Cryptography for Blockchain

A Visual Introduction

Standalone Mini-Lecture

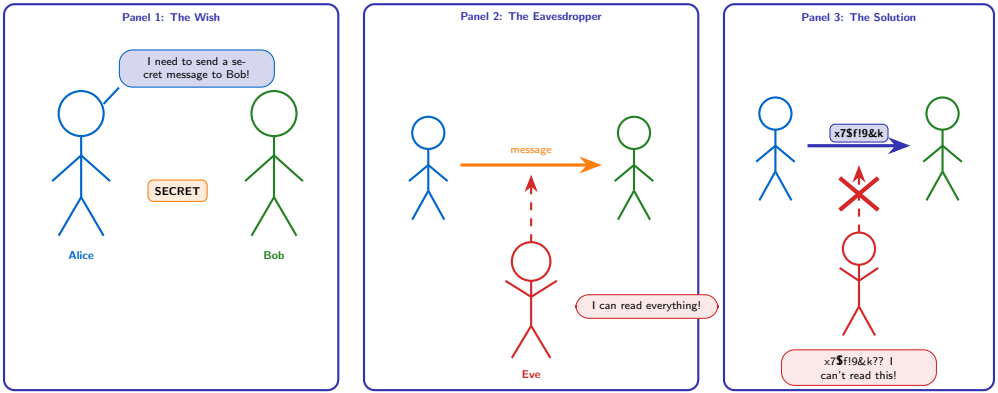
"Don't trust – verify mathematically"

Prof. Dr. Joerg Osterrieder

University Lecture Series

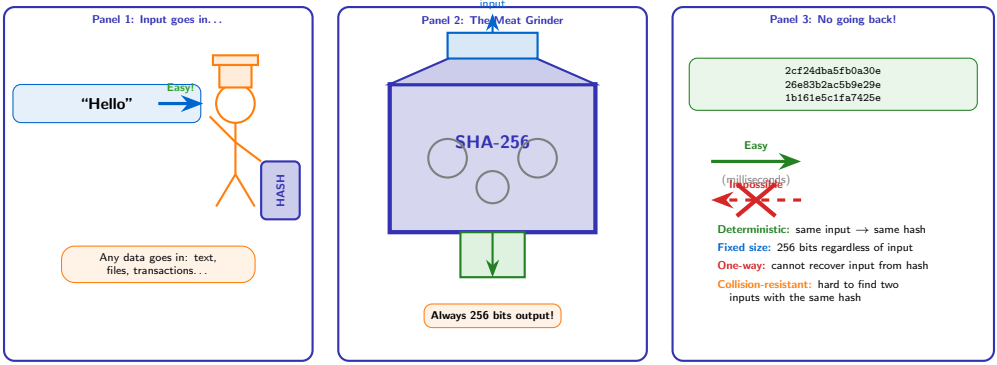
February 19, 2026

The Secret Message Problem



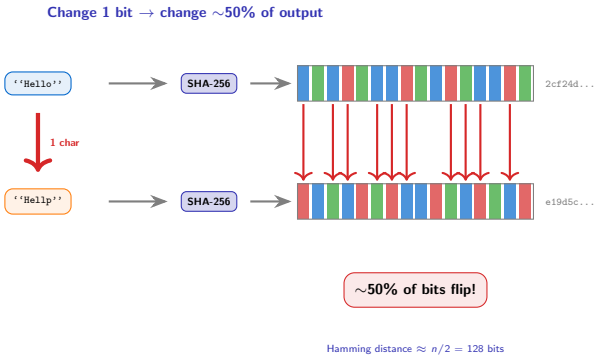
Cryptography lets Alice and Bob communicate securely even when Eve controls the channel.

One-Way Functions: The Meat Grinder



SHA-256 is Bitcoin's hash function. It produces a unique 256-bit "fingerprint" for any input.

The Avalanche Effect



Why It Matters for Blockchain

- **Tamper detection:** Changing even one byte in a block invalidates its hash
- **Mining puzzle:** No shortcut to find a hash starting with k zeros
- **Unpredictable:** Cannot predict output from partial input knowledge

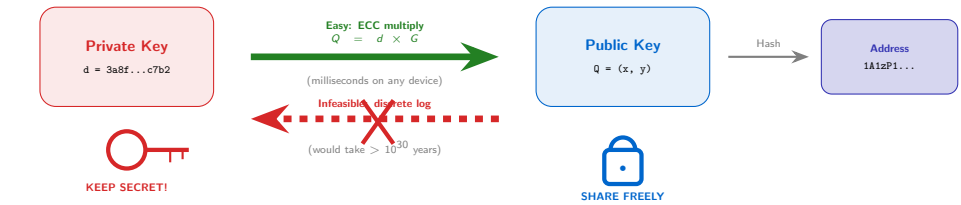
Formal Definition

A hash function H satisfies the **avalanche criterion** if: when a single input bit flips, each output bit flips with probability ≈ 0.5:

$$\Pr\big[\, H(x)_i \neq H(x')_i \,\big] \approx \tfrac{1}{2}$$

The avalanche effect ensures that hash functions behave like random oracles – no pattern leaks through.

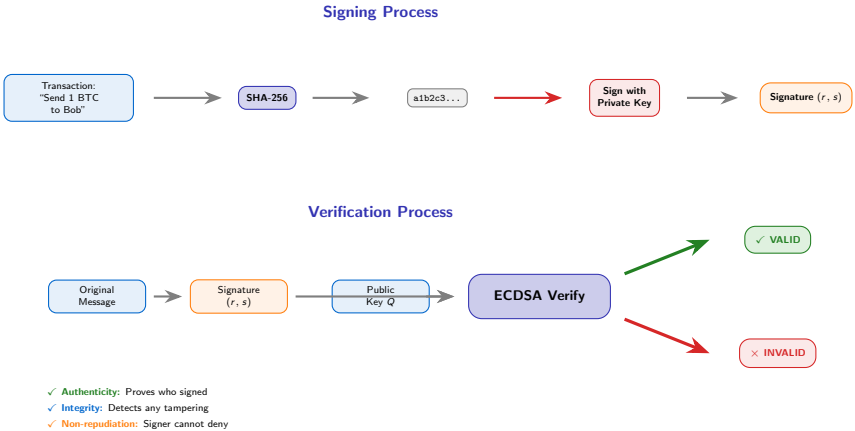
Public & Private Keys



Analogy: Public key = your mailbox address (anyone can send mail to it) | Private key = the mailbox key (only you can open it) | Address = your zip code (short version of mailbox location)

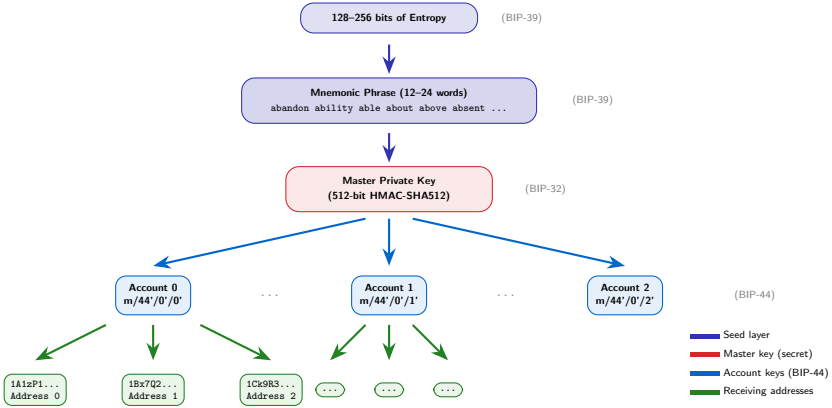
Elliptic Curve Cryptography (secp256k1 in Bitcoin): $Q = d \times G$ **where** G **is a generator point on the curve.**

Digital Signatures: Proving Ownership



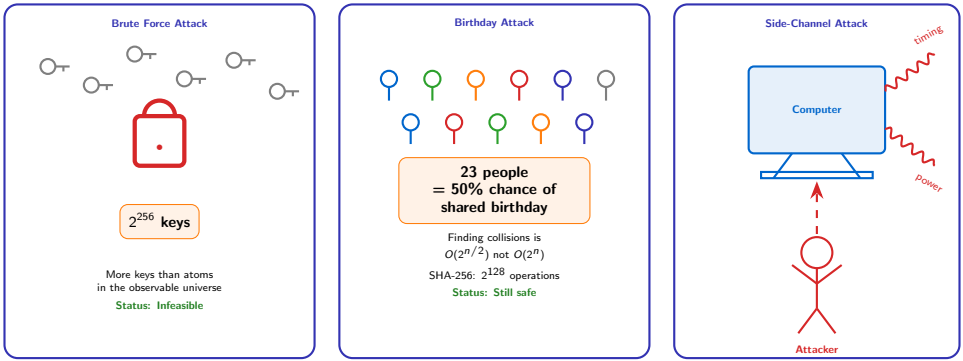
Every Bitcoin transaction is digitally signed. Miners verify signatures before including transactions in blocks.

Wallet Architecture: From Seed to Address



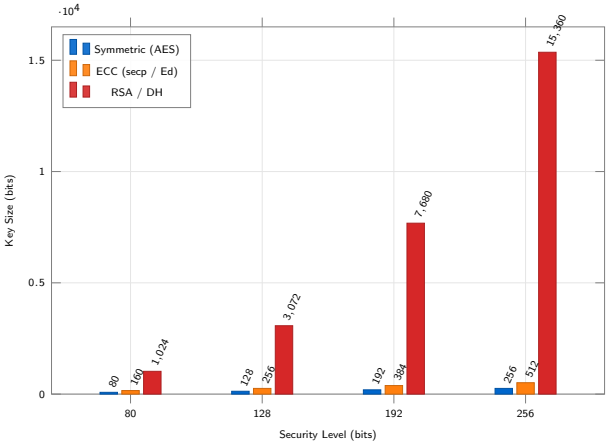
Hierarchical Deterministic (HD) wallets derive unlimited addresses from a single seed – back up once, recover everything.

Real-World Attacks on Cryptography



Defense in depth: use constant-time algorithms, hardware security modules, and key rotation to mitigate side-channel risks.

Crypto by the Numbers: Key Size vs. Security



Key Insight

ECC achieves the **same security** as RSA with **much smaller keys**:

- AES-128: **128** bits
- ECDSA-256: **256** bits
- RSA-3072: **3072** bits

All provide $\sim$**128-bit security**.

Why Blockchain Uses ECC

- Smaller keys $\rightarrow$ smaller transactions
- Faster signing and verification
- Lower bandwidth and storage
- Bitcoin: **secp256k1**
- Ethereum: also secp256k1

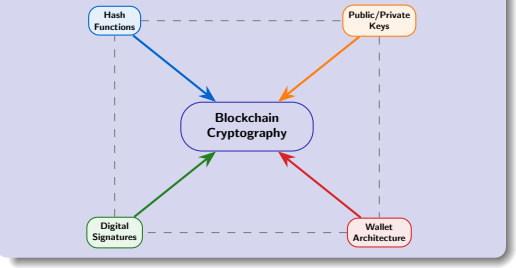
Quantum threat: Shor's algorithm could break ECC and RSA.

Takeaways & Crypto Principles

Five Core Principles

- ✓ **Hash functions** create tamper-evident fingerprints
  SHA-256 secures every Bitcoin block
- ✓ **Asymmetric cryptography** enables trustless identity
  No central authority needed to verify who you are
- ✓ **Digital signatures** prove ownership and intent
  Every transaction is mathematically signed
- ✓ **Key management** is the weakest link in practice
  "Not your keys, not your coins"
- ✓ **Security is measured in bits**, not algorithms
  128-bit security is the current standard

Summary



Next lecture: Consensus mechanisms – how do thousands of nodes agree without a leader?

Cryptography is the mathematical foundation that makes decentralized trust possible.