Preparing Communications Networks for the Quantum Future

ATIS-I-0000089
February 2022

ABSTRACT

Computational problems that would take a classical computer tens of thousands of years to complete can potentially be solved in seconds by a quantum computer — making quantum computers' power exponentially greater than computers in use today for certain classes of problems. There are concerns, however, that quantum's computational power will eventually compromise current encryption algorithms widely used by network operators. New cryptography algorithms and technologies will be required to secure communications and data against the threat of quantum computers.

Although quantum computing is still in the early stages of development, network operators should begin to understand its implications on current communications and data management. Organizations will need to implement a new approach to assessing crypto agility and risk to the business to be quantum resistant in the future.

FOREWORD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-Internet Protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cybersecurity, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

COPYRIGHT INFORMATION

ATIS-I-0000089

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [https://www.atis.org/policy/patent-assurances/] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

TABLE OF CONTENTS

1
INTRODUCTION

The huge leap forward in computational ability to solve certain problems that quantum computing delivers comes from leveraging the quantum properties of entanglement and superposition. While classical bits are independent (i.e., operation on one bit does not impact another bit), operations on quantum bits (qubits) may be made to be correlated using quantum entanglement. Furthermore, unlike the binary bits in classical computing, qubits can exist in a superposition of 0 and 1. This makes it possible to speed up solving specific problems using quantum computers rather than classical computers.

One example of such a problem is factoring the product of two very large primes, which forms the foundation of RSA — a commonly used public key encryption algorithm. While classical computers may require hundreds of years to factor a 2048-bit RSA key, a future quantum computer may be able to do so in a day [1][2]. As a result, future quantum computers using Grover's search algorithm may have the potential to weaken private key cryptography, which uses symmetric key encryption [3].

All digital infrastructure that permeates every sector and part of society uses cryptography to secure and protect them, including – communications, remote connections, computing, IoT devices, etc. Cryptographically Relevant Quantum Computers (CRQC), ones able to break the encryption used for information and secure communication, do not yet exist. However, information encrypted with current cryptographic techniques can be intercepted, stored, and decrypted once such computing capabilities materialize. The retrospective decryption of encrypted data is a genuine threat; thus, any critical data requiring long-term security should be identified and protected now if necessary.

To advance operators' and users' needs in this area, the ATIS Quantum-Safe Communications and Information Initiative (QSCII) brought together industry experts to develop a roadmap of work items, aligned with industry best practices and other quantum standards initiatives. In addition, the initiative is also addressing key regulatory, governance, and interoperability implications to enable quantum-safe security.

This white paper provides a high-level overview of the current activities to ensure communications and information will be resistant to quantum threats in the future. It discusses the potential risk areas for communications infrastructure and the potential timelines for when those risks will emerge, identifying indicators for organizations to assess crypto agility and business risk so that they can plan for this eventuality. These key indicators include:

- Creating awareness of the quantum threat and risk to security.
- Implementing a new approach to managing security.
- Assessing the enterprise's readiness to become crypto-agile and resistant to future classical or quantum threats.
- Monitoring the development of postquantum cryptography standards and solutions.
- Getting started by acting today to set their organization on a path to be quantum resistant.