رمزنگاری کوانتومی

مجتبی خانی

چکیده

رمزنگاری کوانتومی روشی در مقابل رمزنگاری کلید عمومی است که برای تولید و توزیع کلید مورد استفاده قرار می‌گیرد. رمزنگاری کوانتومی، به علت پیچیدگی‌های ریاضیِ رمزنگاری کلید عمومی و کم اثر شدن این پیچیدگی‌ها در مقابل اقدامات هکرها مطرح شد. پروتکل‌های مختلف توزیع کلید بر اساس نوع تکنولوژی کوانتومی مورد استفاده به دو دسته پروتکل‌های مبتنی بر اصل عدم قطعیت Heisenberg و پروتکل‌های مبتنی بر همبستگی کوانتومی تقسیم می‌شوند که در این مقاله به بررسی کلی رمزنگاری کوانتومی و یکی از پروتکل‌های مبتنی بر اصل عدم قطعیت Heisenberg و یکی از پروتکل‌های مبتنی بر همبستگی کوانتومی[1] پرداخته خواهد شد.

مقدمه

به عمل پنهان کردن اطلاعات، رمزنگاری گفته می‌شود که هدف از آن انتقال اطلاعات به صورت امن است. یکی از راه‌های ایجاد امنیت در انتقال پیام استفاده از کلیدهای مشترک است. اگر از رمزنگاری سنتی بگذریم، رمزنگاری کنونی را می‌توان به دو دسته‌ی کلاسیک و نوین تقسیم‌بندی کرد. منظور از رمزنگاری کلاسیک، رمزنگاری منسوخ شده نیست. از روش‌های رمزنگاری کلاسیک می‌توان به روش‌هایی که در آن از الگوریتم‌هایی مانند DES استفاده می‌شود، نام برد. استفاده از این الگوریتم‌ها به علت وابستگی ریاضی کلیدها به یکدیگر قابل رمزگشایی است. محققان IT با موفقیت نشان داده‌اند که اصول فیزیک کوانتومی و رمزنگاری کوانتومی در شبکه‌های نوری قادر به محافظت بهتر از ارتباطات است.

رمزنگاری کوانتمی اولین بار توسط Stephen Wiesner در دهه 1970 مطرح شد. در سال 1991 Artur Ekert دانشجوی دوره دکتری در دانشگاه Oxford، روش دیگری برای رمزنگاری کوانتومی ارائه کرد. این نکته قابل ذکر است که رمزنگاری کوانتومی فقط برای تولید و توزیع کلید استفاده می‌شود و این روش برای رمزنگاری اطلاعات و انتقال آنها کاربردی ندارد. برای بررسی دقیق رمزنگاری کوانتومی و اینکه با اصطلاحات و مفاهیم اولیه آشنا شوید ابتدا مختصری به بررسی امواج الکترومغناطیسی و کوانتوم می‌پردازیم؛ سپس در رمزنگاری کوانتومی و ایجاد و توزیع کلید در این رمزنگاری بررسی عمیق‌تری خواهیم داشت.

امواج الکترومغناطیس

امواج الکترومغناطیسی، رده‌ای از امواج با مشخصات زیر است:

- امواج الکترومغناطیسی دارای ماهیت و سرعت یکسانی هستند؛
- در طیف امواج الکترومغناطیس شکافی وجود ندارد، یعنی هر فرکانس دلخواه را می‌توان تولید کرد.
- این امواج برای انتشار خود نیاز به محیط مادی ندارند.
- امواج الکترومغناطیسی جزو امواج عرضی هستند.

از جمله منابع زمینی امواج الکترومغناطیسی می‌توان به امواج دستگاه رله تلفن، چراغ‌های روشنایی و غیره اشاره کرد.

فوتون

فوتون به عنوان ذره بنیادینی است که واحد کوانتومی نور یا هر نوع تابش الکترومغناطیسی محسوب می‌شود. هر فوتون مقدار معینی انرژی، اندازه حرکت و اندازه حرکت زاویه‌ای یا اسپین[2] دارد.

قطبش[3] (پولاریزاسیون)

1- Quantum correlation
2 - spin
3 - Polarization

قطبش یکی از خاصیت‌های هر موج الکترومغناطیسی مثل نور است. قطبش نور نخستین بار توسط Huygens در سال 1960 میلادی کشف شد. از قطبش می‌توان استفاده‌های فراوانی مثلاً در زمینه رمزنگاری کوانتومی نمود. در ادامه بیشتر به این موضوع پرداخته خواهد شد.

اصول رمزنگاری کوانتومی

همانطور که گفته شد امواج الکترومغناطیسی می‌توانند قطبیده[4] شوند. قطبیدگی بنابر قرارداد با جهت میدان الکتریکی تعریف می‌شود که در آن یا جهت نوسانات میدان الکتریکی ثابت است یا به شکل معینی تغییر می‌کند. اگر در فرآیند قطبیدگی دقت کافی شود می‌توان فرآیند ایجاد فوتون‌ها را به گونه‌ای قرار داد که همیشه فوتون‌هایی با قطبش‌های عمودی و افقی ایجاد شوند.

یک قطبش‌گر یا پولارایزر[5] وسیله‌ای است که تنها اجازه عبور نور با جهت قطبیدگی خاص را می‌دهد. بنابراین اگر نور کاملا قطبیده نشده باشد تنها نیمی از آن از قطبش‌گر عبور می‌کند.

همانطور که گفته شد هر فوتون اندازه حرکت زاویه‌ای یا اسپین دارد. در این نظریه فوتون مستقل از اینکه چه قطبش اولیه‌ای داشته یا از قطبش‌گر رد می‌شود یا خیر، اما اگر رد شد با محور قطبش‌گر هم خط می‌شود.

اصل عدم قطعیت Heiseberg

نظریه کوانتومی بیشتر بر این موضوع استوار است که بعضی از کمیت‌هایی که در فیزیک کلاسیک پیوسته در نظر گرفته می‌شوند، در حقیقت کوانتیده یا گسسته هستند. به طور خلاصه تنها دو نوع توصیف در مورد یک ذره مادی یا یک فوتون وجود دارد: یکی توصیف موجی و دیگری توصیف ذره‌ای. بدین صورت که به یک ذره می‌توان هم خصوصیات مادی (مانند اندازه حرکت و مکان) هم خصوصیات موجی (مانند طول موج و بسامد) نسبت دهیم. تابش الکترومغناطیسی هم جنبه‌های موجی و هم جنبه‌های ذره‌ای را نشان می‌دهد. نظریه عدم قطعیت Heiseberg را می‌توان در دو حالت زیر بیان کرد:

1) اگر تابش الکترومغناطیسی را به زبان ذرات بیان کرده و مکان فوتون را در هر لحظه با دقت کامل تعیین کنیم در آن صورت عدم قطعیت در مکان و زمان صفر می‌شود اما از طرف دیگر عدم قطعیت در آنچه به موج فوتون نسبت داده می‌شود (مانند طول موج) بی‌نهایت بزرگ است.
2) از طرفی دیگر اگر بتوانیم آنچه به موج فوتون منسوب است را دقیق مشخص کنیم در این صورت عدم قطعیت در موج فوتون صفر شده و مکان فوتون نامشخص خواهد بود.

همبستگی کوانتومی

همبستگی کوانتومی یکی از پدیده‌های عجیب کوانتومی است که می‌تواند میان دو ذره که نسبت به هم فاصله دارند ارتباط ایجاد کند به شکلی که هر نوع تغییر در یکی از این ذره‌ها بلافاصله در ذره دیگر نیز تغییر به وجود می‌آورد، حتی اگر هر یک از این ذره‌ها در یک سوی جهان قرار داشته باشند.

رمزنگاری کوانتومی

در این بخش به قسمت اصلی بحث می‌رسیم. همانطور که قبلاً هم گفته شد رمزنگاری کوانتومی تنها برای تولید و توزیع کلید استفاده می‌شود. این کلید در مرحله‌های بعدی می‌تواند همراه با هر الگوریتم رمزنگاری برای تبدیل پیام به رمز یا بالعکس استفاده شود. رمزنگاری کوانتومی به هر دو طرف ارتباط این امکان را می‌دهد که کلید رمز خود را از طریق کانال خصوصی کاملاً امنی انتقال دهند.

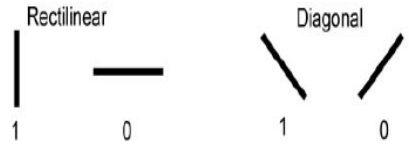
برای تولید و توزیع کلیدهای کوانتومی می‌توان از پروتکل‌های BB84، B92، SARG04، E91 و BBM92 استفاده کرد. در ادامه به بررسی پروتکل BB84 که براساس اصل عدم قطعیت Heisenberg و پروتکل E91 که مبتنی بر همبستگی کوانتومی هستند، می‌پردازیم.

پروتکل BB84 مبتنی بر اصل عدم قطعیت Heisenberg

4- Polarized
5 -polarizer

این پروتکل توسط Bennet و Brassard در سال 1984 ارائه شد که مبتنی بر اصل عدم قطعیت Heisenberg است. بنابر این اصل که در بخش‌های قبلی هم به آن اشاره شد، وقتی در اندازه‌گیری قطبش فوتون جهت اندازه‌گیری خاصی را انتخاب می‌کنیم این انتخاب تمام اندازه‌گیری‌های بعدی را تحت تاثیر قرار می‌دهد. به‌عنوان مثال بدون اینکه بدانیم فوتون دارای چه حالت اولیه‌ای است، اگر جهت عمودی را برای اندازه‌گیری قطبش یک فوتون انتخاب کنیم فوتون با قطبش عمودی از قطبش‌گر رد می‌شود و قطبش افقی اصلاً رد نمی‌شود. حال اگر اندازه‌گیری دیگری در زاویه 45 درجه از اندازه‌گیری اول انجام دهیم احتمال عبور فوتون از قطبش‌گر دوم دقیقاً $\frac{1}{2}$ است و اینگونه بیان می‌کنیم که قطبش‌گر اول اندازه‌گیری قطبش‌گر دوم را کاملاً تصادفی می‌کند. بنابراین در صورتی می‌توان جهت این قطبش را تشخیص داد که یک قطبش‌گر با صفر تا 90 درجه انتخاب گردد. زیرا یک قطبش‌گر 45 یا 135 درجه نیز یک خروجی با همین قطبش‌ها می‌دهد. به شکل زیر توجه کنید. همانطور که در شکل دیده می‌شود دو جفت پایه را می‌توان تعریف کرد:

- پایه قائم (⊞) با دو محور عمودی یا افقی (Rectilinear)
- پایه قطری (⊠) با دو محور 45 درجه یا 135(یا 45-) درجه (Diagonal)

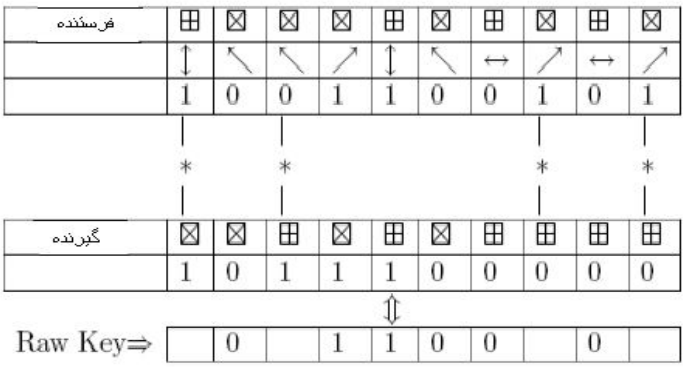


نحوه کد گذاری

به‌طور کلی با توجه به توضیحات داده شده، ارسال‌کننده با استفاده از منبع، یکی از چهار حالت قطبش بالا (صفر، 45، 90، 135) را برای گیرنده ارسال می‌کند. در طرف دیگر از گیرنده برای اندازه‌گیری قطبش استفاده می‌شود.

نمونه عبور فوتون‌ها از قطبش‌گر

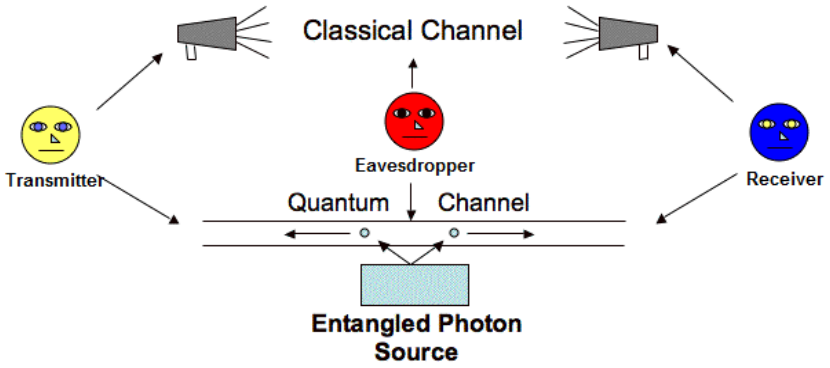
گیرنده نتیجه اندازه‌گیری را ذخیره می‌کند. در ادامه گیرنده با استفاده از کانال عمومی، نوع فیلترهای اندازه‌گیری خود (Rectilinear و Diagonal) را بیان می‌کند. در تمام این مراحل نتیجه اندازه‌گیری توسط گیرنده پنهان نگه داشته می‌شود. سپس فرستنده نیز به گیرنده درباره اینکه کدام فیلتر گیرنده درست بوده اطلاع می‌دهد. تنها در حالتی که فرستنده و گیرنده از نوع یکسانی برای اندازه‌گیری استفاده کرده باشند، می‌توان مطمئن بود که اندازه‌گیری درستی انجام گرفته است. با استفاده از اندازه‌گیری‌های مشترک بین فرستنده و گیرنده و در نهایت به بیت تبدیل شدن آنها، کلید ساخته می‌شود.



نحوه ایجاد و تبادل کلید در BB84

پروتکل E91 مبتنی بر همبستگی کوانتومی

در سال 1991، Artur Ekert پروتکل جدیدی برای توزیع کلید ارائه کرد. این پروتکل از یک کانال کوانتومی و منبع تولید تک‌فوتون استفاده می‌کند. عملکرد این پروتکل به این صورت است که دو زوج همبستگی از یکدیگر تفکیک شده و هر یک از فرستنده و گیرنده یکی از آن دو زوج را دریافت می‌کنند. با توجه به شکل، هر یک فیلتری برای اندازه‌گیری جزئی دریافتی خود استفاده می‌کنند. این پروتکل نیز مانند پروتکل BB84 در قسمت دوم عملکردی خود تبادلاتی در کانال کلاسیک انجام می‌دهد تا فیلترهای اندازه‌گیری هر دو طرف مشخص گردد. در نهایت به ازای هر اندازه‌گیری که فرستنده و گیرنده از فیلتر یکسانی استفاده می‌کنند باید انتظار نتیجه‌ای متضاد بر اساس قوانین همبستگی کوانتومی داشته باشند. این موضوع به این معناست که هر دو طرف تبادل، اندازه‌گیری‌های خود را مثل قبل تفسیر می‌کنند با این تفاوت که رشته بیتی هر یک از آن دو، مکمل باینری دیگری است. در این صورت اگر یکی از طرفین کلید خود را معکوس کند، یک کلید مخفی بین آن دو به اشتراک گذاشته شده است.



تولید کلید کوانتومی مبتنی بر entaglement

نتیجه‌گیری

رمزنگاری کوانتومی مانند همتای کلاسیک خود نیاز به یک کلید مشترک برای رمزگذاری و رمزگشایی پیام‌ها دارد. در این مقاله دیدی از رمزنگاری کوانتومی و پروتکل‌های تولید و توزیع کلید کوانتومی ایجاد شد. فقط با بودن یک کانال کلاسیک و یک کانال کوانتومی ناامن، این امکان بوجود خواهد آمد تا کلیدی مخفی برای ارسال پیام‌های رمزشده بین فرستنده و گیرنده به اشتراک گذاشته شود.

منابع

[1] Shon Harris, CISSP All in one, sixth edition, 2013
[2] C. H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175-179, 1984
[3] Quantum Cryptography : On the Security of theBB84 Key-Exchange Protocol, Thomas Baign`eres
[4] Quantum Key Distribution Protocols and Applications, Sheila Cobourne, 8th March 2011
[5] GILLES VAN ASSCHE, QUANTUM CRYPTOGRAPHY ANDSECRET-KEY DISTILLATION, 2006
[6]http://daneshnameh.roshd.ir/
[7] http://www.iranjoman.com/
[8] http://www.quantiki.org/wiki/BB84_and_Ekert91_protocols
[9] http://www.atomki.hu/atomki/TheorPhys/quantumcor.htm
[10] http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.html