Table of Contents

Secure Computation

(Blind) Signatures and Threshold Encryption

Zero-Knowledge and Security Models

Leakage-Resilience

Hash Functions

Differential Privacy

Pseudorandomness I

Dedicated Encryption I

Security Amplification

Resettable and Parallel Zero Knowledge

Dedicated Encryption II

Pseudorandomness II