|  |  |  |
| --- | --- | --- |
|  | Assemblée mondiale de normalisation des télécommunications (AMNT-24)New Delhi, 15-24 octobre 2024 |  |
|  |
|  |  |
| SÉANCE PLÉNIÈRE | Addendum 42 auDocument 37-F |
|  | 22 septembre 2024 |
|  | Original: anglais |
|  |
| Administrations des pays membres de la Télécommunauté Asie-Pacifique |
| Projet de nouvelle RÉSOLUTION [APT-PQC] – Promouvoir LA MISE EN œUVRE de LA CRYPTOGRAPHIE POST‑QUANTIQUE et la migration vers cette technologie |
|  |
|  |

|  |  |
| --- | --- |
| **Résumé:** | On trouvera dans le présent document une proposition de nouvelle Résolution de l'AMNT, intitulée "Promouvoir la mise en œuvre de la cryptographie post‑quantique et le passage à cette technologie". |
| **Contact:** | M. Masanori KondoSecrétaire généralTélécommunauté Asie-Pacifique | Courriel: aptwtsa@apt.int |

Introduction

Les algorithmes de chiffrement constituent une base essentielle des réseaux et sont primordiaux pour instaurer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication.

Une fois qu'il sera possible d'utiliser des ordinateurs quantiques dans le domaine du chiffrement, la plupart des algorithmes à clé publique existants et leurs protocoles associés seront vulnérables aux attaques lancées depuis ce genre d'ordinateurs. Les ordinateurs quantiques constituent une menace, car ils ont le potentiel, compte tenu de leur puissance de calcul exceptionnelle, de casser des algorithmes de chiffrement largement utilisés, y compris les algorithmes de chiffrement RSA et de cryptographie à courbes elliptiques (ECC). Un ensemble d'algorithmes cryptographiques, appelés cryptographie post-quantique (PQC), est actuellement mis au point. Ces algorithmes sont considérés comme étant "à l'épreuve des attaques quantiques" ou "résistants aux attaques quantiques", c'est‑à‑dire qu'ils devraient rester sûrs même contre des ordinateurs quantiques utilisés dans le domaine cryptographique.

La Résolution tient compte de la définition de la PQC donnée par la CE 17, qui inclut les algorithmes classiques résistants aux attaques quantiques.

À l'heure actuelle, l'infrastructure de confiance des réseaux de communication repose sur des algorithmes de chiffrement traditionnels, tels que les algorithmes Diffie-Hellman et RSA, qui sont vulnérables aux menaces quantiques. Par conséquent, il est crucial d'opérer la transition des réseaux TIC vers une infrastructure de confiance résistante aux attaques quantiques avant l'avènement des ordinateurs quantiques.

Bien que la PQC tire parti de l'infrastructure existante et constitue une solution rentable et bien établie à l'épreuve des attaques quantiques, il faudra beaucoup de temps et de ressources aux organisations pour migrer complètement vers la PQC.

Dans ce contexte, il est urgent que les CE de l'UIT-T entreprennent activement des travaux de normalisation pour promouvoir la mise en œuvre de la cryptographie post-quantique et la migration vers cette technologie dans les réseaux de télécommunication/TIC.

En outre, dans le cadre de son processus de préparation en vue de l'AMNT-24, la CE 17 de l'UIT-T est convenue que "l'utilisation de la cryptographie post-quantique" serait un nouveau thème pour la prochaine période d'études (2025-2028).

Proposition

Compte tenu de ce qui précède, les Administrations des pays membres de l'APT proposent que l'AMNT-24 envisage l'élaboration d'une nouvelle Résolution de l'AMNT visant à promouvoir la mise en œuvre de la cryptographie post-quantique et la migration vers cette technologie.

ADD APT/37A42/1

PROJET DE NOUVELLE RÉSOLUTION [APT-PQC] (New Delhi, 2024)

Promouvoir la mise en œuvre de la cryptographie post-quantique
et la migration vers cette technologie

(New Delhi, 2024)

L'Assemblée mondiale de normalisation des télécommunications (New Delhi, 2024),

rappelant

*a)* la Résolution 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires relative au renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC);

*b)* la Résolution 50 (Rév. Genève, 2022) de l'AMNT sur la cybersécurité;

*c)* la Résolution 57/239 de l'Assemblée générale des Nations Unies, relative à la création d'une culture mondiale de la cybersécurité;

*d)* la Résolution 78/287 de l'Assemblée générale des Nations Unies, relative à l'Année internationale des sciences et technologies quantiques, qui se déroulera en 2025,

considérant

*a)* l'importance des algorithmes de chiffrement dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC);

*b)* que l'avènement de l'informatique quantique dans le domaine cryptographique compromettra bon nombre des algorithmes cryptographiques actuels, en particulier la cryptographie à clé publique, qui est largement utilisée pour protéger les informations numériques;

*c)* que les algorithmes de chiffrement dont dépendent les infrastructures des télécommunications/TIC sont utilisés dans le monde entier dans les composants de nombreux systèmes de communication, de traitement et de stockage;

*d)* qu'une fois qu'il sera possible d'utiliser des ordinateurs quantiques dans le domaine cryptographique, la plupart des algorithmes à clé publique existants et leurs protocoles associés seront vulnérables aux attaques lancées depuis ce genre d'ordinateurs;

*e)* que les algorithmes de PQC peuvent être utilisés dans l'infrastructure existante et qu'il est possible de tirer parti de l'expertise en matière de systèmes pour mettre en œuvre une solution qui permette de contrer les attaques quantiques;

*f)* que les applications types de la PQC peuvent concerner tous les secteurs, comme les IMT 2020/IMT-2030 et la technologie DLT;

*g)* la nécessité d'assurer une collaboration et le partage d'informations à l'échelle internationale pour faire face aux menaces de sécurité que posent les ordinateurs quantiques pouvant être utilisés dans le domaine cryptographique;

*h)* que le rôle de l'UIT est axé sur la mise en œuvre de la PQC et la migration vers cette technologie pour instaurer la sécurité et la confiance dans l'utilisation de l'infrastructure des télécommunications/TIC, et non sur la normalisation des algorithmes ou des protocoles de PQC;

*i)* que la PQC peut permettre de mettre au point des systèmes cryptographiques sécurisés face aux ordinateurs quantiques et classiques, et qui soient compatibles avec les protocoles et les réseaux de communication existants;

*j)* que la migration des systèmes cryptographiques classiques existants vers des systèmes reposant sur la PQC et capables de résister aux attaques quantiques est un projet coûteux et à long terme. À l'heure actuelle, de nombreux secteurs verticaux dans le monde étudient les applications de la PQC et la possibilité de migrer vers celle-ci, et il est nécessaire que le secteur des télécommunications/TIC se prépare dès à présent à cette tendance;

*k)* que le processus de migration vers la PQC est extrêmement complexe et peut prendre des années pour être mené à terme, car il impose de remplacer les algorithmes de chiffrement et de mettre à jour différents protocoles cryptographiques, systèmes, composants ou encore l'infrastructure pour y intégrer des technologies cryptographiques à l'épreuve des attaques quantiques;

*l)* que la migration vers la PQC peut comprendre la conception et l'élaboration de mécanismes permettant de mettre à jour de manière souple les systèmes cryptographiques, ainsi que la mise à jour itérative des systèmes d'information d'applications cryptographiques afin de faciliter la mise en œuvre des futurs algorithmes de PQC;

*m)* l'évaluation de la sécurité des algorithmes de PQC est réalisée de manière continue par l'Institut national des normes et de la technologie des États-Unis (NIST),

considérant en outre

*a)* que la Recommandation UIT-T X.1811 fournit des lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT‑2020, que le rapport technique TR.qs-dlt énonce des lignes directrices propres à créer un système DLT à l'épreuve des attaques quantiques en vue de sécuriser la technologie DLT, et que la CE 17 de l'UIT-T élabore actuellement deux rapports techniques, l'un d'eux étant intitulé "Préconisations d'utilisation de la cryptographie avancée fondée sur la PQC";

*b)* que le groupe ISO/CEI JTC 1/SC 27/WG 2 et l'Institut européen des normes de télécommunication (ETSI) s'emploient à normaliser la cryptographie post-quantique (PQC) et s'échangent des informations à ce sujet;

*c)* que le Centre d'excellence national en matière de cybersécurité du NIST (NCCoE) commence à élaborer des pratiques visant à faciliter la migration de l'ensemble actuel des algorithmes de chiffrement à clé publique vers des algorithmes résistants aux attaques quantiques,

notant

*a)* que l'UIT-T doit jouer un rôle de premier plan dans l'élaboration de normes visant à instaurer la confiance et à garantir la sécurité dans l'utilisation des TIC;

*b)* qu'un processus initié par le NIST est en cours pour recueillir, évaluer et normaliser un ou plusieurs algorithmes de chiffrement à clé publique résistants aux attaques quantiques;

*c)* que le NIST a publié des normes relatives à trois algorithmes de PQC;

*d)* que le Groupe d'étude sur l'ingénierie Internet (IETF) compte un groupe de travail sur l'utilisation de technologies post-quantiques dans divers protocoles (pquip), chargé d'étudier des questions d'ingénierie en matière de PQC et les problèmes liés à la transition vers les technologies de PQC, ainsi que de s'appuyer sur l'expérience pertinente en vue de faire progresser les travaux de l'IETF et d'activement mettre en œuvre la PQC dans les protocoles de l'IETF, y compris IPSec, TLS et OpenPGP;

*e)* que l'ISO/CEI JTC 1/SC 27/WG 2 (*Cryptographie et mécanismes de sécurité*), travaille à la normalisation des algorithmes de PQC sélectionnés par le NIST;

*f)* que le groupe de travail de l'ETSI sur les méthodes de chiffrement à l'épreuve des attaques quantiques (QSC) a publié un rapport technique définissant des stratégies de migration et des recommandations relatives aux systèmes résistants aux attaques quantiques;

*g)* que la Commission d'études 17, en sa qualité de commission d'études directrice en matière de sécurité au sein de l'UIT-T, est chargée de coordonner les activités relatives à la sécurité au sein de l'UIT-T et avec d'autres organisations de normalisation et forums, et de définir des cadres pour améliorer la collaboration,

reconnaissant

*a)* que la définition de la PQC donnée par la CE 17 se réfère aux algorithmes classiques résistants aux attaques quantiques;

*b)* qu'il est essentiel d'élaborer un cadre visant à évaluer et à comprendre le déploiement de systèmes cryptographiques existants pour permettre aux organisations de planifier la migration de l'ensemble actuel d'algorithmes cryptographiques à clé publique actuels vers des algorithmes de PQC résistants aux attaques quantiques;

*c)* que trois processus de travail parallèles sont importants dans la migration vers la PQC, concernant les algorithmes (normalisation des algorithmes de PQC), les protocoles (rendre les protocoles de sécurité compatibles avec la PQC) et les systèmes (intégration de la PQC aux systèmes et processus),

décide

1 de continuer d'élaborer les recommandations nécessaires pour promouvoir la mise en œuvre de la PQC et la migration vers cette technologie dans les réseaux de télécommunication/TIC;

2 d'élaborer de nouvelles recommandations visant à promouvoir la nécessité de mettre en place une infrastructure de confiance fondée sur la PQC et des plans d'action pour la migration vers la PQC dans l'infrastructure des télécommunications/TIC, une fois que les algorithmes, protocoles et normes nécessaires auront été mis au point par les organisations compétentes en la matière;

3 d'élaborer un cadre destiné à aider les organisations à évaluer le déploiement de leurs systèmes cryptographiques existants et à en planifier la migration vers la PQC,

charge la Commission d'études 17, en sa qualité de commission d'études directrice chargée de la sécurité, et les commissions d'études compétentes du Secteur de la normalisation des télécommunications de l'UIT

1 d'évaluer les Recommandations existantes, en cours d'élaboration ou nouvelles du point de vue de la mise en œuvre de la PQC et de la migration vers cette technologie;

2 de continuer d'élaborer des Recommandations et d'autres publications de l'UIT-T qui énoncent des lignes directrices et de bonnes pratiques destinées à aider les organisations à se préparer à la mise en œuvre des technologies de la PQC et à la migration vers cette technologie;

3 d'établir un dialogue avec les parties prenantes du secteur pour recueillir des informations et de bonnes pratiques afin de promouvoir la mise en œuvre la PQC et la migration vers cette technologie dans les réseaux de télécommunication/TIC;

4 de collaborer avec d'autres commissions d'études de l'UIT-T et d'autres organisations en vue de la mise en œuvre de la présente Résolution;

5 d'encourager la diffusion des progrès liés aux faits nouveaux en ce qui concerne la mise en œuvre de la PQC et la migration vers cette technologie dans les réseaux de télécommunication/TIC;

6 de soumettre au Groupe consultatif de la normalisation des télécommunications des recommandations sur la manière de traiter les questions qui ne relèvent pas du mandat des commissions d'études,

charge le Groupe consultatif de la normalisation des télécommunications

d'encourager une action concertée entre les commissions d'études compétentes, afin d'accélérer les travaux de normalisation visant à promouvoir la mise en œuvre de la PQC et la migration vers cette technologie dans les réseaux de télécommunication/TIC,

charge le Directeur du Bureau de la normalisation des télécommunications

1 de fournir l'assistance nécessaire à l'établissement de plans d'action visant à promouvoir la mise en œuvre de la PQC et la migration vers cette technologie dans l'infrastructure des télécommunications/TIC et d'encourager la participation et les contributions des États Membres, des Membres de Secteur, des Associés et des établissements universitaires;

2 d'organiser un ou plusieurs ateliers afin que des parties prenantes très diverses fassent part de leurs recommandations et présentent des contributions sur cette question;

3 d'apporter un appui au Directeur du Bureau de développement des télécommunications (BDT) en vue d'aider les États Membres à promouvoir la mise en œuvre de la PQC et la migration vers cette technologie dans l'infrastructure des télécommunications/TIC,

invite les États Membres, les Membres du Secteur, les Associés et les établissements universitaires

1 à soumettre des contributions pour l'élaboration de Recommandations et d'autres publications de l'UIT-T énonçant les lignes directrices et les bonnes pratiques propres à promouvoir la mise en œuvre de la PQC et la migration vers cette technologie dans l'infrastructure des télécommunications/TIC;

2 d'organiser des ateliers éducatifs et des séances de formation visant à promouvoir la mise en œuvre de la PQC et la migration vers cette technologie dans les réseaux de télécommunication/TIC.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_