چهار شنبه 10 بهمن 1403 - 10:35

اولین سخت افزار ایمن جهان در برابر تهدیدات کوانتومی

شرکت سوئیسی SEALSQ اولین سخت افزار ایمن جهان در برابر تهدیدات کوانتومی را راه‌اندازی کرده است ...

شرکت سوئیسی SEALSQ اولین سخت افزار ایمن جهان در برابر تهدیدات کوانتومی را راه اندازی کرده است که بر خلاف بسیاری از سیستم های آسیب پذیر امروزی، رمزگذاری آن آن قدر قوی است که می تواند در برابر حملات رایانه های فعلی و کوانتومی مقاومت کند.

به گزارش ایسنا، شرکت SEALSQ که یک شرکت سوئیسی فعال در زمینه نیمه رساناهاست، با رونمایی از اولین سخت افزار مقاوم در برابر تهدیدات کوانتومی جهان موسوم به QS7001، در زمینه رمزنگاری کوانتومی پیشتاز است.

این شرکت سوئیسی در راه حل های یکپارچه با استفاده از نیمه رساناها و خدمات تامین تخصص دارد و در عین حال سخت افزار و نرم افزار فناوری پسا کوانتومی را توسعه می دهد.

معیارهای KYBER و DILITHIUM برای امنیت انرژی کارآمد

امروزه اغلب رمزگذاری ها مانند قفلی عمل می کنند که رایانه های کوانتومی آینده می توانند آن را بشکنند. فناوری جدید SEALSQ یک قفل به اندازه کافی قوی ایجاد می کند که در برابر حملات رایانه های فعلی و کوانتومی مقاومت کند. این بسیار مهم است، زیرا رایانه های کوانتومی در نهایت می توانند سیستم های امن امروزی را مختل کنند و داده های حساس و تراکنش های مالی را در معرض خطر قرار دهند.

این پلتفرم برای رمزنگاری مقاوم در برابر حملات کوانتومی ساخته شده است و استانداردهای FIPS و معیارهای مشترک را برآورده می کند. این پلتفرم، الگوریتم های KYBER و DILITHIUM را نشان می دهد و بازده انرژی و زمان آنها را با ریزکنترل کننده های ایمن سنتی مقایسه می کند.

شرکت SEALSQ اشاره کرد که پلتفرم QS7001 که برای هوش مصنوعی، بلاک چین و اینترنت اشیاء طراحی شده است، در برابر تهدیدات کوانتومی محافظت ایجاد می کند.

این شرکت در بیانیه ای اعلام کرد: این پلتفرم با احراز هویت، نشانه گذاری و رمزگذاری کارآمد داده ها و در عین حال پایبندی به گواهی های سختگیرانه مانند FIPS و معیارهای مشترک، استاندارد جدیدی را برای تراکنش های ایمن در عصر کوانتومی تعیین می کند.

این فناوری همچنین تعهد شرکت SEALSQ را به پیشرفت فناوری مقاوم در برابر تهدیدات کوانتومی نشان داد و نیاز روزافزون به راه حل های ایمن در عصر محاسبات کوانتومی را برطرف کرد. پلتفرم QS7001 سطح جدیدی از امنیت را معرفی می کند که برای مقاومت در برابر ابررایانه های آینده طراحی شده است و دسته جدیدی را در بازار امنیت سخت افزاری 7.9 میلیارد دلاری ایجاد می کند.

علاوه بر این، شرکت SEALSQ دارای دو مزیت حیاتی در رقابت برای راه حل های مقاوم در برابر تهدیدات کوانتومی است. به عنوان یک شرکت اولیه در این بازار که به سرعت در حال رشد است، از مزیت حرکت اول بهره می برد و خود را جلوتر از رقبا قرار می دهد. علاوه بر این، پلتفرم آن از ریزکنترل کننده های ایمن سنتی بهتر عمل می کند و امنیت و کارایی انرژی برتر را ارائه می دهد که فاکتورهایی کلیدی برای صنایعی هستند که به دنبال راه حل های پیشرفته و پایدار هستند.

این شرکت می افزاید: پیشرفت سریع محاسبات کوانتومی زمینه هایی مانند هوش مصنوعی و بلاک چین را متحول می کند، اما همچنین آسیب پذیری هایی را در سیستم های رمزنگاری فعلی از جمله الگوریتم های RSA که از میلیون ها تراکنش روزانه محافظت می کند، آشکار می کند.

یک فناوری چشمگیر، اما دارای موانع بر سر راه خود

رمزنگاری پسا کوانتومی یا PQC به آن دسته از روش های رمزگذاری اشاره دارد که برای مقاومت در برابر حملات رایانه های کوانتومی ساخته شده اند. افزایش قدرت محاسباتی کوانتومی ممکن است بتواند سیستم های رمزنگاری فعلی مانند RSA و ECC را که برای محافظت از داده های حساس استفاده می شوند، از بین ببرد.

در حالی که این دستاورد، یک فناوری قابل توجه است، پذیرش گسترده آن با چالش های متعددی روبروست. این چالش ها شامل سرعت انتقال صنعت به استانداردهای مقاوم در برابر تهدیدات کوانتومی است. علاوه بر این، عواملی مانند هزینه و مقیاس پذیری نقش مهمی در تعیین موفقیت این فناوری ها خواهند داشت.

در نهایت، رقابت از سوی بازیگران شناخته شده در صنعت نیمه رساناها می تواند بر اتخاذ راه حل های جدید تأثیر بگذارد.

توسعه یک پلتفرم مقاوم در برابر تهدیدات کوانتومی توسط شرکت SEALSQ نشان دهنده گام مهمی در جهت ایمن سازی سیستم های حیاتی در عصر محاسبات کوانتومی است. تکامل مداوم این زمینه مستلزم تحقیق و توسعه مداوم برای اطمینان از اقدامات امنیتی قوی است که می تواند به طور موثر از داده ها محافظت کند.