Provable Security V

Theoretical construction of pseudorandom functions from pseudorandom generators

Security under Chosen-Plaintext Attacks (CPA)