Challenges in Transitioning to Post quantum Cryptography

Dr. Bharat S. Rawal
Grambling State University
Dr. Bharat S. Rawal
D.Sc, M.Sc, M.B.A, SM-IEEE/EAI
Educational Background

D.Sc.  Information Technology, Towson University, December 2011.
M.B.A.  UB/Towson University, December 2008.
M.Sc.  Physics, South Gujarat University, India, May 1990.
B.Sc.  Physics, South Gujarat University, India, May 1986.
Professional Experience

Industries: (Health Care / Pharmaceuticals) CEO/Chairman

IT/Cybersecurity, Quantum Computing CEO/President

Academia: Assistant Professor / Associate Professor / Full Professor

Administrative: Program Co-Ordinator, Program Director, Department Chair
Scholarly Works

US Patents


Books

  Authorship: First Author

  Authorship: First Author

  Authorship: Co-Author

  Authorship: Co-Author

- Introduction to Quantum Computing Springer Book (2024) In Press
  Authorship: Co-Author
Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. It involves constructing and analyzing protocols that prevent third parties or the public from reading private messages.
SYMMETRIC CRYPTOGRAPHY SCHEMES

Symmetric cryptography schemes
ASYMMETRIC CRYPTOGRAPHY SCHEMES
TYPES OF CRYPTOGRAPHY

- Hash-based Cryptography
- Code-based Cryptography
- Lattice-based Cryptography
- Elliptic Curve Cryptography (ECC)
- Homomorphic Encryption
WIDELY USED CRYPTOGRAPHY

- **Advanced Encryption Standard (AES):** Known for its security and efficiency, AES comes in three key sizes: AES-128, AES-192, and AES-256.
- **Triple Data Encryption Algorithm (TDEA/Triple DES):** DES is used three times in a row with distinct keys in symmetric encryption.
- **Blowfish:** A symmetric block cipher that operates on 64-bit blocks.
- **Twofish:** Another symmetric block cipher designed as a successor to Blowfish.
- **ChaCha20:** A stream cipher known for its speed and security.
- **RC4:** A widely used stream cipher, although it has some vulnerabilities.
- **Serpent:** A symmetric block cipher with a 128-bit block size.
- **Camellia:** A symmetric block cipher developed jointly by Japan and NTT.
- **IDEA (International Data Encryption Algorithm):** A block cipher used in some legacy systems.
SYMMETRIC CRYPTOGRAPHY SCHEMES

AES

AddRondKeys

• SubByte
• ShiftRows
• MixColumns
• AddRondKeys

CypherKey

Initial Round

RoundKey 9
9 Main Rounds

RoundKey 10
Final Round

Cyphertext
ASYMMETRIC CRYPTOGRAPHY SCHEMES

Diffie-Helman Key Exchange
ASYMMETRIC CRYPTOGRAPHY SCHEMES
RIVEST–SHAMIR–ADLEMAN (RSA)
Shor’s algorithms can break the following cryptosystems.
RSA
Diffie-Hellman key-exchange
Elliptical Curve Cryptosystem
Buchmann-William’s Key exchange
Algebraic Homomorphic

When are we expecting the availability of large quantum computers? 10, 15, or 20 years, depending on the speed of technological advancements.

Why do we have to act now?
1) Development and standardization take time.
2) Improvement also takes time.
3) Take time to build confidence in PQC.
4) It takes time to improve the usability of PQC.
5) Last year 2022 NIST announces the list of PQC.
Recently NIST has selected four cryptosystems: CRYSTALS-Kyber, Dilithium, FALCON, and SPHINCS+. CRYSTALS-Kyber is for use in general encryption. It offers several benefits including two parties can exchange relatively modest encryption keys and maintain the required speed of operation. It is faster among cross-platforms, and it is designed for efficient constant time implementation, same optimized routines across all parameters sets.
CRYSTALS-KYBER

CRYSTALS-Kyber uses a set of parameters to define the security level and efficiency of the scheme. The parameters include the dimension of the underlying lattice, the number of rounds for the encryption algorithm, and the number of bits used for public keys, secret keys, and ciphertexts. The specific values of these parameters can be chosen based on the desired security level.

Crystal-Kyber = [ A; Public Key] [s; secret key] + [e: (α, β, θ) small error terms]
= [t; public key]
V = tα, + β + m
U = Aα + θ
D = V - sU
The snapshot of the Falcon cryptosystem is reproduced here under.
Falcon work over the cyclotomic ring $R = \mathbb{Z}[x]/(x^n + 1)$.
Keygen (): Generate matrices $A$, $B$ with coefficients in $R$ such that.

\[ BA = 0 \]

\[ B \text{ has small coefficients} \]

\[ pk \leftarrow A \]
\[ sk \leftarrow B \]

Sign $m, sk$ (Performed using FFT)
Compute $c$ such that $cA = H(m)$
\[ v \leftarrow \text{“a vector in the lattice } \Lambda(B), \text{ close to } c” \]
\[ s \leftarrow c - v \]
The signature $sig$ is $s = (s_1, s_2)$

Verify $m, pk, sig$
Accept if:
\[ s \text{ is short} \]
\[ sA = H(m) \]
The main design goal is compactness: to minimize $|pk| + |sig|$
CRYSTALS-Dilithium

The signature scheme is reproduced here

**Gen**

\[ A \leftarrow Rq(k \times l) \]
\[ (s1,s2) \leftarrow Sl\eta \times Sk\eta \]
\[ t := As1 + s2 \]
\[ \text{return } (pk = (A,t), sk = (A,t,s1,s2)) \]

**Sign** ( sk, M)

\[ z := \bot \]
\[ \text{While } z = \bot \text{ do} \]
\[ y \leftarrow Sl\gamma1 - 1 \]
\[ w1 := \text{HighBits (Ay, } 2\gamma2) \]
\[ c \in B60 := H(M \parallel w1) \]
\[ z := y + cs1 \]
\[ \text{if } \|z\|\infty \geq \gamma1 - \beta \text{ or } \|\text{LowBits}(Ay - cs2, 2\gamma2)\|\infty \geq \gamma2 - \beta, \text{ then } z := \bot \]
\[ \text{return } \sigma = (z,c) \]

**Verify** (pk, M, \sigma = (z,c))

\[ w'1 := \text{HighBits}(Az - ct, 2\gamma2) \]
\[ \text{if return } [\|z\|\infty < \gamma1 - \beta] \text{ and } [c = H(M \parallel w'1)] \]
SPHINCS+ cryptography which utilizes FTS schemes [24]. This method uses a so-called hyper tree to authenticate a large number of key pairs with few-time signatures. Signature schemes known as "few-time signatures’ enable a key pair to generate a limited quantity of signatures. For every new communication, a pseudo-random FTS key pair is chosen to sign it. The FTS signature and the authentication data for that FTS key pair make up the signature. A hyper tree signature, or a signature using a certification tree of a Merkle tree signature, represents the authentication information.
PQC

The comparison of key size with Falcon for security level 1.
Comparisons the public key sizes and signature bytes of Falcon and SPHINICS+ and Dilithium at NIST security level 5.
The fastest (colored bar) and slowest (outlined bar) signature candidates from each family cross the three signature phases, with a message length of 100 Bytes.
We reproduce a quick overview of the NS sequence here [45,46]. If any element cannot be represented as a sum of any subset in a given set, this sequence can be termed an NS sequence. Each of its elements cannot equate to the sum of any combinations of the other non-repeated elements in the sequence where any element is a positive number. The NS sequence reproduced here could be mathematically represented as given in the equation under [37].
**No-Sum Sequence**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
</tr>
<tr>
<td>7</td>
<td>49</td>
</tr>
<tr>
<td>8</td>
<td>50</td>
</tr>
<tr>
<td>9</td>
<td>148</td>
</tr>
<tr>
<td>10</td>
<td>149</td>
</tr>
<tr>
<td>11</td>
<td>445</td>
</tr>
<tr>
<td>12</td>
<td>446</td>
</tr>
<tr>
<td>13</td>
<td>1336</td>
</tr>
<tr>
<td>14</td>
<td>1337</td>
</tr>
<tr>
<td>15</td>
<td>4009</td>
</tr>
<tr>
<td>16</td>
<td>4010</td>
</tr>
<tr>
<td>17</td>
<td>12028</td>
</tr>
<tr>
<td>18</td>
<td>12029</td>
</tr>
<tr>
<td>19</td>
<td>36085</td>
</tr>
<tr>
<td>20</td>
<td>36086</td>
</tr>
</tbody>
</table>
PQC Share

Sender/Receiver Registration

Sender registers with PQCShare manually.

Registered with at least one of these clouds through PQCShare.

Receiver registers with PQCShare.

FIG. 34: Registration process
It is too early to draw a conclusion since we are in the preliminary stages of exploration and standardization, but we observed in PQC that great security comes with an increase in key length, which could delay the handshake process and has an impact on the performance the system. Also, we expect the hardware to scale in performance and hard speed. We can see several solutions exist to overcome the large key sizes, software, and hard hardware faults, and malfunctions due to the complex implementation of PQC.

We proposed other cryptographic primitives to make the most popular cryptosystems quantum safe. We suggest adding additional security for smaller lattice based PQC systems so that our current network system can handle them without significant delays. Also, we explore the technique for verifying the source of the QKD transmission solving NS sequence puzzle at both ends.
Questions ????
REFERENCES

27. NISTIR 8105 Report on Post-Quantum Cryptography 10
REFERENCES

36. Giacomo Pope, CRYSTALS-Kyber Python Implementation [here]
41. https://cryptobook.nakov.com/key-exchange/diffie-hellman-key-exchange