Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

सत्यमेव जयते

G20 भारत 2023 INDIA

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

4th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2023)

SEPTEMBER 8th and 9th 2023

Cryptographic Challenges and Security in Post Quantum Cryptography Migration: A Prospective Approach

Anoop Kumar Pandey, Aashish Banati, Balaji R, S D Sudarsan, **K K Soundra Pandian**

Post Quantum Cryptography

- *Threat to Classical Cryptography*
  - *Shor's Algorithm*
    - *Factorization problem difficulty – From Exponential to Polynomial using Quantum Computing*
    - *Largest integer factored – 21 in 2012 (Relief for now!!!)*
    - *Threat to Asymmetric Cryptography (RSA etc.)*
  - *Grover's Algorithm*
    - *Searching in $O(\sqrt{N})$*
    - *Exhaustive Search in Symmetric Key: time complexity from 2^N to $2^{N/2}$*
    - *Finding Collision: time complexity from $2^{N/2}$ to $2^{N/3}$*
    - *Threat to Symmetric Cryptography (AES etc.)*

Algorithm	Status in Post Quantum World
AES-256	Secure
SHA-256, SHA-3	Secure
RSA	Not Secure
ECDSA, ECDH	Not Secure
DSA	Not Secure

Post Quantum Cryptography

- *Field of research on developing cryptographic Algorithms that can resist attacks from Quantum Computers.*
- *Approaches*
  - *Lattice Based Cryptography*
    - *Based on Computational problems associated with lattices (geometric Structure in N-dimensional spaces)*
      - *Shortest Vector Problem, Learning with Errors, Ring Learning with Errors*
    - *E.g. Crystals-Dilithium*
  - *Code Based Cryptography*
    - *Relies on decoding problems related to error-correcting codes*
    - *E.g. McEliece*
  - *Multivariate Cryptography*
  - *Hash Based Cryptography*

Post Quantum Cryptography

- *Approaches*
  - *Multivariate Cryptography*
    - *Based on the hardness of solving systems of multivariate polynomial equations over finite fields. (NP-Hard)*
    - *E.g. Rainbow*
  - *Hash Based Cryptography*
    - *Relies on properties of cryptographic Hash Functions*
      - *Collision Resistance and One-Wayness*
    - *E.g. Merkle Signature Scheme, Sphincs+*

NIST PQC Competition

- *Launched in 2016 to standardize Quantum-resistant set of cryptographic algorithms*
- *Current Winners (Round 3)*
  - *General Encryption*
    - *Crystals-Kyber*
  - *Digital Signature*
    - *Crystals-Dilithium (Primary Algorithm)*
    - *Fast Fourier Lattice-Based Compact Signatures over NRTU (Falcon) (Smaller Signatures)*
    - *Sphincs+ (Larger but Slower)*
- *Four KEM moved to Round 4*
  - *Classic McEliece*
  - *Bit Flipping Key Encapsulation (BIKE)*
  - *Hamming Quasi Cycle (HQC)*
  - *Supersingular Isogeny Key Encapsulation (SIKE)*

Limitations of PQC

- *Performance Overhead*
- *Large Key Sizes*
- *Standardization still in process*
- *Implementation Complexity*
- *Quantum Computing Progress*
- *Cryptanalysis*
- *Transition Complexity*
- *Limited Deployment Experience*

International Efforts in PQC Standardization

- *ETSI (European Telecommunication Standards Institute)*
  - *Supports NIST PQC (Report in October 2021)*
- *ISO (International Organization for Standardization)*
  - *ISO/IEC JTC 1/SC 27/WG 2 and ISO/TC 68/SC 2/WG 11 working to finalize Post Quantum Cryptography*
  - *Nothing published yet in public domain*
- *IETF (Internet Engineering Task Force)*
  - *Discussions to establish a working group for transition support to PQC*
  - *Proposals for Specifying algo identifiers and ASN.1 encoding for Kyber.*
  - *Usage of Dilithium in X.509 Certificates and CRLs also in discussion*
- *Japan*
  - *CRYPTREC set up to evaluate and recommend crypto techniques for Govt and Industrial Usage*
  - *NIST Competition has many Japanese contributors: Classic McEliece (R3 finalist), Ding Key Exchange etc.*
  - *PQC CARD: PQC enabled Smart Card uses Crystals-Dilithium*
    - *Used to access H-LINCOS (Health Data)*

International Efforts in PQC Standardization

- *United Kingdom*
  - *National Cyber Security Centre (NCSC) nodal agency of UK*
    - *Supports NIST Standards*
    - *Advises to wait for Standards and Protocols*
    - *Advises not to implement own non-standard PQC (security not verifiable)*
- *China*
  - *The Chinese Association for Cryptologic Research (CACR) started PQC Standardization in 2018*
  - *Shortlisted Aigi-Sig (for Signature), LAC.PKE, Aigis-enc (for KEM) in 2020*
  - *Based on Lattice Schemes*
- *Korea*
  - *PQC Standardization through National Contest for Quantum Resistant Cryptography in Nov 2021*
  - *First round in progress (Nov '22 – Nov '23)*

International Efforts in PQC Standardization

- *Other Notable Efforts*
  - *Microsoft*
    - *Working on software libraries for PQC*
    - *Also working on four potential cryptographic solutions*
    - *Support Open Quantum Safe Project (a software prototyping platform)*
    - *Also working on Post Quantum Crypto VPN (a fork of OpenVPN)*
  - *Google*
    - *IN 2016, Deployed "New Hope", a post-quantum-key-exchange scheme for communication between Chrome Browser and Google Servers*
  - *Infineon*
    - *In 2017, Implemented a variant of "New Hope" on contactless smartcard microcontroller commercially available chipset for PQC for embedded systems*
  - *IBM*
    - *Focused on Lattice-based solutions*

Crystals-Dilithium Signature Demo

https://learn.pkiindia.in/pqc-sign.html

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

G20 भारत 2023 INDIA

THANK YOU

भगत संगणन विकास केंद्र
सीडैक CDAC
॥ज्ञानादेव तु कैवल्यम्॥
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

IEEE COMPUTER SOCIETY
Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY
Linking Research to Practice
Bangalore Chapter