## Cryptographic Protocols

**ECDSA** 

**ECDH** 

Digital Signatures

Key Agreement

## Module Operations

$$R = s \cdot P$$

$$R = s \cdot P + t \cdot Q$$

Scalar Multiplication

Twin Multiplication

## Curve Operations over points

$$R = P + Q$$
  $R = P - Q$   $R = 2 \cdot P$ 

$$R = P - O$$

$$R = 2 \cdot P$$

Addition Subtraction

Doubling

## Finite Field Arithmetic

Multiplication

Squaring

Division

Addition

Subtraction

Doubling