



Cryptography Roadmap of India



Cryptography Technique(s)	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047					
Symmetric	Formal Proofs for AES-128 and AES-256 implementations		Formal Proofs for popular light weight block/stream ciphers		New competitive S-box designs for Trusted implementation of AES					Formal proofs of existing cryptographic schemes to evolve trusted cryptosystem					New more efficient, much secure and fast light weight block/stream cipher designs					Discovery of new hard problems for symmetric cryptography and construction of cryptography schemes using them									
	Computation of very high prime order elliptic curves over 512 bit to 1024 bit for Cryptography				Computation of elliptic curves of isogeny class for quantum resistant cryptography				Benchmarking of PQC algorithms on various operating platforms				Formal proofs for PQC algorithms				In-house trusted Implementations of PQC algorithms for PoCs				Research on Fully Homomorphic Encryption with PoC				Discovery of new hard problems for asymmetric cryptography and construction of cryptography schemes using them				
	New SPONGE-like functions for hashing				Novel MAC Algorithms for cryptography				New Boolean functions for hashing and cryptography					Novel non-linear schemes for hashing and cryptography															
	New randomness test suites specifically for quantum random number generators (QRNGs)				Discovery of new entropy harvester				New randomness test suites for predictability and statistical indistinguishability of bitstreams																				
MAC and Hash	New Zero Knowledge Proof Schemes for cryptography (Short term)				New Zero Knowledge Proof Schemes for cryptography (Long term)																								
	Low cost Hardware Security Module (HSM)				Low cost Trusted Platform Module (TPM)																								
Randomness	Cryptanalysis of prime order elliptic curves				Cryptanalysis of isogeny class elliptic curves				Cryptanalysis of PQC algorithms																				

Interested Areas

Tools and Solutions	Formal Proofs and Trusted Implementations	Basic Research	Cryptanalysis	Development of Centre(s) of Excellence
<ul style="list-style-type: none"> Development of low cost HSM Development of low cost TPM Generation of cryptographically safe and trusted elliptic 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> New Competitive 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 Cryptographic Developments