RFC PQC KEY IDENTIFICATION AND SERIALIZATION

PUBLIC

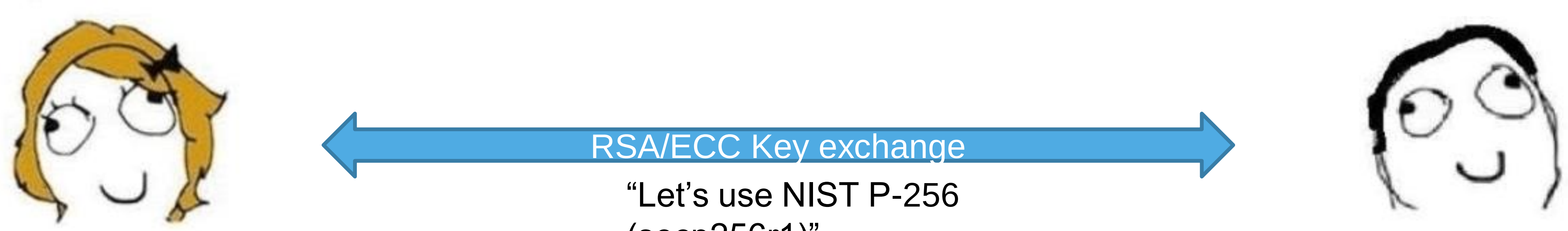
Christine van Vredendaal (NXP)
Joint work with: Dieter Bong (Utimaco), Joppe Bos (NXP) Silvio Dragone (IBM), Basil Hess (IBM), Christopher Meyer (Utimaco), Mike Osborne (IBM), Karen Willbrand (Utimaco)

JUNE 2021

SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

PRE-QUANTUM WORLD



RSA/ECC Key exchange

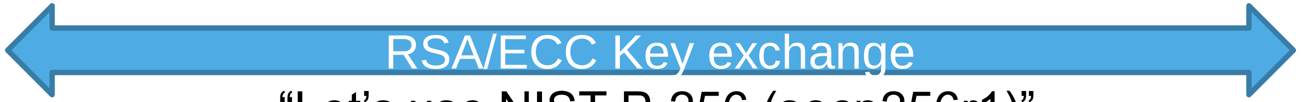
“Let’s use NIST P-256 (secp256r1)”

Alice

Bob

POST QUANTUM WORLD

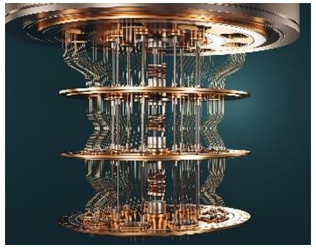
Alice



RSA/ECC Key exchange

“Let’s use NIST P-256 (secp256r1)”

Bob



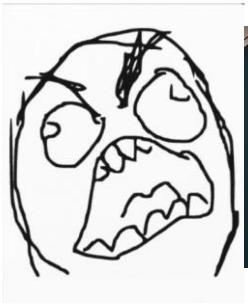
POST-QUANTUM WORLD

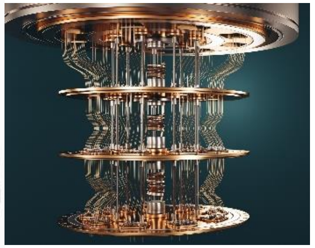
PQC Key exchange

“Let’s use KyberKEM-768”

Alice

Bob





PRE-QUANTUM WORLD

Alice

RSA/ECC Key exchange

“Let’s use NIST P-256 (secp256r1), here’s a key”

Bob

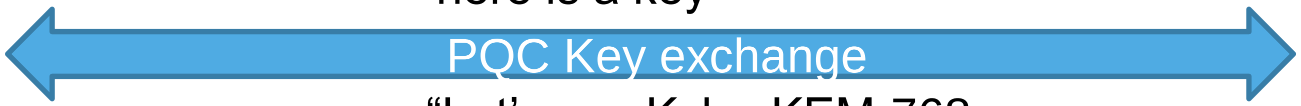
{1 byte}	{32 bytes}	{32 bytes}
04	7132b0b1255f ….. abcdef1337	4961ee7e7a1 ….. 9d9bada551

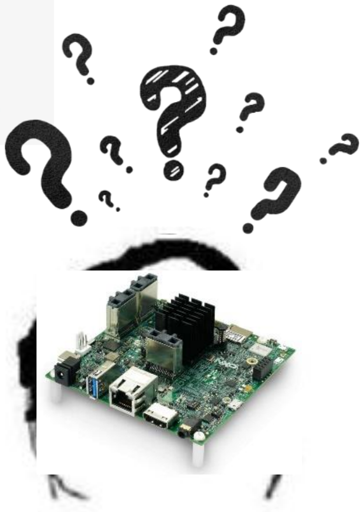
or

{1 byte}	{32 bytes}
03	14916253649 ….. 42deadb33f

POST-QUANTUM WORLD

“Let’s use KyberKEM-768, here is a key”





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

Alice

Bob

PQC KEY SERIALIZATION AND IDENTIFICATION

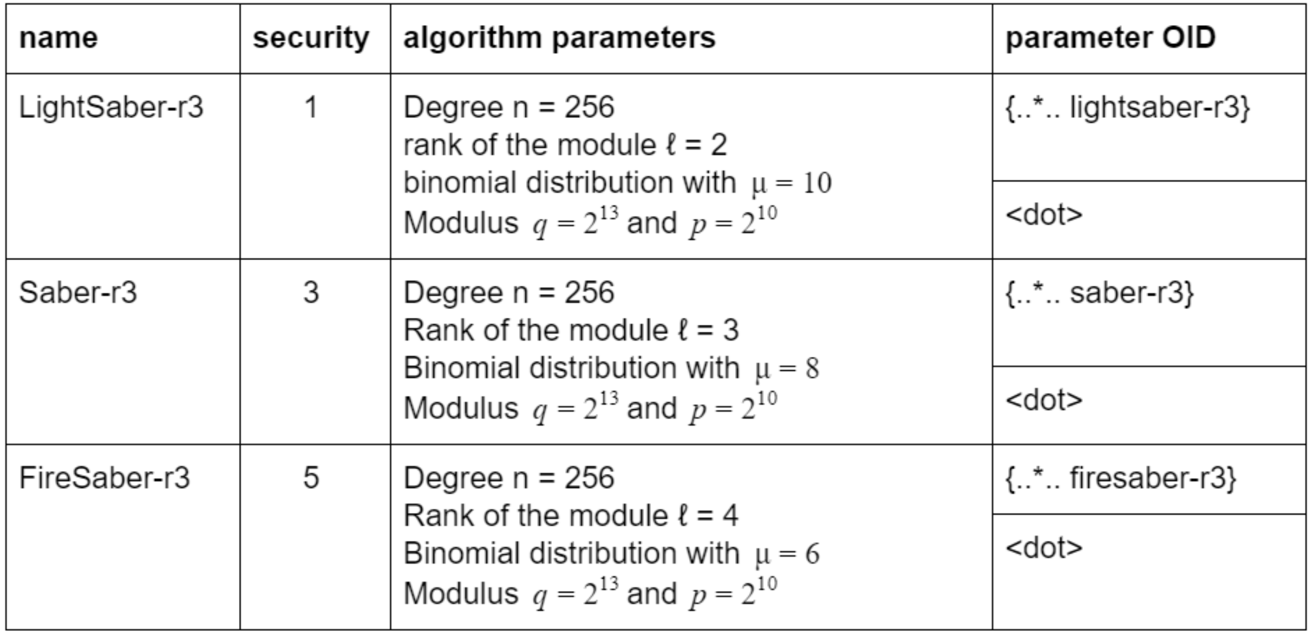
- To ensure correct communication key formats are serialized.
- PQC key formats are unspecified, yet
  - Different versions: Round 1, 2, 3, standardized
  - Different compression choices
  - Higher level (than crypto API) considerations:
    - How to store / load the key from key formats (ordering)
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



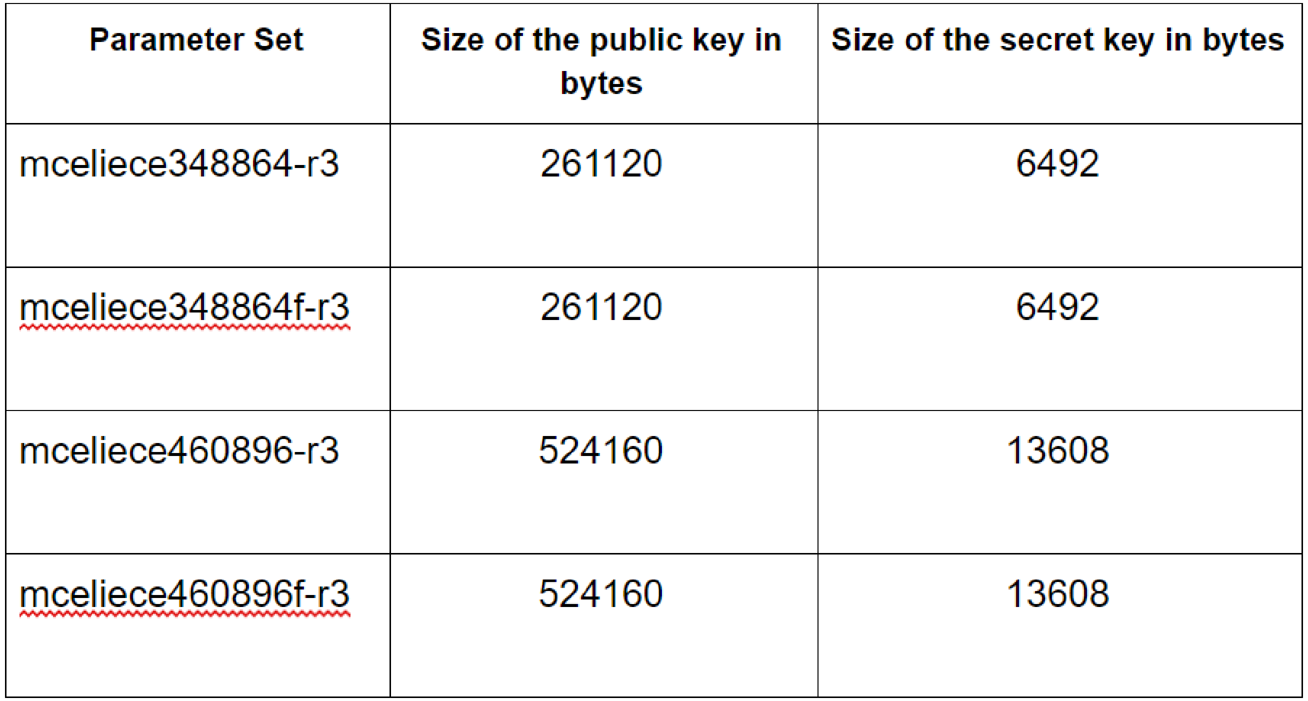
name	security	algorithm parameters	parameter OID
LightSaber-r3	1	Degree n = 256 rank of the module ℓ = 2 binomial distribution with $\mu = 10$ Modulus $q = 2^{13}$ and $p = 2^{10}$	{..*.. lightsaber-r3} <dot>
Saber-r3	3	Degree n = 256 Rank of the module ℓ = 3 Binomial distribution with $\mu = 8$ Modulus $q = 2^{13}$ and $p = 2^{10}$	{..*.. saber-r3} <dot>
FireSaber-r3	5	Degree n = 256 Rank of the module ℓ = 4 Binomial distribution with $\mu = 6$ Modulus $q = 2^{13}$ and $p = 2^{10}$	{..*.. firesaber-r3} <dot>

Describe parameter choices of parameter sets

For now, includes Round 3 finalist sets

OIDs to be filled in

IN THE RFC: KEY DESCRIPTIONS AND SIZES



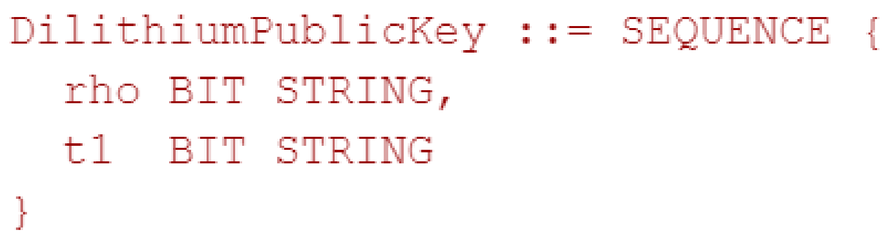
Parameter Set	Size of the public key in bytes	Size of the secret key in bytes
mceliece348864-r3	261120	6492
mceliece348864f-r3	261120	6492
mceliece460896-r3	524160	13608
mceliece460896f-r3	524160	13608

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

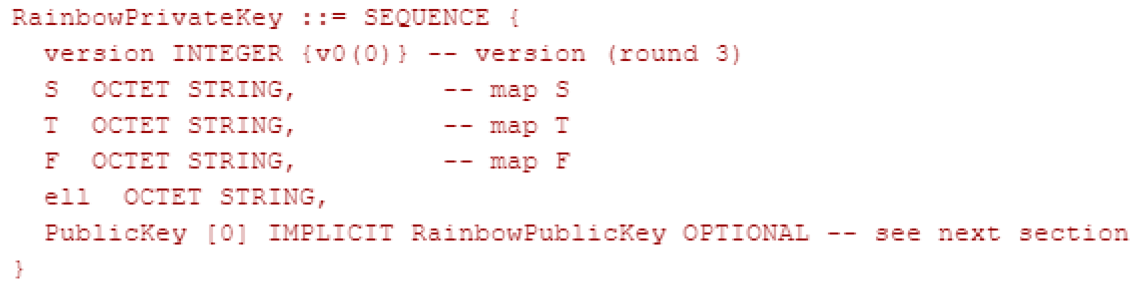
Byte sizes of the full keys

Different compression options, like e.g. Rainbow has, are also included

IN THE RFC: ASN.1 FORMATS



```
DilithiumPublicKey ::= SEQUENCE {
  rho BIT STRING,
  t1  BIT STRING
}
```



```
RainbowPrivateKey ::= SEQUENCE {
  version INTEGER {v0(0)} -- version (round 3)
  S   OCTET STRING,          -- map S
  T   OCTET STRING,          -- map T
  F   OCTET STRING,          -- map F
  ell  OCTET STRING,
  PublicKey [0] IMPLICIT RainbowPublicKey OPTIONAL -- see next section
}
```

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

SECURE CONNECTIONS
FOR A SMARTER WORLD