Table of Contents

Key Exchange, OAEP/RSA, CCA

Attacks

Composition

Computation Delegation and Obfuscation

Multiparty Computation

Pseudorandomness

Quantum