مقدمه‌ای بر سیستم‌های رمزنگاری کوانتومی

داود مجیدی[1]، زین‌العابدین نوروزی[2]

تاریخ دریافت: ۹۰/۰۶/۰۴
تاریخ پذیرش: ۹۰/۰۶/۰۵

چکیده

در جنگ‌های نوین، یکی از مسایل بسیار مهم، حفظ اطلاعات محرمانه و سری است. هر طرف درگیر در جنگ که توانایی دست‌یابی به اطلاعات طرف مقابل را داشته باشد از برتری استراتژیک و تاکتیکی برخوردار خواهد شد و شانس پیروزی او در جنگ دو چندان می‌شود. در این خصوص اقدامات پدافند غیر عامل می‌تواند در کاهش آسیب‌ها نقش بسزایی ایفا نماید. رمزنگاری به عنوان یکی از اقدامات پدافند غیر عامل، به منظور حفاظت از اطلاعات امنیتی طبقه‌بندی شده، اطلاعات نظامی، صنعتی و تجاری حساس، اطلاعات دولتی و اطلاعات فردی بسیار ضروری است. تروریست‌ها و هکرهای رایانه‌ای و افراد سودجو می‌توانند اطلاعات و فعالیت‌های مهم سازمان‌ها، ارتش‌ها و دولت‌ها را از طریق هک‌کردن به‌دست آورده و با این کار سبب ایجاد مشکلاتی در سازمان‌ها شوند. بدین لحاظ و در طی زمان، روش‌های بسیاری برای رمزنگاری جهت امنیت و حفاظت از اطلاعات به وجود آمده است.

اصولاً از روش‌های رمزنگاری جهت حفاظت از اطلاعات انتقالی روی شبکه‌های باز و اطلاعات ذخیره شده بر روی رایانه‌ها استفاده می‌شود. سیستم‌های رمزنگاری کلاسیک به سبب ضعیف بودن الگوریتم رمزنگاری و یا ضعف سیستم مدیریت کلید، آسیب‌پذیر هستند. اگرچه نظریهٔ کوانتومی و نظریهٔ نوین محاسبات کم‌تر از پنجاه سال سابقه دارند، اما به‌تازگی دانشمندان توانسته‌اند پیامدهای یکی را در دیگری به تفصیل بررسی کنند. در این مقاله به اهمیت امنیت و انواع حملات رمزنگاری پرداخته و یکی از پیشرفته‌ترین روش‌های رمزنگاری یعنی رمزنگاری کوانتومی را معرفی می‌نماییم. اهمیت روش رمزنگاری کوانتومی در این است که نشان می‌دهد که ماشین تورینگ، مدلی کلی برای محاسبات عملی نیست.

کلیدواژه‌ها: محاسبات کوانتومی، رمزنگاری کوانتومی، امنیت اطلاعات، پدافند غیر عامل

۱- دانشگاه صنعتی مالک اشتر، دانشکده آمایش و پدافند غیر عامل، Email: d.majidi@lycos.com
۲- استادیار دانشگاه جامع امام حسین(ع)، دانشکده و پژوهشکده فاوا، گروه ریاضی و رمز

۱- مقدمه

امروزه حفاظت از اطلاعات، رکن اساسی و مهمی در تبادل پیام‌ها و مبادلات تجاری ایفا می‌نماید. امنیت اطلاعات، هنر و علمی است که به کاربران غیر مجاز اجازه دیدن، خواندن، دست‌کاری و از بین بردن اطلاعاتی را که برای دیگران ارسال می‌شود را نداده و صیانت از اطلاعات را به عهده می‌گیرد.

رمزنگاری عبارت است از به‌هم ریختگی اطلاعات محرمانه به‌طوری که برای کسی قابل فهم نباشد. فن و هنر رمزنگاری امکان مشاهده، مطالعه و تفسیر پیام‌های ارسالی توسط افراد غیر مجاز را سلب می‌نماید. از رمزنگاری به منظور حفاظت داده‌ها و اطلاعات در شبکه‌های عمومی نظیر اینترنت استفاده می‌گردد. در این رابطه از الگوریتم‌های پیشرفته ریاضی به منظور رمز نمودن پیام‌ها و ضمائم مربوطه استفاده می‌شود. رمزنگاری در دهه‌های اخیر شاهد پیشرفت‌های چشم‌گیری بوده است. در اثنای این پیشرفت‌ها، رمزنگاری به دانشی پیچیده تبدیل شده است که محصول کار مشترک متخصصین با آموزش‌های سطح بالایی در ریاضیات، مخابرات و رایانه است. یک جنبه تخصصی این علم را می‌توان در جنگ جهانی دوم یافت. زیرا شکستن رمز و خواندن پیام‌هایی که آلمانی‌ها با ماشین‌های انیگمای[1] خود رمزگذاری کرده بودند، بسیار نقش تعیین‌کننده‌ای در سرنوشت جنگ به نفع متفقین داشت. در سال ۱۹۷۰ رمزنگاری شاهد تحولی ویژه در قالب رمزنگاری با کلید عمومی شد. تا آن زمان طرف‌های خواهان تبادل پیام می‌بایست یک کلید محرمانه اختیار نموده و پیام مورد نظر با این کلید رمزگذاری و رمزگشایی می‌شد. اما خطر لو رفتن و گم شدن کلید بسیار زیاد بود. به این روش، رمزنگاری متقارن (کلید خصوصی) گفته می‌شود. در روش رمزنگاری نامتقارن (کلید عمومی) خطر فوق مرتفع گردید. اولین روش کلید عمومی روش RSA[2] است. در این روش از دو کلید استفاده می‌گردد. یک کلید رمزگذاری که عمومی بوده و دیگری کلید رمزگشایی که خصوصی می‌باشد. این روش بر مبنای مسئله سخت تجزیه اعداد است. در این‌جا عدد بزرگ $N = p \times q$ طوری در نظر گرفته می‌شود که در آن p و q اعداد اول بوده و تجزیه N یک مسئله سخت (تجزیه این عدد در کلاس NP قرار گیرد) باشد. در روند فوق N به منزله کلید عمومی و اعداد p و q کلید خصوصی هستند.

پرسش اساسی در این جا این است‌که آیا روشی مفید و سریع برای تجزیه اعداد وجود دارد؟ اگر چنین روشی وجود داشته باشد، آنگاه سیستم RSA شکسته خواهد شد. عکس این عبارت صادق نیست. با توجه به رشد روزافزون سرعت محاسبات، برای تضمین عدم تجزیه، می‌بایست عدد N بزرگ و بزرگ‌تر انتخاب گردد.

در سال ۱۹۹۸ پیتر شور[3] به سبب کارهایش بر روی رمزنگاری کوانتیک[4] موفق به دریافت جایزه نوانلینا[5] گردید. طرح سوال این‌گونه بود: آیا امکان ساخت رایانه بر مبنای نظریه مکانیک کوانتوم وجود دارد؛ یعنی رایانه‌ای که کارش بر مبنای قوانین فیزیک کوانتومی باشد؟ زیرا چنین رایانه‌ای قادر به تجزیه اعداد و هم‌چنین حل مسایل سخت دیگر خواهد شد. در صورت تحقق چنین ایده‌ای و به‌کارگیری آن، آنگاه می‌بایست پرونده رمزنگاری متقارن و نامتقارن را برای همیشه بست.

۲- امنیت در سیستم‌های رمزنگاری

در تحلیل یک سیستم رمزنگاری با توجه به نوع امنیت و اطلاعات موجود، تکنیک‌های متفاوتی وجود دارد. در ادامه به انواع حملات و امنیت اشاره می‌کنیم.

۲-۱- انواع حملات

با توجه به میزان و نوع اطلاعاتی که در دست دشمن قرار دارد، چهار نوع حمله وجود دارد که عبارتند از:

۲-۱-۱- حمله متن رمزی[6]: در این نوع حمله، اطلاعات موجود در دست دشمن فقط متن رمزی است و او هیچ‌گونه اطلاعات اضافه‌ای غیر از متن رمزی ندارد.

۲-۱-۲- حمله متن شناخته شده اصلی[7]: در این نوع حمله، دشمن علاوه بر متن رمزی، دنباله‌ای از متن اصلی و متناظر آن، متن رمزی را در دست دارد.

۲-۱-۳- حمله متن اصلی انتخابی[8]: در این نوع حمله، دشمن علاوه بر متن رمزی، قادر است قسمتی از متن اصلی را به دلخواه انتخاب نموده و متناظر آن متن رمزی را به‌دست آورد.

1- Enigma
2- Rivest-Shamir-Adleman

3- Peter Shor
4- Cryptographie quantique
5- Nevanlinna
6- Ciphertext only attack
7- Known plaintext attack
8- Chosen plaintext attack

۲-۱-۴- حمله متن رمـزی انتخـابی[1]: در ایـن نـوع حملـه، دشمن علاوه بر متن رمزی، قادر است قسمتی از متن رمـزی را به‌دلخواه انتخاب نمـوده و متنـاظر آن مـتن اصـلی را مـشاهده نماید.

۲-۲- انواع امنیت

با توجه به نوع مقاومتی که از یک سیستم رمزنگـاری در مقابـل انواع حملات داریم، امکان دسته‌بنـدی امنیـت بـه‌صـورت زیـر وجود دارد:

امنیت محاسـباتی[2]: گـوییم یـک سیـستم رمزنگـاری دارای امنیت محاسباتی است هرگاه بهترین الگـوریتم بـرای شکـستن این سیستم نیاز به N عمل‌گـر داشـته باشـد کـه N عـددی بسیار بزرگ است. در اینجا نوع حمله، جـستجوی کامـل کلیـد بوده و محاسبه N عمل‌گر فوق در کلاس NP قرار می‌گیرد.

امنیت قابل اثبات[3]: در بسیاری از مواقع امکان بررسی امنیـت یک سیستم به‌صورت مستقیم وجود ندارد؛ ولی می‌توان امنیـت این سیستم رمزنگاری را بـه امنیـت یـک سیـستمی (کـه دیـد عمومی بر این باور است که این سیستم امن است) کـاهش داد. به‌عنوان نمونه امنیت سیستم رمز RSA را می‌تـوان بـه امنیـت تجزیه اعداد کاهش داد. زیرا دید عمومی بر این بـاور اسـت کـه تجزیه اعداد یک مسئله سخت است. بنابراین اگر تجزیـه اعـداد شکسته شود، آنگاه سیستم رمـز RSA شکـسته مـی‌شـود. لـذا امنیت رمز RSA به امنیت تجزیه اعداد کاهش می‌یابد. بـا ایـن توجه که عکس مطلب فوق صادق نیست.

امنیت غیرمشروط[4]: گـوییم یـک سیـستم رمزنگـاری دارای امنیت غیرمشروط است هرگاه دشمن بـا هـر تـوان محاسـباتی نامحدود قادر به شکستن این سیستم نباشـد. بـه‌عنـوان نمونـه می‌توان رمز یک بار مصرف (OTP) را نام برد.

۳- رمزنگاری کوانتومی

آغاز نظریهٔ کوانتـومی بـه سـبب اشـکالاتی کـه در پـیش‌بینـی جذب و نشر تابش الکترومغناطیسی از یک جـسم سـیاه پـیش آمده بود، باز می‌گردد. در اواخر قرن نوزدهم، فیزیـک‌دانـان بـه این نکته پی برده بودند که از نظر تجربی، تغییـر شـدت تـابش الکترومغناطیسی از یک جسم سیاه، بـر حـسب طـول مـوج بـا انتظارات تئوریک فیزیک کلاسیک توافق ندارد. مـاکس پلانـک دانشمند آلمانی در سال ۱۹۰۰ میلادی نـشان داد کـه بـازبینی مفاهیم کلاسیکی به کمک مفهـوم کـوانتش انـرژی، منجـر بـه برقراری توافق بین آزمایش و نظریه می‌شود. این نظریه، دنیـای فیزیک و یا به تعبیر بهتـر درک انـسان از طبیعـت را دگرگـون کرد. به بیان دیگر پلانک ثابت کرد که انرژی الکترومغناطیـسی پیوسته نبوده بلکه به‌صورت گسسته و به شکل ذراتی موسوم به فوتون منتقل می‌شود. پلانک فرمول زیر را در ارتباط بـا انـرژی فوتون‌ها ارایه داد:

$$E = nh\upsilon = nhc/\lambda$$

که در فرمول فـوق $h = 6.626\times10^{-34}\ \ J.s$ ثابـت پلانـک، υ فـرکانس موج الکتـرومغناطیس، c سرعت نـور، λ طـول مـوج و $n = 1,2,3,...$ می‌باشد.

امروزه از نظریه کوانتوم به‌صورت گسترده‌ای در فناوری استفاده می‌گردد و از دستاوردهای این نظریه می‌تـوان از ترانزیـستورها، تصویر بردارهای دیجیتالی، دستگاه NMR، لیزرها، سنـسورهای حالت جامد، میکروسـکوپ الکترونـی و غیـره نـام بـرد. یکـی از کاربردهای بـسیار مهـم مکانیـک کوانتـوم در انتقـال اطلاعـات به‌صورت محرمانه و غیرقابل دسترس می‌باشد. با استفاده از این نظریه می‌توان ساختارهایی را برای رمزنگاری نوشـت کـه دارای دو ویژگی زیر باشند:

الف) امنیت بالا،

ب) امکان شناسایی شنود.

موضوعی که پیش از این در ساختارهای کلاسیک دست‌یابی به آن میسر نبود. رمزنگاری کوانتومی، توسط بنـت و براسـارد[5] در دهه هشتاد میلادی، بر پایهٔ اسـتفاده از فوتـون و ارسـال آن در یک کانال فیبر نوری تکامـل یافـت. ایـن روش از چنـان درجـه ایمنی بالایی برخوردار است کـه حتـی اگـر بخـش عمـده‌ای از اطلاعات مربوط به کلید رمز نیز مفقود شود، باز هم می‌توان آن را بدون نگرانی از خطر رمزگشایی، بازسازی کرد.

ویژگی سیستم‌های کوانتومی آن است که به محض آن که نفـر سومی بخواهد پیام‌هایی را که میـان مبـدأ و مقـصد رد و بـدل می‌شود، ردیابی کند و قفل رمز آن را بشکند. ارسال‌کننـدگان و دریافت‌کنندگان اصلی پیام از این دسـت‌کـاری آگـاهی یافتـه و

1- Chosen ciphertext attack
2- Computional security
3- Provable security
4- Uncomditional security

5- Bennet &, Brassard

می‌توانند رّد شنود را پیدا کنند. هر گونه تلاش برای شنود غیر قانونی از کانال کوانتومی منجر به تغییر کامل اطلاعات و آگاهی کاربران مجاز برای تغییر کلید محرمانه می‌شود.

در رمزنگاری کوانتومی یکی از مهم‌ترین مسائل توزیع، کلید کوانتومی است (شکل ۱). دو کاربر مجاز از طریق یک کانال کوانتومی به کلید محرمانه دست پیدا می‌کنند. امنیت کلید به وسیلهٔ اصل عدم قطعیت[1] تضمین می‌شود. کلید رمز به طور معمول عدد بزرگی است که ارقام آن با استفاده از خواص مختلف فیزیکی نظیر شدت میدان مغناطیسی، دامنه موج، قطبش فوتون و تکانه[2] تکمیل می‌شود. نکته مهم در مورد سیستم رمزنگاری کوانتومی آن است که فرستنده و گیرنده اصلی پیام، نه تنها از حملات احتمالی رمزشکنان آگاهی می‌یابند، بلکه در عین حال قادر خواهند بود حتی در صورت از دست رفتن برخی از پیام‌هایی که برای تکمیل کلید رمز مبادله می‌کنند، این کلید را به طور کامل بازسازی نمایند.

شکل ۱- نخستین سیستم توزیع کلید کوانتومی BB84 تجاری در جهان[۱۳].

۳-۱- تاریخچه رمزنگاری کوانتومی

نقطهٔ شروع تحول در این زمینه توسط آلن تورینگ[3] ریاضیدان انگلیسی در سال ۱۹۳۶ میلادی بود. او طی مقاله‌ای مدلی برای محاسبات ارایه داد که هم اکنون به‌عنوان ماشین تورینگ مشهور است. وی نشان داد که یک ماشین تورینگ جهانی وجود دارد که همهٔ ماشین‌های تورینگ را می‌توان با آن شبیه‌سازی کرد. در واقع اساس همهٔ رایانه‌های موجود همین ماشین تورینگ است. بعداز گذشت مدت نه چندان زیادی از مقالهٔ تورینگ، نخستین رایانه ساخته شد. جان فون نویمان[4] ریاضیدان نابغه مجار، تئوریی ساده ارایه داد که چگونه می‌توان اجزاء لازم یک رایانه را در کنار هم قرار داد تا توانایی‌های یک ماشین جهانی تورینگ را داشته باشد. این الگوریتم پایه تمامی رایانه‌های امروزی است. در سال ۱۹۴۷ میلادی با کشف ترانزیستور توسط جان باردین[5]، والتر برادین[6] و ویلیام شاکلی[7] سخت افزار جهش بزرگی کرد. پیشرفت و رشد سخت‌افزار هنوز هم با سرعت ادامه دارد. در سال ۱۹۶۵میلادی گوردن مور[8] قانونی تجربی - مشهور به قانون مور- در ارتباط با رشد قدرت رایانه‌ها ارایه نمود:

قدرت رایانه‌ها هر ۱۸ ماه، دوبرابر می‌شود.

این قانون کم و بیش تا کنون برقرار بوده و به عقیدهٔ بسیاری اگر این روند ادامه یابد، تا سال ۲۰۲۰ میلادی به ابعاد اتمی خواهیم رسید. در واقع یکی از دلایل اصلی برای تلاش در کنترل سیستم‌های کوانتومی در ابعاد بسیار کوچک همین موضوع است.

در اوایل سال ۱۹۸۰ میلادی رابرت سولوی[9] و والکر استراسن[10] نشان دادند که با استفاده از الگوریتم تصادفی، می‌توان اول بودن یک عدد را مشخص نمود. این امتحان از تصادفی بودن[11] به‌عنوان جزء ضروری الگوریتم، بهره می‌جست.

یکی دیگر از اندیشمندانی که سهم مهمی در گسترش محاسبات کوانتومی دارد دویچ[12] است. وی به دنبال نظریه فیزیکی بود که رهیافتی برای تز چرچ تورینگ ارایه دهد. از آن‌جا که قوانین فیزیکی در نهایت کوانتومی هستند، دویچ به این فرض رهنمون شد که اجزاء محاسباتی نیز می‌بایست بر پایهٔ مکانیک کوانتومی عمل کنند[۱].

در طول یک دهه بعد این ایده توسط دانشمندان بسیاری دنبال شد. پیتر شور در سال ۱۹۹۴ میلادی سبب یک نقطه عطف در این رابطه گشت[۲]. کارهای شور نشان‌دهندهٔ برتری رایانه‌های کوانتومی بر رایانه‌های کلاسیک است، و در واقع پاسخ به سئوال اساسی بود که پیش از این بیان گردید. جنبهٔ دیگری از توانمندی بالای رایانه‌های کوانتومی در سال ۱۹۹۵ میلادی نمایان شد، هنگامی که گرور[13] نشان داد که مسئلهٔ جستجو در

1- Uncertainty principle
2- momentum
3- Alan Turing
4- Joha Von Neuman

5- John Bardeen
6- Walter Brattain
7- William Shockley
8- Gordan Moore
9- Robert Solovay
10- Volker Strassen
11- randomness
12- Deutch
13- Lov Grover

یک فضای درهم ریخته را می‌توان با سرعت بالایی در رایانه‌های کوانتومی حل کرد[۳]. البته این افزایش سرعت از مرتبهٔ افزایش سرعت در الگوریتم شور نبود. اما از این نقطه نظر که جستجو می‌تواند به‌عنوان یک زیر روال[۱] در بسیاری از مسایل مهم به کار رود، از اهمیت بسزایی برخوردار است.

ریچارد فاینمن[۲] فیزیک‌دان برجسته و برنده جایزه نوبل فیزیک، در سال ۱۹۸۲ میلادی ایدهٔ زیبای ساخت رایانه‌هایی بر پایهٔ اصول مکانیک کوانتومی را مطرح نمود [۴]. از آن هنگام گروه‌های تحقیقاتی بسیاری در سراسر جهان مشغول بررسی این ایده هستند.

موضوع دیگری که در محاسبات کوانتومی از اهمیت بسیاری برخوردار می‌باشد، مسئلهٔ تصحیح خطای کوانتومی است. در حال حاضر تکنیک‌های تصحیح خطای کوانتومی نیز ابداع شده است،که به رایانه‌های کوانتومی اجازه محاسبهٔ کارآمد را در یک کانال کوانتومی می‌دهد. در سال ۱۹۹۲ میلادی چارلز بنت[۳] و استفان وایسنر[۴] توضیح دادند که چگونه می‌توان دو بیت کلاسیکی اطلاعات را تنها با انتقال یک بیت کوانتومی منتقل کرد. به این نتایج لقب کدگذاری چگال داده‌اند[۵].

از موفقیت‌های بزرگ محاسبات کوانتومی، رمزنگاری است. به این مفهوم که در انتقال پیام، اطلاعات به سرقت نرود و در صورت شنود، بتوان به وجود شخص یا اشخاص شنودگر پی برد. مسئلهٔ اصلی در رمزنگاری انتقال کلید است. موضوع رمزنگاری کوانتومی با ارایه مقاله‌ای در سال ۱۹۶۰ میلادی توسط استفان وایسنر آغاز شد. اما این مقاله حدود پانزده سال بعد، در سال ۱۹۸۳ میلادی به چاپ رسید و در این مدتِ زمانی نیز مورد توجه قرار نگرفت[۶]. در این مقاله وایسنر این ایده را مطرح ساخت که چگونه می‌توان از فیزیک کوانتومی برای تولید اسکناس‌های غیر قابل جعل، حفاظت از صورت حساب‌های بانکی، جلوگیری از تقلب و هم چنین پیاده سازی یک کانال مالتی پلکس[۵] (کانال مرکبی که دو یا چند پیام را منتقل می‌نماید و خواندن یکی از آن‌ها سبب تخریب دیگری می‌شود) استفاده نمود. مفهومی بسیار شبیه به مقوله انتقال فراموش‌کار[۶] که ده سال بعد توسط رابین[۷] مطرح گردید.

بخش عمده‌ای از دهه اول رمزنگاری کوانتومی شامل مقاله چاپ نشده وایسنر می‌شود. البته بنت[۸] از عقاید وایسنر آگاه بود. با وجود این، رمزنگاری کوانتومی هنگامی در کانون توجه قرار گرفت که در سال ۱۹۷۹ میلادی بنت با ژیل براسار[۹] از دانشگاه مونترال همکاری مشترکی را آغاز نمودند و حدود ۵ سال بعد روش توزیع کلید کوانتوم (QKD) توسط آن دو ارایه گردید و در اواخر دهه هشتاد میلادی آن را کاربردی ساختند[۷]. توزیع کلید کوانتومی بهترین مورد استفاده از مکانیک کوانتوم در رمزنگاری است. در این روش از چهار حالت نامتعامد کوانتومی برای انتقال کلید استفاده می‌گردد. در واقع هدف از رمزنگاری کوانتومی این است که با استفاده از اصل عدم قطعیت فیزیک کوانتوم، یک ساختار جدید برای رمزنگاری ارایه شود. در رمزنگاری کوانتومی یک کانال مطمئن و امن ایجاد می‌شود و اگر شنودی در طول کانال انجام شود هم فرستنده و هم گیرنده متوجه آن خواهند شد.

تا اوایل دهه ۹۰ میلادی تعداد کمی از افراد در پژوهش‌های مربوط به رمزنگاری کوانتومی شرکت داشتند. اوج دوران توجه به رمزنگاری کوانتومی وقتی آغاز گردید که اکرت[۱۰] نخستین سمینار بین‌المللی را در مورد رمزنگاری کوانتومی در سال ۱۹۹۴ میلادی در انگلستان ارایه داد[۸].

وقتی اطلاعات توسط وضعیت‌های نامتعامد کوانتومی[۱۱] کد می‌شوند (مثلاً از فوتون‌های قطبیده برای ارسال اطلاعات رقمی استفاده شود) هر تلاشی برای شنود غیر قانونی این اطلاعات کد شده صرف‌نظر از این که به مقصود نخواهد رسید، منجر به تغییر این اطلاعات نیز می‌گردد که این تغییر برگشت‌ناپذیر است (یعنی دشمن نمی‌تواند ارتباط را قطع کرده و سپس اقدام به ارسال مجدد پیام‌های انحرافی نماید). این تغییر سبب بوجود آمدن نرخ خطای بیت بالا در ارسال اطلاعات شده و افرادی که مجاز به استفاده از این اطلاعات هستند از تلاش برای شنود غیرقانونی آگاه خواهند شد.

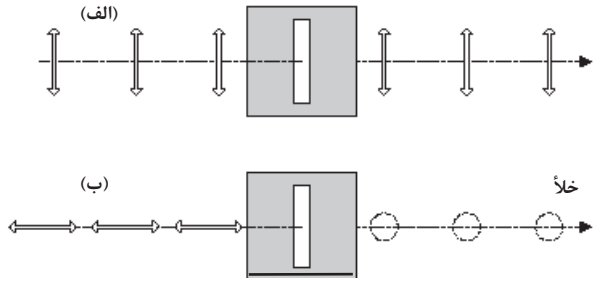
همان‌گونه که پیش‌تر نیز اشاره شد در سال ۱۹۸۴ میلادی بنت و براسار[۱۲] نخستین پروتکل کوانتومی را برای ایجاد توزیعی از کلید بین دو شخص ارایه دادند[۹]. در این پروتکل از دو پایهٔ مکمل برای کد کردن بیت‌ها استفاده می‌شود. در سال‌های بعد

1- subroutine
2- Richard Feynman
3- Charles Bennett
4- Stephen Wiesner
5- Multiplexing Channel
6- Oblivious Transfer
7- Rabin
8- Bennet
9- Brassard
10- Ekert
11- Non-orthogonal Quantum States
12- Gilles Brassard

با استفاده از حالت‌های درهم تنیده، پروتکل‌های دیگری نظیر پروتکل ZLG و پروتکل تعویض درهم تنیدگی ارایه گردید.
رایانه‌های کلاسیکی از بیت (یک سلول دو حالته) به‌عنوان حافظهٔ اطلاعاتی استفاده می‌نمایند. مبنای محاسبات کلاسیکی، دروازه‌های دوحالته‌اند. در رایانه‌های کوانتومی، کیوبیت‌ها همان نقش بیت‌ها را ایفا می‌کنند. در حال حاضر مشکل اساسی در محاسبات کوانتومی محدودیتی است که از لحاظ تجربی روی کنترل تعداد کیوبیت‌ها وجود دارد. به همین دلیل در سال‌های اخیر به مطالعهٔ سیستم‌های d- حالته توجه بسیاری شده است. استفاده از سیستم‌های d- حالته (کیودیت) از آن جهت که برای ایجاد یک بعد دلخواه، احتیاج به کنترل تعداد کمتری کیودیت در مقایسهٔ با کوبیت داریم، با اهمیت است. هم‌چنین با استفاده از سیستم‌های d- حالته، احتمال بدست آوردن اطلاعات توسط شنودگر کاهش می‌یابد.

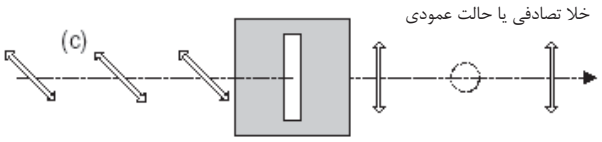
۳-۲- نظریه رمزنگاری کوانتومی

قطبش، یک خاصیت مهم امواج نوری است. می‌گوییم یک موج که در جهت محور x منتشر می‌شود دارای قطبش عمودی (V) است. اگر میدان الکتریکی آن هم‌راستا با محور z باشد، و یک موج دارای قطبش افقی (H) است اگر میدان الکتریکی آن هم‌راستا با محور y باشد. این یک خصوصیت قابل توجه نور است که هر وضعیت قطبش دیگر را می‌توان به دو مؤلفه عمودی و افقی (با یک فاز نسبی خاص) تجزیه کرد. بدیهی است که قطبش اولیه از جمع خطی این دو مؤلفه بدست می‌آید. در حالی که نور دارای قطبش خطی است، اندازه هر کدام از این مؤلفه‌ها برابر با تصویر قطبش اولیه در راستای محورهای قطبش V و H می‌باشد. مثلاً اگر نور قطبش خطی در جهت ۴۵+ درجه در صفحه yz باشد، می‌توان این قطبش را به دو مؤلفه هم‌اندازه و هم‌فاز V و H تجزیه نمود. ولی اگر نور در جهت ۴۵- درجه قطبیده شده باشد مولفه‌های آن هم‌اندازه و در فاز مخالف هم هستند. به قطبش‌های V و H (و هم‌چنین ۴۵+ و ۴۵- درجه) قطبش‌های متعامد می‌گوییم. اگر بخواهیم یک موج نور دارای قطبش خاصی شود باید آن را از یک محیط قطبی‌کننده عبور دهیم. بدیهی است که محور قطبش‌گر این محیط باید در آن جهت خاص قرار داشته باشد. وقتی این نور قطبیده را از یک قطبش‌گر دیگر عبور دهیم فقط مؤلفه هم‌راستا با محور قطبش‌گر دوم در خروجی ظاهر می‌شود (مؤلفه عمود بر محور قطبش‌گر دوم جذب می‌شود). به طور مثال، اگر یک موج نور با قطبش عمودی از یک قطبش‌گر ۴۵+ درجه عبور داده شود، نور خروجی دارای قطبش ۴۵+ درجه بوده و اندازه‌اش به مقدار $1/\sqrt{2}$ کاهش خواهد یافت. هم چنین شدت نور خروجی، نصف شدت نور ورودی است. به همین تر تیب اگر یک نور V وارد یک قطبش‌گرH شود در خروجی نوری نخواهیم داشت. پاراگراف قبل بعضی از ویژگی‌های کلاسیک نور قطبیده را بیان می‌کند ولی در رمزنگاری کوانتومی ما با نوری که شدت آن بسیار پایین است سر و کار داریم و در اینجا باید از مکانیک کوانتوم بهره گرفت. در فیزیک کوانتوم نور می‌تواند هم به‌صورت موجی و هم ذره‌ای منتشر گردد. به‌عنوان مثال رفتار نور در آزمایش دو شکافی یانگ، موجی و در اثر فتو الکتریک، ذره‌ای است. هنگامی که نور رفتار ذره‌ای از خود نشان دهد مسایل جالبی مطرح می‌گردد. به‌عنوان مثال اگر یک فوتون قطبیده با یک محیط قطبش‌گر مواجه شود چه رفتاری از خود بروز می‌دهد؟ می‌دانیم که یک فوتون V از یک قطبش‌گر عمودی عبور می‌کند ولی توسط یک قطبش‌گر افقی جذب می‌شود و به همین ترتیب یک فوتون H از یک قطبش‌گر افقی عبور می‌کند ولی توسط یک قطبش‌گر عمودی جذب می‌شود. شکل (۲) را مشاهده کنید[۱۰]. اما اگر قطبش فوتون و محیط قطبش‌گر نامتعامد باشند چه خواهد شد؟ اینجاست که ویژگی غیرعادی مکانیک کوانتوم آشکار می‌گردد. در نظر بگیرید که یک فوتون با قطبش ۴۵+ درجه با یک محیط قطبش‌گر عمودی مواجه شود، از دیدگاه کلاسیک باید در خروجی یک " نیم فوتون " ظاهر گردد، ولی می‌دانیم که چنین چیزی امکان ندارد.



شکل ۲- عبور یک تک فوتون V از قطبش‌گر عمودی و جذب فوتون H با عبور از همان قطبش‌گر[۱۰].

در نتیجه مکانیک کوانتوم پیش‌بینی می‌کند که در هر بار آزمایش، به احتمال ۵۰٪ فوتون جذب و به احتمال ۵۰٪ فوتونی با قطبش عمودی در خروجی ظاهر می‌شود. این موضوع در شکل (۳) نشان داده شده است[۱۱].



شکل ۳- عبوری تک فوتون با قطبش ۴۵ درجه از یک قطبش‌گر عمودی[۱۰].

یک ویژگی غیرعادی دیگر مکانیک کوانتوم این است که اگر یک فوتون با قطبش ۴۵+ درجه را از یک قطبش‌گر عمودی عبور دهیم (به بیان دیگر اگر فوتون با قطبش ۴۵+ درجه را توسط یک قطبش‌گر عمودی اندازه‌گیری کنیم) تمام خاصیت ۴۵+ درجه بودنش را از دست می‌دهد و به‌طور کامل تبدیل به یک فوتون با قطبش عمودی می‌گردد. حال اگر این فوتون خارج شده از محیط اول را از یک قطبش‌گر دیگر عبور دهیم که دارای محور قطبش ۴۵+ درجه باشد به احتمال ۵۰٪ عبور خواهد کرد و به احتمال ۵۰٪ جذب خواهد شد (بدون توجه به این امر که قبلاً دارای قطبش ۴۵+ درجه بوده است). در اصطلاح مکانیک کوانتوم گویند که قطبش‌گر عمودی تابع موج فوتون را فرو ریخته است[۱]. این تصادفی بودن خواص که به خاطر اندازه‌گیری‌های نامتعامد رخ می‌دهد، نتیجه اصل عدم قطعیت هایزنبرگ بوده و در رمزنگاری کوانتومی یک عامل مهم و اصلی در کشف شنودهای غیرمجاز می‌باشد. اصل عدم قطعیت هایزنبرگ بیان می‌کند که اندازه‌گیری یک ویژگی ذره بر سایر ویژگی‌های آن اثر می‌گذارد. لذا نمی‌توان تمام خصوصیات یک ذره را در یک لحظه اندازه‌گیری کرد؛ به‌عبارت دیگر نمی‌توان موقعیت و تکانه دقیق ذره را به‌طور هم‌زمان اندازه‌گیری نمود. اصل عدم قطعیت هایزنبرگ نتیجه‌ای از مشخصه موجی ذرات است. نمایش اعداد به‌وسیله دو حالت متعامد (دو حالت اسپین ۱/۲ یا دو حالت یک اتم در دو لایه انرژی) یک دستگاه کوانتومی دو حالته را ارایه می‌دهد. تبدیل و پردازش اعداد و اطلاعات کوانتومی از نوع تحولات کوانتومی است که تابع معادله شرودینگر است. تفاوت اصلی میان محاسبات کلاسیک و کوانتومی در اصل برهم‌نهی است. در فیزیک کلاسیک، N سلول حافظه دو حالته، با N بیت قابل توصیف هستند. اما در فیزیک کوانتومی، N سلول حافظهٔ دو حالته با 2^N عدد مختلط توصیف می‌شوند. کیوبیت یک سلول حافظه دو حالته و دو بعدی کوانتومی است. این عنوان در واقع به‌جای بیت در حوزه کلاسیک به کار می‌رود.

۳-۳- رایانه‌های کوانتومی

رایانه‌های کوانتومی رایانه‌هایی هستند که از خواص نامتعارف سیستم‌های کوانتومی بهره می‌گیرند و قادرند با انجام شمار بسیار زیادی از محاسبات به‌صورت هم‌زمان و در فاصله کوتاه، بسیاری از رمزهایی را که برای رایانه‌های کنونی عملاً غیرقابل شکستن است، به سادگی بشکنند. پژوهشگرانی که در حوزه رایانه‌های کوانتومی سرگرم تحقیق هستند از هم اکنون کار ساخت الگوریتم‌هایی را که قادر به انجام محاسبات متعدد در زمان بسیار کوتاه هستند، آغاز کرده‌اند. یکی از این نوع الگوریتم‌ها که شور[۲] نام دارد، سرعت تجزیه اعداد بسیار بزرگ را تا حد زیادی افزایش داده است. از این مضارب برای رمزشکنی استفاده می‌شود.

تولید الگوریتم‌های تازه‌ای که بتواند با خطر رایانه‌های کوانتومی مقابله کند، کار آسانی نیست و به‌علاوه هر الگوریتمی از این‌گونه، دارای حجمی بزرگ خواهد بود که اجرای آن را بر روی رایانه‌های متعارف دشوار و کند می‌کند.

۴-۳- مکانیسم عملکرد رایانه کوانتومی

یک رایانه کلاسیک، اطلاعات را در واحدهایی به نام بیت که به‌صورت ولتاژهای الکتریکی ضعیف یا قوی نمایش داده می‌شوند، ذخیره می‌کند؛ در صورتی‌که رایانه کوانتومی اطلاعات را بر مبنای ذرات بنیادی ذخیره می‌کند. به بیان ساده، یک الکترون در اتم هیدروژن ممکن است در دو سطح انرژی بالا یا پایین قرار داشته باشد، اما از لحاظ مکانیک کوانتوم، حالت یک الکترون تنها داشتن سطح انرژی بالا و یا پایین نمی‌باشد، بلکه حالت یک الکترون می‌تواند ترکیب وزنی (با یک ضریب پیچیده) از این دو حالت باشد. این پدیده، ابر موقعیت[۳] «0» و « 1» خوانده می‌شود. یک الکترون

1- Wave function collapse

2- shor

3- Super Position

به جای نمایش بیت در یک رایانه معمولی، می‌تواند نمایش‌گر یک کیوبیت یا بیت کوانتومی در یک رایانه کوانتومی باشد. حال اگر ورودی به یک رایانه کوانتومی یک کیوبیت باشد، اساساً رایانه در یک زمان دو حالت صفر و یک را به‌عنوان ورودی دریافت خواهد نمود. اگر ورودی N کیوبیت باشد، آنگاه این ورودی می‌تواند 2^N حالت ممکن را در یک لحظه داشته باشد. یک رایانه کوانتومی تمام 2^N حالت ممکن را در یک زمان اجرا خواهد کرد. لذا این توانایی منجر به افزایش‌نمایی قدرت رایانه کوانتومی نسبت به رایانه‌های کلاسیک می‌گردد. قدرت یک رایانه کوانتومی با تنها چند هزار کیوبیت، می‌تواند معادل توان یک رایانه معمولی باشد که حاوی تمام مولکول‌های جهان است!

یک رایانه کوانتومی علاوه بر فاکتورگیری دارای سرعت بالای جستجو در یک بانک اطلاعاتی است و می‌تواند سرعت شبیه‌سازی سیستم‌ها را به‌طور تصاعدی افزایش دهد. در مجموع رایانه‌های کوانتومی به پیشرفت نانوتکنولوژی کمک می‌کنند. منتقدین پیش از این هشدار داده بودند که خطاها موجب غیرعملی بودن رایانه‌های کوانتومی در مقیاس بزرگ می‌شود. نادرستی این مسئله به‌طور مستقل توسط شور و استین با استفاده از روش تئوری تصحیح خطای کوانتومی ثابت گردید. اکنون به‌نظر می‌رسد تا زمانی که رایانه‌های کوانتومی در مقیاس بزرگ ساخته شوند این مسئله اهمیتی نداشته باشد. نمونه‌هایی از محاسبهٔ کوانتومی در مقیاس کوچک در دستگاه طیف سنجی NMR انجام شده است و تحقیق بر روی اجزاء اصلی محاسبه‌گر کوانتومی در زمینه‌هایی همانند فیزیک حالت جامد، فیزیک نوری، فیزیک اتمی و مولکولی در حال انجام است.

۳-۵- نماد گذاری در محاسبات کوانتومی

در محاسبات کوانتومی، کیوبیت جایگزین بیت‌های کلاسیک می‌شود. یک بیت کلاسیک در یک رایانه می‌تواند یک مقدار باینری صفر یا یک را داشته باشد. یک کیوبیت اساساً دارای نمایش‌های متفاوتی است، به‌طوری که هر دو را به‌طور هم‌زمان دارا می‌باشد.

مسایلی که در نتیجهٔ بررسی اثرات اندازه‌گیری بر روی سیستم کوانتومی ایجاد می‌شوند توسط اروین شرودینگر (فیزیکدان اتریشی، یکی از بنیان‌گذاران نظریه مکانیک کوانتوم و برنده جایزه نوبل) به‌صورت مثالی ساده موسوم به « گربهٔ شرودینگر» بیان شده است[۱۲]. او فرض نمود که داخل جعبهٔ بزرگی یک منبع نور، یک قطبش‌گر، یک آشکارساز، یک هفت‌تیرِ پر و یک گربه وجود دارند. به‌علاوه عقربهٔ آشکارساز به طریقی به ماشهٔ هفت تیرِ پر متصل است که اگر فوتون خروجی از قطبش‌گر، قطبیدهٔ عمودی باشد هفت‌تیر شلیک شده و گربه را می‌کشد و اگر فوتون، قطبیدهٔ افقی باشد تاثیری روی هفت‌تیر نداشته و گربه زنده خواهد ماند. هنگامی که در جعبه بسته باشد، گربه و دستگاه به‌طور کامل از نور و صوت و هر علامت دیگری که از داخل جعبه خبر دهد، منفک هستند. حال این پرسش مطرح می‌شود که اگر یک فوتون از منبع نور گسیل شود چه رخ می‌دهد؟ به بیان دیگر ناظر خارج از جعبه چه پیش‌بینی از رویداد داخل جعبه می‌تواند داشته باشد؟

اگر هرگونه اطلاعات بیشتری در بارهٔ گربه بدست آوریم، ما می‌توانیم هر دو احتمال (احتمال زنده بودن و احتمال مرده بودن) را مورد بررسی قرار دهیم. در مکانیک کوانتومی این را جمع آثار حالت‌ها می‌نامند. بنابراین از دیدگاه ما پیش از این که در جعبه را باز کنیم و داخل آن را مشاهده کنیم، گربه می‌تواند هر کدام از دو حالت زنده یا مرده را داشته باشد. یک کیوبیت کوانتومی درست شبیه مثال گربهٔ شرودینگر است. تا ما آن را مشاهده نکرده‌ایم می‌تواند هم صفر و هم یک باشد. عمل مشاهده کردن، این قاعده را تغییر می‌دهد و در آن صورت به طور اجبار یا صفر است یا یک (شبیه هنگامی‌که ما درون جعبه را مشاهده می‌کنیم که در آن صورت، گربه یا زنده است یا مرده). اگر ما بدون مشاهدهٔ کیوبیت یک عملیات کوانتومی بر روی آن انجام دهیم، آنگاه خروجی یک جمع آثار از هر دو حالت خواهد بود (کیوبیت ورودی به‌طور هم زمان برابر صفر و یک خواهد بود)، یعنی در هر اجرا، نتیجه را برای هر دو حالت خواهیم داشت.

قدرت پردازش یک رایانه کلاسیک به‌طور خطی متناسب است با تعداد بیت‌هایی که می‌تواند به‌صورت هم‌زمان پردازش کند (طول کلمه). چون رایانه کوانتومی قادر خواهد بود دو عمل کلاسیک را با یک عمل کوانتومی انجام دهد، می‌توان نشان داد که در یک رایانه کوانتومی، با افزایش تعداد کیوبیت‌ها، قدرت پردازش به‌صورت نمایی افزایش می‌یابد. این افزایش‌نمایی در قدرت پردازش، انگیزه‌ای برای تحقیق در زمینهٔ رایانه‌های کوانتومی است.

۳-۶- فوتون‌ها و کیوبیت‌ها

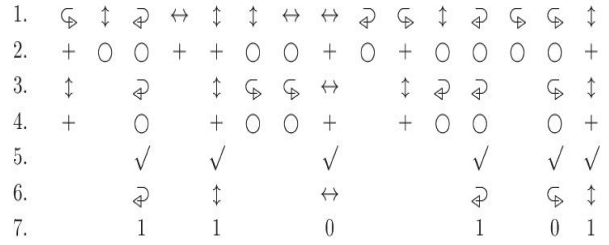
هر کیوبیت می‌تواند برای هر سیستمی که به‌طور واضح حداقل دو حالت قابل تعریف دارد (برای مثال: سطح انرژی یک الکترون در اتم یا قطبش یک فوتون)، وجود داشته باشد. در رمزنگاری کوانتومی، کیوبیت با فوتون‌ها نمایش داده می‌شوند.

۳-۷- پروتکل‌های رمزنگاری کوانتومی

بررسی صوری پروتکل‌های رمزنگاری برای کشف نقایص و رخنه‌های امنیتی در طراحی آن‌ها از اهمیت بسیاری برخوردار است. دو رویکرد کلی در این زمینه، روش‌های تحلیل منطقی و روش‌های ساخت حمله هستند. این روش‌ها هیچ‌کدام به تنهایی راه‌حل فراگیری را برای وارسی امنیت پروتکل‌ها عرضه نمی‌کنند و به‌طور معمول برای تحلیل پروتکل‌ها به‌کارگیری توام آن‌ها مناسب است.

پروتکل‌های رمزنگاری اگر چه دارای ساختار ساده‌ای هستند ولی ویژگی‌های امنیتی که از خود ارایه می‌کنند چندان روشن نبوده و در بسیاری از موارد، از یک قاعده مدون ریاضی استفاده نکرده و بر مبنای یک‌سری ابتکارات خاص پایه‌ریزی می‌گردند. به‌کارگیری روش‌های مختلف رمزنگاری برای حصول اهداف مختلف در یک پروتکل و اثراتی که این روش‌ها بر روی یکدیگر می‌گذارند سبب ایجاد یک سری خواص جبری در پروتکل‌ها می‌شود که یا مانع رسیدن پروتکل به تمامی اهداف مورد نظر شده و یا راه را برای سوء استفاده عوامل مخرب و نفوذی هموار می‌کند.

رابطه دو طرفه‌ای بین دو عامل وجود رخنه در پروتکل و بروز حملات علیه آن‌ها وجود دارد. وجود رخنه در پروتکل، مولد سناریوهای حمله است و حمله به یک پروتکل مبین وجود یک رخنه ظاهر نشده در طراحی پروتکل می‌باشد. بر این اساس تلاش‌های انجام شده برای تحلیل و وارسی پروتکل‌های رمزنگاری نیز در این دو جهت انجام شده است. بعضی از روش‌های تحلیل بر صوری‌سازی مفاهیم تکنیک‌های به کار رفته و اهداف مد نظر از طراحی پروتکل به منظور وارسی صوری عملکرد پروتکل تاکید دارند. هدف از این روش‌ها کشف خطا و نقص در وصول به اهداف مد نظر پروتکل از طریق ایجاد اثبات‌های صوری در مورد این اهداف می‌باشد. از این‌گونه روش‌ها تحت عنوان «روش‌های ساخت استنتاج[1]» یا «روش‌های تحلیل منطقی[2]» و یا روش‌های مبتنی بر«روش‌های باور و دانش[3]» یاد می‌شود. در شکل (۴) پروتکل‌های توزیع کلید کوانتومی معمول نشان داده شده است[۱۳].



شکل۴- پروتکل‌های توزیع کلید کوانتومی[۱۳].

از طرف دیگر، بعضی از روش‌ها به طور مستقیم در راستای کشف سناریوهای حمله علیه پروتکل‌ها از طریق مدل‌سازی پروتکل به همراه عوامل نفوذی و ایجاد فضای حملات امکان‌پذیر، پیش رفته‌اند. در این روش‌ها با تعریف قابلیت‌ها و امکانات نفوذی تلاش می‌شود با بررسی تمامی حالات ممکن به حالتی دست یابیم که در آن عامل نفوذی بتواند اطلاعات مخفی را کشف کند یا این که به نحوی عوامل پروتکل را فریب دهد، به‌عنوان مثال خود را جانشین یکی از طرفین مجاز جلوه دهد. از این‌گونه روش‌ها با نام روش‌های جبری یا روش‌های مبتنی بر « ساخت حمله[4]» یا روش‌های « ماشین حالت[5]» یاد می‌شود.

هیچ‌کدام از روش‌های فوق، روش‌های کاملی برای تحلیل محسوب نمی‌شوند. در روش تحلیل منطقی اثبات اهداف امنیتی در پروتکل بدون فرض وجود نفوذی انجام می‌شود و لذا گرچه با این روش‌ها می‌توان درستی ادعای طراح پروتکل در به وجود آمدن ویژگی‌های امنیتی پس از اجرای پروتکل را مورد بررسی قرار داد ولی نمی‌توان حملات نفوذ به پروتکل - که حاصل انجام بعضی اقدامات حمله‌کننده برای فریب عوامل است - را شناسایی کرد. فریب یک عامل توسط نفوذی به معنی دست‌یابی نفوذی به بعضی اطلاعات امنیتی یا دسترسی وی به بعضی موقعیت‌های غیرمجاز بدون خدشه‌دار کردن ویژگی‌های

1- Inference Construction Methods

2- Logic Analysis Mthods
3- Knowledge and Belief Methods
4- Attack Construction Methods
5- State Machin Methods

امنیتی مورد نظر طراح از نظر آن عامل است. در مقابل در مورد روش‌های ساخت حمله اگر چه دست‌یابی به یک سناریوی حمله نمایان‌گر یک رخنه در پروتکل است ولی عدم کشف یک سناریوی حمله خاص نیز نمایان‌گر درستی عملکرد پروتکل با توجه به اهداف از پیش تعیین شده آن پروتکل نمی‌باشد.

با وجود این، هر کدام از روش‌های فوق مزایایی دارند. روش تحلیل منطقی را می‌توان یک فعالیت در زمان طراحی و روش‌های ساخت حمله را فعالیتی برای ارزیابی پروتکل طراحی شده دانست. در روش تحلیل منطقی، مسئله به شکل طبیعی خود در نظر گرفته می‌شود و حداقل می‌توان ایده‌های طراح را در آن اثبات و یا مشاهده نمود. در روش ساخت حمله، مسئله از دید نفوذی دیده می‌شود و هدف این است که غفلت‌های طراح پروتکل کشف شود. در رویکرد اول سعی بر این است که اثبات شود چه ویژگی‌های امنیتی به‌صورت صحیح برآورده می‌شوند در حالی که در روش دوم به دنبال کشف نقاط ضعف در حصول ویژگی‌های امنیتی هستیم. میدوز[1] ضمن بررسی رویکردهای مختلف تحلیل پروتکل، به‌کارگیری «روش نامتغیرها[2]» را معرفی کرده است. یک نامتغیر در یک روش تحلیل عبارتی است که برای وارسی امنیت، بایستی درستی یا نادرستی آن عبارت را اثبات نمود. اگر بتوان بررسی وجود ویژگی‌های امنیتی در یک پروتکل را به همراه بررسی وجود سناریوهای نقض آن هم‌زمان انجام داد می‌توان مزایای هر دو رویکرد را به‌دست آورد.

۴- نتیجه

موضوع پدافند سیستم‌های اطلاعاتی یکی از موارد بسیار اساسی در جنگ‌های مدرن و نرم است. در صورت بهره‌گیری از فیزیک کوانتوم، پیشرفت شگرفی در سیستم‌های اطلاعاتی- مخابراتی به‌وجود آمده و یکی از نتایج عظیم آن سرعت بسیار زیاد و امنیت قابل قبول فضای تبادل اطلاعات خواهد بود. از دیدگاه پدافند غیر عامل، اکنون در زمانی به سر می‌بریم که هر تکنیک و روشی که بتواند امنیت اطلاعات را تضمین نماید از اهمیت بسیاری برخوردار است.

از منظر رمزنگاری دفاعی، اکنون در زمانی به سر می‌بریم که امکان ساختن سیستم های رمزنگاری با قابلیت چک، کشف و جلوگیری از شنودهای غیر مجاز امکان‌پذیر شده است. برخی زمینه‌هایی که باید جهت حصول این فناوری توسعه یابند، عبارتند از:

- اصلاح و بهبود پروتکل‌های کوانتومی در محیط شبکه‌های رایانه‌ای کوانتومی.
- توسعه الگوریتم‌های تشخیص استراق سمع
- شناخت ژرف‌تر استراق سمع در حضور نویز

در حوزه رمز نگاری کوانتومی *فرصت‌های* پیش رو عبارتند از:

- الف- دستیابی به فناوری‌های پیشرفته نظیر: تولید و آشکارسازی تک فوتون، جدایش پرتو از یک پالس نوری، چرخش قطبش یک پالس نوری، تولید یک زوج فوتون درهم تنیده
- ب- امنیت توزیع کلید
- ج- بهبود یا اصلاح پروتکل‌های رمزنگاری
- د- کشف استراق سمع‌کننده

تهدیدات ناشی از این فناوری عبارتند از:

- رایانه‌های با سرعت پردازش بسیار بالا با ساخت چنین رایانه‌هایی امنیت رمزنگاری‌های کلاسیک ازجمله RSA مخدوش خواهد گردید.
- ابداع تکنیک‌های استراق سمع احتمالی در این حوزه که لازمه آن وجود چنین فناوریی در وهله نخست است تا متخصصان داخلی بتوانند از چگونگی استراق‌سمع احتمالی تجربه کسب نمایند.

1- Meadows
2- Invariant method

مراجع

1. Deutsch, David, Quantum Communication thwarts eavesdroppers, New Scientist, pp:25-6 ,9 Dec. (**1989**).
2. Shor, Peter W., Polynominal - Time Algorithms for Prime Factorization and Discrete Logarithms on Quantum Compute, SIAM J. Computing,p:1484,V.26, (**1997**).
3. Grove,Lov K., How Fast Can a Quantum Computer Search ? , quant-ph/9809029.
4. Feynman,Richard P., Robert B. Leighton, and Matthew Sands, The Feynman Lectures on Physics: Vol. III. Quantum Mechanics, Addison – Weslley Pub. Company,reading ,Massachusetts, (**1965**).
5. Bennett,Charles H., and Stephan J. Weisner, Communication Via One-and two –Particle Operators on Einstein-Podolsky- Rosen States, Physical Review Letters, pp: 2881-84, Vol.69, No.20, 16 Nov. (**1992**).

6. Wiesner,Stephan,Conjugate Coding, SIGACT News, 15:1, pp: 78-88, (Manuscript circa 1970) (**1983**).
7. Bennett,Charles H.,and Gilles Brassard, Quantum Cryptography: Public key distribution and coin tossing , Int.Conf. on Computer, System & Signal Processing, Bagalore, India, Dec.10-12, pp:175-9, (**1984**).
8. Ekert,A.,and R. Jozsa, Notes on Shor's Efficient algorithm for factoring on a quantum computer, Workshop on Quantum computing and communication, Gaithherburh, MD, Aug. 18-19, (1994), (preprint, 21 pages).
9. Ibid [7].
10. Navez, P. and G.Van Assche, A method for secure transmission:Quantum cryptography, TECH-NOPOL IT-SCAN, pp:1-4, Apr. (**2002**).
11. Ibid [10].
12. Dirac,P.M.,The Principle of Quantum Mechanics, (Fourth Ed.), Oxford University Press, (**1958**).
13. Bennett,Charles H.,and Gilles Brassard and Francois Bessette, Experimental Quantum Cryptography, Eurocrypt, Arhus, Denmark, pp: 253- 65, May 21-4, (**1990**).
    Also see: Bennett,C., F. Bessette and et al. Experimental Quantum Cryptography, J. Cryptography, V. 5, No.1, pp:3-28, (**1992**).

An Introduction to Quantum Cryptography Systems

Davood Majidi[1]

Zeinolabedin Noroozi[2]

Abstract

In the modern warfare, one of the most important issues is safeguarding confidential and secret information. Each side of the conflict who is capable to access the information of the other side, will be strategically an tactically superior and his chance of victory at war will be multiplied. In this regard, the passive defense measures can play an effective role in reducing vulnerabilities. Cryptography as one of the passive defense measures, to safeguard the classified information, military intelligence, sensitive business and industrial information, governmental information and individual information is indispensable. Terrorists, hackers and imposters can obtain the important information and activities of armed forces and governments through hacking and cause problems for these organizations. For these reasons and in the course of time, many cryptographic methods were created to secure and safeguard information.

Basically, cryptographic methods are used to safeguard the transferred information on open networks and the stored information on computers, as well. The classic cryptography systems are vulnerable due to their weak cryptographic algorithms or weakness in their key management systems. Although the quantum and the new computation theories are only less than 50 years old, recently, scientists have been able to review completely the consequences of one theory on another. In this essay attention is paid to the importance of security and different kinds of cryptography attacks and one of the most advanced cryptography methods, the quantum method, is introduced. The importance of the quantum cryptography lies in displaying that the Kelby Touring circuit is not used for practical computations.

Key Words: *Quantum Computations, Quantum Cryptography, Information Security, Passive Defense*

1- Malek Ashtar University of Technology- Faculty of Spatial Planning and Passive Defense (Email: d.majidi@lycos.com)
2- Imam Hossein University- Department of Mathematics and Cryptology