

CCS Concepts: • Security and privacy → Public key encryption; • Theory of computation → Cryptographic primitives; Massively parallel algorithms.