رایانش کوانتومی از منظر امنیتی

چالش‌های امنیتی مرتبط با محاسبات کوانتومی چگونه هستند؟

ما در این مطلب ابتدا به تحلیل ارائه شده از سوی مؤسسه گلوبال ریسک نگاهی خواهیم داشت و در ادامه تأثیرگذاری این مدل محاسبات بر رمزنگاری امنیتی را مورد بررسی قرار خواهیم داد.

این مطلب یکی از مجموعه مقاله‌های پرونده ویژه «**کامپیوترهای کوانتومی**» است که در **شماره ۱۸۹ ماهنامه شبکه** منتشر شد. برای دانلود این پرونده ویژه می‌توانید **اینجا** کلیک کنید.

مانند هر فناوری دیگری، محاسبات کوانتومی همراه با یک سری پیامدهای مثبت و منفی با دنیای ما عجین شده و خواهند شد. از جنبه مثبت داستان، این فناوری سرعت پردازش اطلاعات را به‌شکل محسوسی افزایش می‌دهد و به ما کمک می‌کند تا مسائل رام‌نشدنی امروزی را به ساده‌ترین شکل حل کنیم. این فناوری به‌ویژه در ارتباط با تجهیزات هوشمندی که سرعت در آن‌ها حرف اول را می‌زند کمک‌کننده خواهد بود.

مطلب پیشنهادی

اج کامپیوتینگ
غول چند میلیاردی که در سکوت متولد شد

در بعد امنیتی مهم‌ترین دستاورد محاسبات کوانتومی در ارتباط با رمزنگاری است. رمزنگاری ارائه شده از سوی این مدل از محاسبات کاملاً پیچیده و قدرتمند است، به‌طوری که بعضی کارشناسان عنوان کرده‌اند که عملاً شکستن آن‌ها امکان‌پذیر نخواهد بود. اما در طرف مقابل این فناوری چالش‌های امنیتی مختلفی را نیز به‌وجود خواهد آورد. شکسته شدن گذرواژه مورد استفاده از سوی سازمان‌ها ابتدایی‌ترین پیامد منفی است که بسیاری از کارشناسان به آن اشاره کرده‌اند. ما در این مطلب ابتدا به تحلیل ارائه شده از سوی مؤسسه گلوبال ریسک نگاهی خواهیم داشت و در ادامه تأثیرگذاری این مدل محاسبات بر رمزنگاری امنیتی را مورد بررسی قرار خواهیم داد.

تهدید بالقوه‌ای در راه است

مؤسسه کانادایی گلوبال ریسک در جدیدترین گزارش خود عنوان کرده است که محاسبات کوانتومی را باید به‌عنوان یک تهدید بالقوه برشماریم. تهدیدی که قادر است هر گونه سامانه کامپیوتری به‌ویژه سامانه‌هایی که امروزه در زمینه

رمزگذاری مورد استفاده هستند را در معرض یک خطر بالقوه قرار دهد. این سازمان در گزارش خود به این نکته اشاره کرده است که محاسبات کوانتومی با ضریب موفقیت یک به هفت قادر هستند سامانه‌های رمزنگاری عمومی را در خوشبینانه‌ترین حالت در ده سال آینده درهم شکنند. همچنین، این مدل محاسبات به احتمال 50 درصد تا سال 2031 تمام ابزارهای رمزنگاری که امروزه مورد استفاده قرار می‌گیرند را بدون مصرف خواهد کرد. مایکل موکسا مشاور امنیت سایبری مؤسسه Global Risk Institute و از بنیان‌گذاران مؤسسه محاسبات کوانتومی در دانشگاه واترلو که این گزارش را آماده کرده، در این ارتباط گفته است: «فیزیک کوانتوم یکی از مهم‌ترین خطرات بالقوه دنیای امنیت سایبری به‌شمار می‌رود. امروزه هکرها با استفاده از تکنیک‌های مختلفی به سامانه‌های کامپیوتری حمله می‌کنند. آن‌ها در تلاش هستند تا از راهکارهای نوآورانه و خاصی برای نفوذ به سامانه‌های کامپیوتری استفاده کنند.

اما تهدید محاسبات کوانتومی موضوع دیگری است. تهدیدی که از جانب محاسبات کوانتومی متوجه سامانه‌های کامپیوتری می‌شود درست از همان مکان و نقطه‌ای آغاز می‌شود که کامپیوترهای کلاسیک در انجام آن کارها ناتوان هستند. در کامپیوترهای کلاسیک امروزی از مقادیر صفر و یک به‌منظور ذخیره‌سازی و پردازش اطلاعات استفاده می‌شود، اما در کامپیوترهای کوانتومی ما با حالت سومی نیز روبه‌رو هستیم. امروزه محاسبات کوانتومی به‌آرامی از فیزیک نظری عبور کرده‌اند و به دنیای پزشکی، تصویربرداری و اندازه‌گیری دقیق وارد شده‌اند. ما به‌دنبال آن هستیم تا کامپیوترهای کوانتومی را در صنعت مورد استفاده قرار دهیم، به‌طوری که برای حل مشکلات بنیادین جهان امروزی از آن‌ها استفاده کنیم. سازمان‌ها و صنایع پیشگام در عرصه فناوری در رقابت تنگاتنگی با یکدیگر قرار دارند و در تلاش هستند تا این مدل محاسبات را توسعه دهند. یکی از پیامدهای این رقابت شانه به شانه شکسته شدن گذرواژه‌هایی است که از سوی سازمان‌ها و حتی دولت‌ها مورد استفاده قرار می‌گیرد.»

محاسبات کوانتومی آرماگدون دنیای رمزنگاری

رمزنگاری سنگ بنای امنیت اطلاعات را شکل می‌دهد. ما از رمزنگاری به‌منظور رمزگذاری و رمزگشایی داده‌ها در راستای دستیابی به فاکتورهای محرمانگی، یکپارچگی و اصالت داده‌ها استفاده می‌کنیم. این سه فاکتور در کنار یکدیگر سرویس‌های رمزنگاری را معرفی می‌کنند. اما پیشرفت‌های مستمری که در علم رمزنگاری، تجزیه و تحلیل داده‌ها و مهندسی به وقوع پیوسته است، چالش‌های جدیدی را در رابطه با این علم به‌وجود آورده است. RSA یا همان روش رمزنگاری مبتنی بر کلید عمومی که در روزگار قدیم بر پایه کلیدهای 129 بیتی مورد استفاده قرار می‌گرفت، دیگر هیچ گونه کارایی ندارد. به‌دلیل اینکه امروزه اگر از کلیدهایی که کوچک‌تر از 2048 بیت هستند، استفاده کنید در واقع داده‌های خود را در معرض خطر قرار داده‌اید. MD5 نیز که در سال 1992 طراحی شد و یکی

از پرکاربردترین توابع درهم‌ساز بود، سرانجام در سال 2004 شکسته شد. به همین ترتیب، SHA-1 نیز به‌شکل ساده‌تری به‌دنبال حمله Freestart درهم شکسته شد. سرانجام در سال 2016 نرم‌افزار Eurocrypt منتشر شد.

محاسبات کوانتومی به میدان وارد می‌شوند

محاسبات کوانتومی یکی از منابع مهمی است که به‌مرور زمان در جعبه ابزار متخصصان رمزنگاری به‌منظور تحلیل رمزها قرار خواهد گرفت. محاسبات کوانتومی بر مبنای خواص فیزیک‌کوانتومی کار می‌کنند، در نتیجه رفتاری کاملاً متفاوت در مقایسه با کامپیوترهای رایج امروزی دارند. آن‌ها به‌جای آنکه از بیت‌ها استفاده کنند از بیت کوانتومی یا کوبیت استفاده می‌کنند. تئوری به‌کارگیری محاسبات کوانتومی برای حمله به سامانه‌های رمزنگار اولین بار در سال 1994 مطرح شد. زمانی که پیتر شر الگوریتم رمزنگاری را برای پیدا کردن عوامل اول یک عدد صحیح مورد استفاده قرار داد. این الگوریتم به او کمک کرد تا فاکتورگیری اعداد صحیح را به‌راحتی انجام داده و مشکلات گسست لگاریتمی که پایه و اساس بسیاری از الگوریتم‌های رمزنگاری کلید عمومی (نه همه) است را برطرف کند. الگوریتم دیگری که نشانه‌های تخریبی کمتری در آن وجود دارد، اما از قدرت بسیار بالایی برخوردار است، الگوریتم کوانتومی استیفن گراور است. این الگوریتم برای اولین بار در دنیای الگوریتم‌های جست‌وجوگر موفق شد بالاترین سرعت را از آن خود کند. این الگوریتم با توجه به سرعت بسیار بالایی که دارد سامانه‌های رمزنگاری که از الگوریتم AES استفاده می‌کنند را در آینده با چالش اساسی روبه‌رو خواهد کرد. این الگوریتم به اندازه‌ای کارآمد است که می‌تواند تمام الگوریتم‌های رمزنگاری موجود را به چالش کشیده و به‌عبارت ساده‌تر به ما اعلام دارد تمام الگوریتم‌هایی که امروزه از آن‌ها استفاده می‌کنید قابل شکسته شدن هستند. اما چه عاملی باعث شده است تا این الگوریتم‌ها به‌شکل جدی و عملی مورد استفاده قرار نگیرند؟ تنها عامل عدم به‌کارگیری این الگوریتم‌ها نبود یک کامپیوتر کوانتومی به اندازه کافی بزرگ است که بتواند این الگوریتم‌ها را اجرا کرده و بر خصایصی که الگوریتم‌های رمزنگاری رایج از آن استفاده می‌کنند، غلبه کند.

در حوزه محاسبات کوانتومی همه چیز به‌سرعت در حال تکامل است. در آوریل 2016 کمیسیون اروپا اعلام کرد که این اتحادیه در نظر دارد یک میلیارد یورو در ارتباط با پروژه این اتحادیه موسوم به «کشتی فناوری‌های کوانتومی بزرگ در سطح اروپا» سرمایه‌گذاری کند. به فاصله کوتاهی از اعلام این خبر برخی افراد تصمیم گرفتند در صندوق توسعه کامپیوترهای کوانتومی در مقیاس بزرگ سرمایه‌گذاری کنند. در آن سوی کره خاکی و درست در همان ماه پژوهشگران کانادایی خبری در ارتباط با فاکتورگیری انجام شده از سوی کامپیوترهای کوانتومی منتشر کردند. در این گزارش اعلام شد کامپیوتر شرکت دی‌ویو سیستمز موسوم به 2X موفق شد فاکتورگیری عدد 200099 را انجام دهد. اما هنوز به‌درستی مشخص نیست آیا کامپیوتر دی‌ویو توانسته است الگوریتم شر را برای این منظور مورد استفاده قرار دهد یا از تکنیک دیگری استفاده کرده است. به این نکته توجه داشته باشید که 200099 تنها یک عدد 18 بیتی است. در نتیجه کامپیوتر فوق هنوز قدرت لازم برای فاکتورگیری یک عدد صحیح 2048 بیتی و البته شکستن پارامترهای الگوریتم RSA را در اختیار ندارد. سامانه‌های کامپیوتری امروزه از الگوریتم‌های قدیمی همچون دیفن-هلمن (1976)، RSA (1977) و منحنی‌های بیضوی (1985) استفاده می‌کنند.

رمزنگاران به مقابله با محاسبات کوانتومی برمی‌خیزند

رمزنگاران سراسر جهان برای مقابله با رمزگشایی اعمال شده از سوی کامپیوترهای کوانتومی بزرگ بیش از یک دهه است که تلاش می‌کنند سامانه‌های رمزنگار ایمن در برابر حملات کوانتومی را پایه‌ریزی کنند. ماحصل این تلاش‌ها به‌شکل‌گیری سامانه‌های رمزنگار و الگوریتم‌های ویژه‌ای منجر شده است که امروزه به‌نام رمزنگاری پساکوانتومی (PQCrypto) آن‌ها را می‌شناسیم.

وضعیت فعلی PQCrypto چگونه است؟

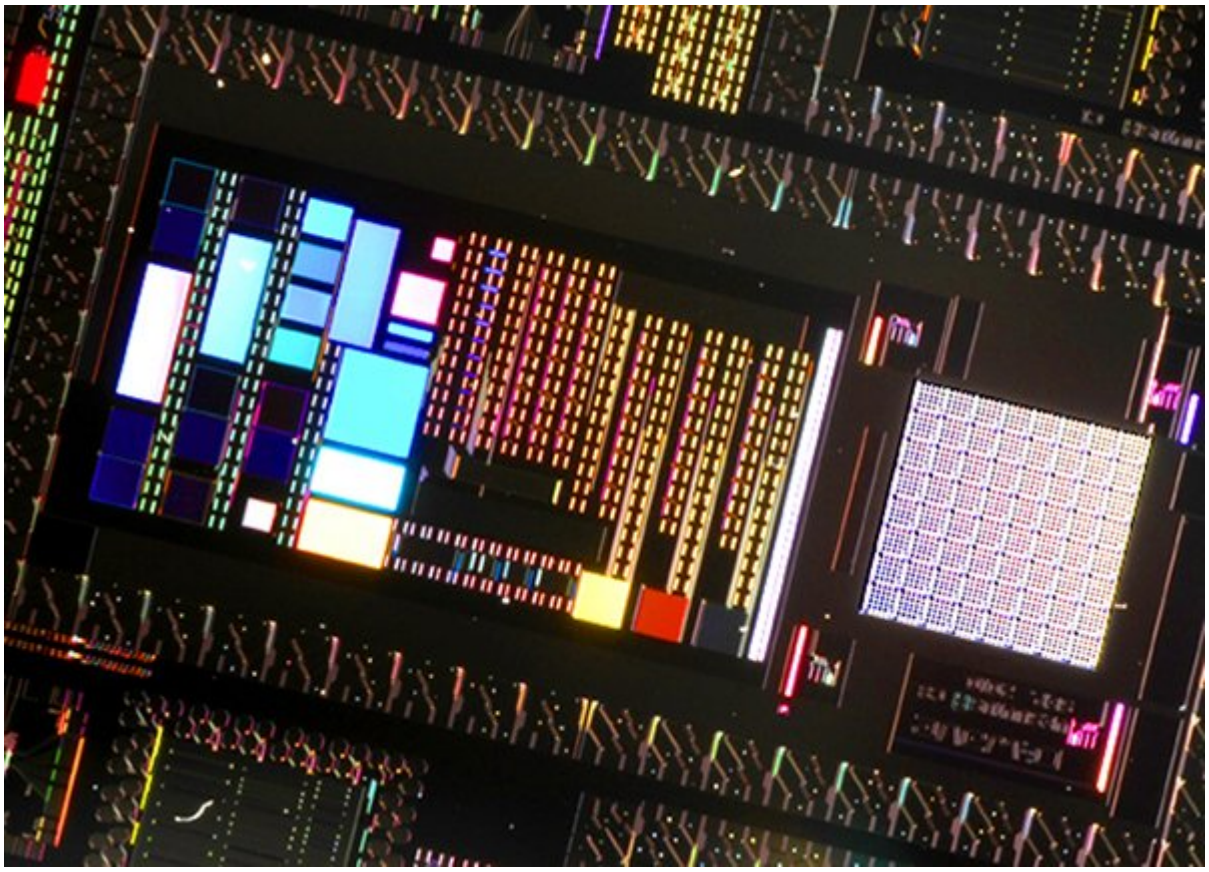
در سال 2006 همایشی در ارتباط با رمزنگاری پساکوانتومی برگزار شد. در این همایش پژوهشگران رمزنگار سراسر جهان گردهم آمدند. آن‌ها در این همایش به معرفی جدیدترین دستاوردهایی پرداختند که برای مقابله با حملات

کوانتومی می‌توان از آن‌ها استفاده کرد. رمزنگاری McEliece (1978)، الگوریتم SAFECrypto که برنامه‌ای برای توسعه رمزنگاری مبتنی بر یک شبکه مقاوم در برابر کوانتوم است، برنامه CryptoWorks21 که یک برنامه کانادایی بوده و به‌منظور طراحی ابزارهای لازم برای نسل بعدی رمزنگاری مقاوم در برابر کوانتوم قرن 21 پیشنهاد شده از جمله راهکارهای ارائه شده در ارتباط با رمزنگاری پساکوانتومی هستند. مهم‌ترین ویژگی ابزارهای معرفی شده این است که اندازه کلید آن‌ها در حد مطلوب و ایده‌آل قرار دارد.

چه زمانی باید در انتظار تهدیدات کوانتومی باشیم؟

ما این توانایی را نداریم تا پاسخ صریح و دقیقی به این پرسش بدهیم، اما بر مبنای شرایط فعلی و مفروضاتی که در اختیار داریم تا حدی قادریم این زمان را پیش‌بینی کنیم. اولین نکته‌ای که باید به آن اشاره داشته باشیم این است که حتی در دنیای کوانتومی امروزی نیز می‌توانیم از سامانه‌های خود محافظت به عمل آوریم، اما این کار تنها زمانی امکان‌پذیر است که سامانه‌های ما از الگوریتم‌های رمزنگاری پساکوانتومی استفاده کنند. به‌عبارت دقیق‌تر زمانی که این الگوریتم‌ها از مرز تئوری به مرز واقعیت برسند.

کارشناسان حوزه رمزنگاری پیش‌بینی کرده‌اند که در آینده سازمان‌ها از الگوریتم‌های کلید عمومی رایج همچون RSA و منحنی‌های بیضوی کمتر استفاده خواهند کرد. همچنین در ارتباط با الگوریتم‌های رمزنگاری متقارن و توابع درهم‌ساز به‌شرطی که ویژگی‌ها و خصایص آن‌ها تغییر پیدا کنند (دو برابر شوند)، این پتانسیل را خواهند داشت تا در دنیای کوانتومی به محافظت از سامانه‌های امنیتی بپردازند. در نتیجه مسئولان تنظیم برنامه‌های امنیتی در سازمان‌های خود باید خود را با تغییراتی که در آینده رخ می‌دهد هماهنگ ساخته و الگوریتم‌های جدید و قدرتمندتر را جایگزین نمونه‌های قبلی کنند. اما اکنون باید به این پرسش پاسخ دهیم که کامپیوترهای کوانتومی بزرگ چه زمانی قادر خواهند بود حملاتی را علیه سامانه‌های رمزنگار ترتیب دهند.



اجازه دهید این گونه فرض کنیم که قانون مور در ارتباط با توسعه محاسبات کوانتومی معتبر خواهد بود. الگوریتم شر به سه کوبیت log2(N) نیاز دارد تا با استفاده از آن عدد صحیح N را فاکتورگیری کند. این به‌معنای آن است که الگوریتم شر به 6 هزار کوبیت نیاز دارد تا یک عدد صحیح 2048 بیتی را بشکند. قانون مور اعلام می‌دارد که تعداد بیت‌ها ـ در این‌جا کوبیت‌ها ـ که روی مدارها قرار می‌گیرند، بین 12 تا 18 ماه دو برابر می‌شوند. اجازه دهید این مورد را با ذکر مثالی مورد بررسی قرار دهیم.

فرض کنید یک کامپیوتر کوانتومی پنج بیتی همانند کامپیوتری که آی‌بی‌ام چند وقت پیش دسترسی عمومی به آن را

امکان‌پذیر ساخت در اختیار داریم. تعداد کل کوبیت‌های در دسترس برای اجرای الگوریتم شر بعد از M بار چرخش قانون مور برابر با 5*M2 خواهد بود و با استناد به زمان 18 ماهه پایان یک دوره عمر از چرخش قانون مور، ما از امروز نزدیک به 16 سال زمان نیاز داریم تا حملاتی را علیه سامانه‌هایی که از الگوریتم RSA که از کلیدهای 2048 بیتی استفاده می‌کنند، پیاده‌سازی کنیم. با استناد به زمان 11 ماهه پایان یک دوره عمر چرخش قانون مور 16.5 سال طول می‌کشد. چنین قاعده‌ای در ارتباط با الگوریتم‌های دیگری همچون AES نیز صدق می‌کند. اگر مثال فوق را بسط دهید، یک زمان تقریبی به‌دست خواهید آورد. در نتیجه این گونه به‌نظر می‌رسد که سامانه‌های مبتنی بر رمزنگاری پساکوانتومی گزینه قابل قبولی در این زمینه به‌شمار می‌روند.

تاریخ انتشار:

18 اردیبهشت 1396

نشانی منبع:
https://www.shabakeh-mag.com/cover-story/7710/%DA%86%D8%A7%D9%84%D8%B4%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D9%85%D8%B1%D8%AA%D8%A8%D8%B7-%D8%A8%D8%A7-%D9%85%D8%AD%D8%A7%D8%B3%D8%A8%D8%A7%D8%AA-

%DA%A9%D9%88%D8%A7%D9%86%D8%AA%D9%88%D9%85%DB%8C-
%DA%86%DA%AF%D9%88%D9%86%D9%87-
%D9%87%D8%B3%D8%AA%D9%86%D8%AF%D8%9F