

Implementing and Preventing Side-Channel Attacks

- **Attack Type:** Timing Attacks, Power Analysis Attacks
- **Application:** Simulate a side-channel attack on encryption algorithms and implement countermeasures.
- **Deliverables:**
 - Attack demonstration
 - Countermeasure implementation
 - Security impact analysis