Table of Contents

Stream Ciphers & Other Primitives

Efficient Implementations

Side-Channel Attacks