Post-Quantum Security in 5G

Ashish Kundu
Head of Cybersecurity Research
Cisco Research

ACM/IEEE 1st 5G Summit, June 14 ‘22
Space Communication Security (NASA)

If terrorists or hackers illegally listen to, or worse, modify communication content, disaster can occur.

The consequences of a nuclear powered spacecraft under control of a hacker or terrorist could be devastating.

Therefore, all communications to and between spacecraft must be extremely secure and reliable.
Quantum threat to communication

Rogue state/entity:
• Break crypto using QC,
• Command, capture, re-route

Target: Navy, Civilian Area

Cisco Research
Cisco Research
Lockheed Martin partners with satellite start-up Omnispace to build a space-based 5G network

Space, Satellites & 5G

Space Companies Are Investing Big in 5G Technology

By Elizabeth Howell published October 20, 2019

Satellite internet is going to be a big thing.

Lockheed Martin And Omnispace Explore Space-Based 5G Global Network

5G satellite hybrid connectivity would bolster terrestrial mobility.
Progress of quantum computing

- **2013**: Google announces Quantum AI Lab
- **2016**: IBM Quantum Experience comes online, the first quantum computer available in the cloud
- **2018**: China announces $10B investment in National Laboratory for Quantum Information Sciences
- **2019**: AWS announces Amazon Bracket cloud service, Microsoft announces Azure Quantum cloud service

- **2010**:
- **2012**: 1QBit launches as first independent quantum software provider
- **2017**: IBM announces IBM Q, plan to build commercially available quantum computers
- **2018**: National Quantum Initiative Act establishes 10-year plan to fund quantum R&D in the US
- **2019**: Google announces it has achieved “quantum supremacy”

Sources: Industry interviews, desk research, Crunchbase, BCG analysis.

IBM's planned 1,121-qubit "Condor" quantum processor, slated for 2023, could be the company's first truly useful quantum computer for businesses.
Risk along the Computing Stack

POTENTIAL SECURITY VULNERABILITY CAUSES

- Poor Passwords or Phishing
- Misconfigured or Unpatched Systems
- Open Source, Vendor or Hardware Flaws
- Poor Implementation or Open Firewall Ports
- Quantum Computer Attack Using Shor’s Algorithm
- Public Key Cryptography
- Architecture
- Platform
- Admin
- User

# The Quantum Threat — Qubits vs Bits

## TABLE 4.1 Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes

<table>
<thead>
<tr>
<th>Cryptosystem Category</th>
<th>Key Size</th>
<th>Security Parameter</th>
<th>Quantum Algorithm Expected to Defeat Cryptosystem</th>
<th># Logical Qubits Required</th>
<th># Physical Qubits Required</th>
<th>Time Required to Break System</th>
<th>Quantum Resilient Replacement Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-GCM</td>
<td>128</td>
<td>128</td>
<td>Grover’s algorithm</td>
<td>2,953</td>
<td>4.61 x 10^6</td>
<td>2.61 x 10^{12} years</td>
<td>Move to NIST-standardized PQC algorithm when available</td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>192</td>
<td></td>
<td>4,449</td>
<td>1.68 x 10^7</td>
<td>1.97 x 10^{22} years</td>
<td></td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>256</td>
<td></td>
<td>6,681</td>
<td>3.36 x 10^7</td>
<td>2.29 x 10^{32} years</td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td>1024</td>
<td>80</td>
<td>Shor’s algorithm</td>
<td>2,050</td>
<td>8.05 x 10^6</td>
<td>3.58 hours</td>
<td>Move to NIST-selected PQC algorithm when available</td>
</tr>
<tr>
<td></td>
<td>2048</td>
<td>112</td>
<td></td>
<td>4,098</td>
<td>8.56 x 10^6</td>
<td>28.63 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4096</td>
<td>128</td>
<td></td>
<td>8,194</td>
<td>1.12 x 10^7</td>
<td>229 hours</td>
<td></td>
</tr>
<tr>
<td>ECC Discrete-log problem</td>
<td>256</td>
<td>128</td>
<td>Shor’s algorithm</td>
<td>2,330</td>
<td>8.56 x 10^6</td>
<td>10.5 hours</td>
<td>Move to NIST-selected PQC algorithm when available</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>192</td>
<td></td>
<td>3,484</td>
<td>9.05 x 10^6</td>
<td>37.67 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>521</td>
<td>256</td>
<td></td>
<td>4,719</td>
<td>1.13 x 10^6</td>
<td>55 hours</td>
<td></td>
</tr>
<tr>
<td>SHA256</td>
<td>N/A</td>
<td>72</td>
<td>Grover’s Algorithm</td>
<td>2,403</td>
<td>2.23 x 10^6</td>
<td>1.8 x 10^4 years</td>
<td>Move away from password-based authentication</td>
</tr>
<tr>
<td>PBKDF2 with 10,000 iterations</td>
<td>N/A</td>
<td>66</td>
<td>Grover’s algorithm</td>
<td>2,403</td>
<td>2.23 x 10^6</td>
<td>2.3 x 10^7 years</td>
<td></td>
</tr>
</tbody>
</table>

Figure C.3.3-1: Decryption based on ECIES at home network

Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.3.0 Release 16)
Deploying and operating cloud-based 5G networks, Jan 24 2022, https://cloud.google.com/blog/topics/telecommunications/how-csps-can-use-cloud-networks-to-deliver-5g
5G Threat Surface

Device Threats
- Malware
- Sensor Susceptibility
- TFTP MitM attacks
- Bots DDoS
- Firmware Hacks
- Device Tampering

Air Interface Threats
- MitM attack
- Jamming

RAN Threats
- MEC Server Vulnerability
- Rogue Nodes

Backhaul Threats
- DDoS attacks
- CP/UP Sniffing
- MEC Backhaul sniff

5G Packet Core & OAM Threats
- Virtualization
- Network Slice security
- API vulnerabilities
- IoT Core integration
- Roaming Partner vulnerabilities
- DDoS & DoS attacks
- Improper Access Control

SGI/N6 & External Roaming Threats
- IoT Core integration
- VAS integration
- App server vulnerabilities
- Application vulnerabilities
- API vulnerabilities

Legend
- Slice 1
- Slice 2
- Slice 3
- Slice 4

References
[1] 5G Security innovation with Cisco, White paper, 2018
5G Threat Surface

Quantum Threats

Device Threats
- Malware
- Sensor Susceptibility
- TFTP MitM attacks
- Bots
- DDoS
- Firmware Hacks
- Device Tampering

Air Interface Threats
- MitM attack
- Jamming

RAN Threats
- MEC Server Vulnerability
- Rogue Nodes

Backhaul Threats
- DDoS attacks
- CP/UP Sniffing
- MEC Backhaul sniff

5G Packet Core & OAM Threats
- Virtualization
- Network Slice security
- API vulnerabilities
- IoT Core integration
- Roaming Partner vulnerabilities
- DDoS & DoS attacks
- Improper Access Control

SGI/N6 & External Roaming Threats
- IoT Core integration
- VAS integration
- App server vulnerabilities
- Application vulnerabilities
- API vulnerabilities

Device Trust, Endpoint

RAN unsafe crypto

Quantum unsafe cryptography implementation, usage

[1] 5G Security innovation with Cisco, White paper, 2018