یکشنبه 24 اردیبهشت 1402 - 07:11

انقلاب در امنیت اطلاعات با فناوری کوانتومی

شرکت آی‌بی‌ام می‌گوید با جدیدترین فناوری‌های کوانتومی ایمن که آسیب‌پذیری بالقوه الگوریتم‌های رمزنگاری فعلی را در برابر حملات کوانتومی برطرف می‌کند، امنیت داده‌ها را متحول می‌کند.

شرکت آی بی ام می گوید با جدیدترین فناوری های کوانتومی ایمن که آسیب پذیری بالقوه الگوریتم های رمزنگاری فعلی را در برابر حملات کوانتومی برطرف می کند، امنیت داده ها را متحول می کند.

به گزارش ایسنا و به نقل از آی ای، فناوری کوانتومی ایمن دقیقا چیست و چرا مهم است؟ برای درک این موضوع باید یک قدم به عقب برگردیم و محاسبات کوانتومی را بررسی کنیم.

رایانه های کوانتومی برخلاف رایانه های سنتی که اطلاعات را با استفاده از ارقام یا بیت های باینری ذخیره و پردازش می کنند، از بیت ها یا کیوبیت های کوانتومی استفاده می کنند که می توانند در چندین حالت به طور همزمان وجود داشته باشند. این به رایانه های کوانتومی اجازه می دهد تا وظایف خاصی مانند فاکتورگیری اعداد بزرگ را بسیار سریع تر از رایانه های سنتی انجام دهند.

با این حال، این بدان معناست که برخی از الگوریتم های رمزنگاری مانند RSA و ECC که در حال حاضر برای ایمن سازی داده ها استفاده می شوند، می توانند توسط رایانه های کوانتومی شکسته شوند. اینجاست که فناوری کوانتومی ایمن وارد می شود.

فناوری کوانتومی ایمن مجموعه ای از الگوریتم های رمزنگاری است که در برابر حملات رایانه های کوانتومی مقاوم هستند. این فناوری تضمین می کند که اطلاعات و داده ها در دنیای پسا کوانتومی ایمن باقی می مانند.

به تازگی شرکت آی بی ام(IBM) در کنفرانس سالانه Think که در فلوریدا برگزار شد، از «فناوری کوانتومی ایمن انتها به انتها» خود رونمایی کرد. فناوری کوانتومی ایمن آی بی ام فقط یک الگوریتم یا یک ابزار نیست، بلکه مجموعه ای جامع از ابزارها و قابلیت هایی است که می تواند توسط سازمان ها برای ایمن سازی داده های خود استفاده شود. این فناوری شامل رمزنگاری ایمن کوانتومی است که از الگوریتم هایی مانند رمزنگاری مبتنی بر شبکه و رمزنگاری مبتنی بر هَش و همچنین پروتکل های تبادل کلید پسا کوانتومی استفاده می کند.

چه چیزی فناوری کوانتومی ایمن آی بی ام را متمایز می کند؟

چیزی که فناوری کوانتومی ایمن شرکت آی بی ام را متمایز می کند، فقط خود این فناوری نیست، بلکه تخصص عمیق این شرکت در زمینه امنیت است.

آی بی ام بیش از یک دهه است که روی رمزنگاری ایمن کوانتومی کار می کند و به توسعه بسیاری از الگوریتم هایی که اکنون ایمن-کوانتومی تلقی می شوند کمک کرده است. این بدان معنی است که مفهوم ایمن-کوانتومی آی بی ام فقط یک مفهوم تئوری نیست، بلکه یک راه حل عملی است که در سناریوهای دنیای واقعی آزمایش و تأیید شده است.

این امر به ویژه برای سازمان های دولتی و مشاغلی که برخی از با ارزش ترین و حساس ترین داده ها را مدیریت می کنند، بسیار مهم است. در دنیای پسا کوانتومی، اگر اطلاعات با فناوری کوانتومی ایمن محافظت نشود، امنیت این داده ها به خطر می افتد.

فناوری کوانتومی ایمن آی بی ام راهی را برای این سازمان ها فراهم می کند تا امنیت خود را در آینده تثبیت کنند و اطمینان حاصل کنند که داده های آنها حتی در مواجهه با پیشرفت های محاسبات کوانتومی همچنان امن باقی می مانند.

معرفی فناوری کوانتومی ایمن آی بی ام هیجان زیادی را در صنعت فناوری ایجاد کرده است. با پیشرفت محاسبات کوانتومی، نیاز به فناوری کوانتومی ایمن افزایش خواهد یافت و این راهکار آی بی ام یک راه حل عملی برای این مشکل ارائه می دهد و پتانسیل تبدیل شدن به یک استاندارد صنعتی برای رمزنگاری پسا کوانتومی را دارد.

جینی رومِتی مدیرعامل آی بی ام در سخنرانی خود در کنفرانس Think بر اهمیت فناوری کوانتومی ایمن در تضمین امنیت داده ها تأکید کرد و گفت: ما در یک نقطه عطف در صنعت خود هستیم. ما باید اطمینان حاصل کنیم که داده هایمان در دنیای پسا کوانتومی امن باقی می مانند. به همین دلیل است که ما IBM Quantum Safe را برای ارائه راه حلی کاربردی و جامع که می تواند توسط سازمان ها در هر اندازه و در همه صنایع مورد استفاده قرار گیرد، توسعه داده ایم.

کارشناسان می گویند فناوری جدید آی بی ام با تخصص عمیق این شرکت در حوزه امنیت و تعهد آن به توسعه راه حل های عملی، این پتانسیل را دارد که به استانداردی طلایی برای فناوری کوانتومی ایمن تبدیل شود.