مزایا و چالشهای رمزنگاری کوانتومی درمقابل رمزنگاری کلاسیک

اسفندیار لشنی

گروه ریاضی، واحد دورود، دانشگاه آزاد اسلامی، دورود، ایران

چکیده

محاسبات کوانتومی انقلابی در قابلیت‌های محاسباتی ایجاد می‌کند و با بهره‌گیری از اصول مکانیک کوانتومی، داده‌ها را به روش‌هایی کاملاً نوین پردازش می‌نماید. در این مقاله اصول اساسی مکانیک کوانتومی، از جمله برهم نهی و درهم تنیدگی، که پایه‌های محاسبات و رمزنگاری کوانتومی را تشکیل می‌دهند، مرور می‌کنیم. سپس اصول و پروتکل های رمز نگاری کلاسیک را مطرح کرده و مشکلات این سیستم ها را در مقابل محاسبات کوانتمی ذکر کرده و همچنین الگوریتم‌های رمزنگاری کوانتومی، به‌ویژه پروتکل‌های توزیع کلید کوانتومی (QKD) را بررسی کرده و به قابلیت‌های آن‌ها در تأمین امنیت ارتباطات در عصر کوانتوم می‌پردازیم.

واژگان کلیدی: رمزنگاری کوانتومی، توزیع کلید کوانتومی، مکانیک کوانتومی، ارتباطات کوانتومی، رمزنگاری کلاسیک

مقدمه

محاسبات کوانتومی به عنوان یک تحول انقلابی در فناوری محاسباتی مطرح شده است. برخلاف رایانه‌های کلاسیک که از بیت‌ها استفاده می‌کنند، رایانه‌های کوانتومی از کیوبیت‌ها بهره می‌برند .کیوبیت‌ها به دلیل خاصیت برهم‌نهی و درهم‌تنیدگی می‌توانند هم‌زمان در چندین حالت قرار بگیرند. این ویژگی به رایانه‌های کوانتومی امکان می‌دهد محاسبات پیچیده را با سرعتی خارق‌العاده انجام دهند و مسائلی را حل کنند که برای رایانه‌های کلاسیک غیرممکن است. ایده محاسبات کوانتومی در اوایل دهه ۱۹۸۰ توسط ریچارد فاینمن و دیوید دویچ معرفی شد. ظهور محاسبات کوانتومی تهدیدی جدی برای سیستم‌های رمزنگاری کلاسیک ایجاد کرده است. در رمزنگاری کلاسیک برای محافظت از اطلاعات حساس در برابر دسترسی‌های غیرمجاز و تهدیدات سایبری استفاده می شود. الگوریتم‌های رمزنگاری، داده‌های خوانا را با استفاده از یک کلید به فرمتی ناخوانا تبدیل می‌کنند تا تنها افراد مجاز بتوانند آن را رمزگشایی و به اطلاعات دسترسی پیدا کنند. این فرایند برای امنیت ارتباطات، تراکنش‌های مالی، داده‌های شخصی و اطلاعات محرمانه دولتی حیاتی است .رمزنگاری مبتنی بر کلید عمومی، مانند RSA و رمزنگاری منحنی بیضوی(ECC) ، از پیچیدگی محاسباتی مسائلی مانند فاکتورگیری اعداد بزرگ و محاسبه لگاریتم گسسته استفاده می‌کنند. ازاین رو لزوم رمزنگاری کوانتومی احساس می شود.

رمزنگاری کوانتومی به طرز قابل توجهی از همتای کلاسیک خود متفاوت است. که امروزه به طور گسترده‌ای مورد مطالعه قرار گرفته و یکی از نخستین کاربردهای مکانیک کوانتومی در سطح تک‌فوتون‌ها است. و شامل ارسال اطلاعات ایمن بر پایه اصول بنیادی فیزیک کوانتومی است. مهم‌ترین دستاورد رمزنگاری کوانتومی، توزیع کلید کوانتومی (QKD) است که به دو طرف ارتباط (آلیس و باب) اجازه می‌دهد که یک رشته بیت مخفی را به اشتراک بگذارند و یک کلید رمز مشترک و ایمن ایجاد کنند. امنیت این روش برخلاف روش‌های کلاسیک، بر پایه فرضیات محاسباتی نیست، بلکه کاملاً مبتنی بر اصول فیزیکی مکانیک کوانتومی است.

از زمان ارائه پروتکل BB۸٤ توسط بنِت و براسارد در سال ۱۹۸۴، این حوزه پیشرفت‌های قابل توجهی در نظریه و آزمایش‌های تجربی داشته است. در سال‌های اخیر، پیاده‌سازی‌های تجربی QKD در فیبرهای نوری و فضای آزاد انجام شده است، و مسیر را برای کاربردهای عملی این فناوری هموار کرده است. با این حال، چالش‌های تکنولوژیکی متعددی، مانند تولید تک‌فوتون‌های مناسب، ارسال آن‌ها از طریق کانال‌های نوری، و آشکارسازی کارآمد، همچنان باقی است.

QKD بر اساس یک ویژگی ذاتی از مکانیک کوانتومی است: "استخراج اطلاعات در مورد یک حالت کوانتومی ناشناخته به‌طور اجتناب‌ناپذیری آن را مختل می‌کند"، که اجازه می‌دهد فعالیت‌های شنود در اصل شناسایی شوند. در واقع، QKD می‌تواند به‌طور بدون قید و شرط امن باشد، یعنی در برابر او که تنها با مکانیک کوانتومی محدود است. علاوه بر این، QKD حتی اگر حالات کوانتومی از طریق یک کانال کوانتومی نویزی ارسال شوند، همچنان ایمن می‌ماند.

در QKD فرض می‌شود که آلیس و باب با یک کلید اولیه کوچک K_i (برای اهداف احراز هویت) شروع می‌کنند. آنها به داده های تصادفی مستقل دسترسی دارند که تحت کنترل آنها نیستند. آنها می‌توانند پیام‌های کوانتومی و کلاسیک را در هر دو جهت از طریق کانال‌هایی که کاملاً تحت کنترل آنها است، تبادل کنند و ممکن است عملیات و اندازه‌گیری‌های کوانتومی انجام دهند. بر اساس نتایج اندازه‌گیری خود، آلیس و باب یا QKD را متوقف می‌کنند یا کلیدهای مربوطه خود K_A و K_B را تولید می‌کنند. به همین ترتیب،

می‌گوییم که آزمایش QKD شکست خورده یا موفقیت‌آمیز بوده و این رویدادها را می‌توان به صورت $M = ۰$ یا $M > ۰$ توصیف کرد، که در آن M طول کلید تولید شده است. با این حال این سیستم دارای مشکلات امنیتی نیز می باشد.

یکی از نخستین مشکلات امنیتی شناخته‌شده در QKD به شرح زیر است:

QKD نیاز به یک کلید برای احراز هویت دارد که ممکن است در نوبت قبلی QKD حاصل شده باشد. از آنجا که هر اجرای QKD کمی ناقص است، QKD به تکرار کلیدهای کم امنیت تری تولید می‌کند.

به نظر می‌رسد که موارد دیگری نیز وجود دارد که باید به حملات مشترک بر روی QKD و استفاده بعدی از کلید تولید شده پرداخته شود. برای مثال، فرض کنید آلیس و باب QKD را برای به‌دست آوردن یک کلید انجام دهند و سپس از کلید برای رمزگذاری حالات کوانتومی استفاده کنند. چنین به نظر می رسد که ممکن است اطلاعات قابل دسترسی بیشتری نسبت به مجموع اطلاعات به‌دست‌آمده در دو اندازه‌گیری جداگانه برای شخص سوم فراهم کند. (Kumar Sahu S, Mazumdar K, ۲۰۲٤)

مبانی محاسبات و رمزنگاری کوانتومی

اصول اولیه مکانیک کوانتومی: مکانیک کوانتومی شامل چندین اصل کلیدی است که درک و استفاده از محاسبات و رمزنگاری کوانتومی را ممکن می‌سازد. در این بخش، مفاهیم بنیادی مکانیک کوانتومی را که پایه‌های این فناوری پیشرفته را تشکیل می‌دهند، بررسی می‌کنیم:

اصل برهم نهی(Superposition)

یکی از اصول اساسی مکانیک کوانتومی، برهم نهی است. این اصل بیان می‌کند که یک سیستم کوانتومی تا زمانی که اندازه‌گیری نشود، می‌تواند به‌طور هم زمان در چندین حالت مختلف قرار داشته باشد. در مقابل، یک سیستم کلاسیک در هر لحظه تنها می‌تواند در یک حالت مشخص باشد.

در مکانیک کوانتومی، وضعیت یک ذره با تابع موج $|\psi\rangle$ توصیف می‌شود. برای یک کیوبیت، تابع موج به صورت ترکیب خطی از دو حالت پایه $|۱\rangle$ و $|۰\rangle$ نمایش داده می‌شود:

$$|\psi\rangle = \alpha|۰\rangle + \beta|۱\rangle$$

با این شرط که:

$$|\alpha|^۲ + |\beta|^۲ = ۱$$

α و β مقادیر مختلطی هستند که احتمال حضور کیوبیت در هر یک از حالات $|۱\rangle$ و $|۰\rangle$ را مشخص می‌کنند.

در یک رایانه کلاسیک، یک بیت می‌تواند مقدار ۰ یا ۱ داشته باشد، اما یک کیوبیت در حالت برهم نهی می‌تواند ۰، ۱ یا ترکیبی از این دو مقدار باشد. این ویژگی به رایانه‌های کوانتومی اجازه می‌دهد پردازش اطلاعات را به صورت موازی انجام دهند.

اصل درهم‌تنیدگی(Entanglement)

درهم‌تنیدگی یک پدیده کوانتومی است که در آن دو یا چند ذره به‌گونه‌ای به یکدیگر وابسته می‌شوند که صرف نظر از فاصله بین آن‌ها، تغییر در وضعیت یک ذره بلافاصله وضعیت ذره دیگر را تحت تأثیر قرار می‌دهد. این ارتباط غیرمحلی یکی از مفاهیم اسرارآمیز و مهم در مکانیک کوانتومی محسوب می‌شود.

به‌عنوان مثال، یک جفت کیوبیت می‌توانند در یک حالت درهم‌تنیده مانند حالت بل (Bell State) قرار داشته باشند:

$$|\Phi\rangle = \frac{۱}{\sqrt{۲}}(|۰۰\rangle + |۱۱\rangle)$$

این حالت نشان می‌دهد که اگر یکی از کیوبیت‌ها در وضعیت $|۰\rangle$ اندازه‌گیری شود، کیوبیت دیگر نیز قطعاً در وضعیت $|۰\rangle$ خواهد بود و اگر یکی از آن‌ها در وضعیت $|۱\rangle$ قرار بگیرد، کیوبیت دیگر نیز بدون توجه به فاصله فیزیکی آن‌ها همان مقدار را خواهد داشت.

درهم‌تنیدگی نقش حیاتی در پروتکل‌های توزیع کلید کوانتومی (QKD) مانند پروتکل $E^{۹۱}$ ایفا می‌کند .در این روش، ذرات درهم‌تنیده برای تولید کلیدهای رمزنگاری امن استفاده می‌شوند. ارتباط قوی بین ذرات درهم‌تنیده تضمین می‌کند که هرگونه تلاش برای استراق سمع، سیستم را مختل کرده و حضور شنودگر را آشکار می‌کند.

کیوبیت‌ها(Quantum bits - Qubits)

کیوبیت‌ها واحدهای اساسی اطلاعات در محاسبات کوانتومی هستند و معادل بیت‌ها در محاسبات کلاسیک محسوب می‌شوند. با این‌حال، کیوبیت‌ها ویژگی‌های منحصربه‌فردی دارند که قابلیت‌های پیشرفته رایانه‌های کوانتومی را ممکن می‌سازند.

کیوبیت‌ها را می‌توان از طریق روش‌های مختلفی پیاده‌سازی کرد، از جمله:

یون‌های به دام افتاده: (Trapped Ions) یون‌هایی که در تله‌های الکترومغناطیسی محصور شده‌اند و با استفاده از لیزر، حالت‌های کوانتومی آن‌ها کنترل می‌شود. (Krutyanskiy, et al, ۲۰۲۳)

مدارهای ابررسانا : (Superconducting Circuits) مدارهای الکتریکی که در دماهای نزدیک به صفر مطلق عمل می‌کنند و در آن‌ها جریان الکتریکی بدون مقاومت حرکت می‌کند. کیوبیت ها در این روش بر اساس پیوندهای جوزفسون (Josephson Junctions) شکل می‌گیرند. (Vepsäläinen AP, et al, ۲۰۲۰)

نقاط کوانتومی : (Quantum Dots) ذرات نیمه‌رسانا که الکترون‌ها را در خود محبوس کرده و از حالت‌های اسپینی آن‌ها به‌عنوان کیوبیت استفاده می‌کنند. (Saraiva A, et al, ۲۰۲۲)

کیوبیت‌های فوتونی : (Photonic Qubits) کیوبیت‌هایی که بر اساس قطبش فوتون‌ها نمایش داده می‌شوند و به طور گسترده در ارتباطات کوانتومی استفاده می‌شوند. (Niemietz D, et al, ۲۰۲۱)

عملیات کوانتومی، یا همان گیت‌های کوانتومی(Quantum Gates) ، برای تغییر حالت کیوبیت‌ها به کار می‌روند. ترکیب این گیت ها باعث ایجاد مدارهای کوانتومی (Quantum Circuits) می‌شود که پایه اجرای الگوریتم‌های کوانتومی هستند. مدارهای کوانتومی با بهره‌گیری از برهم نهی و درهم‌تنیدگی، محاسبات پیچیده‌ای را انجام می‌دهند که در رایانه‌های کلاسیک دشوار یا غیرممکن است.

اندازه‌گیری در مکانیک کوانتومی

در فیزیک کوانتومی، اندازه‌گیری نقش بسیار مهمی دارد، زیرا باعث فروپاشی (Collapse) برهم نهی کیوبیت به یکی از دو حالت پایه $|۱\rangle$ یا $|۰\rangle$ می‌شود. نتیجه اندازه‌گیری احتمالی است و پس از اندازه‌گیری، تابع موج $|\psi\rangle$ به حالت اندازه‌گیری شده فرو می‌ریزد و برهم نهی از بین می‌رود. این فروپاشی غیرقابل بازگشت است و به طور اساسی با اندازه‌گیری در سیستم‌های کلاسیک تفاوت دارد.

پایه ای که در آن اندازه‌گیری انجام می‌شود، بر نتیجه تأثیر می‌گذارد. به عنوان مثال اندازه‌گیری یک کیوبیت در پایه محاسباتی $(|۰\rangle, |۱\rangle)$ احتمال متفاوتی را نسبت به اندازه‌گیری در پایه هادامارد$(|-\rangle, |+\rangle)$ ارائه می‌دهد. (Mercier de Lépinay L, et al, ۲۰۲۱)

قضیه عدم تکثیر (No-Cloning Theorem)

مفاهیم اساسی مکانیک کوانتومی که در رمزنگاری کوانتومی نقش دارند شامل برهم نهی، درهم تنیدگی و اصل عدم قطعیت هستند. یکی از نتایج مهم این اصول، قضیه عدم تکثیر است که بیان می‌کند نمی‌توان یک نسخه کاملاً مشابه از یک حالت کوانتومی ناشناخته را ایجاد کرد. طبق قضیه عدم تکثیر، هیچ روش واحدی (عملیات یکنواخت یا مدار کوانتومی) نمی‌تواند یک کیوبیت $|\psi\rangle$ را به دو کیوبیت $|\psi\rangle \otimes |\psi\rangle$ تبدیل کند بدون اینکه حالت اصلی را از بین ببرد. امنیت پروتکل‌های رمزنگاری کوانتومی به این قضیه وابسته است، زیرا نشان می‌دهد که شنودگران نمی‌توانند بدون ایجاد اختلال، کیوبیت‌ها را کپی کنند. این ویژگی لایه‌ای بنیادی از امنیت را در توزیع کلید کوانتومی (QKD) فراهم می‌کند. (Chen YC, et al, ۲۰۲۱)

درک این اصول مکانیک کوانتومی به ما کمک می‌کند تا بفهمیم چگونه این مفاهیم، قابلیت‌های منحصربه فرد محاسبات و رمزنگاری کوانتومی را ممکن می‌سازند. این اصول پایه و اساس توسعه الگوریتم‌های پیشرفته کوانتومی و پروتکل‌های ارتباطی امن را تشکیل می‌دهند و مسیر را برای دوران کوانتومی هموار می‌کنند.

مروری بر رمزنگاری کلاسیک

رمزنگاری کلاسیک داده‌ها را از طریق تبدیل آن‌ها به یک فرمت غیرقابل خواندن رمزگذاری می‌کند. این روش از مسائل سخت محاسباتی برای تضمین امنیت استفاده می‌کند، اما با ظهور محاسبات کوانتومی، این امنیت به چالش کشیده می‌شود. در رمزنگاری کلاسیک، امنیت اطلاعات معمولاً به دو روش اصلی تأمین می‌شود:

رمزنگاری متقارن

در رمزنگاری متقارن، یک کلید واحد هم برای رمزگذاری و هم برای رمزگشایی استفاده می‌شود، به همین دلیل به آن "رمزنگاری کلید خصوصی" نیز گفته می‌شود. این روش از نظر محاسباتی ساده و کارآمد است، اما چالش اصلی آن توزیع ایمن کلید است. در این روش

فرستنده، پیام را با استفاده از یک کلید مخفی از متن ساده (Plaintext) به متن رمز (Ciphertext) تبدیل می‌کند. گیرنده با استفاده از همان کلید مخفی، متن رمز را به متن اصلی بازمی‌گرداند. (Bellizia D, et al, ۲۰۲۰)

یکی از چالش‌های اصلی در رمزنگاری متقارن، توزیع ایمن کلید مخفی است. اگر این کلید در طول انتقال به دست مهاجم بیفتد، محرمانگی پیام به خطر می‌افتد. برای حل این مشکل، روش‌های تبادل کلید دستی و روش تبادل کلید دیفی- هلمن استفاده می شود.

رمزنگاری نامتقارن

در رمزنگاری نامتقارن از دو کلید استفاده می‌شود: یک کلید خصوصی برای رمزگشایی و یک کلید عمومی برای رمزگذاری. این روش مشکل اساسی توزیع کلید در رمزنگاری متقارن را برطرف می‌کند. در رمزنگاری نامتقارن، هر کاربر دارای یک کلید خصوصی و یک کلید عمومی است. کلید خصوصی محرمانه نگه داشته می‌شود، در حالی که کلید عمومی با دیگران به اشتراک گذاشته می‌شود. پیامی که با کلید عمومی یک کاربر رمزگذاری شده است، تنها با کلید خصوصی متناظر آن کاربر قابل رمزگشایی است، که این امر امنیت ارتباطات را تضمین می‌کند.

الگوریتم‌های رایج:

الگوریتم RSA (ریوست-شامیر-آدلمن):

RSA یکی از نخستین سیستم‌های رمزنگاری کلید عمومی است که همچنان برای انتقال امن داده‌ها به‌طور گسترده مورد استفاده قرار می‌گیرد. امنیت آن مبتنی بر سختی تجزیه اعداد مرکب بزرگ است. طول کلیدهای RSA معمولاً ۲۰۴۸ یا ۴۰۹۶ بیت است.

رمزنگاری منحنی بیضوی(ECC) :

ECC از ریاضیات منحنی‌های بیضوی بر روی میدان‌های متناهی برای تأمین امنیت استفاده می‌کند. این روش سطح امنیتی مشابه RSA را ارائه می‌دهد اما با طول کلیدهای کوتاه‌تر، که آن را کارآمدتر می‌سازد. ECC به‌طور فزاینده‌ای برای کاربردهایی که نیاز به امنیت بالا و منابع محاسباتی محدود دارند، مانند دستگاه‌های موبایل و اینترنت اشیا (IOT)، محبوب شده است.

چالش‌ها: هم رمزنگاری متقارن و هم نامتقارن با چالش‌های مربوط به توزیع و مدیریت کلید مواجه‌اند. در رمزنگاری متقارن، توزیع ایمن کلیدهای مخفی همچنان یک چالش اساسی است. روش‌هایی مانند تبادل کلید دیفی-هلمن به عنوان راه حل ارائه شده‌اند، اما این روش‌ها نیز آسیب‌پذیری‌های خاص خود را دارند و نیازمند تبادلات ایمن اولیه هستند.

در حالی که سیستم‌های نامتقارن بسیاری از مشکلات توزیع کلید را حل می‌کنند، چالش‌های جدیدی را نیز معرفی می‌کنند، از جمله نیاز به زیرساخت کلید عمومی (PKI) برای مدیریت و تأیید کلیدهای عمومی است. این زیرساخت‌ها باید به اندازه‌ای قوی و ایمن باشند که در برابر حملات مقاوم بمانند.

امنیت الگوریتم‌های رمزنگاری کلاسیک به دشواری محاسباتی مسائل ریاضی خاص بستگی دارد. امنیت الگوریتم‌های متقارن به طول کلید و پیچیدگی الگوریتم وابسته است؛ هرچند کلیدهای طولانی‌تر امنیت بیشتری فراهم می‌کنند، اما به توان پردازشی بیشتری نیز نیاز دارند.

امنیت الگوریتم‌های نامتقارن مانند RSA و ECC نیز به دشواری فاکتورگیری اعداد صحیح بزرگ یا محاسبه لگاریتم گسسته بستگی دارد. با این حال، پیشرفت‌های محاسبات کوانتومی این فرضیات را به چالش می‌کشند.

رمزنگاری کوانتومی

با بهره‌گیری از اصول مکانیک کوانتومی، الگوریتم‌های رمزنگاری کوانتومی روش‌های امنی را برای رمزنگاری ارائه می‌دهند که در برابر تهدیدات کلاسیک و کوانتومی مقاوم هستند. این الگوریتم‌ها برای تضمین محرمانگی، یکپارچگی و اصالت اطلاعات طراحی شده‌اند، حتی در برابر مهاجمانی که از توانایی‌های رایانش کوانتومی برخوردارند. این بخش مفاهیم اساسی و الگوریتم های برجسته رمزنگاری کوانتومی را بررسی می‌کند که پتانسیل رمزنگاری کوانتومی را به نمایش می‌گذارند. رمزنگاری کوانتومی از حالت‌های کوانتومی برای رمزگذاری اطلاعات استفاده می‌کند، که این امر به‌طور ذاتی آن را در برابر استراق سمع و حملات رایانش کوانتومی ایمن می‌سازد. این الگوریتم‌ها را می‌توان به دو دسته اصلی تقسیم کرد: رمزنگاری مبتنی بر توزیع کلید کوانتومی(QKD) و رمزنگاری کاملاً کوانتومی که در اینجا پروتکل های حالت اول را معرفی می کنیم:

پروتکل BB۸٤

پروتکل BB۸٤ اولین و مشهورترین پروتکل QKD است که توسط چارلز بنت و گیلز براسارد طراحی شده است. این پروتکل از حالت‌های قطبش فوتون‌ها برای تبادل ایمن کلیدهای رمزنگاری بین دو طرف استفاده می‌کند.

مراحل این پروتکل شامل موارد زیر است:

۱. تولید کلید: آلیس یک رشته تصادفی از بیت‌ها تولید می‌کند و هر بیت را در یکی از چهار حالت قطبش فوتون (افقی، عمودی، +۴۵ درجه، -۴۵ درجه) رمزگذاری می‌کند.

۲. انتقال فوتون‌ها: آلیس این فوتون‌های قطبیده را از طریق یک کانال کوانتومی برای باب ارسال می‌کند.

۳. اندازه‌گیری فوتون‌ها توسط باب: باب به‌صورت تصادفی یکی از دو مبنای مستطیلی (افقی/عمودی) یا مورب (+۴۵/-۴۵ درجه) را برای اندازه‌گیری فوتون‌های دریافتی انتخاب می‌کند.

٤. توافق بر روی مبناها: آلیس و باب از طریق یک کانال کلاسیک، مبناهای استفاده شده را مقایسه می‌کنند و بیت هایی که در آن‌ها مبناها یکسان است، حفظ می‌شوند.

٥. تصحیح خطا و تقویت امنیت: آن‌ها برای اصلاح خطاها و افزایش امنیت کلید، مراحل تصحیح خطا و تقویت حریم خصوصی را انجام می‌دهند.

کلید نهایی تولیدشده توسط این پروتکل در کنار یک الگوریتم رمزنگاری متقارن کلاسیک مانند AES برای رمزگذاری و رمزگشایی پیام ها استفاده می‌شود.

پروتکل E۹۱

پروتکل E۹۱ که توسط آرتور اکرت پیشنهاد شد، از درهم‌تنیدگی کوانتومی برای تبادل ایمن کلیدهای رمزنگاری استفاده می‌کند.

مراحل این پروتکل شامل موارد زیر است:

۱. تولید جفت فوتون‌های درهم‌تنیده: یک منبع، جفت‌های فوتونی درهم‌تنیده تولید کرده و یکی را به آلیس و دیگری را به باب ارسال می‌کند.

۲. اندازه‌گیری فوتون‌ها: آلیس و باب قطبش فوتون‌های خود را با استفاده از مبناهای تصادفی اندازه‌گیری می‌کنند.

۳. تحلیل همبستگی: آلیس و باب مبناهای اندازه‌گیری‌شان را از طریق یک کانال کلاسیک مقایسه کرده و بیت هایی را که مبناهای یکسانی دارند، حفظ می‌کنند.

٤. تولید کلید: بیت‌های همبسته‌ای که از مبناهای منطبق باقی مانده‌اند، کلید خام را تشکیل می‌دهند.

٥. تصحیح خطا و تقویت حریم خصوصی: با اعمال تصحیح خطا و تقویت امنیت، یک کلید نهایی امن تولید می‌شود.

این پروتکل از ویژگی‌های منحصربه‌فرد درهم‌تنیدگی کوانتومی برای شناسایی هرگونه استراق سمع بهره می‌برد.

پروتکل SARG۰٤

پروتکل SARG۰٤ توسط اندرو شیلدز، رابرت یانگ و پاول تاونسند مطرح شد که نسخه‌ای بهبود یافته از BB۸٤ است و از شش حالت کوانتومی به‌جای چهار حالت استفاده می‌کند.

مراحل کلیدی این پروتکل عبارتند از:

۱. آلیس فوتون‌ها را در یکی از شش حالت قطبشی مختلف آماده می‌کند.

۲. باب این فوتون‌ها را دریافت کرده و آن‌ها را در یکی از سه مبنای اندازه‌گیری تصادفی اندازه‌گیری می‌کند.

۳. آلیس و باب مبناهای اندازه‌گیری‌شان را مقایسه کرده و فقط بیت‌های مشترک را حفظ می‌کنند.

کلید نهایی پس از تصحیح خطا و تقویت حریم خصوصی به دست می‌آید.

SARG۰٤ با استفاده از تعداد بیشتری از حالات قطبشی، امنیت و نرخ تولید کلید را نسبت به BB۸٤ افزایش می‌دهد.

توزیع کلید کوانتومی Twin-Field (TF-QKD)

این پروتکل از دو کانال نوری مستقل برای توزیع کلید استفاده می‌کند. در آن آلیس یک زوج فوتونی متشکل از یک پالس ضعیف همدوس (WCP)و یک پالس قوی همدوس (SCP) آماده کرده و آن‌ها را از دو مسیر جداگانه برای باب ارسال می‌کند.

باب قطبش فوتون‌ها را اندازه‌گیری کرده و سپس مقایسه مبناهای اندازه‌گیری را انجام می‌دهد .با حفظ نتایج مشترک، کلید خام تولید می‌شود و در نهایت با تصحیح خطا و تقویت امنیت، کلید نهایی حاصل می‌شود .این پروتکل نسبت به سایر روش‌هایQKD ، نرخ تولید کلید بالاتر و مقاومت بیشتری در برابر تلفات کانال دارد. (Ze-Lin Meng, Hong Lai, ۲۰۲۳)

توزیع کلید کوانتومی(Coherent-One-Way (COW

این پروتکل برای توزیع کلید در فواصل طولانی و با سرعت بالا مناسب است. مراحل این پروتکل شامل موارد زیر است:

۱. آلیس یک سری پالس‌های همدوس ضعیف تولید می‌کند و آن‌ها را از طریق یک کانال کوانتومی ارسال می‌کند.

۲. باب فاز این پالس‌ها را اندازه‌گیری کرده و سپس داده‌های خود را با آلیس مقایسه می‌کند.

۳. پس از پردازش داده‌ها و اعمال تصحیح خطا، یک کلید نهایی امن تولید می‌شود.

این روش برای شبکه‌های ارتباطی با فواصل طولانی و نرخ تولید کلید بالا ایده‌آل است. (Emilien Lavie, et al, ۲۰۲۲)

چالش‌ها و مسیرهای آینده

با وجود مزایایQKD ، این فناوری با چالش‌های متعددی روبه‌رو است:

محدودیت فاصله و افت سیگنال: بهبود دامنه عملکرد QKD و کاهش تلفات کانال برای استقرار عملی آن ضروری است.

اثبات‌های امنیتی: ارائه اثبات‌های امنیتی دقیق و مقابله با حملات نوظهور از اهمیت بالایی برخوردار است.

یکپارچه سازی و مقیاس پذیری: ترکیب QKD با زیرساخت‌های مخابراتی موجود و توسعه آن برای شبکه‌های گسترده یک چالش کلیدی است.

پیشرفت‌های فناوری: پیشرفت در فناوری‌هایی مانند تقویت‌کننده‌های کوانتومی و حافظه‌های کوانتومی می‌تواند کارایی QKD را افزایش دهد.

کاربردهای رمزنگاری کوانتومی

رمزنگاری کوانتومی رویکردهای انقلابی جدیدی را برای تضمین ارتباطات ایمن معرفی می‌کند. حوزه‌های کاربردی فعلی این فناوری عبارتند از:

ارتباطات امن: توزیع کلید کوانتومی (QKD) تحول بزرگی در ارتباطات امن ایجاد کرده است، به ویژه در برنامه‌های دولتی و نظامی. این فناوری امکان تبادل کلیدهای رمزنگاری را با امنیت اثبات شده بر اساس اصول مکانیک کوانتومی فراهم می‌کند. سازمان‌های دولتی و نظامی از QKD برای محافظت از اطلاعات محرمانه و ایمن‌سازی کانال‌های ارتباطی در برابر استراق سمع و جاسوسی سایبری استفاده می‌کنند. توانایی شناسایی هرگونه تلاش برای شنود، یکپارچگی و محرمانگی داده‌های حساس را تضمین می‌کند و QKD را به ابزاری ضروری در امنیت ملی تبدیل می‌سازد.

کاربردهای تجاری: صنایعی مانند امور مالی، دفاعی و مخابراتی به طور فزاینده‌ای از رمزنگاری کوانتومی برای حفاظت از اطلاعات حساس استفاده می‌کنند. شبکه‌های ارتباطی امن کوانتومی از استراق سمع و نقض داده‌ها جلوگیری کرده و معاملات مالی و ارتباطات محرمانه را ایمن می‌سازند.

امنیت اینترنت اشیا: رمزنگاری کوانتومی آسیب‌پذیری‌های دستگاه‌های IOT را با ایجاد کانال‌های ارتباطی ایمن میان حسگرها، عملگرها و سیستم‌های کنترل مرکزی کاهش می‌دهد. الگوریتم‌ها و پروتکل‌های مقاوم در برابر کوانتوم در حال توسعه هستند تا تهدیدات احتمالی ناشی از رایانش کوانتومی را کاهش دهند.

شبکه‌های هوشمند : رمزنگاری کوانتومی امنیت زیرساخت‌های شبکه‌های هوشمند را افزایش داده و انتقال داده‌ها را در شبکه‌های توزیع انرژی ایمن می‌کند. محافظت در برابر تهدیدات سایبری و تضمین یکپارچگی سیگنال‌های اندازه‌گیری و کنترل برای حفظ پایداری و قابلیت اطمینان شبکه برق حیاتی است.

فضانوردی و ارتباطات ماهواره‌ای: رمزنگاری کوانتومی انتقال داده‌های امن را در شبکه‌های ماهواره‌ای تضمین می‌کند و از داده‌های تله متری، اطلاعات سنجش از دور و ارتباطات ماهواره‌ای با زمین محافظت می‌کند. سیستم‌های ناوبری و زمان‌بندی تقویت‌شده کوانتومی، دقت و قابلیت اطمینان کاربردهای هوافضا را افزایش می‌دهند.

مخابرات: شرکت‌های مخابراتی در حال ادغام QKD در زیرساخت‌های خود هستند تا امنیت شبکه‌هایشان را ارتقا دهند. با افزایش حجم داده‌های انتقال‌یافته در شبکه‌های مخابراتی، خطر حملات سایبری نیز افزایش می‌یابد. استفاده از QKD به تأمین امنیت کانال‌های انتقال داده در برابر استراق سمع و دسترسی غیرمجاز کمک می‌کند. (Kumar Sahu S, Mazumdar K, ۲۰۲٤)

چشم‌اندازهای آینده

در آینده، چندین مسیر تحقیقاتی و توسعه‌ای نویدبخش وجود دارد:

هم‌افزایی بین رمزنگاری کوانتومی و رایانش کوانتومی فرصت‌های بی‌سابقه‌ای ایجاد می‌کند. مطالعات آینده می‌توانند پیامدهای عملی رایانش کوانتومی را در گسترش توزیع کلید ایمن و فرآیندهای رمزگذاری بررسی کنند.

ایجاد شبکه‌های کوانتومی که قادر به انتقال اطلاعات کوانتومی در مسافت‌های طولانی باشند، یک حوزه مهم برای پیشرفت‌های آینده محسوب می‌شود. این امر شامل پیشرفت در فناوری تکرارگرهای کوانتومی و حافظه کوانتومی است.

تحقیقات آینده باید بر کشف روش‌های رمزنگاری جایگزین و انتقال به استانداردهای مقاوم در برابر کوانتوم متمرکز باشد.

نتیجه‌گیری

رمزنگاری کوانتومی، که بر اساس اصول بنیادین مکانیک کوانتومی بنا شده است، نمایانگر یک تغییر اساسی در امنیت شبکه‌های ارتباطی در برابر تهدیدات کلاسیک و کوانتومی می‌باشد. رایانش کوانتومی روش‌های کلاسیک رمزنگاری مانند RSA و ECC را به راحتی می شکند و این ضرورت توسعه راه حل‌های مقاوم در برابر کوانتوم هر چه بیشتر نمایان می کند. ما مفاهیم اساسی مکانیک کوانتومی، از جمله برهم‌نهی و درهم‌تنیدگی را بررسی کرده‌ایم و اینکه چگونه این مفاهیم در رمزنگاری کوانتومی مورد استفاده قرار می‌گیرند. این پروتکل‌ها تضمین می‌کنند که هر گونه تلاش برای استراق سمع، اختلالات قابل شناسایی ایجاد می‌کند و بنابراین یکپارچگی و محرمانگی ارتباط را حفظ می‌نماید.

منابع

Kumar Sahu S, Mazumdar K, State-of-the-art State-of-the-art analysis of quantum cryptography: applications and future prospects, Front. Phys., Sec. Quantum Engineering and Technology, Volume ۱۲ - ۲۰۲٤

Krutyanskiy V, Galli M, Krcmarsky V, Baier S, Fioretto DA, Pu Y, et al. Entanglement of trapped-ion qubits separated by ۲۳۰ meters. Phys Rev Lett (۲۰۲۳) ۱۳۰(٥):٠٥٠٨٠۳. doi:۱۰,۱۱۰۳/physrevlett.۱۳۰,٠٥٠٨٠۳

Vepsäläinen AP, Karamlou AH, Orrell JL, Dogra AS, Loer B, Vasconcelos F, et al. Impact of ionizing radiation on superconducting qubit coherence. Nature (۲۰۲۰) ٥٨٤(۷۸۲۲):٥٥۱–٦. doi:۱۰,۱۰۳۸/s٤۱٥۸٦-۰۲۰-۲٦۱۹-۸

Lim WH, Yang CH, Escott CC, Laucht A, Dzurak AS. Materials for silicon quantum dots and their impact on electron spin qubits. Adv Funct Mater (۲۰۲۲) ۳۲(۳):۲۱۰٥٤۸۸. doi:۱۰,۱۰۰۲/adfm.۲۰۲۱۰٥٤۸۸

Niemietz D, Farrera P, Langenfeld S, Rempe G. Nondestructive detection of photonic qubits. Nature (۲۰۲۱) ٥۹۱(۷۸٥۱):٥۷٠–٤. doi:۱۰,۱۰۳۸/s٤۱٥۸٦-۰۲۱-۰۳۲۹۰-z

Mercier de Lépinay L, Ockeloen-Korppi CF, Woolley MJ, Sillanpää MA. Quantum mechanics–free subsystem with mechanical oscillators. Science(۲۰۲۱) ۳۷۲(٦٥٤۲):٦۲٥–۹. doi:۱۰,۱۱۲٦/science.abf٥۳۸۹

Chen YC, Gong M, Xue P, Yuan HD, Zhang CJ. Quantum deleting and cloning in a pseudo-unitary system. Front Phys (۲۰۲۱) ۱٦:٥۳٦۰۱–۷. doi:۱۰,۱۰۰۷/s۱۱٤٦۷-۰۲۱-۱۰٦۳-z

Bellizia D, Bronchain O, Cassiers G, Grosso V, Guo C, Momin C, et al. Mode-level vs. implementation-level physical security in symmetric cryptography: a practical guide through the leakage-resistance jungle. In: Advances in cryptology–CRYPTO ۲۰۲۰: ٤۰th annual international cryptology conference, CRYPTO ۲۰۲۰, santa barbara, CA, USA, august ۱۷–۲۱, ۲۰۲۰, proceedings, Part I ٤۰. Springer International Publishing (۲۰۲۰). p. ۳٦۹–٤۰۰.

Ze-Lin Meng, Hong Lai, Twin-field quantum key distribution based on twisted photon, Author links open overlay panel, Physics Letters A Volume ۳۸٤, Issue ۱٦, ٤ June ۲۰۲۰, ۱۲٦۳۲۲

Emilien Lavie, Charles C.-W. Lim, Improved Coherent One-Way Quantum key Distribution for High-Loss Channels, PHYSICAL REVIEW APPLIED ۱۸, ۰٦٤۰٥۳ (۲۰۲۲)

Advantages and Challenges of Quantum Cryptography vs. Classical Cryptography

Esfandiyar Lashani
Department of Mathematics, Doroud Branch, Islamic Azad Univercity, Doroud Iran

Abstract

Quantum computing revolutionizes computational capabilities by leveraging the principles of quantum mechanics to process data in entirely new ways. In this article, we review the fundamental principles of quantum mechanics, including superposition and entanglement, which form the foundation of quantum computing and cryptography. We then discuss the principles and protocols of classical cryptography, highlighting its vulnerabilities against quantum computing. Furthermore, we examine quantum cryptographic algorithms, particularly Quantum Key Distribution (QKD) protocols, and explore their potential in ensuring secure communications in the quantum era.

Keywords: Quantum Cryptography, Quantum Key Distribution (QKD), Quantum Mechanics, Quantum Communication, Classical Cryptography