واشنطن تطور حاسوبا يستطيع اختراق كل أنواع التشفير

كتبه نون بوست | 3 يناير ,2014

كشفت صحيفة واشنطن بوست الأمريكية عن أن وكالة الأمن القومي الأمريكية تعمل -في مسعى آخر لاختراق خصوصية المواطنين عبر العالم- على بناء جهاز كمبيوتر جديد يتمكن من فك واختراق "جُل" أنواع التشفير المستخدمة على الإنترنت حاليا.

وأضافت الصحيفة أن الجهاز المراد تطويره يعرف باسم "الحاسوب الكمي" Quantum Computer.

ووفق وثائق العميل إدوارد سنودن المسربة فإن هذا الحاسوب المطور سيكون قادرا على فك جميع رموز التشفير التي تحمي المعلومات السرية المتعلقة بالأسرار المصرفية والطبية والعلمية والمعلومات الحكومية، وحتى تلك المتعلقة ببرامج التجسس لدول أخرى.

لكن ما الذي يميز الكمبيوتر الكمي عن الأجهزة التقليدية التي يستخدمها الناس عبر العالم؟

بحسب الفيديو المنشور (باللغة الإنجليزية فقط) على موقع يوتيوب، والذي ضمنته واشنطن بوست في تقريرها، فإن أجهزة الكوانتم (الكمية) يمكنها التعامل مع العمليات الحسابية بشكل مختلف تماما عن الأجهزة الكلاسيكية أو التقليدية.

باختصار -قد يكون مخلا- فإن الكمبيوتر التقليدي يعتمد في بناء بياناته على النظام الثنائي Binary System ما يعني أن كل وحدة بيانات bit يستخدمها الحاسوب ستكون إما صفر أو واحد 0,1 لكن الأمر يختلف في حالة الكمبيوتر الكمي.

فكل البيانات في حالة الكمبيوتر الكمي يمكنها أن تمثل في حالة مختلفة عن 0,1، ولذلك ففي الكمبيوتر التقليدي، إذا أردت الوصول إلى معلومة ما تتكون من وحدتين من البيانات، فإن ما تحتاج إلى معرفته هو قيمة تلك الوحدتين، إما صفر أو واحد.

لكن في حالة الكمبيوتر الكمي فإنك ستحتاج إلى معرفة قيمة أربع وحدات من البيانات، كي تستطيع الوصول للمعلومة ذاتها.

الأمر يعني، أنه للوصول إلى معلومة ما تتكون من عدد (س) من البيانات، فإنني سأحتاج لمعرفة قيم 2 أس (س)، فمثلا اذا احتجت أن تعرف قيمة معلومة تحتوي على ثلاثة وحدات بيانية، فأنت بحاجة إلى معرفة قيم ٨ وحدات بيانية وليس ثلاثة فحسب كما في حالة الكمبيوتر التقليدي، وإذا كانت المعلومة تحتوي على أربع وحدات بيانية فإن ما تحتاج إلى معرفته سيكون 2 أس 4 أي 16 وحدة بيانية.

هذا يعني من ضمن ما يعني أن الكمبيوتر الكمي يستطيع التعامل مع احتمالات أكثر وبشكل أسرع لمعرفة البيانات من هذا النوع. لأن الكمبيوتر الكمي يمكنه إنجاز حسابات أعقد كثيرا في وقت أقل كثيرا لأنه يستطيع التعامل مع الأرقام بالتوازي.

ويأتي مشروع الحاسوب الجديد ضمن مشروع أبحاث ضخم تقارب كلفته 79.7 مليون دولار ويحمل اسم "اختراق الأهداف الصعبة"

وكالة الأمن القومي ليست الأولى في إنتاج حواسيب من هذا النوع، فقد استطاعت شركة كندية أن تنتج حواسيب كمية منذ العام ٢٠٠٩، وباعت منها في العام ٢٠١٢ قطعا لشركة غوغل و لوكالة الفضاء الأمريكية ناسا بسعر يتجاوز عشرة ملايين دولار للحاسوب الواحد.

ويقول عالم الحاسوب تيموثي بي لي من معهد ماساتشوستس للتكنولوجيا أن إنتاج وحدات بيانية للعمل على كمبيوتر كمي ستكون عملية شاقة للغاية يستبعد حدوثها قريبا، كما يؤكد أن المجتمع العلمي يشكك في إمكانية الشركة الكندية على إنتاج حواسيب من هذا النوع

لكن بحسب الوثائق فإن المرحلة التي بلغتها أبحاث وكالة الأمن القومي تُعتبر متقدمة للغاية بالنسبة لشركات التقنية المدنية الأخرى، أو حتى لعلماء الكمبيوتر النظريين، وتقول الوثائق إن وكالة الأمن القومي تعمل على هذا المشروع في غرف خاصة يطلق عليها "أقفاص فاراداي" وهي غرف معزولة محمية من جميع أنواع التلوث الكهرومغناطيسي الآتية من الخارج.

وبعيدا عن فضيحة التجسس، فإن الحواسيب الكمية لا يُتوقع مستقبلا أن تحل محل الحواسيب

التقليدية، لأن الحواسيب الكمية، وإن كانت قادرة على إنجاز عمليات حسابية معينة بشكل أسرع، إلا أنها في الاحتياجات الخطية التقليدية للمستخدمين (مثل مشاهدة فيديو أو كتابة مستند أو تصفح الإنترنت) قد تكون أبطأ من الحواسيب التي نستخدمها جميعا، لأنها تفترض وجود البيانات في احتمالات كثيرة مختلفة بشكل يجعل الحواسيب التقليدية أكثر سلاسة وسرعة.

رابط المقال : https://www.noonpost.com/1430/