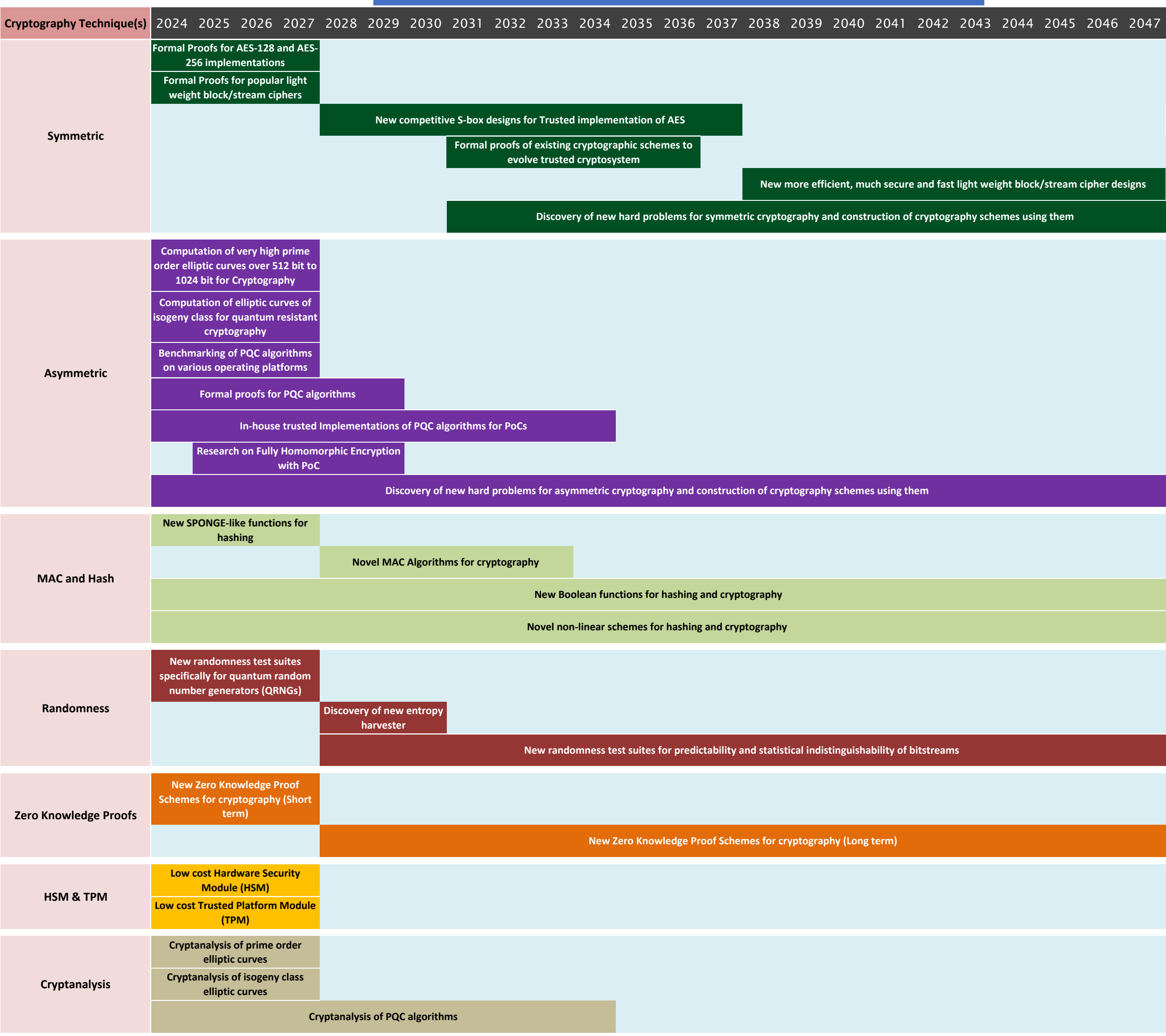
इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

Cryptography Roadmap of India

प्रगत संगणन विकास केंद्र
सी डैक CDAC
॥ज्ञानादेव तु कैवल्यम्॥
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING



Interested Areas

Tools and Solutions

- Development of low cost HSM
- Development of low cost TPM
- Generation of cryptographically safe and trusted eliptic curves over prime fields of sizes ranging from 512 bits to 1024 bits
- Development of new randomness test suites for evaluation of RNG, PRNG, CSPRNG, QRNG
- Development of Indigenous Public Key Infrastructures
- Development of Tools for confidential computing
- Development of indigenous cryptographic applications

Formal Proofs and Trusted Implementations

- Formal proofs for AES-128/256 implementations
- Formal proofs for popular light weight block/stream ciphers
- Formal proof for popular PQC algorithms
- Formal proofs for any other cryptographic schemes of interest
- Trusted implementations of any cryptographic schemes of interest

Basic Research

- New Competititve S-box designs for trusted implementation of AES
- Construction of new, more efficient, secure, fast and light-weight stream/block ciphers
- Discovery of new hard problems for symmetric and asymmetric cryptography
- Construction of AI enabled cryptography
- Construction of new sponge-like functions for hashing
- New MAC Algorithms for Cryptography
- Construction of New Boolean functions for hashing and cryptography
- Construction of novel, non-linear schemes for hashing and cryptography
- Construction of new zero-knowledge proof schemes for cryptography
- Construction of new post quantum cryptography algorithms and schemes
- Construction of New Tokenization Schemes

Cryptanalysis

- Cryptanalysis of prime order elliptic curves
- Cryptanalysis of isogeny class elliptic curves
- Cryptanalysis of RSA
- Cryptanalysis of PQC algorithms
- Cryptanalysis using AI
- Cryptanalysis of any cryptographic schemes of interest

Development of Centre(s) of Excellence

- Indigenization of cryptographic solutions, protocols/schemes or applications
- Scaling of the existing hard problems for cryptography
- Trusted security and formal proofs of cryptographic solutions, protocols/schemes, and applications
- Establishment of certifying agencies for cryptographic security validation/certification
- Standardization of Indian Crypotographic Developments