WELLS FARGO

April 2024

Wells Fargo Technology Case Study

Quantum Entropy injection into HSMs for Post Quantum Cryptographic (PQC) Key Generation

Wells Fargo Technology
Cybersecurity Data Science (CSDS)
Post Quantum Cryptography (PQC)

Contents

Abstract

In cybersecurity, entropy is the measure of randomness in a string of bits. In cryptography, entropy is used to produce random numbers, which in turn are used to produce cryptographic keys. As entropy increases, randomness gets better, keys become more difficult to be determined, and security improves. Entropy is also important for the generation of random numbers and other critical security parameters such as seeds, salts, and initialization vectors for cryptographic algorithms.

Financial institutions must deal with the constant risk of cyber-attacks, underlining the responsibility to maintain and strengthen digital security for customers' trust and integrity. A foundational step for addressing these issues is generating stronger cryptographic keys with better entropy. Using random bits (from quantum sourced entropy) that are proven for improved randomness and unpredictability is pivotal for both today's classical cryptography and tomorrow's quantum resistant cryptography.

Challenge Statement

Generating cryptographic keys with weak entropy makes systems less secure because the keys are more susceptible to attacks. So, in cryptography, the random numbers are not only conforming to uniform distributions; those random numbers must possess unpredictability too.

If an adversary manages to guess the cryptographic key, they can compromise the fundamental requirements of information security, namely confidentiality, integrity, and availability. To prevent this, it is crucial that the entropy for the key generation process is sufficiently high, making it very challenging for the adversary to guess the keys.

Introduction

When cryptanalytically-relevant quantum computers (CRQC) become available, they will make today's public key cryptography (PKC) obsolete. Encryption, digital signatures, and key management based on mathematics, such as factorization (RSA), discrete logs (Diffie-Helman), and elliptic curves (ECC), that would take thousands of years to break using classical computers, could be broken with ease by a quantum computer. Designing security solutions for the post-quantum world (also known as post-quantum cryptography), means new techniques and algorithms must be developed, adopted, standardized, and widely deployed. Compounding the quantum threat, is the use of weak entropy to generate cryptographic keys.

A brute-force attack can be used to predict the keys if there is not sufficient entropy, as was shown by Ahmad in [1]. There are several cases of incorrect RNG implementation that have led to serious vulnerabilities. Bernstein et al [2] found how FIPS 140-2 level 2 certified smart card generated repeated or guessable keys due to the low-quality hardware RNG. Quantum entropy, a measure of randomness or uncertainty in a quantum state, can be harnessed to generate verifiable true random numbers. These random numbers can then be used to create strong quantum-resistant cryptographic keys.

Wells Fargo, Thales, and Quantinuum, working in collaborative research, demonstrated the ability to generate strong cryptographic keys within the cryptographic boundary of Thales Luna HSM, a FIPS 140-2 level 3 cryptographic module with external entropy from Quantinuum Origin. The keys were generated using random bits with verified quantum entropy. The entropy was acquired from the Quantinuum Origin trapped ion-based quantum computer and validated using the Bell Test to prove it met the threshold for quantum entropy. This cryptographic solution gives Wells Fargo a proven quantum entropy source to generate ultra-secure keys that can be designed and deployed at scale.

Through this collaborative research project, Wells Fargo created a strong foundation for cryptographic agility that supports legacy and post-quantum cryptographic (PQC) algorithms. This gives Wells Fargo, and demonstrates to the financial industry, a proven, integrated solution that allows new quantum-resistant algorithms with secure key generation to be implemented on commercially available hardware. It also allows the use of a hybrid strategy that can provide the necessary agility to react to future threats quickly and with minimal disruption to everyday operations.

Figure 1 illustrates a basic framework for an entropy source and its consumer. The preparation and transfer of the entropy bits is enabled using an “Entropy as a Service” (EaaS). If the entropy source harnesses quantum mechanical phenomena to generate random bits, then the RNGs are referred to as Quantum RNG (QRNG).

Figure 1 : Basic Framework Entropy Source and Consumer

Technical Description

Our experiment relies on a QRNG to provide the high-quality entropy, the QRNG includes entropy evaluation and randomness extraction when using quantum mechanical phenomena as the source for entropy, similar to what was disclosed by Ma et al in [3].

Figure 2 : Generic QRNG - Entropy as a Service

Since entropy offers a measure of randomness, there are two key steps to provide Entropy as a Service. As shown in Figure 2, the entropy source consists of a physical system such as one that produces quantum phenomena, followed by the measurement of the quantum phenomena. The output from the entropy source i.e., the digitized entropy (“raw bits”) undergoes processing and testing before being made available as random bitstring to a webserver for downstream distribution.

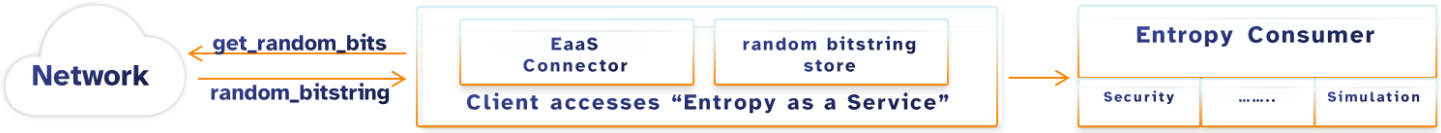

Figure 3 : Generic QRNG - Using the Entropy

On the client side, a connector retrieves and stores the random bitstring received from the EaaS. An application that consumes the random bitstring, receives or retrieves the random bitstring from the store.

Proof of Technology Setup

To achieve this solution, the research team integrated entropy from Quantinuum’ s Quantum Origin into the Thales Luna cryptographic Hardware Security Module (HSM). Quantum Origin harnesses quantum mechanical phenomena to generate the highest quality entropy. A specialized functionality module (FM) for the Luna, which combines Quantum Origin’s quantum entropy with the Luna HSMs local source of entropy to provide better entropy for generating stronger keys.

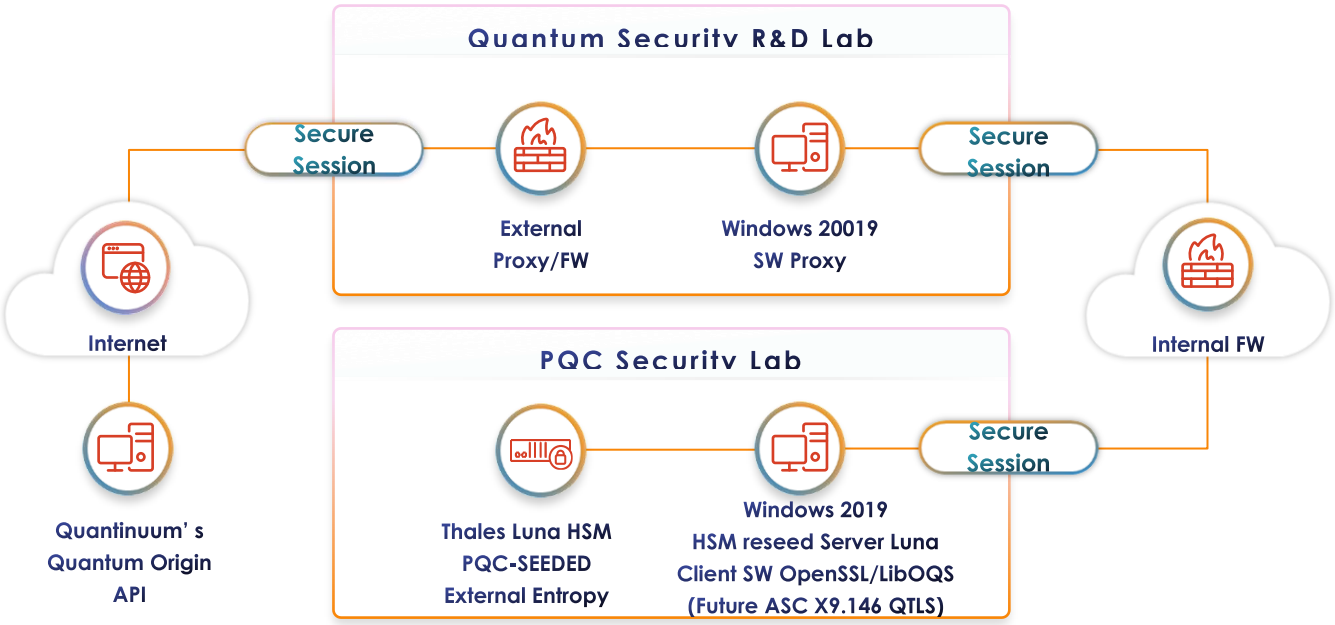

Figure 4 : Overview of the QRNG Proof of Technology

Figure 4 illustrates the primary elements that enabled the experiment. The Reseed Server and Thales Luna HSM resided in the PQC Security Lab, while the internal Windows proxy and external proxy resided in the Quantum Security R&D Lab. The Reseed server retrieved random bitstrings through the Windows 2019 proxy in the Quantum Security R&D Lab from the external Quantum Origin Server, the random bitstrings were then injected into the Luna HSM. The Luna HSM then derived high-quality entropy at the HSM, allowing Wells Fargo to generate stronger encryption keys that can be generated and designed at scale to transition [4] from legacy cryptography to PQC.

Figure 5 shows the functional details of various software components that made this experiment possible. Other than the infrastructure devices, those software components resided with four distinct elements:

- **Proxy server** provides internet connectivity, using STunnel, to the machines in the PQC lab.
- **Reseed server** runs the Quantum Origin (QO) client which made API calls to the external Quantum Origin Server to get random bitstring. Though the Reseed server had the Luna HSM Client software installed, a service provided the random bitstring to the HSM. The HSM service and the QO client were built into a Windows service. The following software packages were installed on the Reseed server:
  - Luna HSM Client 10.5.0 (to connect to HSMs).
  - QOLunaReseedService (to connect to QO, it includes the 'HSM Service' and the 'Quantum Origin Client').
  - OpenSSL 1.1.1o
- **Thales Luna HSM** with a functionality module (FM), which received the random bitstrings to be mixed with a local entropy to prepare better entropy used to generate stronger cryptographic keys.
- **Quantum Origin** provided the random bitstrings.

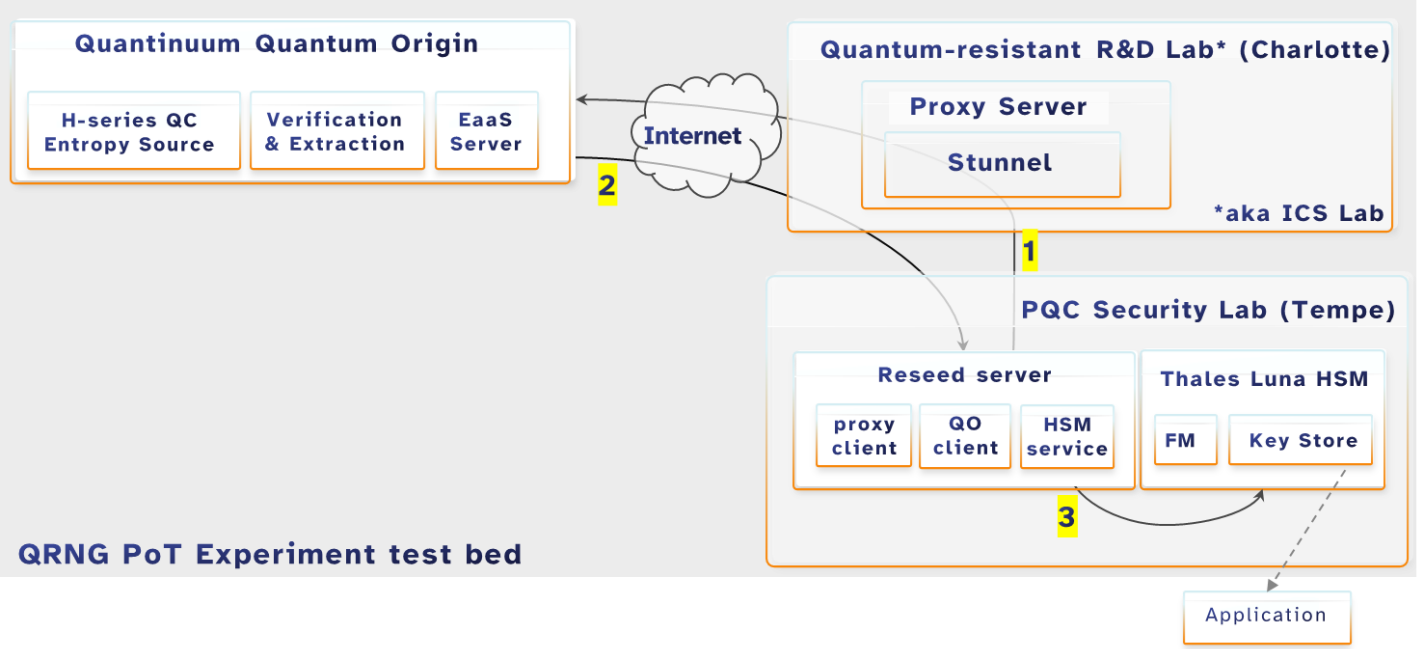

Figure 5 : Experiment Test Bed

The reseed server made the REST API calls to the Quantum Origin (shown as **1** in Figure 5) through the proxy server. The Quantum Origin service responded with the random bitstring (shown as **2**); when the QO client received the random bitstring, and it was made available to the HSM service. The HSM service handed the random bitstrings over to the Thales Luna HSM (shown as **3**). The HSM then used the random bitstrings to generate better entropy to be used during the key generation process. The generated keys were stored in a specific partition of the HSM.

Observations

Connectivity from the internal proxy server to the Quantum Origin service was tested as shown in Figure 6. The test for connectivity was performed using OpenSSL.

```
C:\>openssl s_client -connect qo-us.cambridgequantum.com:443
66976:error:0200274C:system library:connect:reason(1868):crypto\bio\b_sock2.c:110:
66976:error:2008A067:BIO routines:BIO_connect:connect error:crypto\bio\b_sock2.c:111:
connect:errno=0

C:\>ping qo-us.cambridgequantum.com

Pinging api989a0d60da6046ddbb6d215dbb27c392nzfcsfg81x4hrjpzqydus.eastus.cloudapp.azure.com [20.88.185.124] wit
h 32 bytes of data:
Request timed out.

Ping statistics for 20.88.185.124:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\>openssl s_client -proxy [redacted] -connect qo-us.cambridgequantum.com:443
CONNECTED(0000013C)
depth=1 C = US, O = "DigiCert, Inc.", CN = GeoTrust Global TLS RSA4096 SHA256 2022 CA1
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = qo-us.cambridgequantum.com
verify return:1
---
Certificate chain
 0 s:CN = qo-us.cambridgequantum.com
   i:C = US, O = "DigiCert, Inc.", CN = GeoTrust Global TLS RSA4096 SHA256 2022 CA1
 1 s:C = US, O = "DigiCert, Inc.", CN = GeoTrust Global TLS RSA4096 SHA256 2022 CA1
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root CA
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIHqDCCBYigAwIBAgIQCiOuqlQ86SImuiYiF1Je7TANBgkqhkiG9w0BAQsFADBc
```

Figure 6 : Connecting to Quantum Origin Service

The Luna Client Module utility was used, as shown in Figure 7 to test and confirm the HSM was up and running and the connectivity was confirmed.

```
C:\Program Files\SafeNet\LunaClient>lunacm
lunacm (64-bit) v10.5.0-470. Copyright (c) 2022 SafeNet. All rights reserved.


        Available HSMs:

        Slot Id ->              0
        Label ->                CQ-SEEDED
        Serial Number ->        [redacted]88287[redacted]
        Model ->                LunaSA 7.7.1
        Firmware Version ->     7.[redacted]
        Bootloader Version ->   1.[redacted]
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         FM

        Slot Id ->              1
        Label ->                CQ-RESEED
        Serial Number ->        [redacted]88287[redacted]
        Model ->                LunaSA 7.7.1
        Firmware Version ->     7.[redacted]
        Bootloader Version ->   1.[redacted]
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         FM


        Current Slot Id: 0


lunacm:> exit
```

Figure 7 : Confirming connection to the HSM

Once the Luna HSM was running, the lunareseed service on the reseed server was configured to obtain the entropy from the QO and provide it to the HSM. There are two logs that were verified:

(i) The STunnel log below in Figure 8 indicates that qo-us.cambridgequantum.com has been connected.

```
2022.10.21 17:36:18 LOG5[main]: Configuration successful
2022.10.21 17:39:20 LOG5[0]: Service [origin-inbound-tls] accepted connection from 10.255.26.201:54704
2022.10.21 17:39:20 LOG5[0]: s_connect: connected 127.0.0.1:8080
2022.10.21 17:39:20 LOG5[0]: Service [origin-inbound-tls] connected remote server from 127.0.0.1:59954
2022.10.21 17:39:20 LOG5[1]: Service [origin-outbound-tls] accepted connection from 127.0.0.1:59954
2022.10.21 17:39:20 LOG5[1]: s_connect: connected 159.45.225.47:8080
2022.10.21 17:39:20 LOG5[1]: Service [origin-outbound-tls] connected remote server from 10.251.65.52:59955
2022.10.21 17:39:20 LOG5[1]: Certificate accepted at depth=0: CN=qo-us.cambridgequantum.com
```

Figure 8 : Confirming connection to the QO Server

(ii) Luna HSM seeded message: Here is the Event Viewer on the Reseed server with a message indicating that the HSM is getting entropy from the QO. In Figure 7 it was shown that the partition on the HSM to receive the random bitstring was CQ-SEEDED.

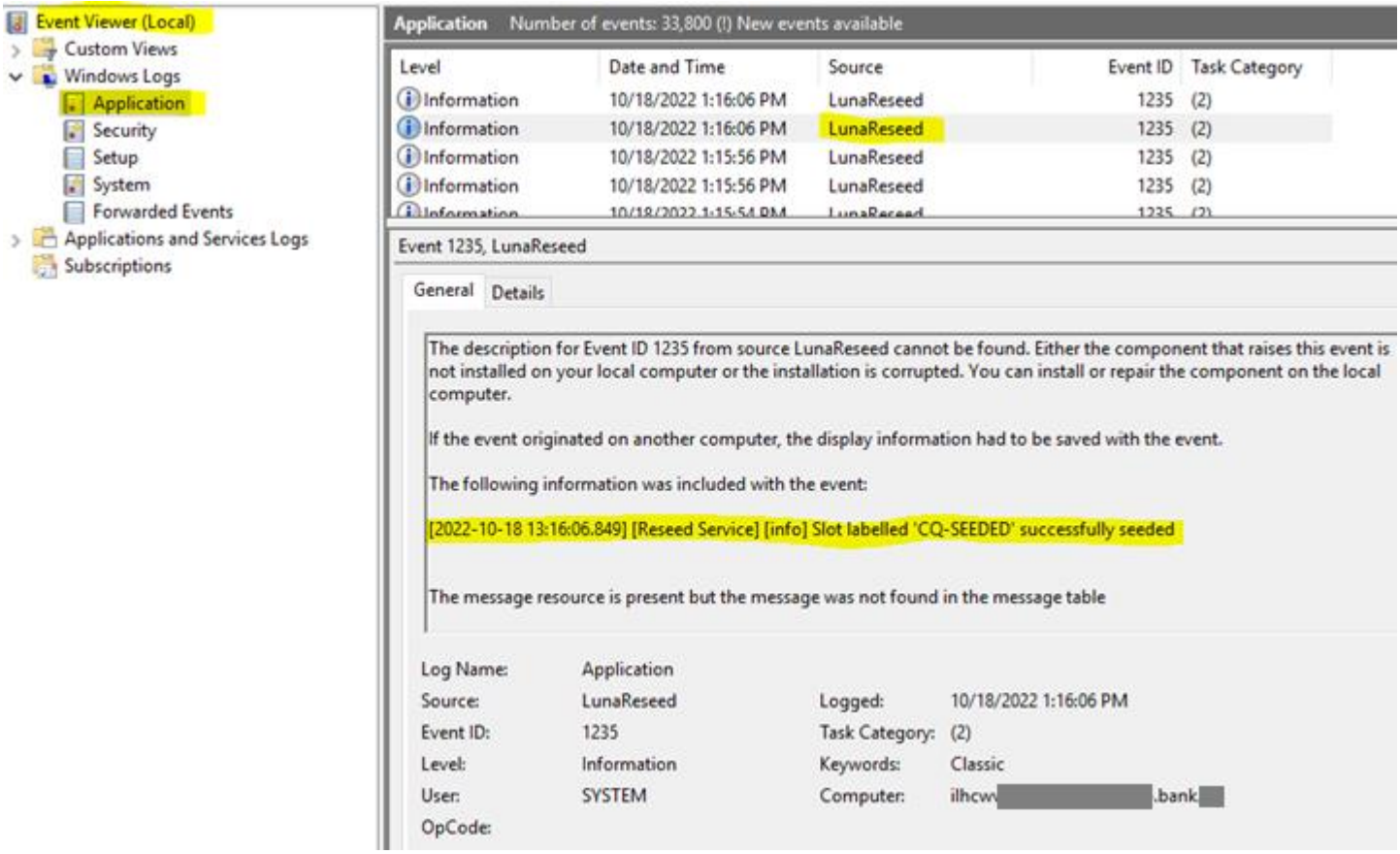

Figure 9 : HSM receives Random Bitstring

The highlighted message in Figure 9 indicates the HSM service successfully transferred the random bitstring to the HSM device.

The Thales Luna HSM is ready to generate stronger cryptographic keys using better entropy i.e., entropy sources from the Quantum Origin Entropy-as-a-Service. Thus, the experiment that the quantum entropy injection into HSMs for creation of Post Quantum Cryptographic (PQC) Keys was demonstrated.

Results

Wells Fargo leveraged solutions from Thales and Quantinuum to generate quantum-resistant asymmetric cryptographic keys in conformity within the boundaries of the Federal Information Processing Standards (FIPS) 140-3 level 3 cryptographic module.

Through this demonstration, Wells Fargo has created a solid foundation that allows cryptographic agility to be implemented in legacy and post-quantum cryptographic (PQC) algorithms. This gives Wells Fargo a proven, integrated solution that allows new quantum-resistant algorithms with secure key generation to be implemented on commercially available hardware, as well as demonstrating to the financial industry in large of the capabilities of said solutions.

Conclusion

Developing quantum-resistant capabilities is crucial to maintaining data security and integrity for critical applications and infrastructure. To achieve that, Wells Fargo is leading the development of quantum secure infrastructure through their PQC program. It is important to ensure cryptographic agility for legacy and PQC algorithms while they are still in development to stay ahead of the curve in the cybersecurity race. The advances in quantum secure crypto solutions are achievable through cooperation from respective leaders in their tech space. Peter Bordow, Wells Fargo's Distinguished Engineer and PQC and Emerging Technologies leader, emphasized that "*Wells Fargo continues to proactively formulate strategic and robust technical solutions so that the data, systems, and applications our customers rely upon can remain safe in an inevitable new paradigm of quantum technology*."

Wells Fargo is a recognized thought leader in PQC and leads several external efforts to define and publish standards, define and drive PQC strategy for the financial sector, while helping to coordinate national and international efforts. Wells Fargo also Chairs the PQC Workgroup within the national Financial Services Information Sharing and Analysis Center (FS-ISAC) that brings together experts from various financial institutions to help solve and provide guidance on PQC migration and crypto-agility. Wells Fargo also provides a supportive role at ASC X9 [5].

Quantinuum provided a high-quality unpredictable entropy source for the generation of quantum-computing-hardened encryption keys.

Thales Luna HSMs provided high level of security to generate and store cryptographic keys in an intrusion-resistant, tamper-evident, FIPS-validated appliance, which enables a crypto agile solution to be implemented quickly to help navigate the changes required for the transformation to Post-Quantum Cryptography.

The research team comprising Quantinuum, Thales, and Wells Fargo collaborated, to generate strong cryptographic keys in a tailored experiment to show how the bank could formulate a pathway to further strengthen and secure its cryptographic framework. This joint effort not only demonstrated how to solve the immediate cryptography challenge but has also paved way for ongoing research collaboration amongst Thales, Quantinuum and Wells Fargo aiming to develop more robust cryptographic solutions as the next steps.

References

[1]: D. Ahmad, "Two Years of Broken Crypto: Debian's Dress Rehearsal for a Global PKI Compromise," in *IEEE Security & Privacy*, vol. 6, no. 5, pp. 70-73, Sept.-Oct. 2008, doi: 10.1109/MSP.2008.131.

[2]: Bernstein et al. "Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild". ASIACRYPT 2013. Lecture Notes in Computer Science, vol 8270. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-42045-0_18

[3]: Ma et al. "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction." *Physical Review A* 87.6 (2013): 062327.

[4]: Stapleton et al. "Cryptographic transitions," *2006 IEEE Region 5 Conference*, San Antonio, TX, USA, 2006, pp. 22-30, doi: 10.1109/TPSD.2006.5507465.

[5]: X9 Informative Report – X9 IR F01-2022, (11/29/2022) Prepared by ASC X9 Quantum Computing Risk Study Group