الحوسبة الكمومية ونظام DNS

مكتب كبير المسؤولين الفنيين (OCTO) في ICANN

پول هوفمان

OCTO-031
11 فبراير (شباط) 2022

ICANN

قائمة المحتويات

هذه الوثيقة جزء من سلسلة وثائق مكتب كبير المسؤولين الفنيين (OCTO) في ICANN. يرجى الاطلاع على صفحة إصدارات مكتب المدير الفني المسؤول OCTO للاطلاع على قائمة الوثائق في سلسلة الإصدارات. إذا كانت لديك أسئلة أو مقترحات حول أي من هذه المستندات، يرجى إرسالها إلى octo@icann.org.

تدعم هذه الوثيقة هدف ICANN الاستراتيجي المتمثل في تحسين مستوى المسؤولية المشتركة لدعم أمن واستقرار نظام أسماء النطاقات (DNS) من خلال تعزيز تنسيق نظام اسم النطاق DNS بالشراكة مع أصحاب المصلحة المعنيين. يعد تعزيز أمن نظام أسماء النطاقات ونظام خادم الجذر (RSS) لنظام أسماء النطاقات جزءًا ضمن هدف ICANN الاستراتيجي.

الملخص التنفيذي

لقد جذبت أجهزة الكمبيوتر الكمومية انتباه المجتمع الأمني في السنوات الأخيرة نظرًا لاحتمالية تمكنها من تقويض خوارزميات التشفير المشهورة حاليًا.

وفي الوقت الحالي، لا توجد أجهزة كمبيوتر كمومية تتسم بالقوة الكافية بما يُمكّنها من أداء هذه المهمة، ولكن مع التحسن البطيء للتكنولوجيا، قد يأتي اليوم الذي يمكن فيه كسر بعض الخوارزميات المستخدمة في هذه الآونة بسهولة باستخدام هذا النوع الجديد من أجهزة الكمبيوتر.

ومع ذلك، وبما أن تكنولوجيا الحوسبة الكمومية لا تزال جديدة ونظرًا لكون عمليات بناء أجهزة الكمبيوتر الكمومية وتشغيلها مكلفة للغاية، فمن الصعوبة بمكان التكهن بالوقت الذي قد يأتي فيه ذلك اليوم في المستقبل القريب.

ويجري حاليًا توحيد الخوارزميات الجديدة التي يُفترض أنها منيعة على أجهزة الكمبيوتر الكمومية وغير ملاءمة لها. تدرس هذه الورقة العمل الأخير الذي يعرض تقديرات أفضل بشأن الوقت الذي يتعين فيه على مجتمع نظام أسماء النطاقات (DNS) التفكير في التحول من خوارزميات التشفير الحالية إلى خوارزميات التشفير الجديدة.

1 مقدمة

هناك بعض الخوارزميات في التشفير الحديث تعتمد على صعوبة بعض المسائل الرياضية التي تستغرق وقتًا طويلاً لحلها. وقد تكون لدى أجهزة الكمبيوتر الكمومية القدرة على حل هذه المشكلات بشكلٍ أسرع، وهو ما سيؤدي بعد ذلك إلى إضعاف الضمانات التي تقدمها تلك الخوارزميات. وتختلف أجهزة الكمبيوتر القائمة على المبادئ الكمومية بشكلٍ جوهري عن تلك التي أُستخدمت على نطاق واسع خلال السنوات الـ 70 الماضية. حيث تعتمد معالجة البيانات على أجهزة الكمبيوتر الكمومية على وحدات البت الكمومية، التي تُسمى *"كيوبت أو البت الكمومي"* ، وليس وحدات البت الثنائية التي تستخدمها جميع أجهزة الكمبيوتر في الوقت الراهن.

إذا كان يمكن بناء أجهزة كمبيوتر كمومية كبيرة الحجم، فقد يكون لديها القدرة على حل بعض المشكلات المستحيل حلها من خلال تكنولوجيا الحوسبة الحالية حيث تتميز أجهزة الكمبيوتر الكمومية بالقدرة على التعامل مع العديد من العمليات المعقدة في نفس الوقت. وبرغم إمكانية أجهزة الكمبيوتر الحالية، التي يُطلق عليها *أجهزة الكمبيوتر الكلاسيكية*، من التعامل مع العمليات المتوازية، غير أن أجهزة الكمبيوتر الكمومية يمكنها أداء هذه المهمة باستخدام روابط أكثر إحكامًا بين أجزاء البيانات التي يجري تحليلها.

لقد ظل العمل على وضع النظريات المتعلقة بالمفاهيم الكامنة وراء أجهزة الكمبيوتر الكمومية طوال مدة تقارب 50 عامًا، ورغم ذلك يصعب للغاية بناء أجهزة كمبيوتر كمومية صغيرة للغاية. وتعتبر المعلومات الموجودة في وحدات البت الكمومي (الكيوبت) هشة للغاية، لذا يجب عزل وحدات الكيوبت تمامًا عن البيئة الخارجية عن طريق إبقائها في درجات حرارة قريبة من صفر درجة كلفن أثناء العمليات الحسابية؛ ويقتضي القيام بذلك توافر الكثير من الآلات والمساحة المادية اللازمة. ومع ذلك، تعتبر وحدات الكيوبت معرضة بشكلٍ كبير للأخطاء أثناء عملية المعالجة. علاوة على ذلك، يتطلب الكمبيوتر الكمومي إلى المئات أو الآلاف من وحدات الكيوبت المبردة الإضافية حتى يمكنه تصحيح الأخطاء لكل وحدة كيوبت مستخدمة في العملية الحسابية؛ وقد يكون صنع جهاز كمبيوتر كمومي ينطوي على الملايين من وحدات الكيوبت أمرًا مستحيلاً بالنظر إلى المتطلبات المتعلقة بالتبريد والاتصال.