Cryptography Roadmap of India

MeitY — Government of India

Years: 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047

1. Symmetric Cryptography
- New competitive S-box Designs for trusted implementation of AES
- Novel fast, secure and efficient block ciphers/stream Ciphers
- Formal proofs for block/stream ciphers
- Fast, secure and efficient symmetric cryptographic schemes for resource constraint devices

2. Asymmetric Cryptography
- New Elliptic curves defined over more than 512 bit prime field sizes for cryptography
- Quantum resistant elliptic curves of isogeny class for cryptography
- Development of quantum resistant cryptography
- Development of post quantum cryptography (Lattices, code-based, multivariate, hash-based cryptographic schemes)
- Fast, secure and efficient asymmetric cryptographic schemes for resource constraint devices
- Public key infrastructures

3. Hashing
- New construction of SPONGE-like functions for hashing
- New Boolean functions for hashing and cryptography
- Novel non-linearity schemes for cryptography

4. Randomness
- Novel Random Number Generators (RNGs) for trust building
- New randomness test suites for predictability and statistical indistinguishability of bitsteams
- New randomness test suits specifically for quantum random number generators (QRNGs)

5. Cryptography for small resource constraint devices
- PKI for IoT
- Novel Key establishment/distribution schemes in IoT
- Development of resilient cryptography based critical infrastructures for IoT environments

6. Cryptography for ultra security sensitive applications
- Quantum safe PKI
- Post Quantum Cryptography and Quantum Resistant Cryptography
- Novel Keys Establishment/Distribution Schemes and Keys Management Protocols

7. Creation of Center of Excellences (CoEs) for
- Indigenisation of all cryptographic solutions, protocols/schemes
- Scaling up the existing hard problems for cryptography