RFC PQC
KEY IDENTIFICATION
AND SERIALIZATION
PUBLIC

Christine van Vredendaal (NXP)
Joint work with: Dieter Bong (Utimaco), Joppe Bos (NXP)
Silvio Dragone (IBM), Basil Hess (IBM), Christopher Meyer (Utimaco), Mike Osborne (IBM), Karen Willbrand (Utimaco)

JUNE 2021
PRE-QUANTUM WORLD

Alice

RSA/ECC Key exchange

“Let’s use NIST P-256 (secp256r1)”

Bob
POST QUANTUM WORLD

Alice

RSA/ECC Key exchange

“Let’s use NIST P-256 (secp256r1)”

Bob
POST-QUANTUM WORLD

Alice

PQC Key exchange
“Let’s use KyberKEM-768”

Bob
RSA/ECC Key exchange
“Let’s use NIST P-256 (secp256r1), here’s a key”

{1 byte}  {32 bytes}  {32 bytes}

04 7132b0b1255f ..... abcdef1337 4961ee7e7a1 ..... 9d9bada551

or

{1 byte}  {32 bytes}

03 14916253649 ..... 42deadb33f
“Let’s use KyberKEM-768, here is a key”

PQC Key exchange

“Let’s use KyberKEM-768, here is a 90s version key and I assume the round 2 structuring”
PQC KEY SERIALIZATION AND IDENTIFICATION

• To ensure correct communication key formats are serialized.
• PQC key formats are unspecified, yet
  - Different versions: Round 1, 2, 3, standardized
  - Different compression choices
  - Higher level (than crypto API) considerations:
    ▪ How to store / load the key from key formats (ordering)
    ▪ Optional choices (for performance / size considerations)
  - Hybrid modes?

• Popular submissions are being deployed in practice NOW (positive!)
  → interoperability gets challenging
• Solving this now will avoid larger problems in the future
SOLUTION DIRECTION

• We cannot solve the world, but we can take first step in the right direction
• An RFC specifying key formats will help
  - Help manage algorithm versions and compatibility in key formats
  - Help interoperability of both testing and integration
  - Help make choices in future standards clear
  - Help prevent delays in integration and adoption
• Draft RFC “PQC Key Identification and Serialization” is shared with the cryptographic community
### IN THE RFC: PARAMETER IDENTIFIERS

Describe parameter choices of parameter sets

For now, includes Round 3 finalist sets

OIDs to be filled in

<table>
<thead>
<tr>
<th>name</th>
<th>security</th>
<th>algorithm parameters</th>
<th>parameter OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>LightSaber-r3</td>
<td>1</td>
<td>Degree ( n = 256 )&lt;br&gt;rank of the module ( t = 2 )&lt;br&gt;binomial distribution with ( \mu = 10 )&lt;br&gt;Modulus ( q = 2^{13} ) and ( p = 2^{10} )</td>
<td>{..*.. lightsaber-r3}</td>
</tr>
<tr>
<td>Saber-r3</td>
<td>3</td>
<td>Degree ( n = 256 )&lt;br&gt;Rank of the module ( t = 3 )&lt;br&gt;Binomial distribution with ( \mu = 8 )&lt;br&gt;Modulus ( q = 2^{13} ) and ( p = 2^{10} )</td>
<td>{..*.. saber-r3}</td>
</tr>
<tr>
<td>FireSaber-r3</td>
<td>5</td>
<td>Degree ( n = 256 )&lt;br&gt;Rank of the module ( t = 4 )&lt;br&gt;Binomial distribution with ( \mu = 6 )&lt;br&gt;Modulus ( q = 2^{13} ) and ( p = 2^{10} )</td>
<td>{..*.. firesaber-r3}</td>
</tr>
</tbody>
</table>
### IN THE RFC: KEY DESCRIPTIONS AND SIZES

For each parameters sets, descriptions of the various components key and their sizes

<table>
<thead>
<tr>
<th>Parameter Set</th>
<th>Size of the public key in bytes</th>
<th>Size of the secret key in bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>mceliece348864-r3</td>
<td>261120</td>
<td>6492</td>
</tr>
<tr>
<td>mceliece348864f-r3</td>
<td>261120</td>
<td>6492</td>
</tr>
<tr>
<td>mceliece460896-r3</td>
<td>524160</td>
<td>13608</td>
</tr>
<tr>
<td>mceliece460896f-r3</td>
<td>524160</td>
<td>13608</td>
</tr>
</tbody>
</table>

Byte sizes of the full keys

Different compression options, like e.g. Rainbow has, are also included
In the RFC: ASN.1 Formats

Indicates the version and order of the parameters

Optional fields for public keys / optional algorithm parameters

BIT/OCTET choice currently on what seemed logical from the specs
WHAT’S NEXT?

• Post draft as IETF RFC
• Align with NIST on algorithm OIDs
• Align with ETSI / OASIS SAM / PKCS11 / KMIP TC / more
• Resolve issues around hybrid modes (IP, key serialization)
  - Encouraged format for migration
  - Path is uncertain
• Alternate Round 3 candidates

Interested in keeping updated? Or contributing as a reviewer?
Contact us through: pqc@nxp.com