Cryptographic Foundations

Lesson 3: Summary

Prof. Joerg Osterrieder

Spring 2026

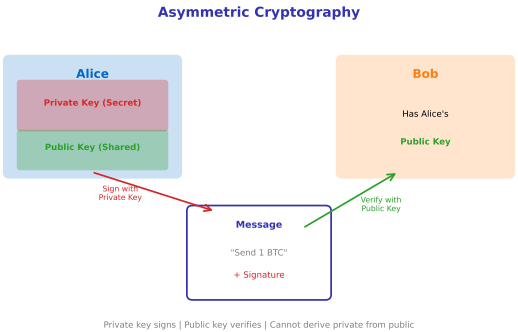
Hash Functions

Definition: Fixed-size output from any input. $H : \{0,1\}^* \to \{0,1\}^{256}$
Key Properties:

- Deterministic, fast, one-way
- Collision-resistant, avalanche effect

SHA-256: produces 256-bit fingerprint, used in Bitcoin

Public Key Cryptography

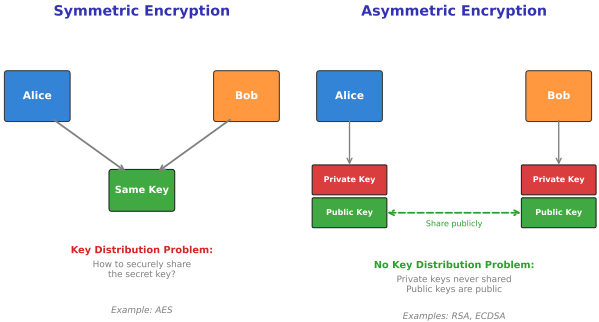


Key Insight: Easy to compute public from private, impossible to reverse.

Priva

key = secret, Public key = shared, Address = hash of public

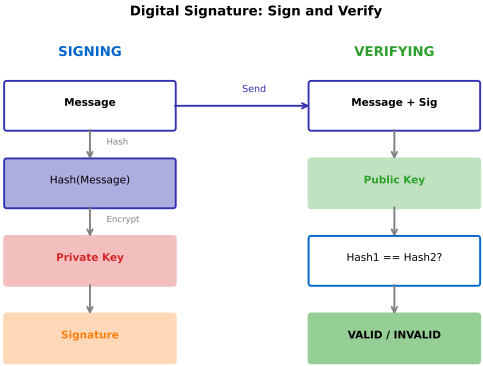
Symmetric vs. Asymmetric Encryption



Asym

solves key distribution problem, enables trustless transactions

Digital Signatures

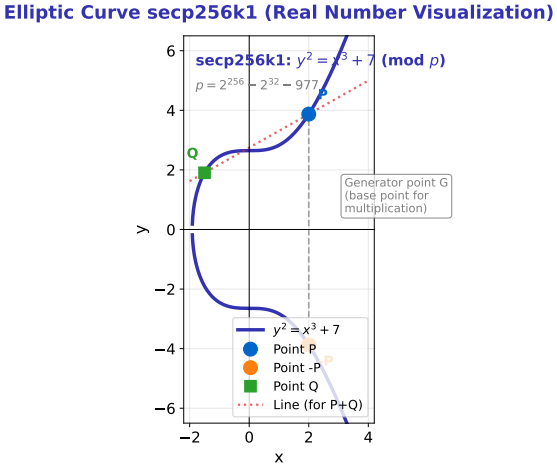


Properties: Authentication, non-repudiation, integrity.

ECDS

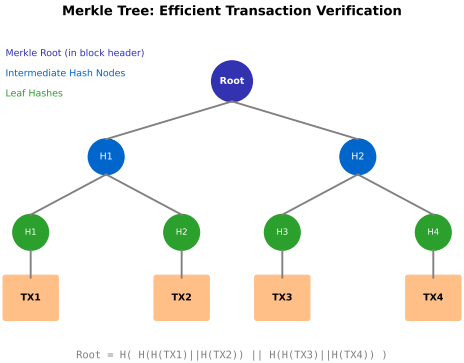
Sign with private key, verify with public key

The secp256k1 Elliptic Curve



use secp256k1: $y^2 = x^3 + 7$ **(mod** p**)**

Merkle Trees



Efficiency: Verify any transaction with $O(\log n)$ hashes.

Merk

root in block header summarizes all transactions

How They Work Together

Bitcoin Transaction Flow:

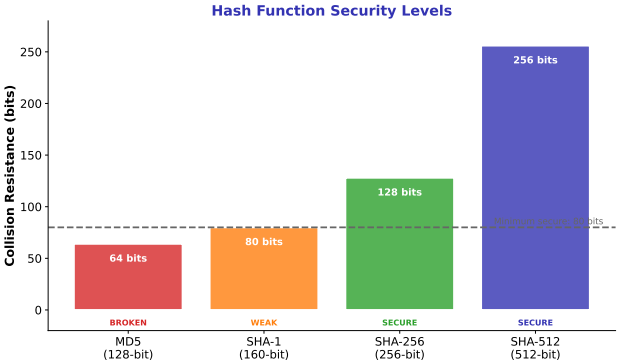
1. Generate key pair (ECDSA on secp256k1)
2. Create address from public key hash
3. Sign transaction with private key
4. Network verifies signature
5. Transaction added to Merkle tree
6. Block hash links to chain

Every step uses cryptographic primitives

Complete Bitcoin Cryptography Flow

cryptographic steps: key generation through blockchain linkage

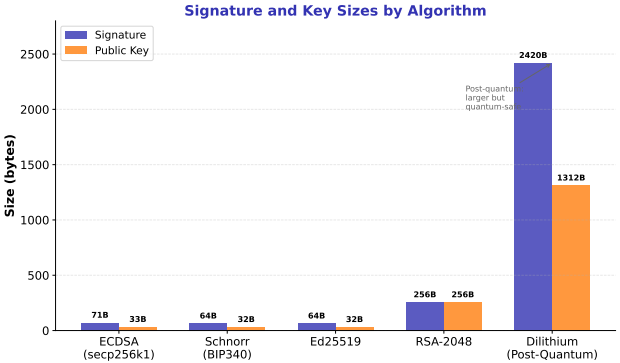
Hash Function Security Levels



MD5

1 broken—use SHA-256 or better for blockchain applications

Signature Schemes Comparison



Post-quantum schemes larger but necessary for future security

Key Takeaways

1. **Hash functions**: One-way, collision-resistant fingerprints
2. **Public/private keys**: Asymmetric cryptography for ownership
3. **Digital signatures**: Prove ownership without revealing secrets
4. **Merkle trees**: Efficient verification with logarithmic complexity

Core Insight: Blockchain security = mathematical hardness assumptions.

Next:

Consensus Mechanisms

Thank You

Questions?