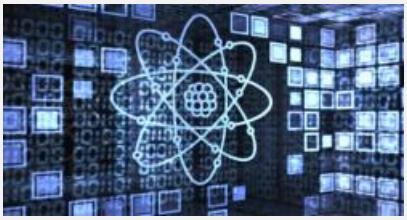

سه شنبه 27 مهر 1395 - 09:58

کامپیوترهای کوانتومی به شکستن رمزنگاری RSA نزدیک شدند

از کامپیوترهای کوانتومی برای جستجویی هوشمندتر و عملکرد خیلی سریع تر اغلب یاد می‌شود. اما مهارت‌های ریاضی شگفت انگیز، خود نیز ممکن است خطرات امنیتی عمیقی برای اطلاعاتی که مدتها با خیال آسوده رد و بدل می‌شد به وجود بیاورند.

از کامپیوترهای کوانتومی برای جستجویی هوشمندتر و عملکرد خیلی سریع تر اغلب یاد می‌شود. اما مهارت‌های ریاضی شگفت انگیز، خود نیز ممکن است خطرات امنیتی عمیقی برای اطلاعاتی که مدتها با خیال آسوده رد و بدل می‌شد به وجود بیاورند.

به گزارش کلیک، دانشمندان دانشگاه‌های MIT و Innsbruck اعلام کردند اولین کامپیوتر کوانتوم ۵ بیتی موسوم به کوبیت‌ها (qubits) تولید شده است.

در حال حاضر بسیاری از داده‌های دیجیتال توسط کلید عمومی رمزنگاری محافظت می‌شود. رمزنگاری کلید عمومی یا رمزنگاری نامتقارن روشی از رمزنگاری است که کلید مورد استفاده برای رمزگذاری با کلید مربوط برای رمزگشایی با هم متفاوت است (برخلاف رمزنگاری متقارن که در آن رمزگذاری و رمزگشایی با یک کلید انجام می‌شود). در رمزنگاری نامتقارن، کاربر یک جفت کلید در اختیار دارد.کلید عمومی برای رمزگذاری متن اصلی و راست‌آزمایی امضای دیجیتال و کلید خصوصی برای رمزگشایی متن رمز و امضای دیجیتال داده‌ها. مشخص است که کلید خصوصی مخفی باقی می‌ماند ولی کلید عمومی ممکن است به طور وسیع منتشر شود. پیام‌های دریافتی کد شده توسط کلید عمومی کاربر فقط برای خودش قابل خواندن می‌باشد زیرا تنها خود کاربر کلید خصوصی جهت رمزگشایی را در اختیار دارد .دو کلید با هم رابطه‌ای ریاضی دارند ولی عملاً کلید خصوصی از روی کلید عمومی محاسبه پذیر نیست.

به طور سنتی، کامپیوترها برای انجام محاسبات از روش‌های محافظت شده استفاده می‌کنند، بنابراین داده‌ها در این راه به صورت ایمن منتقل می‌شوند. چند روز گذشته، دو نفر از پشگامان این روش، به نام‌های Whitfield Diffie و .Martin E Hellman موفق به کسب جایزه Turing در سال ۲۰۱۵ شدند. این جایزه بالاترین افتخار در علوم کامپیوتر محسوب می‌شود. آنها محور اصلی کار خود در رمزنگاری را بر روی روشی موسوم به الگوریتم RSA قرار داده بودند. RSA شیوه‌ای برای رمزنگاری به روش کلید عمومی است. این روش نخستین بار در سال ۱۹۷۷ توسط سه نفر از متخصصین دانشگاه MIT به نام های Ronald Adi Shami ، Linn Rivest و Len Adleman مطرح شد.

Matthew Green، متخصص رمزنگاری در موسسه امنیت اطلاعات Johns Hopkins می‌گوید: RSA در همه جا استفاده می شود. هنگامیکه شما به یک وب سایت مراجعه می‌کنید، احتمالاً از الگوریتم RSA استفاده شده است. ارسال پیام متنی در آیفون با استفاده از رمزنگاری RSA صورت می‌گیرد.

کامپیوترهای کوانتومی از پدیده‌ها و قوانین مکانیک کوانتوم مانند برهم‌نهی و درهم تنیدگی برای انجام محاسباتش استفاده می‌کند. این کامپیوترها می‌توانند از خواص و قوانین فیزیک کوانتوم برای ذخیره‌سازی و انجام عملیات روی داده‌ها استفاده کنند.

کامپیوترهای کوانتومی، بر خلاف کامپیوترهای کلاسیک که از بیت‌های ۰ و ۱ برای ذخیره اطلاعات استفاده می‌کنند، برای انجام عملیات از کوبیت ها استفاده می‌کنند. در یک کامپیوتر کلاسیک ، هر بیت در هر لحظه یا در حالت ۰ و یا در حالت ۱ است، اما اصول مکانیک کوانتومی به کوبیت اجازه می‌دهد که در همان حال، حالتی را برابر با برهم نهی دو حالت اصلی نیز اختیار کند، این همان ویژگی بنیادی در پردازش کوانتومی است. به عبارتی، یک کوبیت هم ممکن است در حالت‌های کلاسیک ۰ و ۱ وجود داشته باشد و هم می‌تواند در حالت ترکیب این دو قرار گیرد (یعنی همزمان دارای هر دو حالت صفر و یک باشد). در واقع همین پدیده، تفاوت اصلی بین بیت‌های کلاسیک و کوبیت‌ها است.

Peter Shor استاد ریاضی دانشگاه MIT، اولین الگوریتم را در محاسبات کوانتومی برای تجزیه عددی به اعداد اول مطرح کرد که معروف ترین الگوریتم رمزنگاری با کلید عمومی ، RSA را به چالش کشید، اما راهی برای آزمایش آن پیدا نکرد. در سال ۲۰۰۱، Isaac Chuang مهندس برق و فیزیکدان دانشگاه MIT، با استفاده از فاکتور شماره ۱۵ در استفاده از این الگوریتم موفق بود، اما سیستم کوانتومی او نمی‌توانست به نسبت ثابت برای عامل‌های با پیچیدگی بیشتر افزایش پیدا کند.

Chuang و تیم تحقیقاتی‌اش، در آخرین کار خود، قصد داشت یک کامپیوتر کوانتومی برای فاکتورهای بزرگتر از ۱۵ ایجاد کند. آنها قصد داشتند نوعی کامپیوتر کوانتومی ایجاد کنند که کیوبیت ها خود را در مد پایدار ذخیره کنند.

آنها به یک نمونه اولیه از کامپیوتر کوانتومی به نام ion trap دست یافتند. در این نوع کامپیوتر، کوبیت‌ها به واسطه یک میدان الکتریکی و پالس‌هایی از لیزر نوری اقدام به نگهداری یک رشته یون می‌کنند. در این کامپیوتر، نیاز به چهار کوبیت برای انجام عملیات الگوریتم شور دارد، و این در حالی است که کوبیت پنجم خروجی حاصل از عملیات را در خود ذخیره می‌کند.

چانگ و تیم تحقیقاتی‌اش توانستند با یک کامپیوتر کوانتومی ۵ اتمی فاکتور ۱۵ را محاسبه کنند، پیش از این کارشناسان گمان می‌کردند چنین محاسبه‌ای حداقل نیاز به یک کامپیوتر ۱۲کوبیتی دارد. چوانگ معتقد است، مادامی که ion trap بتواند کوبیت را در محل خود نگهدارد، این مدل ۵ اتمی می‌تواند به نسبت ثابت برای عامل‌های با پیچیدگی بیشتر افزایش پیدا کند. نتایج تحقیق آنها در آخرین شماره مجله Science به چاپ رسیده است.

هرچند یک کامپیوتر کوانتومی کاربردی اندازه لازم برای شکستن رمزنگاری RSA را داراست، ولی هنوز هم کارشناسان امنیت دیجیتال به این کامپیوتر به دیده تردید می‌نگرند. در ماه ژانویه، آژانس امنیت ملی ایالات متحده جلسه پرسش و پاسخی در خصوص خطرات این کامپیوتر برگزار کرد.

آقای گرین می گوید: من فکر می‌کنم مردم برای شروع استفاده از این کامپیوتر مردد هستند. آنها هنوز هم فکر می‌کنند با این کامپیوتر ۱۵ تا ۳۰ سال امنیت اطلاعات برقرار است، اما داده ها برای زمانهای بسیار طولانی وجود خواهند داشت. آنچه که باید بدانید این است که بسیاری از داده ها تا ۳۰ سال امن نگه نخواهند ماند.

حتی اگر روزی کد امنیتی مدرن دیجیتالی شکسته شود، چانگ این موضوع را به عنوان فرصتی برای رفع آسیب پذیری برای نسل‌های آتی می‌داند.