کاربردهای بسیاری از جمله موارد زیر را دارند:

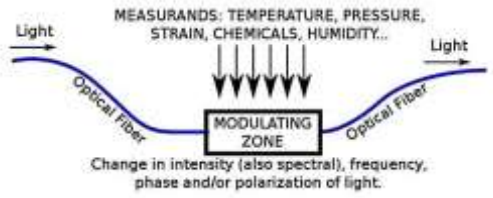
- ❖ حفاظت فیزیکی خطوط انتقال
- ❖ حفاظت فیزیکی فیبر نوری و فناوری آنتی تپ حفاظت فیزیکی خطوط انتقال
- ❖ مرزبانی برای مسافت‌های بسیار طولانی
- ❖ حسگرهای صوت

وقتی که لرزش در جایی از فیبر نوری به فیبر اعمال شود، طبیعتاً ضریب شکست خیلی کم تغییر می‌کند که منجر به تغییر فاز در پالس ارسال شده خواهد شد. سامانه حسگر صوتی توزیع‌شده (DAS) از بازتاب سنجی دامنه نوری حساس به فاز برای شناسایی و یافتن وقایع حتی لرزش‌های ضعیف استفاده می‌کند. این سامانه از یک لیزر پالسی همدوس استفاده می‌کند. لرزش باعث تغییر فاز می‌شود و تغییر سیگنال تداخلی را موجب می‌شود. با تغییر شدت سیگنال رایلی در زمان‌ها و مکان‌های متفاوت، امکان آشکارسازی لرزش و مکان لرزش در جای‌جای فیبر فراهم می‌شود.

اساس کار سامانه حسگر توزیع شده صوت و لرزش در شکل ۳

[1] .Optical Time-domain Reflectometer

نشان داده شده است [۲].

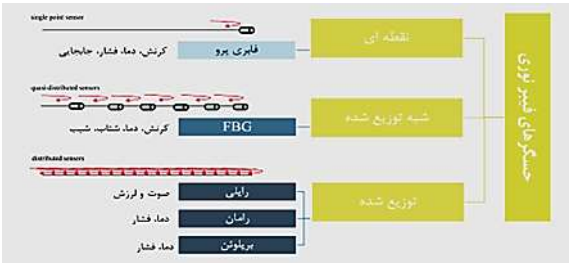


شکل (۳): اساس کار سامانه **DAS** [۲]

طرح کارکردی حسگرهای فیبر نوری در شکل ۴ آمده است [۲].

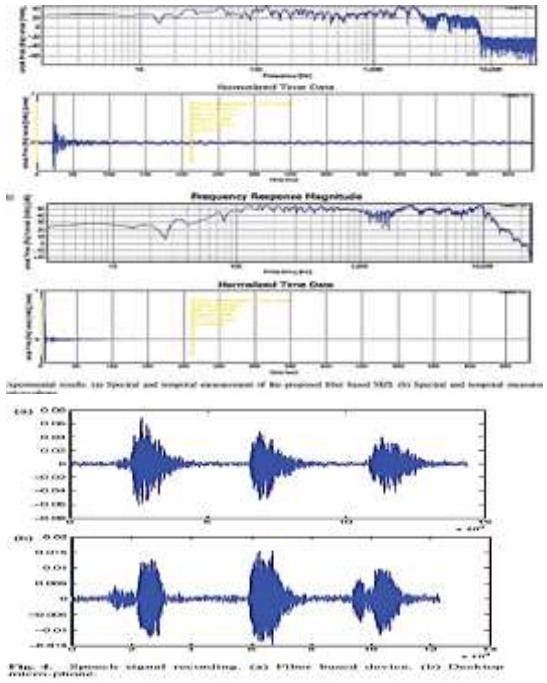
این سامانه‌ها بردی معادل ۵۰ تا ۱۵۰ کیلومتر و دقت مکان یابی زیر ۱۰ متر دارند.

نمونه‌ای از آشکارساز بلوک دیاگرام جمع‌آوری و پردازش صوت پیرامونی فیبر نوری در شکل ۴ به نمایش درآمده است[۲].

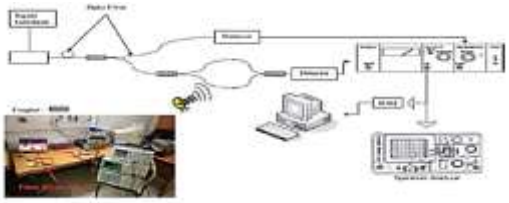


شکل (۴): نمونه‌ای از آشکارساز بلوک دیاگرام جمع‌آوری و پردازش صوت پیرامونی فیبر نوری [۲]

نمودار نتایج تست‌های انجام شده در شکل ۵ و نمونه‌ای از صوت جمع‌آوری شده و پردازش پیرامونی در شکل ۶ نشان‌داده‌شده است[۲].



شکل (۵): نمودار نتایج تست‌های انجام شده[۲]



شکل (۶): نمونه‌ای از صوت جمع‌آوری شده و پردازش پیرامونی [۲]

از قابلیت سامانه حسگر صوتی توزیع‌شده می‌توان به موارد زیر اشاره نمود:

- ✓ حساسیت بالا
- ✓ ابعاد کوچک و وزن سبک
- ✓ پهنای باند بزرگ
- ✓ عملکرد در دمای بالا
- ✓ توانایی سنجش توزیع‌شده
- ✓ ایمنی در برابر تداخل الکترومغناطیسی

نتایجی که از این ویژگی در سامانه حسگر توزیع‌شده صوت و لرزش (DAS) حاصل می‌شود عبارت‌اند از:

- ✓ تشخیص هم‌زمان چند نقطه هدف و اعلام زنگ هشدار برای تمام نقاط تشخیص‌داده‌شده
- ✓ شناسایی هوشمند انواع رویداد برای کاربردهای مختلف
- ✓ نظارت بر نشت
- ✓ نظارت بر نفوذ شخص متجاوز
- ✓ نظارت بر عوارض زمین‌شناسی مانند رانش زمین و تشخیص اولیه لرزش زمین

۳- ۴- تپ زنی

یکی از چالش‌های جدی امنیت فیبر نوری، تلاش دشمن برای بهره‌برداری از روش‌های تب زنی و دسترسی به محتوای داده‌های روی فیبر است. سازمان‌ها با رمزنگاری تلاش می‌نمایند دستیابی به اطلاعات فیبر نوری را برای دشمن غیرممکن یا زمان‌بر نمایند. اما این امر مانع از نزدیکی دشمن به فیزیک فیبر نوری، تغییر در محتوای داده‌های روی فیبر و یا تزریق و تحکم و کنترل روی داده‌های فیبر نوری نمی‌شود.

روش‌های مرسوم استفاده از OTDR و سامانه‌های ONMS[1] نیز برای تشخیص افت ناشی از دسترسی‌های غیرمجاز به فیبر نوری کفایت از حل مشکلات ناشی از چالش‌های فوق نیست.

باتوجه‌به روش‌های تپ زنی در حال حاضر، تپ زنی بدون ایجاد ارتعاش یا بدون لمس کابل فیبر نوری، غیرممکن است؛ لذا سیستم‌های تپ زن باید بتوانند به کابل فیبر نوری دسترسی پیدا کنند. تپ زنی امروزه یکی از تهدیدات بزرگ زیرساخت‌های ارتباطی نظیر فیبر نوری است که مخاطرات ناشی از آن می‌تواند هر سازمانی را با چالش‌های جدی و شکست‌های بزرگ روبرو

[1] Optical Network Management System

نماید. استراتژی برخورد با تپ به سه بخش تقسیم می‌گردد.[۲]

- ✓ پیشگیری از تپ زنی‌های آتی
- ✓ پیداکردن تپ‌های موجود روی خطوط
- ✓ تضمین امنیت خط

برای آشکارسازی تپ‌های موجود روش‌های استفاده از OTDRهای دقیق موسوم به VOTDR[1] توصیه شده است. متأسفانه به دلیل شرایط خطوط فیبر نوری این روش، نقاط خطای بسیار بالایی دارد که استفاده از این سیستم‌ها را با سختی مواجه می‌کند. در نتیجه استفاده از سیستم‌های بر خط VOTDR به‌صورت کمکی در کنار تکنیک پیشنهادی توصیه می‌گردد. در مرجع [۳]موضوع امن‌سازی ارتباط با هشدارهای کوانتوم مفصل بحث شده.

۴- ۵- توزیع کلید کوانتومی

در رمزنگاری کلاسیک هنگامی که یک کلید برای رمزگذاری و رمزگشایی وجود دارد به آن رمزنگاری متقارن گفته می‌شود. با استفاده از علم ریاضیات و کمک رایانه‌ها، می‌توان کلیدهایی تولید کرد که بسیار بزرگ‌تر باشد و حدس‌زدن آن بسیار سخت‌تر باشد. اما مسئله بالقوه دیگر این است که این امکان وجود دارد که این کلیدها توسط یک فرد غیرمجاز خوانده شود. پس در زمینه رمزنگاری متقارن دو چالش عمده وجود دارد. یکی آن که کلیدی که انتخاب می‌شود باید از پیچیدگی لازم برخوردار باشد. دوم آن که کلید انتخابی باید به طور امن بین دو طرف تبادل گردد، طور یکه هیچ‌کس قادر به کشف یا شنود آن نباشد[۴]. رمزنگاری با کلید عمومی که با نام رمزنگاری نامتقارن نیز شناخته می‌شود، راه‌حلی دقیق برای حل چالش‌های فوق دارد. این روش رمزنگاری اجازه می‌دهد تا هر فرد در یک مکالمه دو کلید عمومی و خصوصی ایجاد کند. اگر پیامی را با استفاده از کلید عمومی شخص گیرنده رمزگذاری شود، گیرنده می‌تواند آن را با استفاده از کلید خصوصی منطبق خود رمزگشایی کند.

رمزنگاری کلید عمومی این مزیت را دارد که شما نیازی به انتقال مخفیانه کلید رمزگشایی به گیرنده پیام مخفی خود را نداشته باشید؛ زیرا آن شخص قبلاً کلید رمزگشایی را دارد. کلید رمزگشایی کلید خصوصی آنهاست؛ بنابراین، تنها چیزی که برای ارسال پیام نیاز است کلید رمزگذاری عمومی و منطبق با گیرنده است. شما می‌توانید کلید عمومی گیرنده را به‌راحتی به دست آورید، زیرا گیرنده می‌تواند کلید عمومی خود را با هر کسی به اشتراک بگذارد، زیرا کلیدهای عمومی فقط برای رمزگذاری پیام‌ها استفاده می‌شوند نه رمزگشایی آنها؛ بنابراین بر خلاف رمزنگاری متقارن، در رمزنگاری نامتقارن نیازی به تعویض کلید قبل از برقراری ارتباط نیست و این مزیت مهمی قلمداد می‌شود. معمولاً مرحله تبادل کلید رمزنگاری متقارن نیز با استفاده از طرح تبادل کلید عمومی انجام می‌شود.

با ظهور رایانه‌های کوانتومی، این امکان وجود دارد که روش‌های رمزنگاری نامتقارن نیز امنیت کنونی خود را از دست بدهند و تبادل کلید عمومی و متعاقباً رمزگذاری کلید خصوصی نیز با چالش جدی مواجه شود. امنیت رمزنگاری کلید عمومی بر فرض اثبات نشده دشواری در انجام برخی مسائل پیچیده ریاضی استوار است که در زمان معقولی با استفاده از رایانه‌های کلاسیک قابل‌حل نیستند. اما الگوریتم شُر نشان داد که پروتکل‌های رمزنگاری کلاسیک نظیر RSA[2] که مبتنی بر اعداد اول هستند به طور بالقوه در برابر رایانه‌های کوانتومی آسیب‌پذیر هستند[۵]. در واقع، رایانه‌های کوانتومی این پتانسیل را دارند که بتوانند چنین مسائل پیچیده ریاضی را در زمان کوتاهی بر روی رایانه‌های کوانتومی حل کنند[۵]. در نتیجه ظهور رایانه‌های کوانتومی، سیستم‌های رمزنگاری کلاسیک مانند DES[3]، RAS، DLP[4] و IEF[5] را منسوخ و توزیع کلید کنونی را غیر امن می‌کنند. پد یکبار مصرف یا OTP[6] نوعی رمزگذاری متقارن است که اگر به‌درستی پیاده‌سازی شود، از امنیت زیادی برخوردار بوده و خطر رایانه‌های کوانتومی را نیز برطرف می‌سازد. این روش می‌تواند چالش اول که حفظ پیچیدگی لازم است را با افزایش تعداد بیت‌ها برطرف سازد. از طرف دیگر به دلیل اینکه کلید فقط یک‌بار استفاده می‌شود به طور قابل اثباتی امن است. اما چالش دوم همچنان پابرجا است و توزیع خود کلید خصوصی از طریق یک کانال بالقوه ناامن یک چالش جدی قلمداد می‌شود.

تولید تک فوتون‌های کوانتومی از طریق تضعیف فوتون‌ها انجام می‌شود و یکی از بیشترین کاربردهای تبادل تک فوتون‌های کوانتومی استفاده در توزیع کلید کوانتومی یا QKD است.QKD این پتانسیل را ارائه می‌دهد که برای اولین‌بار در تاریخ بشر کانال‌های ارتباطی امن بین طرفین دور در لینک ارتباطی ایجاد شود. کانال‌های کوانتومی را می‌توان با فیبرهای نوری استاندارد مخابراتی یا با کانال‌های نوری فضای آزاد دارای دید مستقیم، تا حدودی تحقق بخشید.

برای چالش توزیع کلید خصوصی از طریق یک کانال بالقوه ناامن برای اولین‌بار آقای استفان ویزنر در سال ۱۹۷۰ ایده رمزنگاری کوانتومی را مطرح کرد و نشان داد که از ویژگی‌های منحصربه‌فرد ذرات کوانتومی می‌توان برای حل مشکل انتقال امن کلیدهای رمزنگاری استفاده کرد.

[1]The High Refresh Rate of The Instrumen Optical Time Domain Reflectometer

[2] Rivest–Shamir–Adleman
[3] Data Encryption Standard
[4] Data Loss Prevention
[5] International Energy Forum
[6] One Time Pad

۵- ۶- پروتکل‌های کوانتومی

پروتکل‌های کوانتومی مختلفی تاکنون ارائه شده است که در ادامه به طور اجمال توضیح هر کدام خواهد آمد[۵].

❖چرخاندن سکه کوانتومی

چرخاندن سکه کوانتومی یا QCF[1] پروتکلی است که برای برقراری ارتباط بین دو طرفی که به یکدیگر اعتماد ندارند استفاده می‌شود. مشابه توزیع کلید کوانتومی، شرکت‌کنندگان از طریق یک کانال کوانتومی ارتباط برقرار می‌کنند و از طریق انتقال کیوبیت‌ها اطلاعات را مبادله می‌کنند. بازیکن پذیرنده تا زمانی که اندازه‌گیری را انجام ندهد، اطلاعات موجود در کیوبیت را نمی‌داند. اطلاعات مربوط به هر کیوبیت روی یک فوتون ذخیره شده و توسط آن حمل می‌شود. اگرچه ورق‌زدن سکه کوانتومی وسیله‌ای امن برای برقراری ارتباط در تئوری است، اما به دلیل نیاز به حافظه‌های کوانتومی، منابع تک فوتون و آشکارسازهای تک فوتون، انجام آن دشوار است و سطح آمادگی فناوری بالایی ندارد.

❖امضای دیجیتال کوانتومی

امضای دیجیتال کوانتومی یا QDS[2] روشی برای حفاظت از رمزهای کلید عمومی در مقابل حملات کامپیوترهای کوانتومی است. امضای دیجیتال کلاسیک که در حال حاضر مورداستفاده قرار می‌گیرد قابلیت جعل دارد، ولی امضای دیجیتال کوانتومی در حالت ایده‌آل در برابر قدرتمندترین کامپیوترهای کلاسیک و کوانتومی مقاوم خواهد بود. سخت‌افزار موردنیاز برای پیاده‌سازی QDS مشابه سیستم‌های موردنیاز برای QKD است و ممکن است هر دو طرح QDS و QKD بتوانند به طور موازی در امتداد فیبرهای نوری مشابه با استفاده از سخت‌افزار ارسال و دریافت یکسان عمل کنند.

❖اشتراک‌گذاری راز کوانتومی

به‌اشتراک‌گذاری راز، یکی از مأموریت‌های ارتباطی اساسی در رمزنگاری کلاسیک است. هدف آن این است که یک پیام را به چند قسمت تقسیم کند به‌گونه‌ای که هیچ زیر مجموعه غیرمجاز برای بازسازی پیام اصلی کافی نباشد[۷].

ازآنجایی‌که در فعالیت‌های مشترک امن نقش دارد، اشتراک‌گذاری راز، یک مأموریت رمزنگاری اصلی برای ارتباطات چندجانبه، از جمله کنترل موشک‌ها را تشکیل می‌دهد[۸].

طرح‌های کلاسیک به‌اشتراک‌گذاری راز را می‌توان تنها بر اساس پیچیدگی ریاضی پیاده‌سازی کرد؛ بنابراین، با ظهور کامپیوترهای کوانتومی، اشتراک‌گذاری راز نیز مجبور می‌شود با قوانین مکانیک کوانتومی وارد عصر امن اطلاعاتی شود که به آن اشتراک‌گذاری راز کوانتومی یا QSS[3] اطلاق می‌شود. اولین پروتکل اشتراک‌گذاری مخفی کوانتومی در سال ۱۹۹۹ با استفاده از حالت درهم‌تنیده سه فوتون برای سه شرکت‌کننده پیشنهاد شد[۹].

بااین‌وجود، مشکلات در آماده‌سازی و انتقال حالت‌های درهم‌تنیده، نرخ کلید مخفی و فاصله انتقال QSS را محدود می‌کند و پیاده‌سازی عملی آن را با چالش جدی QSS مواجه کرده است. بر خلاف QKD، این روش در مقابل حملات اسب تروآ مقاوم است برای ارتباطات کوانتومی چندجانبه که یکی از سنگ بناهای اینترنت کوانتومی آینده است، ضروری است[۱۰].

در واقع QSS روشی برای به اشتراک گذاشتن پیام‌های مخفی بین اعضای یک گروه با حفظ کامل امنیت اطلاعات است. بااین‌حال، محدودیت‌های نرخ - فاصله به‌شدت نرخ کلید امن و فاصله انتقال QSS را محدود می‌کند.

❖پروتکل BB84[4]

در سال ۱۹۸۴، چارلز بنت و ژیل براسارد اولین پروتکل رمزنگاری کوانتومی که امروزه با نام BB84 شناخته می‌شود را معرفی کردند[۱۱].

پروتکل BB84 یکی از روش‌های توزیع کلید کوانتومی است و به طور قابل اثباتی امن است. در این پروتکل وجود یک کانال کوانتومی برای انتقال کلید کوانتومی و یک کانال کلاسیک معتبر برای انتقال داده الزامی است. معمولاً از فوتون‌های قطبش یافته برای انتقال اطلاعات از طریق کانال کوانتومی استفاده می‌شود، جایی که فرستنده به طور تصادفی حالت‌های قطبش را با استفاده از مولد اعداد تصادفی ایجاد می‌کند. معمولاً به‌عنوان روشی برای برقراری ارتباط امن کلید خصوصی ازیک‌طرف به‌طرف دیگر برای استفاده در رمزگذاری پد یکبار مصرف استفاده می‌شود. این روش هنوز هم یکی از پروتکل‌های مهم توزیع کلید کوانتومی به شمار می‌رود. در علم رمزنگاری، پد یکبار مصرف یک تکنیک رمزگذاری است که در آن از یک کلید یکبار مصرف استفاده می‌شود. طول این کلید کوچک‌تر از پیام ارسال شده نیست و بایستی از قبل به اشتراک گذاشته شده باشد. در این تکنیک، اطلاعات رمزگذاری نشده با یک کلید مخفی تصادفی یا همان پد یکبار مصرف جفت می‌شود، سپس با استفاده از ترکیب هر بیت یا کاراکتر اطلاعات رمزگذاری نشده با بیت یا کاراکتر مربوطه از پد یکبار مصرف به روش هم‌نهشتی اطلاعات رمزگذاری می‌شود. در حالت ایده‌آل،

[1] Qualifications and Credit Framework
[2] Quantom Digital Signature
[3] Quick Security Setup
[4] Charles Bennett and Gilles Brassard in 1984

پروتکل BB84 در برابر حملات آسیب‌ناپذیر است. اما در عمل، عوامل مختلفی مانند فقدان منابع و آشکارسازهای تک فوتون ایده‌آل و همچنین پیدایش تکنیک‌های استراق سمع پیشرفته پیاده‌سازی عملیاتی این پروتکل را با چالش مواجه کرده است.

❖ پروتکل T12

در پروتکل T12 به‌جای استفاده از منبع تک فوتون، فرض می‌شود که فرستنده دارای یک منبع با فاز تصادفی از حالت‌های همدوس است[۱۲]. پالس‌های نوری هم در شدت و هم در درجه آزادی دیگری مدوله می‌شوند که برای رمزگذاری اطلاعات کوانتومی استفاده می‌شود. این درجه آزادی می‌تواند قطبش یا فاز نسبی یک تداخل‌سنج ماخ زندر نامتقارن باشد. برای مدولاسیون شدت، فرستنده به طور تصادفی از بین سه مقدار ممکن انتخاب می‌کند. همچنین برای رمزگذاری، فرستنده به طور تصادفی یکی از چهار حالت ممکن را انتخاب می‌کند، درست مانند پروتکل استاندارد BB84. شدت‌ها و حالت‌ها به طور مستقل از هم توسط فرستنده انتخاب می‌شوند، به‌طوری‌که امکان جفت‌کردن هر حالت با شدت متفاوت وجود دارد. این امکان اجرای ساده‌تر را فراهم می‌کند و از همبستگی اتفاقی بین شدت و رمزگذاری اطلاعات جلوگیری می‌کند. علاوه بر این، می‌توان بیت‌های کلید را از هر دوپایه انتخاب کرد و در نتیجه مدل استاندارد BB84 را به‌عنوان یک مورد خاص زمانی به دست آورد. این سازگاری در عمل مفید است، زیرا نسبت بهینه بین پایه‌ها می‌تواند به ویژگی‌های کانال کوانتومی بستگی داشته باشد.

❖ پروتکل Decoy state

پروتکل حالت فریب به‌عنوان یکی از مهم‌ترین روش‌ها برای محافظت از امنیت توزیع کلید کوانتومی با استفاده از یک منبع همدوس تضعیف شده در نظر گرفته شده است. این پروتکل که در سال ۲۰۰۵ پیشنهاد شد در واقع روشی استاندارد برای بهبود پروتکل‌های توزیع کلید ارائه کرد[۱۳]. برای تولید حالت‌های فریب با شدت‌های مختلف معمولاً از مدولاسیون جریان پمپ در لیزرهای نیمه‌هادی و یا مدولاسیون خارجی توسط مدولاتورهای نوری استفاده می‌شود. استفاده از پروتکل BB84 همراه با روش حالت فریب در حال حاضر کاربردی‌ترین پروتکل توزیع کلید کوانتومی است که در رژیم کلید محدود در برابر حملات عمومی امن شده است. دلایل این موضوع عبارت‌اند از:

- ✓ در شرایطی که کانال کوانتومی تلفات بالایی داشته باشد، این پروتکل عملکرد مناسبی از خود نشان می‌دهد.
- ✓ تحقق آن با منابع نوری ارزان‌قیمت امکان‌پذیر است. گروه‌های تحقیقاتی متعددی نشان داده‌اند که در شرایط دنیای واقعی این روش انتقال کلید امکان‌پذیر است و از امنیت بالایی نیز برخوردار است. در حال حاضر، دستیابی به نرخ تولید کلید مخفی بالاتر و فاصله انتقال امن طولانی‌تر از مهم‌ترین روندهایی است که در گروه‌های تحقیقاتی و شرکت‌های فعال در این حوزه دنبال می‌شود.

❖ پروتکل SARG04[1]

این پروتکل در سال ۲۰۰۴ پیشنهاد شد. این یک پروتکل ساده است که از چهار حالت غیرمتعامد استفاده می‌کند. فرستنده به طور تصادفی یکی از چهار حالت ممکن را انتخاب می‌کند و رشته فوتون‌ها را برای گیرنده می‌فرستد. سپس گیرنده σx یا σz را اندازه‌گیری می‌کند.

بنابراین، در سطح کوانتومی مشابه BB84 است. اما تغییری در فرآیند غربال‌کردن کلاسیک وجود دارد. در این پروتکل، میانگین تعداد فوتون‌ها در هر پالس باید بزرگ‌تر در نظر گرفته شود. در جبران آن، این پروتکل سپر بهتری در برابر حمله تقسیم تعداد فوتون یا PNS در QBER=0 فراهم می‌کند[۱۴].

❖ پروتکل SSP[2]

پروتکل شش‌حالته یا به‌اختصار SSP در سال ۱۹۹۹ پیشنهاد شد. [۱۵]همان‌طور که از نام آن مشخص است، این پروتکل از شش حالت قطبش ممکن استفاده می‌کند؛ بنابراین در مجموع سه‌پایه به‌جای دوپایه در پروتکل BB84 وجود دارد. فرستنده به طور تصادفی از بین این شش حالت یک حالت را انتخاب می‌کند و آن را برای گیرنده می‌فرستد. گیرنده آن را در پایهx ، yیا z به طور تصادفی اندازه‌گیری می‌کند. در اینجا احتمال اینکه گیرنده و فرستنده یک‌پایه را انتخاب کنند به یک‌سوم کاهش می‌یابد، به این معنی که آنها باید به طور متوسط دو سوم بیت‌های ارسال شده را برای ایجاد یک کلید امن کنار بگذارند. اما به دلیل وجود حالت‌های احتمالی بیشتر از BB84، میزان خطای ناشی از اندازه‌گیری شنودگر افزایش خواهد یافت؛ بنابراین، حداکثر اطلاعات شنودگر کمتر از اطلاعات شنودگر در پروتکلBB84 خواهد بود. به‌این‌ترتیب، این پروتکل در برابر استراق سمع تک کیوبیت‌ها نسبت به طرح BB84 امن‌تر است.

❖ پروتکل E91

در این پروتکل که در سال ۱۹۹۹۱ پیشنهاد شد[۱۶]. از جفت فوتون‌های درهم‌تنیده برای توزیع کلید استفاده می‌شود. این جفت فوتون‌ها می‌تواند توسط فرستنده، گیرنده، و یا توسط منبعی جدا از هر دو ایجاد شود. فوتون‌ها به‌گونه‌ای توزیع

1.Valerio Scarani, Antonio Acin, Gregoire Ribordy, and Nicolas Gisin
2.State Scholarship Portal

می‌شوند که گیرنده و فرستنده هر کدام یک فوتون از هر جفت را داشته باشند. این پروتکل بر دو ویژگی درهم‌تنیدگی متکی است.
الف: حالت‌های درهم‌تنیده کاملاً همبستگی دارند به این معنا که اگر گیرنده و فرستنده هر دو اندازه‌گیری کنند که آیا ذرات آنها قطبش عمودی یا افقی دارند، همیشه یک پاسخ را با احتمال ۱۰۰ درصد دریافت می‌کنند. اگر هر دو جفت پلاریزاسیون مکمل (متعامد) دیگری را اندازه‌گیری کنند، همین امر صادق است.
ب: هر گونه تلاش برای استراق سمع توسط شنودگر، این همبستگی‌ها را به‌گونه‌ای از بین می‌برد که گیرنده و فرستنده می‌توانند تشخیص دهند. مشابهBB84 ، این پروتکل شامل یک پروتکل اندازه‌گیری خصوصی قبل از تشخیص حضور شنودگر است. برای تشخیص استراق سمع، گیرنده و فرستنده می‌توانند با پیاده‌سازی آزمایش‌های تست بل، نقض قضیه بل به واسطه شنود را مشاهده کنند. به‌طورکلی، پیاده‌سازی پروتکل‌های مبتنی بر درهم‌تنیدگی کوانتومی مثل E91 از پیاده‌سازی پروتکل‌های آماده‌سازی و اندازه‌گیری مثل BB84 دشوارتر است، به این دلیل که کانال کوانتومی درهم‌تنیدگی را در فواصل طولانی از بین می‌برد. بااین‌حال، هر دو نوع پروتکل در میان یک لینک ۱۰۰۰ کیلومتری با استفاده از ماهواره مدار پایین زمین آزمایش شده‌اند.

❖ پروتکل B92

این پروتکل در سال ۱۹۹۲ پیشنهاد شد.[۱۷]تفاوت اصلی B92 با BB84 در این است که فقط دو حالت قطبش به‌جای چهار حالت قطبش ممکن در BB84 ضرورت دارد. نتایج به‌دست‌آمده از یک تحقیق نشان می‌دهد که پروتکل BB84 عملکرد بهتری نسبت به B92 در توزیع امن کلید در فواصل طولانی از خود نشان می‌دهد، طور یکه برای یک نرخ تکرار ۱۰ مگاهرتز در ارتفاع مداری ۱۰۰ کیلومتر، نرخ بیت ارتباط امن برای پروتکل BB84 حدود ۲۸۰ کیلوهرتز و برای پروتکل B92 حدود ۷۰ کیلوهرتز ارزیابی شده است[۱۸].

❖ پروتکل BBM92

پروتکل BBM92 یک پروتکل توزیع کلید کوانتومی است که شامل جفت فوتون‌های درهم‌تنیده است و می‌تواند به‌عنوان یک نسخه مبتنی بر درهم‌تنیدگی از پروتکل BB84 در نظر گرفته شود. این پروتکل برای اولین‌بار در سال ۱۹۹۲ پیشنهاد شد[۱۹]. درحالی‌که پروتکل BB84 بر اساس آماده‌سازی و اندازه‌گیری حالت قطبش فوتون‌ها کار می‌کند، در پروتکل BBM92 یک تصادفی بودن ذاتی ناشی از اندازه‌گیری جفت فوتون‌های درهم‌تنیده وجود دارد. در این پروتکل، یک فرستنده مشترک اقدام یک جفت فوتون درهم‌تنیده تولید می‌کند و آنها را از طریق یک کانال کوانتومی برای هر دو طرف فرستنده و گیرنده کلید می‌فرستد. کانال‌های کوانتومی می‌توانند فضای آزاد، آب یا فیبر نوری باشند. گیرنده و فرستنده به طور مستقل اندازه‌گیری‌های خود را به‌صورت تصادفی انجام می‌دهند. هنگامی که اندازه‌گیری انجام شد، هر دو انتخاب‌های پایه خود را از طریق کانال عمومی اعلام می‌کنند. تنها آن اندازه‌گیری‌هایی که فرستنده و گیرنده پایه یکسانی را برای آن انتخاب کرده‌اند برای تولید کلید مورداستفاده قرار می‌گیرند و بقیه اندازه‌گیری‌ها ارزشی ندارند و کنار گذاشته می‌شوند. به کلیدی که پس از این فرآیند ساخته می‌شود، کلید غربال شده گفته می‌شود. علاوه بر این، برای دستیابی به یک کلید امن عملیات تصحیح خطا و تقویت حریم خصوصی بر روی کلید غربال شده انجام می‌شود. لازم به ذکر است که پروتکل‌های توزیع کلید مبتنی بر درهم‌تنیدگی یا به‌اختصار EBQKD[1] برای ارتباطات کوانتومی از راه دور مانند ماهواره به زمین ایده‌آل است، زیرا می‌تواند بین دو ایستگاه زمینی دور از هم یک ارتباط امن برقرار کند. همچنین، صرف‌نظر از اینکه ماهواره توزیع‌کننده جفت فوتون‌های درهم‌تنیده قابل‌اعتماد است یا خیر، امنیت به خطر نمی‌افتد. لازم به ذکر است که EBQKD ماهواره به زمین قبلاً انجام شده است[۲۰]. محدودیت فعلی استفاده از EBQKD نرخ تولید کلید پایین آن است، زیرا جفت فوتون‌های درهم‌تنیده معمولاً توسط فرآیند تبدیل پایین پارامتری خود به خودی SPDC تولید می‌شود که راندمان بسیار پایینی دارد. یکی از عوامل اصلی که نرخ تولید کلید را محدود می‌سازد، راندمان پایین تولید جفت فوتون‌های درهم‌تنیده و جذب و اتلاف فوتون‌ها در کانال ارتباطی است.

راندمان پایین را می‌توان با استفاده از منابع تولید جفت فوتون با درخشندگی و فیدلیتی بالا جبران کرد. انتخاب طول‌موج مناسب برای فوتون‌های درهم‌تنیده یکی از راه‌های کاهش اثر کانال بر نرخ تولید کلید امن است.

❖ پروتکل MSZ96

پروتکلMSZ96 یک پروتکل توزیع کلید کوانتومی است که بر اساس نور چلانده کار می‌کند، طور یکه بدون استفاده از قطبش فوتون مشابه آنچه در پروتکل BB84 داریم و یا استفاده از فوتون‌های درهم‌تنیده مشابه آنچه در پروتکل E91 داریم، اقدام به توزیع امن کلید می‌کند. این پروتکل برای اولین‌بار در سال ۱۹۹۶ پیشنهاد شد[۲۱]. این پروتکل بر اساس پرتوهای نور ضعیف کار می‌کند و نیازی به منبع تک فوتون ندارد. در شرایطی که تلفات فوتون‌ها در کانال کوانتومی زیاد است این پروتکل کارایی بالایی دارد. دلیل آن این است که گیرنده می‌تواند تمام بیت‌هایی را که معیار غربال‌گری را برآورده نمی‌کنند دور بیندازد

1 .Entanglement Based Quantum Key Distribution

و آنهایی را که معیار غربالگری را برآورده می‌کنند نگه دارد. مزیت دیگر این پروتکل این است که اگر تلفات کانال بسیار زیاد باشد، فرستنده می‌تواند سیگنال ارسالی خود را کمی قوی‌تر کند. این افزایش اندک در توان سیگنال ارسالی تأثیر شدیدی بر کاهش امنیت توزیع کلید نخواهد داشت.

❖ پروتکل COW

پروتکل همدوس یک‌طرفه COW برای اولین‌بار در سال ۲۰۰۵ پیشنهاد شد[۲۲]. این یک پروتکل ساده برای مبارزه با حمله تقسیم عدد فوتون PNS است. در این پروتکل، در سمت فرستنده اطلاعات به‌صورت همدوس بین پالس‌های لیزری مختلف رمزگذاری می‌شود و در سمت گیرنده بررسی می‌شود که آیا چنین همدوسی حفظ شده است یا خیر. حمله PNS این همدوسی را می‌شکند، بنابراین پروتکل COW می‌تواند آن را شناسایی کند. توزیع کلید کوانتومی در فواصل طولانی با استفاده از این روش پیاده‌سازی شده است و حتی محصولات تجاری بر اساس این پروتکل نیز روانه بازار شده‌اند. در ترکیب با آشکارسازهای کم‌نویز، پروتکل COW مخصوصاً برای فیبرهای بلند یا پرتلفات کاربرد دارد. علی‌رغم محبوبیت زیاد این پروتکل، COW در برابر انواع دیگر حملات قوی نیست.

❖ پروتکل DPS[1]

پروتکل تغییر فاز تفاضلی یاDPS یک پروتکل توزیع کلید کوانتومی است که برای اولین‌بار در سال ۲۰۰۲ پیشنهاد شد[۲۳]. در این پروتکل رمزنگاری ابتدا یک فوتون منفرد در یک حالت برهم‌نهی خطی از سه حالت پایه آماده می‌شود و در قالب سه پالس متوالی از سمت فرستنده تولید شده و به گیرنده فرستاده می‌شود. در این پروتکل اختلاف‌فاز بین دو پالس متوالی اطلاعات بیت کوانتومی را حمل می‌کند. گیرنده با استفاده از یک سیستم تشخیص فاز تفاضلی غیرفعال اقدام به اندازه‌گیری اطلاعات کوانتومی می‌کند. این طرح برای پیاده‌سازی در بستر فیبر نوری مناسب است و کارایی ایجاد کلید با راندمان بالاتر از BB84 مبتنی بر فیبر معمولی را ارائه می‌دهد. طرح DPS در برابر حمله تقسیم پرتو برای نور همدوس تضعیف شده بهتر از BB84عمل می‌کند.

❖ پروتکل KMB09

پروتکل KMB09 یک پروتکل توزیع کلید کوانتومی است که در آن گیرنده و فرستنده از دوپایه بایاس نشده استفاده می‌کنند که یکی از آنها کد "۰ "و دیگری "۱ "را کد می‌کند. امنیت این پروتکل به دلیل افزایش نرخ خطای انتقال شاخص ITER و نرخ خطای بیت کوانتومی QBER است که توسط یک استراق سمع ایجاد می‌شود.

❖ پروتکل HD

توزیع کلید کوانتومی با ابعاد بالا، امکان نرخ بالای کلید امن با بازده اطلاعات فوتونی بالا را ارائه می‌دهد. این پروتکل که می‌تواند بر اساس درهم‌تنیدگی زمان - انرژی پیاده‌سازی شود، در برابر حملات جمعی امن است. نرخ پایین تولید کلید امن از مهم‌ترین معایب این پروتکل به شمار می‌رود.

❖ پروتکل CV^{2}

پیاده‌سازی پروتکل توزیع کلید کوانتومی متغیر پیوسته برای رمزنگاری کوانتومی امن به‌خوبی امکان‌پذیر است. این پروتکل بر فناوری استاندارد مخابراتی موجود قابلیت پیاده‌سازی دارد و نرخ کلید مخفی بالاتری را در هر پالس در فاصله نسبتاً کوتاهی به دلیل امکان رمزگذاری بیش از یک بیت در هر پالس نشان می‌دهد. اصطلاح "متغیر پیوسته" به این دلیل برای این پروتکل استفاده می‌شود که به‌جای استفاده از آشکارساز تک فوتون که در BB84و بسیاری دیگر از پروتکل‌ها استفاده می‌شود، از آشکارساز همودین استفاده می‌شود.

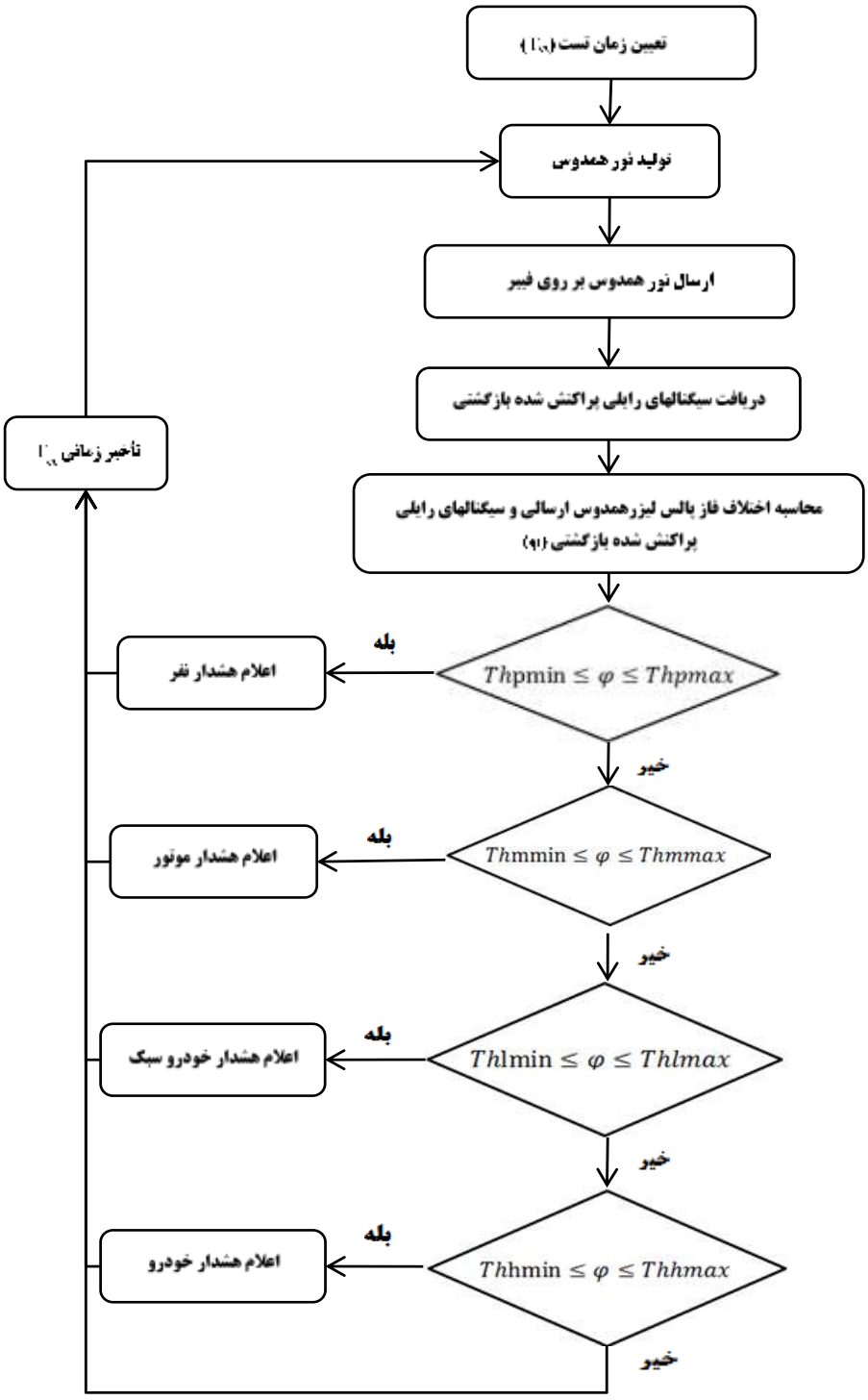
۵- روش پیشنهادی

به‌کارگیری سامانه‌های فعلی حسگر صوتی توزیع شده صوت و لرزش DAS پاسخگوی رفع چالش‌های بزرگ سازمان‌ها برای جلوگیری از دسترسی دشمن به محتوای داده‌های روی فیبر، جلوگیری از نزدیکی دشمن به فیزیک فیبر نوری، تغییر در محتوای داده‌های روی فیبر و یا تزریق و تحکم و کنترل روی داده‌های فیبر نوری با روش‌های مختلف نظیر انواع روش‌های تپ زنی نیست. هنوز مشکلاتی در تشخیص برد، مسافت، تلورانس محل دقیق تشخیص فیبر نوری ناشی از دست‌پیچ داخل حوضچه‌ها و همچنین میزان دقت در نتایج سامانه‌ها وجود دارد. ضمن آن که اگر روی فیبر نوری سیستم‌های شنود قرار گرفته باشد با سامانه‌های DAS نیز قابل‌تشخیص نمی‌باشد؛ لذا این موضوع ما را بر آن داشت برای رفع چالش‌های فوق، اقدام به ارائه پیشنهاد بهینه‌سازی سامانه حسگر توزیع شده صوت و لرزش DAS نماییم.

بلوک دیاگرام روش فعلی عملکرد سامانه حسگر توزیع‌شده صوت و لرزش DAS در شکل شماره ۷ نمایش داده شده است.

1.Differential-Phase-Shift

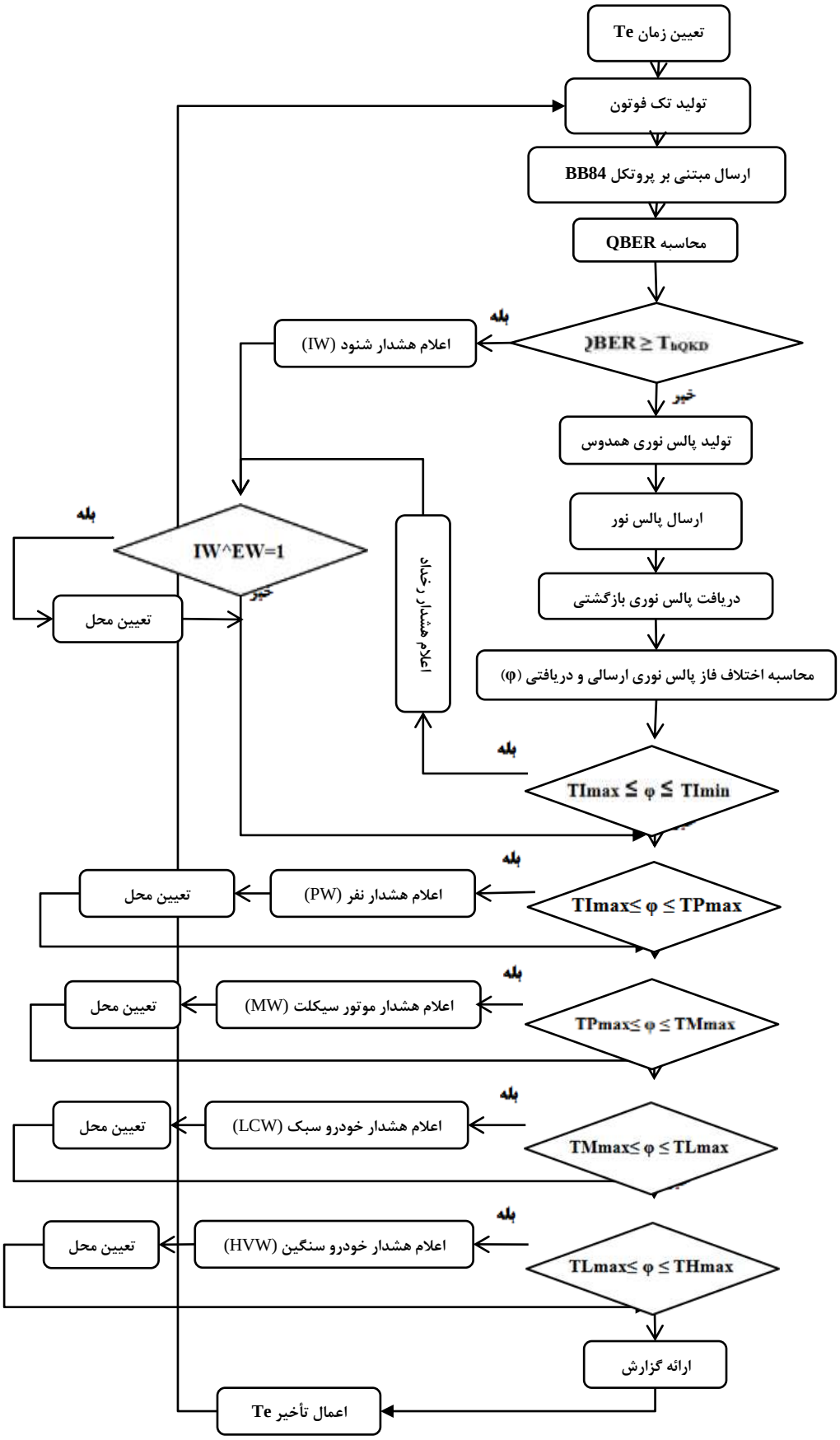
2.Continuous-Variable



شکل (۷): الگوریتم عملکرد DAS

پیشنهاد ما در این مقاله روش بهینه‌سازی عملکرد سامانه DAS وش ارسال تک فوتون‌های کوانتومی و توزیع کلید کوانتومی است. این روش با تکنیک استفاده از روش‌های توزیع کلید کوانتومی پیوسته QKD-CV[1] و روش‌های توزیع کلید کوانتومی گسسته QKD-DV[2] امکان‌پذیر است. این تکنیک می‌تواند خط را در صورت عدم آشکارسازی تپ هم امن نماید. الگوریتم روش پیشنهادی که از خواص کوانتومی برای بهبود عملکرد DAS در شناسایی تب و شنود غیرمجاز بهره می‌گیرد در شکل ۸ آمده است.

[1] Quantum Key Distribution Continuse-Variable
[2] Quantum Key Distribution Discrete-Variable



شکل (۸): الگوریتم روش پیشنهادی

۶- همان‌طور که در شکل ۸ آمده است ابتدا فاصله زمانی بین دو ارزیابی (Te) را تعیین می‌شود. سپس تولید تک فوتون نموده و با پروتکل توزیع کلید کوانتومیBB84 نسبت به ارسال آن و محاسبه نرخ خطای بیت کوانتومی (QBER) اقدام می‌گردد. درصورتیکه QBER از مقدار مرسوم آن در توزیع کلید کوانتومی بیشتر باشد شنود از فیبر تشخیص داده و اعلام هشدار شنود (IW) صادر می‌گردد. علت این موضوع جذب تک فوتون‌ها توسط سیستم شنود است که در حالت غیر تک فوتون این موضوع ممکن نیست. در ادامه تولید پالس نوری همدوس نموده در لینک فیبر نوری ارسال شده و سپس با مقایسه پالس نوری رفت و برگشت مقدار اختلاف فاز (φ) محاسبه می‌گردد [۲۴].

۷- درصورتی‌که میزان اختلاف‌فاز $TImin \leq \varphi \leq TImax$ باشد اعلام هشدار رخداد (EW) صادر می‌شود در صورت هشدار توأمان EW و IW تعیین محل شنود انجام می‌شود. درصورتی‌که اختلاف‌فاز در این بازه نباشد با تحلیل آن به شرح زیر نسبت شناخت نوع رویداد و تعیین محل آن اقدام می‌گردد.

- درصورتی‌که میزان اختلاف‌فاز $TImax \leq \varphi \leq TPmax$ باشد اعلام هشدار رخداد تشخیص نفر صادر می‌شود.
- درصورتی‌که میزان اختلاف‌فاز $TPmax \leq \varphi \leq TMmax$ باشد اعلام هشدار رخداد تشخیص موتورسیکلت صادر می‌شود.
- درصورتی‌که میزان اختلاف‌فاز $TMmax \leq \varphi \leq TLmax$ باشد اعلام هشدار رخداد تشخیص خودرو سبک صادر می‌شود.
- درصورتی‌که میزان اختلاف‌فاز $TLmax \leq \varphi \leq THmax$ باشد اعلام هشدار رخداد تشخیص خودرو سنگین صادر می‌شود.

تعیین محل از اختلاف زمان رفت‌وبرگشت نور به طور دقیق محاسبه می‌شود. بدین صورت که از حاصل‌ضرب سرعت در زمان رفت‌وبرگشت تقسیم بر دو، فاصله از مبدأ دقیقاً محاسبه شده و تعیین محل صورت می‌گیرد.

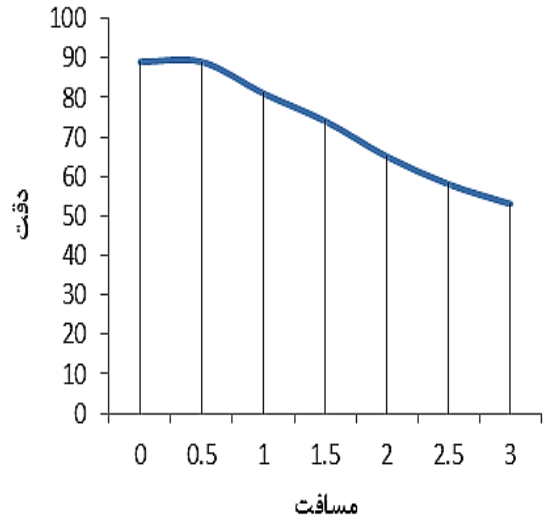
در انتها پس از تعیین محل رخدادها نسبت به ارائه گزارش وضعیت رویدادهای طول مسیر فیبر اقدام می‌شود و پس از تأخیر Te مجدداً فرایند ارزیابی صورت می‌پذیرد.

۸- ۷- ارزیابی و نتیجه گیری

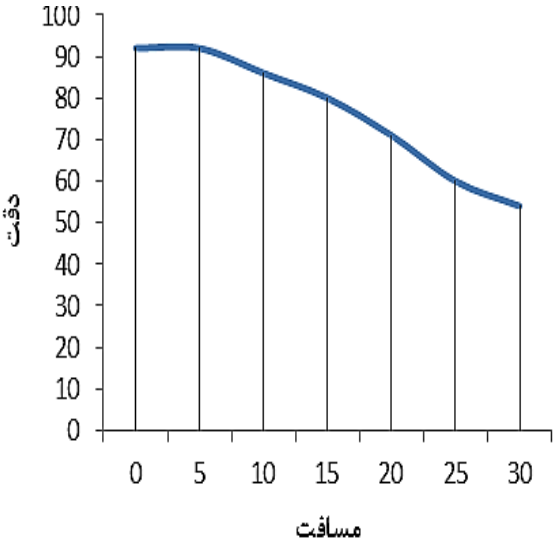
همان‌طور که در بند قبل بیان شد روش پیشنهادی بهبودیافته سیستم حسگر صوتی (DAS)می‌باشد که با بهره‌گیری از خواص فناوری کوانتومی علاوه بر تشخیص رویدادهای مرسوم قادر به تشخیص تب‌ها و سامانه شنود از فیبر می‌باشد. به عبارتی می‌توان گفت الگوریتم پیشنهادی دارای قابلیت‌های زیر است:

- ✓ تشخیص انواع تب‌ها
- ✓ تشخیص سامانه‌های شنود
- ✓ تشخیص نفوذ و تجاوز افراد به حریم فیبر
- ✓ تشخیص نفوذ و تجاوز موتورسیکلت به حریم فیبر
- ✓ تشخیص نفوذ و تجاوز خودرو سبک به حریم فیبر
- ✓ تشخیص نفوذ و تجاوز خودرو سنگین به حریم فیبر

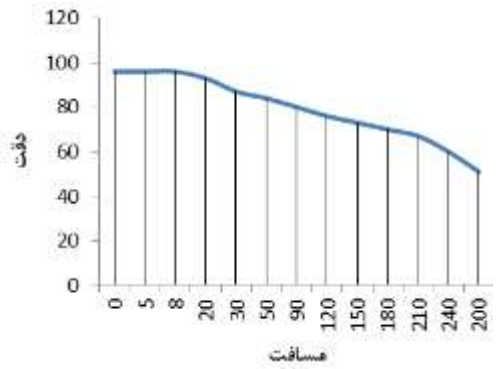
نتایج حاصله از ارزیابی الگوریتم پیشنهادی با داده‌های جمع‌آوری‌شده برای دقت تشخیص نسبت به مسافت نفر، موتورسیکلت، خودرو سبک و خودرو سنگین به ترتیب در شکل‌های ۹، ۱۰، ۱۱ و ۱۲ آمده است.



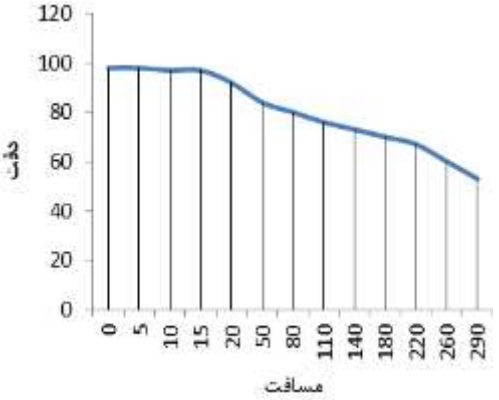
شکل (۹): دقت روش پیشنهادی در تشخیص" نفر"



شکل (۱۰): دقت روش پیشنهادی در تشخیص" موتورسیکلت"

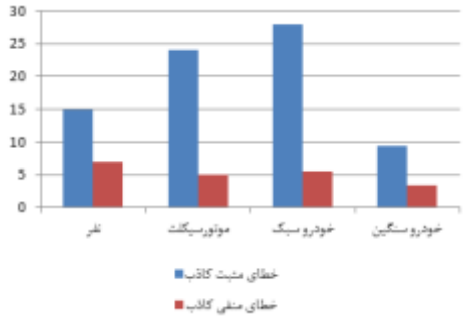


شکل (۱۱): دقت روش پیشنهادی در تشخیص" خودرو سبک"



شکل (۱۲): دقت روش پیشنهادی در تشخیص" خودرو سنگین"

میانگین خطای مثبت کاذب و خطای منفی کاذب در مسافت‌های مختلف برای تشخیص عامل‌های مختلف در شکل ۱۳ آمده است.



شکل (۱۳): خطای مثبت کاذب و خطای منفی کاذب روش پیشنهادی

مطابق ارزیابی‌های صورت‌گرفته روش پیشنهادی بادقت ۹۸ درصد وجود سامانه شنود از فیبر را تشخیص داده و مطابق شکل‌های فوق الذکر بادقت بالای ۷۰ درصد قادر به تشخیص نفر در شعاع ۲ متری و بادقت بالای ۷۲ درصد قادر به تشخیص موتورسیکلت در شعاع ۲۰ متری و بادقت بالای ۷۵ درصد قادر به تشخیص خودرو سبک در شعاع ۱۲۰ متری و بادقت بالای ۷۶ درصد قادر به تشخیص خودرو سنگین در شعاع ۱۸۰ متری می‌باشد.

۶- مراجع

[1]"Electical & Computer Technical Website", http://microrf.ir, 2023.

[2] "Distributed sound and vibration sensor" project reports, Sharif University of Technology, Photonics and Quantum Center, Abolfazl Bahrampur, 2018.

[3] Y. Gong1, R. Kumar2, A. Wonfor, "Secure optical communication using a quantum alarm", Official journal of the CIOMP 2047-7538 , pp 180-192, 2020.

[4]The first report of the project "Performance Comparison of Discrete Quantum Key Distribution Protocols", Sharif University of Technology, Photonics and Quantum Center, Morteza Nikayin, 2018.

[5] Project "Map of entry into the field of communication and quantum cryptography", the detailed political document of the Kausar Thought Center, Hossein Taleb, 1400.

[6] Bruss, D., Erdelyti, G., Meyer, T., Riege, T., Rothe, J., "Quantum Cryptography: A Survey", ACM Computing Surveys, Vol. 39, No. 2, Article 6, 2007.

[7] A. Shamir, Communications of the ACM 22, 612, 1979.

[8] G. J. Simmons, in Workshop on the Theory and Application of of Cryptographic Techniques pp. 436–467, 1989.

[9] M. Hillery, V. Bu˘zek, and A. Berthiaume," Quantum secret sharin", Physical Review. A 59, 1829 , 1999.

[10] Jie Gu, Xiao-Yu Cao, Hua-Lei Yin, Zeng-Bing Chen, "Differential phase shift quantum secret sharing using twin field", Opt. Express 29, 9165, 2021.

[11] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York,,1984.

[12] 2 M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoystate quantum key distribution with quantified security", Opt. Express 21, 24550-24565,2013.

[13] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, "Decoy State Quantum Key Distribution" Physical Review Letters. 94, 230504, 2005.

[14] Scarani, Valerio & Acín, Antonio & Ribordy, Grégoire & Gisin, Nicolas. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". Physical review letters. 92. 057901. 2004.

[15] Bruss, Dagmar "Optimal Eavesdropping in Quantum Cryptography with Six States", Physical Review Letters, 81.

10.1103/PhysRevLett.81.3018 (1998).
[16] A. K. Ekert, "Quantum cryptography based on bell's theorem", Physical Review Letters. 67, pp. 661–663, 1991.
[17] C. Bennett, "Quantum cryptography using any two nonorthoganol states", Physical Review Letters. 68, pp. 3121-3124,1992.
[18] R. Etengu, F. M. Abbou, H. Y. Wong, A. Abid, N. Nortiza, A.Setharaman," Performance Comparison of BB84 and B92 Satellite-Based Free Space Quantum Optical Communication Systems in the Presence of Channel Effects" Journal of Optical Communications, Volume 32, Issue 1, pp.37-47, 2011.
[19] C. H. Bennet, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem", Physical Review Letters. 68, pp. 557-559, 1992.
[20] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang,, … J.-W. Pan, "Satellite-Relayed Intercontinental Quantum Network", Physical Review Letters, 120(3), 2018.
[21] Mu, Yi; Seberry, Jennifer; Zheng, Yuliang, "Shared cryptographic bits via quantized quadrature phase amplitudes of light" Optics Communications. pp. 344–352,1996.
[22] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden: "Fast and simple one-way quantum key distribution" Applied Physics Letters. 87(19); 194108, 2005.
[23] K. Noue, E.Waks, & Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution" Physical Review Letters, 89(3), 2002.
[24] A. Fichtner, A. Bogris, T. Nikas, Theory of phase transmission fibre-optic deformation sensing, Geophysical Journal International, Volume 231, Issue 2, Pages 1031–1039, 2022.
[25] Project No. 2 "Performance Comparison of Discrete Quantum Key Distribution Protocols", Sharif University of Technology, Photonics and Quantum Center, Morteza Nik Ayin, 2018.
[26] Project reports "Reviewing the Principles and Basics of Quantum Communication Technology", Imam Hossein University (AS), Faculty and Research Institute of Fawa, Communication and Network Science and Technology Center, Ali Naseri, 2018.