|  |  |  |  |
| --- | --- | --- | --- |
|  | **世界电信标准化全会（WTSA-24）**  2024年10月15-24日，新德里 | |  |
|  | | | |
|  | |  | |
| 全体会议 | | 文件 37 (Add.42)-C | |
|  | | 2024年9月22日 | |
|  | | 原文：英文 | |
|  | | | |
| 亚太电信组织各成员国主管部门 | | | |
| 第[APT-PQC]号新决议草案 – 促进后量子加密技术的实施和向之迁移 | | | |
|  | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **摘要：** | 本文件包含一项关于促进后量子加密技术实施和向之迁移的WTSA新决议的提案。 | |
| **联系人：** | 亚太电信组织秘书长 Masanori Kondo先生 | 电子邮件：[aptwtsa@apt.int](mailto:aptwtsa@apt.int) |

引言

加密算法是网络树立使用ICT的信心和提高安全性的重要基础。

一旦可以访问与加密相关的量子计算机，大多数现有的公钥算法及其相关协议将易受基于量子计算机的攻击。量子威胁来自量子计算机，凭借其卓越的计算能力，量子计算机有可能破解广泛使用的加密算法，包括RSA和ECC（椭圆曲线加密技术）。正在开发一套被称为后量子加密技术（PQC）的加密算法，它们被认为是“量子安全的”或“抗量子的”，这意味着即使在存在加密相关的量子计算机的情况下，这些算法也有望保持安全。

本决议认可第17研究组对PQC的定义，该定义指的是抗量子的经典算法。

目前，通信网络的可信基础设施基于传统的加密算法，如Diffie-Hellman和RSA，它们易受量子威胁。因此，在量子计算机出现之前，ICT网络向抗量子的可信基础设施的过渡就变得至关重要。

虽然PQC利用现有的基础设施并提供经济高效且成熟的量子安全解决方案，但各组织需要大量的时间和资源才能完全实现向PQC的迁移。

有鉴于此，迫在眉睫的要求是ITU-T研究组要积极开展标准化工作，以促进电信/ICT网络中后量子加密技术的实施和向后量子加密技术的迁移。

此外，ITU-T第17研究组在其WTSA-24筹备进程中同意将“后量子加密技术的使用”作为下一研究期（2025-2028年）的一个新议题。

提案

基于上述背景，APT各成员国主管部门提议WTSA-24考虑制定一项关于促进后量子加密技术实施和向之迁移的WTSA新决议。

ADD APT/37A42/1

第[APT-PQC]号新决议草案（2024年，新德里）

促进后量子加密技术的实施和向之迁移

（2024年，新德里）

世界电信标准化全会（2024年，新德里）

忆及

*a)* 全权代表大会关于加强国际电联在树立使用信息通信技术的信心并提高安全性方面的作用的第130号决议（2022年，布加勒斯特，修订版）；

*b)* 关于网络安全的WTSA第50号决议（2022年，日内瓦，修订版）；

*c)* 联合国大会（UNGA）关于培育全球网络安全文化的第57/239号决议；

*d)* 联合国大会关于2025年国际量子科学技术年的第78/287号决议，

考虑到

*a)* 加密算法在树立使用信息通信技术（ICT）的信心和提高安全性方面的重要性；

*b)* 与加密相关的量子计算技术的出现将损害当前的许多加密算法，特别是广泛用于保护数字信息的公钥加密技术；

*c)* 电信/ICT基础设施所依赖的加密算法在世界范围内广泛应用于许多不同的通信、处理和存储系统的组件中；

*d)* 一旦可以访问与加密相关的量子计算机，大多数现有的公钥算法及其相关协议将易受到基于量子计算机的攻击；

*e*) PQC算法可用于现有基础设施，并利用系统专业知识来实施量子安全的解决方案；

*f*) PQC的典型应用可包括所有行业，如IMT-2020/IMT-2030和DLT；

*g*) 有必要开展国际协作和信息共享，以应对与加密相关的量子计算机对安全的威胁；

*h)* 国际电联的作用侧重于PQC的实施及其迁移，以树立使用电信/ICT基础设施的安全性和信心，而不是标准化PQC算法或协议；

*i)* PQC可以帮助开发可对抗量子计算机和经典计算机的可信基础设施，并可与现有的通信协议和网络进行互操作；

*j*) 将现有的经典加密系统迁移到可抵御量子计算攻击的基于PQC的系统是一项长期且成本高昂的项目。目前，世界上已经有许多垂直行业在探索应用PQC和向PQC的迁移，电信/ICT行业有必要立即为此趋势做好准备；

*k*) PQC迁移过程极为复杂，需要很多年才能完成，因为它需要替换加密算法，将加密协议、方案、组件、基础设施等更新为量子安全的加密技术；

*l*) 向PQC的迁移可能包括设计和开发可灵活更新加密系统的机制，以及对加密应用信息系统的迭代更新，以便简化未来PQC算法的实施；

*m*) PQC算法的安全评估是NIST（国家标准和技术研究所）持续开展的工作，

进一步考虑到

*a*) ITU-T X.1811建议书为在IMT-2020系统中应用量子安全的算法提供了安全导则，TR.qs-dlt为量子安全的DLT系统提供了导则，以保护DLT的安全，而ITU-T第17研究组正在起草包括“基于PQC的先进加密技术使用指南”在内的两份技术报告；

*b*) ISO/IEC JTC 1/SC 27/WG 2和欧洲电信标准协会（ETSI）正在开展关于后量子加密技术（PQC）的标准化工作和关于PQC的信息交流工作；

*c*) NIST国家网络安全高级培训中心（NCCoE）正在启动制定相关做法，以简化从现有公钥加密算法向可抵御量子计算机攻击的替代算法的迁移，

注意到

*a)* ITU-T应在制定树立使用ICT的信心和确保安全性的标准方面发挥主导作用；

*b)* NIST发起的进程正在征集、评估和标准化一个或多个抗量子的公钥加密算法；

*c)* NIST已经发布了三个有关PQC算法的标准；

*d)* IETF设有后量子协议使用工作组（pquip），以解决PQC工程和过渡问题，积累与IETF工作相关的经验，并在IETF协议（包括IPSec、TLS和OpenPGP）中积极实施PQC；

*e)* ISO/IEC JTC 1/SC 27/WG 2“加密技术和安全机制”正在开展关于NIST选定的PQC算法的标准化工作；

*f*) ETSI量子安全的加密技术（QSC）工作组发布了一份技术报告，确定了量子安全方案的迁移策略和建议；

*g)* ITU-T第17研究组是ITU-T内关于安全问题的牵头研究组，就安全活动负责在ITU-T内部以及与其他标准制定组织和论坛之间的协调工作，并制定旨在改进协作的框架，

认识到

*a)* 第17研究组对PQC的定义是指抗量子的经典算法；

*b)* 制定用于评估和理解现有加密系统部署的框架对于各组织规划从当前的公钥加密算法集向抵御量子计算机攻击的PQC算法的迁移至关重要；

*c)* 在算法（PQC算法的标准化）、协议（使安全协议成为PQC支撑）和系统（将PQC集成到系统和流程中）的PQC迁移中，三个并行的工作流程很重要，

做出决议

1 继续制定必要的建议书，以促进电信/ICT网络内PQC的实施和迁移；

2 制定新建议书，以推动建立基于PQC的可信基础设施的必要性，以及一旦最适合从事这项工作的组织开发出必要的算法、协议和标准即迁移到PQC以便在电信/ICT基础设施中使用之的行动计划；

3 制定一个框架，协助各组织评估其现有的加密系统部署和规划向PQC的迁移，

责成作为国际电联电信标准化部门牵头研究组的第17研究组和其他相关研究组

1 就PQC实施和向之迁移，对现有、正在演进和新的建议书做出评估；

2 继续制定有关导则和最佳做法的建议书和其他ITU-T出版物，这将帮助各组织为实施PQC和向之迁移做好准备；

3 与行业利益攸关方合作，收集有关在电信/ICT网络内实施PQC和向之迁移的见解和最佳做法；

4 与其他ITU-T研究组和其他组织开展协作，以落实本决议；

5 鼓励分享有关PQC实施以及电信/ICT网络向PQC迁移的相关开发工作的进展情况；

6 就如何解决研究组职权以外的议题向电信标准化局顾问组（TSAG）提出建议，

责成电信标准化顾问组

推动各相关研究组之间共同努力，加速标准化工作，促进PQC实施和电信/ICT网络向PQC迁移，

责成电信标准化局主任

1 提供必要的援助，以制定有关促进PQC实施和电信/ICT基础设施向PQC迁移的行动计划，并鼓励成员国、部门成员、部门准成员和学术成员参与并为之做出贡献；

2 组织讲习班，从广大利益攸关方处收集关于此议题的建议书和输入意见；

3 支持电信发展局（BDT）主任协助成员国促进PQC的实施和电信/ICT基础设施向PQC的迁移，

请成员国、部门成员、部门准成员和学术成员

1 为制定有关促进PQC实施和电信/ICT基础设施向PQC迁移的导则和最佳做法的建议书、ITU-T其他出版物提交文稿；

2 为举办教育讲习班和培训班提供便利，以促进PQC的实施和电信/ICT网络向PQC的迁移。