Panel Discussion on Challenges in Adoption and Implementation of Post Quantum Cryptography

4th International Conference on
Public Key Infrastructure and its Applications: PKIA 2022
IEEE CS&IAS Chapter Bangalore
08-09, September 2022

C.E.Veni Madhavan

Department of Computer Science and Automation
Indian Institute of Science, Bangalore
C.R.Rao Advanced Institute of Math., Stats., and Computer Science

8 September 2022

Panelists

C.E.Veni Madhavan	IISc, CRRAIMSCS	PQC-PKI algorithms, analysis
Shantanu Sarkar	IITM	PQC-PKI algorithms, analysis
S.D.Sudarshan	CDAC	PQC-PKI development
Ananda Mohan	CDAC	PQC-PKI evaluation
N.Subramanian	SETS	PQC-PKI management
Asish Banati	CCA-MeitY	PQC-PKI migration
Sunita Verma	MeitY	PQC-PKI migration

Contents

1. PQC-NIST CRYSTALS: cutting, polishing, adopting

1. debugging tools
2. approximations, errors analysis tools
3. traps, measurements, side-channels tools
4. enhancements, correctness, performance tools
5. counter-measures, counter-counter-measures tools
6. evaluation, certification, pacakging tools
7. deployment, migration, maintenance, management tools

2. PQC-NIST CRYSTALS: mathematical and algorithmic issues

1. lattice geometry, linear algebra, finite fields and polynomial rings
2. fast computation (quadratic to linear to "near" constant time)
3. large key material, message expansion, LUT, encodings
4. compaction, truncation, rounding errors- delicate tolerance bounds
5. cryptanalysis: algebraic + combinatorial + probabilistic structures (?)
6. cryptanalysis: LWE, LWR,(R/M)LW(E/R) - SVP, CVP, SIS (?)
7. cryptanalysis: classical (NP-complete ground problems) (?)
8. cryptanalysis: quantum (absence of hidden subgroup structures) (?)
9. cryptanalysis: additional obfuscation due to hash functions (?)
10. cryptanalysis: side channels - hardware, software (?)
11. cryptanalysis: side channels - parametric, algorithmic aspects (?)
12. cryptanalysis: hybrid : classical + quantum (?)

2. PQC-NIST CRYSTALS: mathematical and algorithmic issues

Preliminaries

1. structures: field: $\mathbf{Z}_q, q = 7681 or 3321$, rings: $Z, Z[X], R = Z[X[/(X^n + 1), R_q = Z_q[X]/(X^n + 1)$, $n = 2^{m-1}$, $X^n + 1$ is the 2^mth cyclotomic polynomial; $n = 256, m = 9, q = 7681$
2. l_∞, l_2 norms of scalars, vectors and matrices over the field and rings
3. modular reductions: $\pm$ least residues; rounding; small norm elements
4. deterministic, probabilistic sampling (uniform, binomial distributions)
5. extendable output function (XOF), hash functions (SHAKE, Keccak)
6. compression (MSB extraction) with rounding, decompression (MSB re-construction) with rounding; bounds on the discrepancy $|x - y|$, where y =decompression(compression(x)
7. NTT number theoretic transforms for fast discrete Fourier transform based convolution produt of ring elements with appropriate powers of roots unity in Z_q,($O(n^2)$ to $O(n \log n)$ multiplication)

3. PQC-NIST CRYSTALS: Kyber mathematical and algorithmic issues

keygen:

1. parameters: q, k, d_t, d_u, d_v, generator, root of unity in Z_q
2. uniformly generated scalars $\rho, \sigma \in \{0.1\}^{256}$
3. matrix $\mathbf{A}$ over R_q^{kxk} by determininistic sampling ρ
4. vectors $\mathbf{s}, \mathbf{e}$ over β_η^k sampling σ
5. public key pk: $\mathbf{t} = \text{compress}(\mathbf{As} + \mathbf{e}, d_t)$
6. private key sk : $\mathbf{s}$

3. PQC-NIST CRYSTALS: Kyber mathematical and algorithmic issues

encryption:

1. generate $r \in \{0,1\}^{256}$
2. uniformly generated $(\mathbf{r}, \mathbf{e_1}, e_2)$ by sampling r,
3. encoded message m
4. message mask : $\mathbf{u} = \mathbf{A}^T\mathbf{r} + \mathbf{e_1}$: (sampling r) compressed(d_u)
5. $\mathbf{t} \leftarrow$ decompress$(\mathbf{t}, d_t)$
6. encryption : $v = \mathbf{t}^T\mathbf{r} + e_2 + \lceil q/2 \rfloor .m$: compressed(d_v)
7. cipher : $c = (\mathbf{u}, v)$

3. PQC-NIST CRYSTALS: Kyber mathematical and algorithmic issues

decryption: $\mathbf{s}, c = (\mathbf{u}, v)$

1. $\mathbf{u} \leftarrow \text{decompress}(\mathbf{u}, d_u)$
2. $v \leftarrow \text{decompress}(\mathbf{v}, d_v)$
3. decrypted message $= \text{compress}(v - \mathbf{s}^T\mathbf{u}, 1)$

3. PQC-NIST CRYSTALS: Kyber mathematical and algorithmic issues

key encapsulation:

1. gnerate $r \in \{0,1\}^{256}$
2. uniformly generated $(\mathbf{r}, \mathbf{e_1}, e_2)$ by sampling r,
3. encoded message $m \leftarrow \{0,1\}^{256}$
4. $(\hat{K}, r) \leftarrow G(H(pk, m))$ *hash functions G, H)
5. $(\mathbf{u}, v) \leftarrow Encrypt((\mathbf{t}, \rho), m, r)$
6. cipher : $c = (\mathbf{u}, v)$
7. $K \leftarrow H(\hat{K}, H(c))$
8. send (c, K)

3. PQC-NIST CRYSTALS: Kyber mathematical and algorithmic issues

key decapsulation:

1. $m' \leftarrow \text{Decrypt}(\mathbf{s}, (\mathbf{u}, v))$
2. $\hat{K}', r') \leftarrow G(H(pk, m')$
3. $(\mathbf{u}', v') \leftarrow Encrypt((\mathbf{t}, \rho), m', r')$
4. if$(\mathbf{u}', r') = (\mathbf{u}, r)$ then send $K \leftarrow H(\hat{K}', H(c))$
   else send $K \leftarrow H(z, H(c))$