SESSION ID: SDS-R02

Building the Roots of the Quantum-Safe World

Avesta Hojjati, PhD (in progress)
Head of R&D
DigiCert Inc.

Alexander Truskovsky, MBA, MCompSc, CISSP
Director, Technical Strategy
ISARA Corporation
Avesta Hojjati, PhD (in progress)

Avesta is the head of R&D at DigiCert where he manages advanced development of cybersecurity products. Prior to DigiCert, Avesta was part of the Symantec and Yahoo security teams. Avesta focuses on applied cryptography, post-quantum cryptography, blockchain, and IoT. Avesta earned his Master’s in Computer Science from University of Illinois at Urbana Champaign and is currently completing his PhD.

Alexander Truskovsky, MBA, MCompSc, CISSP

Alexander is responsible for technical strategy at ISARA. Previous to ISARA, he provided technical leadership in the development of core security protocols and features at BlackBerry and designed and built enterprise software at Oracle. He has a Master of Computer Science focusing on applied cryptography, an MBA, and holds a CISSP designation. He holds 20 patents in areas of security protocols.
Agenda

- Quantum Computing
- Threat & Mitigation
- Migration Challenges & Crypto Agility
- Quantum-safe Roots of Trust and Code Signing
- Conclusions
QUANTUM MECHANICS

THE WORLD IS NOT WHAT IT SEEMS
If you think you understand quantum mechanics, you don't understand quantum mechanics.

— Richard P. Feynman —
QUANTUM COMPUTING IS THE MARRIAGE OF...

INFORMATION THEORY

QUANTUM MECHANICS
QUANTUM vs CLASSICAL

Horsepower
December 17, 1903

1st Flight of Wright Flyer I
December 17, 1903
POSITIVE DISRUPTIONS

MATERIAL DESIGN
CHEMICAL DISCOVERY
DRUG DESIGN
OPTIMIZATION
SEARCH/BIG DATA
MACHINE LEARNING
TIMELINE TO QUANTUM

ANALOG QC

NOISY QC

UNIVERSAL QC
The Quantum Race is on
Threat & Mitigation
# The Quantum Effect on Today’s Cryptography

<table>
<thead>
<tr>
<th>Type</th>
<th>Algorithm</th>
<th>Key Strength Classic (bits)</th>
<th>Key Strength Quantum (bits)</th>
<th>Quantum Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asymmetric</td>
<td>RSA 2048</td>
<td>112</td>
<td>0</td>
<td>Shor’s Algorithm</td>
</tr>
<tr>
<td></td>
<td>RSA 3072</td>
<td>128</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECC 256</td>
<td>128</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECC 521</td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symmetric</td>
<td>AES 128</td>
<td>128</td>
<td>64</td>
<td>Grover’s Algorithm</td>
</tr>
<tr>
<td></td>
<td>AES 256</td>
<td>256</td>
<td>128</td>
<td></td>
</tr>
</tbody>
</table>
Cause of security breaches today

Quantum: an unprecedented threat looming
IBM less than 20 years

Microsoft less than 11 years

ETSI less than 10 years

NIST less than 11 years

European Commission after 2025
THE "NEW" MATH

- Hash-based
- Code-based
- Lattice-based
- Multivariate-based
- Isogeny-based
Hash-Based Cryptography

- Introduced by Merkle in 1979
- Uses “one-time signatures”
- Small public key, medium signature size, very large private key
- Key generation can be slow, but signing & verification is fast
- Private key is stateful
- Can be used today
# Quantum-safe Asymmetric Algorithms (Table 1 of 2)

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Family</th>
<th>Type</th>
<th>Secret Key (Octets)</th>
<th>Public Key (Octets)</th>
<th>Signature (Octets)</th>
<th>Ciphertext (Octets)</th>
<th>Shared Secret (Octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMS</td>
<td>Stateful Hash-based</td>
<td>Signature</td>
<td>56 + (2,064 - 2,147,483,664)</td>
<td>32</td>
<td>1,296 - 9,328</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>XMSS</td>
<td>Stateful Hash-based</td>
<td>Signature</td>
<td>104 + (65,568 - 67,108,896)</td>
<td>32</td>
<td>2,500 – 2,820</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>SPHINCS</td>
<td>Stateless Hash-based</td>
<td>Signature</td>
<td>64 - 128</td>
<td>32 - 64</td>
<td>8,080 - 49,216</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIKE</td>
<td>Code-based</td>
<td>KEM</td>
<td>3,194 - 11,749</td>
<td>1,478 - 11,217</td>
<td>–</td>
<td>1,478 - 11,217</td>
<td>32</td>
</tr>
<tr>
<td>Classic McElieic</td>
<td>Code-based</td>
<td>KEM</td>
<td>6,452 - 14,080</td>
<td>261,120 - 1,357,824</td>
<td>–</td>
<td>128 - 240</td>
<td>32</td>
</tr>
<tr>
<td>HQC</td>
<td>Code-based</td>
<td>KEM</td>
<td>40</td>
<td>3,125 - 8,897</td>
<td>–</td>
<td>6,234 - 17,777</td>
<td>64</td>
</tr>
<tr>
<td>LEDAcrypt</td>
<td>Code-based</td>
<td>KEM</td>
<td>24 - 40</td>
<td>1,872 - 8,520</td>
<td>–</td>
<td>1,872 - 4,616</td>
<td>32 - 64</td>
</tr>
<tr>
<td>ROLO</td>
<td>Code-based</td>
<td>KEM</td>
<td>40</td>
<td>465 - 2,493</td>
<td>–</td>
<td>465 - 2,621</td>
<td>40 - 64</td>
</tr>
<tr>
<td>RQC</td>
<td>Code-based</td>
<td>KEM</td>
<td>40</td>
<td>853 - 2,284</td>
<td>–</td>
<td>1,690 - 4,552</td>
<td>64</td>
</tr>
<tr>
<td>Kyber</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>1,632 – 3,168</td>
<td>800 – 1,568</td>
<td>–</td>
<td>736 – 1,568</td>
<td>32</td>
</tr>
<tr>
<td>FrodoKEM</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>19,888 - 43,088</td>
<td>9,616 - 21,520</td>
<td>–</td>
<td>9,720 - 21,623</td>
<td>16 - 32</td>
</tr>
<tr>
<td>LAC</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>1,056 - 2,080</td>
<td>544 - 1,056</td>
<td>–</td>
<td>712 - 1,424</td>
<td>32</td>
</tr>
<tr>
<td>NewHope</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>1,888 - 3,680</td>
<td>928 - 1,824</td>
<td>–</td>
<td>1,120 - 2,208</td>
<td>32</td>
</tr>
</tbody>
</table>
## Quantum-safe Asymmetric Algorithms (Table 2 of 2)

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Family</th>
<th>Type</th>
<th>Secret Key (Octets)</th>
<th>Public Key (Octets)</th>
<th>Signature (Octets)</th>
<th>Ciphertext (Octets)</th>
<th>Shared Secret (Octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTRU</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>935 - 1,592</td>
<td>699 - 1,230</td>
<td>–</td>
<td>699 - 1,230</td>
<td>32</td>
</tr>
<tr>
<td>NTRUPrime</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>1,125 - 1,999</td>
<td>897 - 1,322</td>
<td>–</td>
<td>897 - 1,184</td>
<td>32</td>
</tr>
<tr>
<td>Round5</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>16 - 32</td>
<td>445 - 14,264</td>
<td>–</td>
<td>549 - 14,288</td>
<td>16 - 32</td>
</tr>
<tr>
<td>SABER</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>1,568 - 3,040</td>
<td>672 - 1,312</td>
<td>–</td>
<td>736 - 1,472</td>
<td>32</td>
</tr>
<tr>
<td>Three Bears</td>
<td>Lattice-based</td>
<td>KEM</td>
<td>40</td>
<td>804 - 1,584</td>
<td>–</td>
<td>917 - 1,697</td>
<td>32</td>
</tr>
<tr>
<td>Dilithium</td>
<td>Lattice-based</td>
<td>Signature</td>
<td>96 - 2096</td>
<td>896 – 1,760</td>
<td>1,387 – 3,366</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Falcon</td>
<td>Lattice-based</td>
<td>Signature</td>
<td>4,097 – 8,193</td>
<td>897 – 1,793</td>
<td>618 – 1,233</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>qTesla</td>
<td>Lattice-based</td>
<td>Signature</td>
<td>1,216 - 12,352</td>
<td>1,504 - 38,432</td>
<td>1,376 - 5,920</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>GeMSS</td>
<td>Multivariate-based</td>
<td>Signature</td>
<td>13,415 - 77,712</td>
<td>36,0643 - 3,210,845</td>
<td>33 - 75</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>LUOV</td>
<td>Multivariate-based</td>
<td>Signature</td>
<td>32</td>
<td>5,120 – 77,312</td>
<td>311 – 4,390</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>MQDSS</td>
<td>Multivariate-based</td>
<td>Signature</td>
<td>16 – 24</td>
<td>46 – 64</td>
<td>20,854 – 43,728</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Rainbow</td>
<td>Multivariate-based</td>
<td>Signature</td>
<td>95,232 - 1,256,551</td>
<td>152,576 - 1,746,432</td>
<td>64 - 204</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>SIKE</td>
<td>Supersingular Isogeny-Based</td>
<td>KEM</td>
<td>374 - 644</td>
<td>330 - 564</td>
<td>–</td>
<td>346 - 596</td>
<td>16 - 32</td>
</tr>
<tr>
<td>Picnic</td>
<td>Zero-Knowledge Proof/MPC</td>
<td>Signature</td>
<td>16 - 32</td>
<td>32 - 64</td>
<td>13,802 - 209,506</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>
POST-QUANTUM STANDARDS
NIST PQC Evaluation & Standardization Timeline

2016

NSA Suite-B Announcement

2017

Formal Call for Submissions

2018

Submission Deadline
Initial Submissions: 82
Accepted Submissions: 69

1st NIST PQC Standardization Conference

2019

Today

2020

2nd NIST PQC Standardization Conference

NIST Round 2 Announcement
Signature Algorithms: 9
Key Encapsulation Algorithms: 17

2021

Analysis Complete

2022

2023

2024

2025

Standards Ready
Hypothetical 15-year View For PQ Crypto

Dec 2017 – Dec 2023
NIST PQ Standardization Process

~ 2030
Quantum Computer Breaks Asymmetric Crypto

R&D
PILOTS

WE ARE HERE

ROLLOUTS
MIGRATION
STANDARDS DISCUSSIONS
DECOMMISSION

Learning from the past

- Internet Protocol Version 4 (IPv4) has been around since 1981
- In 1998, IPv6 became a Draft Standard for the IETF
- 49 countries deliver more than 5% of traffic over IPv6, with new countries joining all the time.
- Alexa Top Million Websites: 17% with working IPv6

- India, 44%
- USA, 21%
- Brazil, 6%
- Germany, 6%
- Other, 7%
- Australia, 1%
- Vietnam, 1%
- Malaysia, 1%
- Korea, 1%
- Belgium, 1%
- Canada, 1%
- France, 2%
- UK, 3%
- Japan, 5%
Lessons Learned

- Secure Hash Algorithm 1 (SHA1) was introduced in 1993
- In 2005, it was shown that SHA1 is not collision-resistant
- In 2017, Chrome announced SHA1 to be insecure
- 0% of public websites are using SHA1!

Microsoft tells CAs to stop issuing new SHA-1 certs

Facebook’s server stop accepting SHA-1 for developers using its SDKs

Google will remove SHA-1 certificate in Chrome

Windows will stop accepting SHA-1 end-entity certificates

Microsoft cuts off support for SHA-1 in Edge and Internet Explorer 11
Lessons Learned

- Secure Hash Algorithm 1 (SHA1) was introduced in 1993
- In 2005, it was shown that SHA1 is not collision-resistant
- In 2017, Chrome announced SHA1 to be insecure
- 0% of the public websites are using SHA1
As the replacements for currently standardized public key algorithms are not yet ready, a focus on maintaining crypto agility is imperative. Until new quantum-resistant algorithms are standardized, agencies should continue to use the recommended algorithms currently specified in NIST standards.

What is Crypto Agility?

- **Users**: Employees, Contractors, Military Personnel
- **Products**: VPNs, PKIs, IoT Devices, Vehicles, Apps
- **Protocols**: TLS, IPsec, SSH, S/MIME, Signal
- **Cryptosystems**: RSA, ECC, DH
- **Administrators**: Policies
BRIDGING THE GAP

Hybrid-Crypto (Current + Quantum-Safe)

Current Public Key Cryptography  Crypto-Agility  Quantum-safe Cryptography

Today  ?
HOW ARE SECURE COMMUNICATIONS VULNERABLE?

- Shor's Algorithm breaks current public-key algorithms
- Grover's Algorithm weakens symmetric encryption (square root)
A HARVEST & DECRYPT ATTACK ON VPN

VPN Session

Handshake

Key Establishment

Quantum attack using Shor's algorithm

Data Exchange

Obtain private key

Ciphertext

Decrypt using extracted key

Plaintext
HYBRID KEY ESTABLISHMENT

- Classic Algorithm
- Quantum-Safe Algorithm 1
- Quantum-Safe Algorithm 2

Key Derivation

Quantum-Safe Key
THE MIGRATION CHALLENGE
KEY ESTABLISHMENT vs AUTHENTICATION

Key establishment can be **easily upgraded** because the client and server negotiate which algorithm to use.

1) Use quantum-safe **key transport** or **key agreement** algorithms
2) Use **hybrid keys**, a mix of both classic and quantum-safe algorithms

The complexity and interconnectivity of public key infrastructure demands action today in order to be ready for the quantum age, and difficult to do while maintaining backward compatibility.
DoD PKI MIGRATION

There’s more than 4.5 million active users in the DoD identity management system.

Creating a quantum-safe duplicate infrastructure is time-consuming and cost prohibitive.
Certificates Support a Single Algorithm

User/server needs to select which certificate to use

PKI management costs increase
Quantum-safe Roots of Trust and Code Signing
Prioritizing the Fix for Tomorrow’s Threat

Public-key cryptography broken

Development & Production = 6-8 years
Life of an Average Vehicle = 11.5 years

What’s at risk?
Durable connected devices (IoT) with long in-field lives (i.e. connected cars, medical devices, satellites).

What’s the attack?
Forged software updates: quantum-enabled adversaries will be able to sign software updates that appear authentic, injecting malicious code onto the device to take it over.

How to protect against it?
Physically embed stateful hash-based roots of trust today to avoid costly, logistically challenging recalls in the future.
NIST on Stateful Hash-based Signatures (HBS)

• HBS schemes are good candidates for early standardization because they’re trusted, mature, and well understood

• NIST is actively reviewing XMSS and LMS for early approval outside the Post-Quantum Standardization Process

• NIST is considering stateful HBS for specific use-cases, such as code-signing

• The security of an HBS scheme relies on the same basis as many current NIST-approved cryptographic algorithms and protocols, and no known quantum algorithms pose a practical threat
Stateful HBS Implementation Considerations in HSM

- If not implemented properly, stateful HBS are vulnerable to misuse
- Stateful HBS signing keys are strictly one time use only
- The full private key needs to be split up for 1) back up and 2) to reserve a part of it for revocation, all parts need to be managed completely independently
- The full tree, or a part of it, is often too large to fit in an HSM without using tree compression
- At run time a range of keys needs to be loaded but before any of them are used, they need to be marked as used up
Operational Implications When Using HBS

- The private key of a stateful HBS scheme is an “exhaustible” resource, so careful planning is required or you’ll run out of keys.
- Signature size grows as the size of the private key grows.
- Private key splitting and state management is not something the industry has had to deal with before.
- For extremely high-value root keys that don’t produce many signatures during their validity a manual process for state management may be required.
### Certificate Manager

#### Your Certificates

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Security Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>DigiCert Root CA</td>
<td>Software Security Device</td>
</tr>
<tr>
<td>Digital Signature Trust Co.</td>
<td>Builtin Object Token</td>
</tr>
<tr>
<td>DST Root CA X3</td>
<td>Builtin Object Token</td>
</tr>
<tr>
<td>Disig a.s.</td>
<td>Builtin Object Token</td>
</tr>
<tr>
<td>CA Disig Root R2</td>
<td>Builtin Object Token</td>
</tr>
<tr>
<td>E-Tugra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.</td>
<td>Builtin Object Token</td>
</tr>
<tr>
<td>E-Tugra Certification Authority</td>
<td>Builtin Object Token</td>
</tr>
<tr>
<td>Entrust, Inc.</td>
<td>Builtin Object Token</td>
</tr>
<tr>
<td>Entrust Root Certification Authority</td>
<td>Builtin Object Token</td>
</tr>
</tbody>
</table>

#### Edit Trust

- View
- Edit Trust
- Import
- Export
- Delete or Distrust
Conclusions
THE CHALLENGE

With increased connectivity, the scale of what needs to be updated also increases.

Maintain Interoperability  
Migrate Critical Systems Faster  
Reduce Switching Costs
Summary of the Journey

• Identified long-lived devices as critical assets we need to protect today

• Selected a mature post-quantum algorithm suitable for this purpose

• Worked with Gemalto to implement HSS and XMSS on Luna7 HSM, including tree splitting, tree compression, and other state management strategies

• Updated operational procedures to include planning for exhaustible private key resource and private key state management across multiple key instances
Apply What You Have Learned Today

• Next week you should:
  – Conduct your own research on how large-scale quantum computing will impact public-key cryptography and how it will affect your business

• In the first three months following this presentation you should:
  – Perform an archeological expedition to understand how cryptography is used in your organization
  – Identify and prioritize high-value assets for migration

• Within six months you should:
  – Collaborate with your internal team to create a migration plan
  – Share your needs with key vendors to ensure their roadmap aligns
Thank You

avesta.hojjati@digicert.com
alex@isara.com