هک کوانتومی و آینده فاجعه بار امنیت در دنیای تکنولوژی - دیجیاتو

شایان ضیایی | یکشنبه، ۲۹ بهمن ۱۳۹۶

اطلاعات شما شاید در حال حاضر از حملات کوانتومی در امان باشد، اما احتمالاً زمان آن فرا رسیده تا برای وقتی که کامپیوترهای کوانتومی از قابلیت دور زدن مکانیزم های رمزگذاری های امروزی بهره مند می شوند آماده باشیم.

در حال حاضر، رمزگذاری بسیاری از اطلاعات براساس رمزنگاری با کلیدهای عمومی انجام می شود که بر قاعده ساده ای متکی هستند: چند مسئله ریاضی مثل فاکتور کردن اعداد بزرگ در اعداد اول که کاری سخت برای کامپیوترهای معمولی به حساب می آید. اما نوعی الگوریتم متفاوت به نام «الگوریتم شور» (Shor) وجود دارد که با کمک یک کامپیوتر کوانتومی، این محاسبات را به راحتی انجام می دهد.

بنابراین طبیعی است که محققان حالا به دنبال راه هایی باشند تا بتوانند استراتژی های رمزنگاری امروزی بر اساس کلیدهای عمومی را از حملات کوانتومی مصون نگه دارند. لیلی چِن، ریاضی‌دان و مدیر انستیتو ملی استانداردها و تکنولوژی های رمزنگاری می گوید: «برای رمزنگاری با کلیدهای عمومی، خسارت وارده از سوی کامپیوترهای کوانتومی مصیبت بار خواهد بود. ما باید به دنبال مقاومت کوانتومی برای این سیستم های رمزگشایی باشیم.»

کامپیوترهای کوانتومی، پردازنده هایی هستند که بر اساس قوانین مکانیک کوانتومی با یکدیگر تعامل دارند. اگرچه این تکنولوژی هنوز در ابتدای مسیر است اما کامپیوترهای کوانتومی پتانسیل های فراوانی برای حل مشکلاتی دارند که کامپیوترهای کلاسیک قادر به حل شان نیستند. پردازش بر اساس الگوریتم شور ممکن است زودتر از هر راهکار دیگری از راه برسد؛ اما آمادگی برای دورنمای پسا-کوانتومی نیازمند کارهای بیشتر نسبت به دانلود صرف یک پچ است.

چن می گوید «در نسل پیش، تقریباً 20 سال طول کشید تا کلیدهای عمومی رمزنگاری برای استفاده مردم منتشر شوند. می توانیم از این هم بهتر کار کنیم، اما در هر صورت مدتی زمان می برد.» انستیتوی مورد اشاره قصد دارد استانداردهای کوانتومی را در آینده نزدیک جایگزین استانداردهای فعلی کند.

بعد از یک فراخوان عمومی، آنها 69 الگوریتم دریافت کردند که می توانند در برابر حملات

کوانتومی مقاوم باشند. حالا کافی است تمام آنها در برابر حملات کلاسیک و کوانتومی مقاومت سنجی شوند و امید است تا سال 2022 الی 2023 میلادی، پی سی های معمولی از این حملات مصون باشند.

دیجیاتو