الحواسيب الكمية والمخابرات: خنجر في اليد، أم في الظهر؟

كتبه فريق التحرير | 5 مارس ,2016

في 2014 سرب الموظف السابق في الاستخبارات الأمريكية "إدوارد سنودين" وثائق سرية، كشفت للعالم خطة تجسس لوكالة الأمن القومي، التي خصصت ما يقرب من 80 مليون دولار لبناء حاسوب كمومي، يهدف إلى اختراق أي نوع من التشفيرات على الإنترنت، تلك التي تحمي بيانات البنوك والمستشفيات وأكثر الأهداف سرية لدى الحكومات والمؤسسات والمواطنين في كل أرجاء العالم، وقد أطلقت على مشروعها اسم "اختراق الأهداف الصعبة".

لا بد أن هذا جعلك تشعر بالقلق على رسائلك الخاصة الموجودة في صندوق واردك الآن، وهذا حقك، فهذا المشروع يشبه مشروع "مانهاتن"، الذي جرى منذ 75 عامًا عندما كانت دول العالم تتسابق للحصول على القنابل الذرية، لكن السلاح الذي يسعى الجميع له هذه المرة هو "الحاسوب الكمي" أو الكمومي Quantum Computer.

تعرية العالم: الحواسيب الكمية خطة تنصت المخابرات القادمة

الكمبيوتر التقليدي الذي تقوم باستخدامه الآن يستخدم الثنائيات أو "البتات"، والتي تخزن في شكل واحد أو صفر، أما حواسيب الكوانتم فإنها تستخدم وحدة تخزينية مختلفة للبيانات تسمى "الكيوبيت"، والذي يعتمد على فكرة غاية في السحرية والغموض تسمى "التراكب الكمي"، الذي يسمح له بالتواجد في عدة حالات في نفس الوقت، مثل أن يكون صفرًا وواحد في نفس الوقت،

ولذلك، فإن الحواسيب الكلاسيكية قادرة على ممارسة عملية حسابية واحدة فقط في اللحظة، أما الحواسيب الكمومية فإن خواصها الغريبة وغير المفهومة حتى الآن، تسمح لها بإجراء عدة عمليات متوازية في نفس الوقت.

في كل مرة تدخل على موقع إنترنت يبدأ عنوانه بـ "HTTPS"، فإن البيانات التي تقوم بإرسالها أو استقبالها تكون مشفرة بمفتاح تشفيري عام، وهو الشيء الذي كان اختراعًا ثوريًا في السبعينات، فقبل ذلك، كان التشفير شيئًا حصريًا للجواسيس والحكومات.

الحاسوب الكمي قادر على اختراق أقوى أساليب التشفير العام الحالية، مثل خوارزمية التشفير RSA، التي يعتمد أمانها على طولها البالغ بسبب عدم وجود خوارزميات حتى الآن قادرة على تحليل عدة عوامل بسرعة عالية، فصحيح أنه في 2009 استطاعت الوسائل الكلاسيكية أن تفك شفرة خوارزمية RSA مكونة من 768 بت، لكنك ستتفاجأ عندما تعرف أن هذا استغرق سنتين متواصلتين ومئات من الحواسيب، أما كسر شفرة تصل بطولها إلى 1024 بت، وهو الرقم التقليدي للمعاملات التجارية على الإنترنت، فإن هذا سيستغرق وقتًا أطول بألف مرة، الحواسيب الكمية قادرة على فك هذه الشفرة أسرع بكثير، اعتمادًا على قدرة أدائها للعمليات بشكل متوازٍ.

الوثيقة المسربة ذكرت بالنص: "إن تطبيق التكنولوجيا الكمية على خوارزميات التشفير يهدد بتأثيرات دراماتيكية على قدرات الحكومة الأمريكية على كلٍ من حماية اتصالاتها، والتنصت على اتصالات الحكومات الأجنبية".

الاستخبارات الأمريكية في قلق من وصول أحد قبلها لهذه التكنولوجيا، وهو ما أعربت عنه في الوثائق المسربة عندما ذكرت منافسي الولايات المتحدة في الوصول إلى الحواسيب الكمومية مثل الاتحاد الأوروبي وسويسرا، هذا التسريب هو لكمة في وجه الشركة الكندية التي قامت ببيع أنظمة حاسوب كمومية أولية لجوجل وناسا، تسمى "دي ويف"، فمع أن الشركة تقر أنها لا تبيع أجهزة حاسوب كمومية كاملة الوظيفة، وأنها غير قادرة على فك التشفيرات، إلا إنها استطاعت أداء عمليات حسابية بسرعة كمومية في مجموعة متنوعة من المهام الحاسوبية.

هناك تحديان صعبان في بناء الحواسيب الكمومية، الأول هو طبيعتها بالغة الهشاشة لأنها تتكون من ذرات مفردة وفوتونات وإلكترونات، ولذلك، فإنك إذا فشلت في حمايتها من البيئة المحيطة فإنها سوف تكون بلا قيمة، أما الثاني، والأكثر صعوبة على الإطلاق، فهو رفع عدد "الكيوبيتات" التي تكون هذا الحاسوب.

الخبراء يقولون إن العقبة الأعظم أمام كسر التشفير بحاسوب كمومي هو في بناء حاسوب به عدد كافٍ من الكيوبيتات، بسبب هشاشة وضعها المعروفة، لكن الوكالة نجحت بالفعل في الحصول على بعض الكيوبيتات، والتي وصفتها الوثيقة المسربة بأنها "سيطرة كمومية كاملة على اثنتين من كيوبيتات مصنوعة من أشباه الموصلات"، وهي خطوة عظيمة، لكنها ما تزال خطوة صغيرة على الطريق نحو بناء حاسوب كمومي ضخم.

وكالة الأمن القومي تحارب للوصول إلى ذلك، لكن، بحسب وثائق سنودين، فإن الوكالة هي أبعد ما تكون عن تحقيقه، كل الملايين المذكورة تستخدم للتجربة واختبار ما إن كان بالإمكان بناء نظام قائم على "خوارزمية شور" الرياضية الشهيرة للتحليل الكوانتي لعديدات الحدود، وليس هناك أي ذكر عن وجود خوارزمية كوانتية لفك الشفرات.

خنجر في اليد أم في الظهر؟

في أغسطس 2015، أعلنت وكالة الأمن القومي الأمريكية في صفحة غامضة على موقعها الإلكتروني أن خوارزميات التشفير، التي أنفقت عقدًا من الزمان وهي تقول للعالم إنها أفضل تشفير للمعلومات السرية، أصبحت غير آمنة الآن، هذا يعني أن عليها أن تبحث عن تشفيرات جديدة، والسبب هو شيء واحد: الحواسيب الكمومية.

الوكالة قالت إن عليها أن "تتصرف الآن" في ظل التقدم الحاصل في سباق الحواسيب الكمومية، لكن إليك الفكرة، لا أحد حتى الآن يعرف كيف يستطيع بناء تشفير مضاد للحواسيب الكمومية، كل ما استطاعت وكالة الأمن القومي فعله هو إخبار الشركات التي تبني الأنظمة الجديدة أن تستخدم خوارزميات معينة، وأن تبحث وضع معايير جديدة مع المعهد الوطني للمعايير والتكنولوجيا، يعتقد أنها سوف تنجو في عصر "ما بعد الكوانتم".

الحواسيب الكمومية التي تستخدم "خوارزمية شور"، قادرة على معرفة الأرقام الأولية المكونة للشفرة العامة واسعة الانتشار RSA، كما سبق وذكرنا، كما أنها قادرة على كسر نظام ترميز ديفي – هيلمان، ونظم المنحنيات الإهليلجية، وهو الشيء الذي يجعل معظم مفاتيح ترميز العصر الحديث غير آمنة.

ومع أن الحديث مبكر عن الحواسيب الكمومية العملية القادرة على الاختراق، إلا أن بداية هذا العصر لن تعني موت تكنولوجيا التشفير الحالية بشكل كلي، فهناك أساليب ترميز عامة أقل شهرة بين الجمهور من التي نستخدمها الآن، مثل ماك ليس، والخوارزميات القائمة على التشابكات، ومع أنها أقل فعالية من تلك التي نستخدمها الآن، إلا أنها الآن آمنة – كما يُعتقد – ضد الحواسيب الكمومية.

الصيغة التي يُعتَقد أنها سوف تكون الملجأ الأفضل للتشفير، قائمة على رياضيات "التشابكات"، المكونة من شبكات من نقاط متكررة متعددة الأبعاد، وهذه الشفرة تعتمد في قوتها، على صعوبة إيجاد المعلومات المخبأة في شبكة مكونة من مئات الأبعاد المكانية، إلا إذا كنت تعرف الطريق السري.

إدارة أمن المعلومات التابعة لوكالة الأمن القومي قامت بتطوير قائمتها من المجموعة B من الخوارزميات الإهليلجية، وقد أعلنت بصراحة عن تهديد الحواسيب الكمية قائلة إنها سوف تبدأ الانتقال إلى خوارزميات مقاومة للحواسيب الكمومية في المستقبل غير البعيد، مضيفة أنها تعمل مع شركائها في جميع أنحاء الدولة، بالإضافة إلى هيئات المعايير، كي تتأكد من وجود خطة واضحة للوصول إلى مجموعة جديدة من الخوارزميات مطورة بطريقة منفتحة وشفافة، لتكوّن الأساس

للجيل الجديد من خوارزميات التشفير.

"المجموعة B"، هي عائلة من خوارزميات التشفير المعتمدة من قبل وكالة الأمن القومي الأمريكية، وهي جزء من برنامج تحديث التشفير في الوكالة، ومع أن خوارزميات الوكالة تكون في العادة غير قابلة للاستخدام إلا في أجهزة مبنية بشكل خاص، إلا أن المجموعة B، عامة، ويمكن استخدامها في أي شيء، هذا لا يعني أنها من الدرجة الثانية أو أنها سهلة الكسر أو أي شيء من هذا القبيل، لهذا تستخدم لحماية أسرار الولايات المتحدة بالتعاون مع المجموعة A.

نحن نعتقد أن الحواسيب الكمية القادرة على العمل بشكل حقيقي، لن تظهر قبل سنين طويلة، لكن طريقة تصرف وكالة الأمن القومي إزاء أمر الحواسيب الكمية، يجعلنا في حالة تساؤل عميق: هل هي أقرب مما نظن؟

رابط المقال : https://www.noonpost.com/10601/