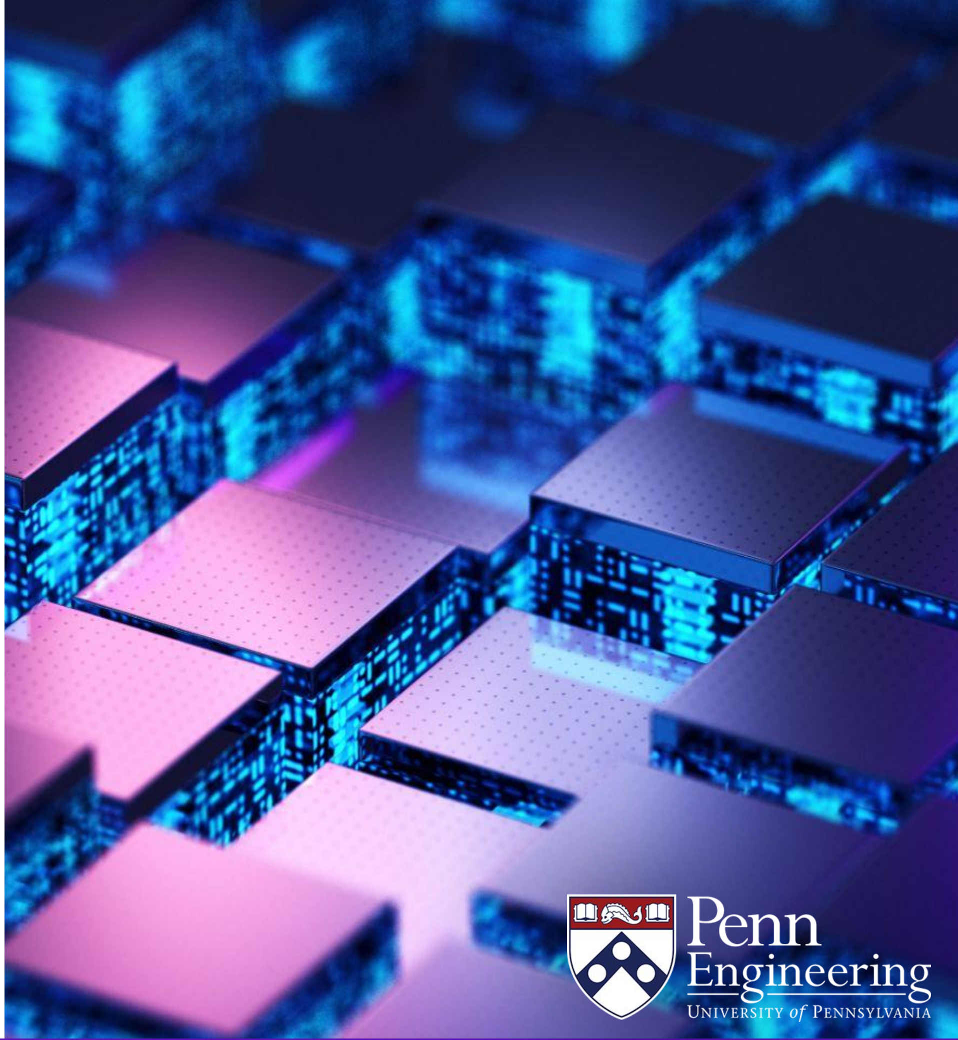
EAS 5830: BLOCKCHAINS

Cryptography on the blockchain

Professor Brett Hemenway Falk



Cryptography

- Collision-resistant hash functions
    - Symmetric-key cryptography
- Digital signatures
    - Public-key cryptography
- **No Encryption**

Signatures

- **Key Generation**
  - Generates a random private key
    - Usually a uniformly random 256-bit string
  - Computes a corresponding public key
    - Usually an element in an elliptic curve group
    - Address is derived from public key
- **Signing** (private)
  - Takes a message and the private key and produces a signature
- **Verification** (public)
  - Takes a message, signature and public key, and checks whether the signature was computed using the corresponding private key

The Elliptic-Curve Digital Signature Algorithm (ECDSA)

- Accepted as ANSI standard in 1999
- Accepted as NIST standard in 2000
- Security rests on the elliptic-curve discrete-log problem
  - Discrete-log problem modulo p
    - Given integers g, h, p find a such that $g^a = h \bmod p$
  - Elliptic-curve discrete-log problem:
    - Given a curve C, a generator G, and a point H, find an integer a such that $a \cdot G = H$

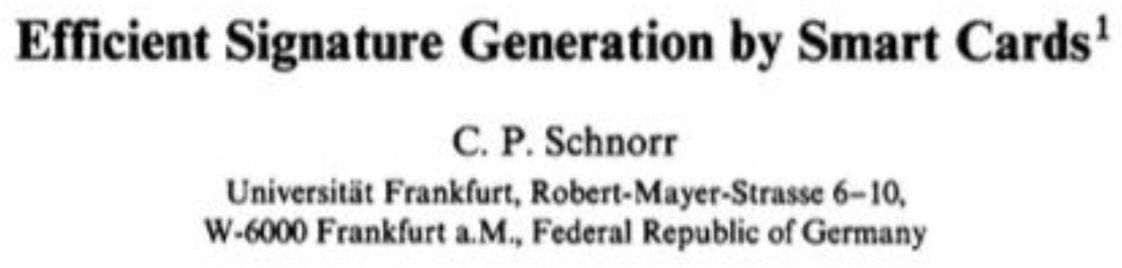
Signatures

- Bitcoin - ECDSA
    - Taproot - Schnorr
- Ethereum - ECDSA
    - Attestations - BLS
- BNB - ECDSA
- Ripple - ECDSA + ED25519
- Solana - ED25519
- Cardano - ED25519
- TRON - ECDSA
- Polkadot - Schnorr
- Avalanche - ECDSA
- Cosmos - ECDSA + ED25519

Signatures

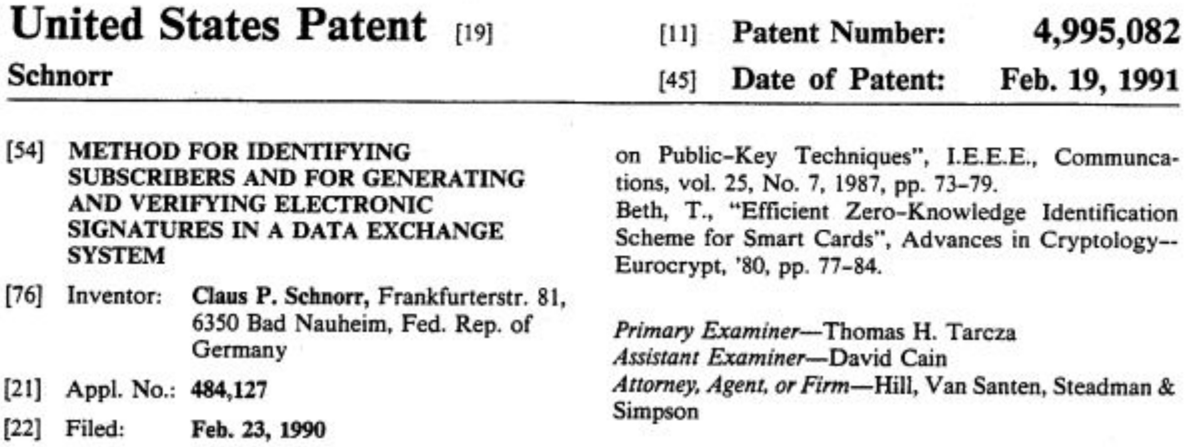
- Bitcoin - ECDSA
  - Taproot - Schnorr
- Ethereum - ECDSA
  - Attestations - BLS
- BNB - ECDSA
- Ripple - ECDSA + ED25519
- Solana - ED25519
- Cardano - ED25519
- TRON - ECDSA
- Polkadot - Schnorr
- Avalanche - ECDSA
- Cosmos - ECDSA + ED25519

All these schemes are vulnerable to quantum attacks



Efficient Signature Generation by Smart Cards[1]

C. P. Schnorr
Universität Frankfurt, Robert-Mayer-Strasse 6–10,
W-6000 Frankfurt a.M., Federal Republic of Germany



United States Patent [19]

Schnorr

[11] **Patent Number: 4,995,082**

[45] **Date of Patent: Feb. 19, 1991**

[54] **METHOD FOR IDENTIFYING SUBSCRIBERS AND FOR GENERATING AND VERIFYING ELECTRONIC SIGNATURES IN A DATA EXCHANGE SYSTEM**

[76] Inventor: **Claus P. Schnorr,** Frankfurterstr. 81, 6350 Bad Nauheim, Fed. Rep. of Germany

[21] Appl. No.: **484,127**

[22] Filed: **Feb. 23, 1990**

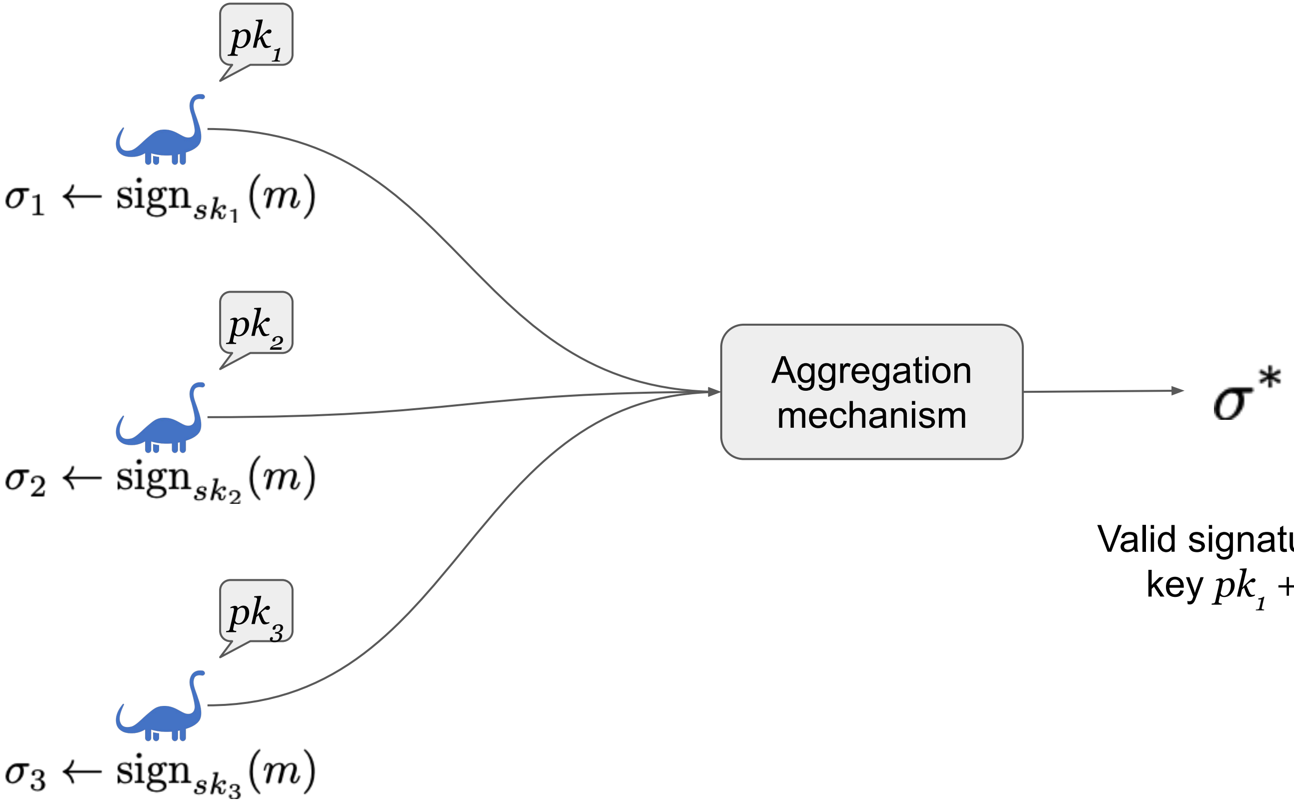
on Public-Key Techniques", I.E.E.E., Communcations, vol. 25, No. 7, 1987, pp. 73-79.

Beth, T., "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Advances in Cryptology--Eurocrypt, '80, pp. 77-84.

Primary Examiner—Thomas H. Tarcza

Assistant Examiner—David Cain

Attorney, Agent, or Firm—Hill, Van Santen, Steadman & Simpson



pk_1

$\sigma_1 \leftarrow \text{sign}_{sk_1}(m)$

pk_2

$\sigma_2 \leftarrow \text{sign}_{sk_2}(m)$

pk_3

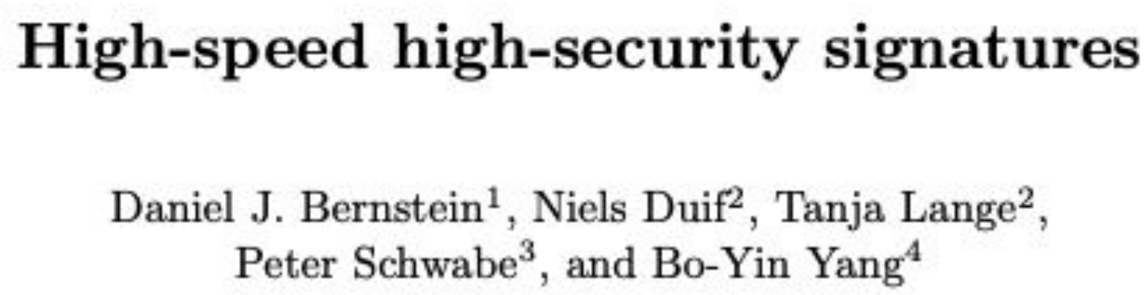
$\sigma_3 \leftarrow \text{sign}_{sk_3}(m)$

Aggregation mechanism

σ^*

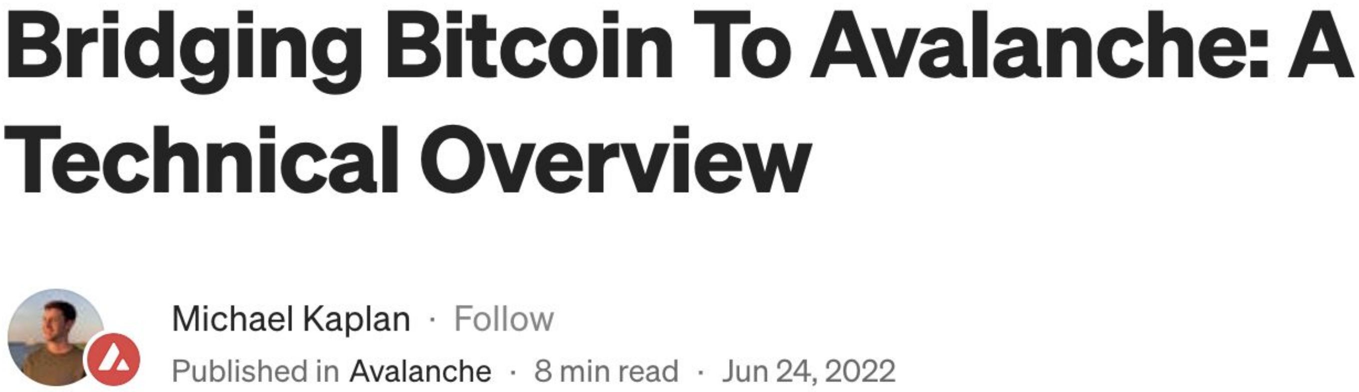
Valid signature under the key $pk_1 + pk_2 + pk_3$

ED25519



High-speed high-security signatures

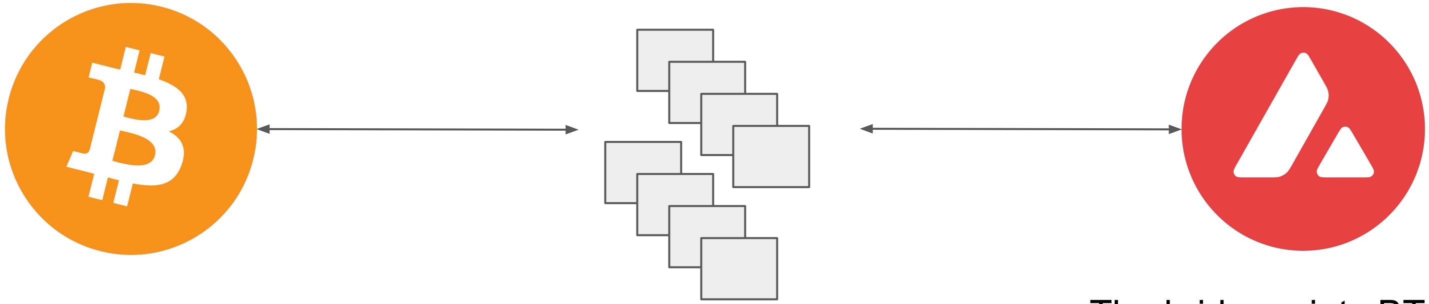
Daniel J. Bernstein[1], Niels Duif[2], Tanja Lange[2],
Peter Schwabe[3], and Bo-Yin Yang[4]



Bridging Bitcoin To Avalanche: A Technical Overview

Michael Kaplan · Follow

Published in Avalanche · 8 min read · Jun 24, 2022



When you send BTC to the warden address

Bridge wardens

The bridge mints BTC.e to the address corresponding to the same key on Avalanche

There are different curves

- NIST recommends secp256r1
- Bitcoin / Ethereum use secp256k1
  - Apple’s cryptokit supports ECDSA
    - But won’t generate signatures over secp256k1