Quantum Computing
Cyber Threats: Resistant Algorithms Help Prevent the Most Advanced Attacks

Overview
Quantum computing stands at the very forefront of the future of the computing landscape. It has the potential to revolutionize the way militaries encrypt data and communicate. These supercomputer-busters promise a new era in computing, but bad actors are already looking for ways to use this advance for cyber-attacks.

In this whitepaper, we will learn the fundamentals of quantum computing, how quantum computing may be used to circumvent cryptographic algorithms and a discussion of the measures you can take to minimize this new threat.

Quantum Computing Basics
Quantum computing stands at the very forefront of the future of the computing landscape. To understand quantum computing, first you must understand some principles of subatomic physics.

Quantum physics seems almost like magic when researchers use its power to create computing solutions. However, subatomic particles behave in a way predictable enough to harness their connections to build machines that put enormous supercomputers to shame.

Quantum computing accomplishes this by harnessing the power of the qubit. Traditional computers work, fundamentally, in binary – a series of 0s and 1s. Qubits are subatomic particles like photons and electrons, and when they are connected, they provide almost unimaginable computing powers with certain fundamental properties: superposition and entanglement.

Superposition refers to the ability of qubits to simultaneously exist in multiple states. Imagine many versions of 1s and 0s existing in the same qubit at the same time, vastly magnifying computing power. Instead of processing one “thing” at a time, with superposition a qubit can process multiple strings at once.

Entanglement is the still-mysterious process of binding one qubit to another, creating a pair that increases computing power exponentially, even across long distances.
The Cryptographic Danger of Quantum Computing

After learning a bit about quantum computing, you may be able to foresee the problem it could cause for cybersecurity in general, and cryptography in particular. Cryptography is essentially complex strings of binary information. Commonly used 256-bit cryptography contains 256 1s and 0s, for example.

To put it in context, a quantum computer with a billion qubits (and remember, these are subatomic particles) can crack an RSA 2,048-bit encryption in just eight hours. While many researchers believe quantum attacks are a few years away, progress in the field is unpredictable and tends to move forward in fits and starts.

With the emergence of quantum computers, current secure public-key algorithms such as RSA and DSA become breakable. The problem with these algorithms is that their security relies on one of three mathematical problems: integer factorization, discrete logarithm or elliptic curve discrete logarithm.

These problems can be easily solved on large quantum computers. Government agencies, for instance, are planning for the risk mitigation of the current vulnerabilities with the existing cryptographic algorithms. Commercial enterprises should do the same if they house sensitive information like financial or health records.

Quantum-safe cryptographic solutions must be devised sooner rather than later to protect sensitive and classified data from potentially catastrophic breaches. And, while truly quantum-safe cryptography is still on the horizon, you can utilize quantum-resistant technology today to ensure the integrity of classified data and secure operations.

Quantum-Resistant Cryptographic Solutions

The U.S. National Security Agency (NSA) formerly published Suite-B guidelines for commercial cryptographic security. In response to the threat of quantum computing, the NSA has augmented these guidelines with the Commercial National Security Algorithm Suite (CNSA). The military has its own separate set of guidelines.

What does this mean for your data? Table 1 is a comprehensive list of the cryptographic algorithms that should be avoided. Based on the vulnerabilities summarized above, the CNSA is a subset of existing Suite-B:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA 3072 bits +</td>
<td>Key establishment, Digital signature</td>
</tr>
<tr>
<td>Diffie-Hellman(DH) 3072+, group 15-18</td>
<td>Key establishment</td>
</tr>
<tr>
<td>ECDH with NIST P-384</td>
<td>Key establishment</td>
</tr>
<tr>
<td>ECDSA with NIST P-384</td>
<td>Digital signature</td>
</tr>
<tr>
<td>SHA-384</td>
<td>Integrity</td>
</tr>
<tr>
<td>AES-256</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>

Table 1: Cryptographic algorithms to avoid.

Due to the vulnerabilities, some algorithms are explicitly removed, and they should NOT be used:

- ECDH and ECDSA with P-256
- SHA1, SHA256
- AES-128
- RSA 2048 (RSA 1024 was disallowed after 2013)
- Diffie-Hellman with 2048-bits key

Products must implement CNSA ciphers listed in the table above and support a functional mode that utilizes those ciphers only to be compliant with NSA’s Quantum Resistance guidelines.
Ultra’s Quantum-Resistant Solutions

Ultra has several quantum-resistant solutions to ensure that your organization is compliant with CNSA guidelines.

Ultra CyberFence

CyberFence products offer cyber security protection for edge network devices. They protect data-in-transit via VNP/IPsec encryption and VLAN encryption based on the edge network device's security needs. CyberFence products support the NSAs CNSA ciphers, thus meeting all quantum resistance requirements.

IPSec Encryption

IPsec interface is used by CyberFence as the VPN tunnel for secure IP/TCP/UDP data transport. This VPN tunnel is also used to securely transport audit logs and connection to other IT elements such as an NTP server. CyberFence supports a “CNSA” mode for the end user to hide the details of configuration. Under the hood, our IPsec implementation uses the following ciphers:

ike=aes256-sha384-ecp384-modp3072
esp=aes256gcm128-aes256ccm128-aes256gcm96-aes256ccm96-aes256gcm64-aes256ccm64-aes256-sha384

VLAN Encryption

VLAN interface is used by CyberFence for layer-2 encryption. For “CNSA mode” it limits the cipher choices to AES_GCM-256, AES_CCM-256, AES_ECB-256-SHA384 and AES_CCB-256-SHA384.

Management Interface

CyberFence supports HTTPS/TLS based web GUI management interface. Its TLS implementation is fully compliant with RFC 5246 (TLS 1.2), with cipher extensions defined in RFC 5289. In CNSA mode of operation, it supports CNSA ciphers only which is a subset of RFC 5289.

1. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
2. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
3. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Ultra WiFiProtect Products

Ultra WiFiProtect products are secured Wi-Fi routers developed for government customers. They support the same IPsec/VPN for trusted path communication with external IT elements and an HTTPS/TLS based management interface. The IPsec/VPN and web GUI management interfaces are CNSA/Quantum computer resistance compliant.

However, in its main functional interface, WiFiProtect is not yet CNSA compliant. The WiFi standard as defined by IEEE 802.11 only employs AES-CMMP cipher with 128 bits key length to protect the data over the air. Newer WiFi standard such as 802.11ac (WiFi 5) and 802.11ax (WiFi 6) support AES-CCM/GCM with 256 bits key. WiFi 5 and 6 are part of Ultra’s WiFiProtect roadmap. These new WiFiProtect WiFi 5 and WiFi 6 products will be fully compliant with Quantum Resistance CNSA requirements.

Conclusion

Quantum computing will only continue to advance, both in capability and availability to bad actors. However, rest assured that there are steps you can take now to create a quantum resistant cryptographic infrastructure that will help ensure your organization's data remains intact and private.

Learn more about Ultra’s Quantum-Resistant Solutions at sales@ultra-us-gbs.com or ultra.group/intelligence-communications