|  |  |  |  |
| --- | --- | --- | --- |
|  | الجمعية العالمية لتقييس الاتصالات (WTSA-24)  نيودلهي، 24-15 أكتوبر 2024 | |  |
|  | |  | |
|  | |  | |
| الجلسة العامة | | ‏الإضافة 42 ‏للوثيقة ‎37-A‏ | |
|  | | 22 سبتمبر 2024 | |
|  | | الأصل: بالإنكليزية | |
|  | | | |
| إدارات أعضاء جماعة آسيا والمحيط الهادئ للاتصالات | | | |
| مشروع قرار جديد [APT-PQC] – تعزيز تنفيذ التجفير ما بعد  الحوسبة الكمومية والانتقال إليه | | | |
|  | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **ملخص:** | تتضمن هذه الوثيقة مقترحاً بخصوص قرار جديد للجمعية العالمية لتقييس الاتصالات بشأن تعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه. | |
| **للاتصال:** | السيد Masanori Kondo الأمين العام لجماعة آسيا والمحيط الهادئ للاتصالات | البريد الإلكتروني: [aptwtsa@apt.int](mailto:aptwtsa@apt.int) |

مقدمة

تُعدّ خوارزميات التجفير ركائز أساسية للشبكات لبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.

وبمجرد أن يُتاح النفاذ إلى الحواسيب الكمومية ذات الصلة بالتجفير، فإن معظم خوارزميات المفاتيح العمومية القائمة والبروتوكولات المرتبطة بها ستكون عرضة للهجمات القائمة على الحواسيب الكمومية. ويأتي التهديد الكمومي من الحواسيب الكمومية التي تتميز بقوتها الحسابية الاستثنائية، والتي لديها القدرة على كسر خوارزميات التجفير المستخدمة على نطاق واسع، بما في ذلك RSA وECC (تجفير المنحنى الإهليلجي). ويجري حالياً تطوير مجموعة من خوارزميات التجفير، يُشار إليها باسم التجفير ما بعد الحوسبة الكمومية (PQC) والتي يُعتقد أنها "آمنة من حيث الحوسبة الكمومية" أو "مقاومة للحوسبة الكمومية"، مما يعني أنه من المتوقع أن تظل آمنة حتى في وجود حواسيب كمومية ذات صلة بالتجفير.

ويعترف القرار بتعريف لجنة الدراسات 17 لمصطلح التجفير ما بعد الحوسبة الكمومية، والذي يُشير إلى الخوارزميات الكلاسيكية المقاومة للحوسبة الكمومية.

وفي الوقت الحالي، تعتمد البنية التحتية الموثوقة لشبكات الاتصالات على خوارزميات التجفير التقليدية مثل ديفي-هيلمان وRSA، والتي تكون عرضة للتهديدات الكمومية. لذلك، يصبح انتقال شبكات تكنولوجيا المعلومات والاتصالات إلى بنية تحتية موثوقة ومقاومة للحوسبة الكمومية أمراً بالغ الأهمية قبل ظهور الحواسيب الكمومية.

ورغم أن التجفير ما بعد الحوسبة الكمومية يستفيد من البنية التحتية الحالية ويقدم حلاً فعّالاً من حيث التكلفة وراسخاً وآمناً من حيث الحوسبة الكمومية، فإن الأمر يستغرق وقتاً وموارد كبيرة حتى تتمكن المنظمات من الانتقال بالكامل إلى التجفير ما بعد الحوسبة الكمومية.

وفي ضوء ذلك، هناك حاجة ملحة إلى أن تتولى لجان دراسات قطاع تقييس الاتصالات أعمال التقييس بنشاط لتعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات.

وبالإضافة إلى ذلك، فإن لجنة الدراسات 17 لقطاع تقييس الاتصالات قد وافقت، خلال أعمالها التحضيرية للجمعية العالمية لتقييس الاتصالات لعام 2024، على أن يكون "استخدام التجفير ما بعد الحوسبة الكمومية" ضمن المواضيع الناشئة لفترة الدراسة المقبلة (2025-2028).

المقترح

بناءً على السياق المذكور أعلاه، تقترح إدارات أعضاء جماعة آسيا والمحيط الهادئ للاتصالات أن تنظر الجمعية العالمية لتقييس الاتصالات لعام 2024 في وضع قرار جديد للجمعية بشأن تعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه.

ADD APT/37A42/1

مشروع قرار جديد [APT-PQC] (نيودلهي، 2024)

تعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه

(نيودلهي، 2024)

إن الجمعية العالمية لتقييس الاتصالات (نيودلهي، 2024)،

إذ تذكّر

*أ )* بالقرار 130 (المراجَع في بوخارست، 2022) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ب)* بالقرار 50 (المراجَع في جنيف، 2022) للجمعية العالمية لتقييس الاتصالات، بشأن الأمن السيبراني؛

*ج)* بقرار الجمعية العامة للأمم المتحدة (UNGA) 239/57، بشأن إنشاء ثقافة عالمية للأمن السيبراني؛

*د )* بقرار الجمعية العامة للأمم المتحدة 287/78، بشأن السنة الدولية لعلوم وتكنولوجيا الكم، 2025،

وإذ تضع في اعتبارها

*أ )* أهمية خوارزميات التجفير لبناء الثقة وضمان الأمن في استخدام تكنولوجيا المعلومات والاتصالات (ICT)؛

*ب)* أن ظهور تكنولوجيا الحوسبة الكمومية ذات الصلة بالتجفير من شأنه أن يعرّض العديد من خوارزميات التجفير الحالية للخطر، وخاصة تجفير المفاتيح العمومية، الذي يستخدم على نطاق واسع لحماية المعلومات الرقمية؛

*ج)* أن خوارزميات التجفير التي تعتمد عليها البنى التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات في جميع أنحاء العالم تُستخدم في مكونات العديد من أنظمة الاتصالات والمعالجة والتخزين المختلفة؛

*د )* أن معظم خوارزميات المفاتيح العمومية الحالية والبروتوكولات المرتبطة بها ستكون عرضة للهجمات القائمة على الحواسيب الكمومية، بمجرد توافر النفاذ إلى الحواسيب الكمومية ذات الصلة بالتجفير؛

*هـ )* أنه يمكن استخدام خوارزميات التجفير ما بعد الحوسبة الكمومية (PQC) في البنية التحتية القائمة والاستفادة من خبرة النظام لتنفيذ حل آمن من حيث الحوسبة الكمومية؛

*و )* أن التطبيقات النموذجية للتجفير ما بعد الحوسبة الكمومية يمكن أن تشمل جميع القطاعات مثل الاتصالات المتنقلة الدولية-2020/الاتصالات المتنقلة الدولية-2030 وتكنولوجيا سجل الحسابات الموزَّع (DLT)؛

*ز )* الحاجة إلى التعاون الدولي وتبادل المعلومات لمعالجة التهديدات الأمنية التي تشكلها الحواسيب الكمومية ذات الصلة بالتجفير؛

*ح)* أن دور الاتحاد يركز على تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه لبناء الأمن والثقة في استخدام البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات، وليس على تقييس خوارزميات أو بروتوكولات التجفير ما بعد الحوسبة الكمومية؛

*ط)* أن التجفير ما بعد الحوسبة الكمومية يمكن أن يساعد في تطوير بنية تحتية موثوقة تكون آمنة ضد الحواسيب الكمومية والكلاسيكية على حد سواء، ويمكنها التفاعل مع البروتوكولات وشبكات الاتصالات القائمة؛

*ي)* أن الانتقال من أنظمة التجفير الكلاسيكية الحالية إلى الأنظمة القائمة على التجفير ما بعد الحوسبة الكمومية والتي يمكنها مقاومة هجمات الحوسبة الكمومية، تعد مشروعاً مكلفاً وطويل الأجل. وفي الوقت الحالي، تستكشف العديد من الصناعات الرأسية حول العالم بالفعل تطبيق التجفير ما بعد الحوسبة الكمومية والانتقال إليه، ومن الضروري أن تستعد صناعة الاتصالات/تكنولوجيا المعلومات والاتصالات لهذا الاتجاه الآن؛

*ك)* أن عملية الانتقال إلى التجفير ما بعد الحوسبة الكمومية معقدة للغاية وستستغرق سنوات عديدة لإكمالها، لأنها تتطلب استبدال خوارزميات التجفير، وتحديث بروتوكولات التجفير، والمخططات والمكونات، والبنية التحتية وغيرها، بتكنولوجيات التجفير الآمنة من حيث الحوسبة الكمومية؛

*ل)* أن الانتقال إلى التجفير ما بعد الحوسبة الكمومية قد يشمل تصميم وتطوير آليات تمكن من التحديث المرن لأنظمة التجفير والتحديث التكراري لأنظمة معلومات تطبيقات التجفير من أجل تسهيل تنفيذ خوارزميات التجفير ما بعد الحوسبة الكمومية المستقبلية؛

*م )* أن تقييم أمن خوارزميات التجفير ما بعد الحوسبة الكمومية هو عمل مستمر يضطلع به (المعهد الوطني للمعايير والتكنولوجيا (NIST))،

وإذ تضع في اعتبارها كذلك

*أ )* أن التوصية ITU-T X.1811 تقدم مبادئ توجيهية تتعلق بالأمن من أجل تطبيق خوارزميات آمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية-2020، وأن التقرير التقني TR.qs-dlt يقدم مبادئ توجيهية بشأن نظام تكنولوجيا سجل الحسابات الموزَّع (DLT) الآمن من حيث الحوسبة الكمومية لتأمين هذه التكنولوجيا، بينما تقوم لجنة الدراسات 17 بإعداد تقريرين تقنيين، بما في ذلك "إرشادات حول استخدام التجفير المتقدم القائم على التجفير ما بعد الحوسبة الكمومية"؛

*ب)* أن فريق العمل ISO/IEC JTC 1/SC 27/WG 2 ومعهد معايير الاتصالات الأوروبي (ETSI) يعملان على توحيد معايير التجفير ما بعد الحوسبة الكمومية (PQC) وتبادل المعلومات حول التجفير ما بعد الحوسبة الكمومية؛

*ج)* أن مركز التميز الوطني للأمن السيبراني (NCCoE) التابع للمعهد الوطني للمعايير والتكنولوجيا شرع في تطوير ممارسات لتسهيل الانتقال من المجموعة الحالية من خوارزميات تجفير المفاتيح العمومية إلى خوارزميات بديلة مقاومة للهجمات القائمة على الحواسيب الكمومية،

وإذ تشير إلى

*أ )* أن قطاع تقييس الاتصالات ينبغي أن يؤدي دوراً رائداً في وضع المعايير لبناء الثقة وضمان الأمن في استخدام تكنولوجيا المعلومات والاتصالات؛

*ب)* أن العملية التي بدأها المعهد الوطني للمعايير والتكنولوجيا جارية لطلب وتقييم وتقييس خوارزمية أو أكثر من خوارزميات تجفير المفاتيح العمومية المقاومة للحوسبة الكمومية؛

*ج)* أن المعهد الوطني للمعايير والتكنولوجيا قد أصدر معايير لثلاث من خوارزميات التجفير ما بعد الحوسبة الكمومية؛

*د )* أن معهد معايير الاتصالات الأوروبي لديه فريق عمل معني باستخدام خوارزميات ما بعد الحوسبة الكمومية في البروتوكولات (pquip) لمعالجة قضايا هندسة التجفير ما بعد الحوسبة الكمومية والانتقال إليه والخبرة ذات الصلة بالعمل الذي يجري في معهد معايير الاتصالات الأوروبي، وتنفيذ التجفير ما بعد الحوسبة الكمومية بنشاط في بروتوكولات معهد معايير الاتصالات الأوروبي بما في ذلك أمن بروتوكول الإنترنت (IPSec) وأمن طبقة النقل (TLS) وOpenPGP؛

*هـ )* أن فريق العمل ISO/IEC JTC 1/SC 27/WG 2، "*آليات التجفير والأمن*"، يعمل على تقييس خوارزميات التجفير ما بعد الحوسبة الكمومية التي اختارها المعهد الوطني للمعايير والتكنولوجيا؛

*و )* أن فريق العمل التابع للمعهد الأوروبي لمعايير الاتصالات والمعني بالتجفير الآمن من حيث الحوسبة الكمومية (QSC) قد نشر تقريراً تقنياً يحدد استراتيجيات الانتقال والتوصيات الخاصة بالمخططات الآمنة من حيث الحوسبة الكمومية؛

*ز )* أن لجنة الدراسات 17 لقطاع تقييس الاتصالات هي لجنة الدراسات الرئيسية المعنية بمعايير الأمن داخل قطاع تقييس الاتصالات، والمكلفة بمهمة تنسيق أنشطة الأمن داخل قطاع تقييس الاتصالات ومع المنظمات والمنتديات الأخرى المعنية بوضع المعايير، وتطوير أطر لتحسين التعاون،

وإذ تدرك

*أ )* أن تعريف لجنة الدراسات 17 لمصطلح التجفير ما بعد الحوسبة الكمومية يُشير إلى الخوارزميات الكلاسيكية المقاومة للحوسبة الكمومية؛

*ب)* أن تطوير إطار لتقييم وفهم عمليات نشر أنظمة التجفير الحالية أمر ضروري بالنسبة للمنظمات، من أجل التخطيط لانتقالها من المجموعة الحالية لخوارزميات تجفير المفاتيح العمومية إلى خوارزميات التجفير ما بعد الحوسبة الكمومية المقاومة للهجمات القائمة على الحواسيب الكمومية؛

*ج)* أن هناك ثلاثة مشاريع متوازية مهمة في الانتقال إلى التجفير ما بعد الحوسبة الكمومية بالنسبة للخوارزميات (تقييس خوارزميات التجفير ما بعد الحوسبة الكمومية)، والبروتوكولات (جعل بروتوكولات الأمن ممكّنة بالتجفير ما بعد الحوسبة الكمومية)، والأنظمة (دمج التجفير ما بعد الحوسبة الكمومية في الأنظمة والعمليات)،

تقرر

1 مواصلة إعداد التوصيات اللازمة لتعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات؛

2 وضع توصيات جديدة لتعزيز الحاجة إلى بناء بنية تحتية موثوقة تعتمد على التجفير ما بعد الحوسبة الكمومية وخطط عمل للانتقال إلى التجفير ما بعد الحوسبة الكمومية لاستخدامه في البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات، بمجرد وضع الخوارزميات والبروتوكولات والمعايير اللازمة من قبل المنظمات الأكثر ملاءمة للقيام بهذا العمل؛

3 وضع إطار لمساعدة المنظمات في تقييم نشر أنظمة التجفير الحالية الخاصة بها والتخطيط للانتقال إلى التجفير ما بعد الحوسبة الكمومية،

تكلّف لجنة الدراسات 17 باعتبارها لجنة الدراسات الرئيسية المعنية بالأمن ولجان الدراسات المعنية الأخرىالتابعة لقطاع تقييس الاتصالات

1 بتقييم التوصيات الحالية والمتطورة والجديدة فيما يتعلق بتنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه؛

2 بمواصلة إعداد التوصيات والمنشورات الأخرى لقطاع تقييس الاتصالات بشأن المبادئ التوجيهية والممارسات الفضلى، والتي ستساعد المنظمات على الاستعداد لتنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه؛

3 بالتواصل مع أصحاب المصلحة في دوائر الصناعة لجمع الأفكار وأفضل الممارسات لتعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات؛

4 بالتعاون مع لجان دراسات قطاع تقييس الاتصالات الأخرى والمنظمات الأخرى من أجل تنفيذ هذا القرار؛

5 بتشجيع تبادل التقدم المحرز في التطورات ذات الصلة فيما يتعلق بتنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه داخل شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات؛

6 بتقديم توصيات إلى الفريق الاستشاري لتقييس الاتصالات بشأن كيفية تناول المواضيع التي تقع خارج اختصاصات لجان الدراسات،

تكلّف الفريق الاستشاري لتقييس الاتصالات

بالعمل على بذل جهود منسقة بين لجان الدراسات ذات الصلة لتسريع أعمال التقييس بشأن تعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات،

تكلف مدير مكتب تقييس الاتصالات

1 بتقديم المساعدة اللازمة لوضع خطط عمل لتعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه في البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات، وتشجيع مشاركة ومساهمات الدول الأعضاء وأعضاء القطاع والمنتسبين إليه والأوساط الأكاديمية؛

2 بتنظيم ورش عمل لجمع التوصيات والمساهمات من مجموعة واسعة من أصحاب المصلحة حول هذا الموضوع؛

3 بدعم مدير مكتب تنمية الاتصالات (BDT) في مساعدة الدول الأعضاء على تعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه في البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات،

تدعـو الدول الأعضاء وأعضاء القطاع والمنتسبين إليه والهيئات الأكاديمية إلى

1 تقديم مساهمات من أجل وضع التوصيات والمنشورات الأخرى لقطاع تقييس الاتصالات بشأن المبادئ التوجيهية والممارسات الفضلى لتعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه في البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات؛

2 تيسير ورش العمل التعليمية والدورات التدريبية لتعزيز تنفيذ التجفير ما بعد الحوسبة الكمومية والانتقال إليه في البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات.