کد خبر: ۷۸۹۹۲۱
یکشنبه ۲۹ مهر ۱۴۰۳ ۱۴:۲۰

موفقیت چینی‌ها در هک اطلاعات نظامی رد شد

در حالی که چند روز قبل خبری مبنی بر موفقیت محققان چینی در هک رایانه‌های کوانتومی در سطح نظامی منتشر شد، اکنون مشخص شده که اینچنین نبوده و برداشتی اشتباه از مقاله محققان چینی انجام شده است.<;br&#۴۷;><br&#۴۷>

به گزارش سایت خبری پرسون، چند روز پیش خبری درباره استفاده محققان چینی از رایانه‌های کوانتومی D-Wave برای هک کردن رمزگذاری درجه نظامی منتشر شد که حالا مشخص شده این خبر در واقع درست و دقیق نبوده است.

مقاله منتشر شده در مجله چینی Computers در ماه مه ۲۰۲۴ به «تبرید کوانتومی» از طریق سامانه‌های D-Wave با استفاده از مدل‌های Ising و QUBO برای فاکتور کردن اعداد صحیح محافظت‌شده با RSA که یک جزء حیاتی در شکستن رمزگذاری است، می‌پردازد.

این مقاله در ادامه، موفقیت محققان چینی را در شکستن رمزگذاری ۵۰ بیتی RSA و همچنین فرآیندی که در آن این کار را انجام دادند، توضیح می‌دهد.

این در حالی است که در این مقاله هیچ اشاره‌ای به تلاش برای شکستن رمزگذاری AES نشده است. ضمن اینکه هیچ اشاره‌ای به رمزشکنی در سطح نظامی نیز نشده است.

همانطور که در خبر اصلی از کلمه «ادعا» استفاده شده بود، اکنون مشخص شده که این تنها یک ادعا بوده و محققان چینی حداقل هنوز موفق به شکستن رمزگذاری کوانتومی در سطح نظامی نشده‌اند.

رمزگذاری RSA رمزگذاری استانداردی است که ما روزانه هر بار که ایمیل خود را بررسی می‌کنیم یا در اینترنت می‌چرخیم، در واقع از آن استفاده می‌کنیم. در این روش رمزگذاری یک کلید عمومی و یک کلید خصوصی وجود دارد و آنها از نظر ریاضی از طریق یک عدد بسیار بلند به هم مرتبط هستند که تجزیه آنها به عوامل اولیه خود و شکستن رمز آنها بدون کلید بسیار دشوار است.

ما چندین دهه است که از RSA استفاده می‌کنیم. علاوه بر این، هنگامی که به وای-فای متصل می‌شویم، دستگاه‌های ما معمولاً از رمزگذاری آی ای اس(AES ۱۲۸ یا ۲۵۶ بیتی استفاده می‌کنند.

بله، محققان چینی توانسته‌اند یک کلید رمزگذاری ۵۰ بیتی را با استفاده از رایانه‌های کوانتومی هک کنند، اما در رمزگذاری امروزی از رمزگذاری RSA از نوع ۲۰۴۸ بیتی استفاده می‌شود که رمزگشایی آن به طور تصاعدی دشوارتر می‌شود. این یعنی یک رشته عدد مانند ۱ با ۶۰۱ صفر در پی آن که حتی یک نام رسمی برای توصیف چنین عددی وجود ندارد.

برای توصیف دشواری این کار باید گفت که در سال ۲۰۱۰ گروهی از محققان از سراسر جهان پس از دو سال و نیم کار متوالی بر روی صدها رایانه که به طور شبانه‌روزی کار می‌کردند، توانستند یک کلید ۷۶۸ بیتی را بشکنند.

همانطور که پیشتر ذکر شد، این مقاله حاوی هیچ اشاره‌ای به تلاش برای شکستن رمزگذاری AES نیست.

گفتنی است که «رمزگذاری سطح نظامی» معادل یک کلید آراس‌آ(۱۵ (RSA هزار و ۳۶۰ بیتی است.