STRĀTUMN

CRYPTO NIGHTS №1

# SCHNORR RING SIGNATURES

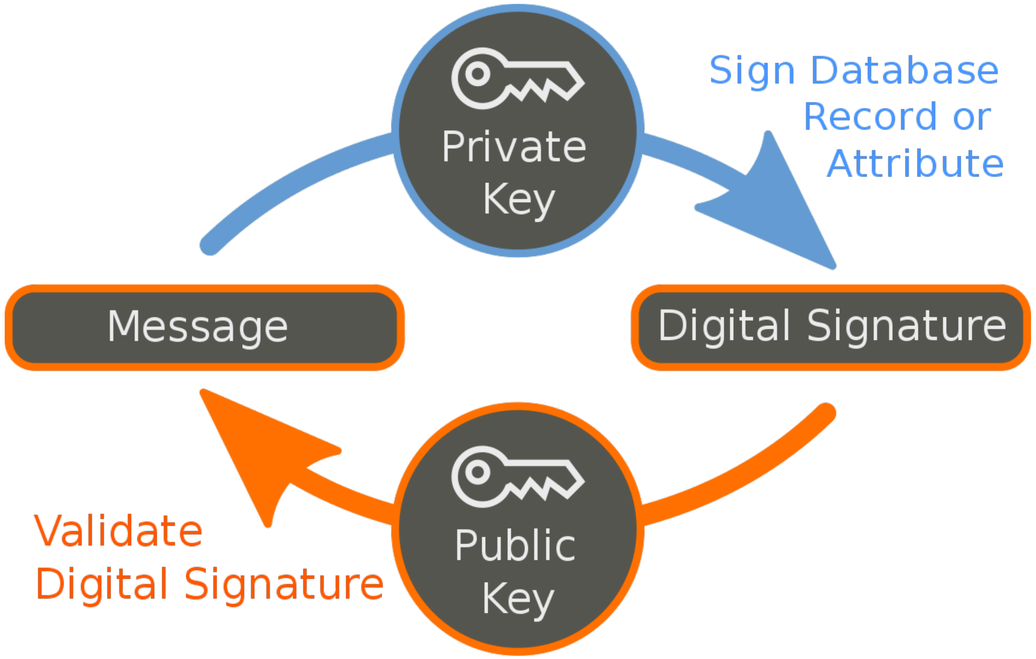
BASTIEN TEINTURIER

–

11.06.2018

# Digital Signatures

- Public Key Cryptography
- Message integrity
- Message authentication
- Non-repudiation
- KeyGen: public & private key
- Sign: $\mathbb{SK} \times \mathbb{M} \rightarrow \mathbb{S}$
- Verify: $\mathbb{PK} \times \mathbb{M} \times \mathbb{S} \rightarrow \{0,1\}$
- RSA, ElGamal, ECDSA, etc
- Single signer, multiple verifiers



# Schnorr Signatures

- Patent expired
- Small (compared to ECDSA)
- Efficient
- Hardness of discrete logarithm
- Bitcoin ❤️ Schnorr:
  - Multi-signature
  - Signature aggregation

- Protocol parameters:
  - $p \geq 2^{512}$ prime
  - $q \geq 2^{140}$ prime: $q \mid p-1$
  - $\alpha \neq 1 \in \mathbb{Z}p$: $\alpha^q \equiv 1 \; [p]$
  - h hash function
- KeyGen:
  - Private key: $s \in \mathbb{Z}q$
  - Public Key: $v = \alpha^{-s} \; [p]$
- Sign:
  - (pre-processed) $r \in \mathbb{Z}q$, $x = \alpha^r \; [p]$
  - $e = h(x, m)$, $y = r + se \; [q]$
  - Signature = $(e, y)$
- Verify:
  - Compute $x' = \alpha^y v^e \; [p]$
  - Verify $e = h(x', m)$

# Ring Signature

How to leak a secret, Rivest, Shamir, Tauman (2001)

–

Hiding the signer in a “ring”

–

Verifying a signature only tells you that “someone” in the given ring signed the message

–

No group manager, no setup phase

–

Requires a PKI

# An Example

Alice, Bob & Carol work for a government agency

Bob wants to leak internal documents to the press

Bob uses his public key along with Alice and Carol's to form a ring

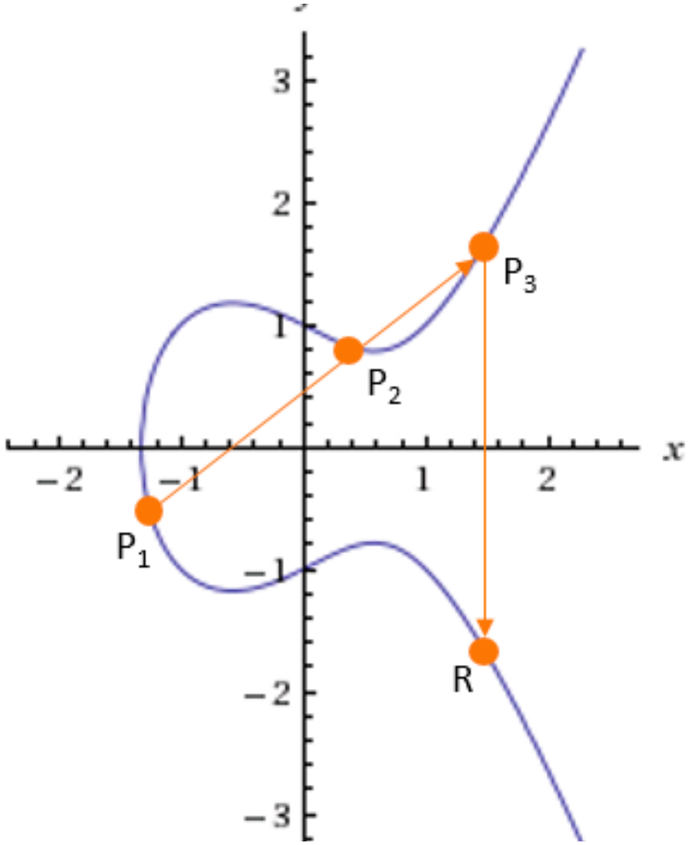
Bob uses this ring to sign the leaked documents

The press can verify the signature and know that it comes from inside the government agency

But no-one can ever know it came from Bob

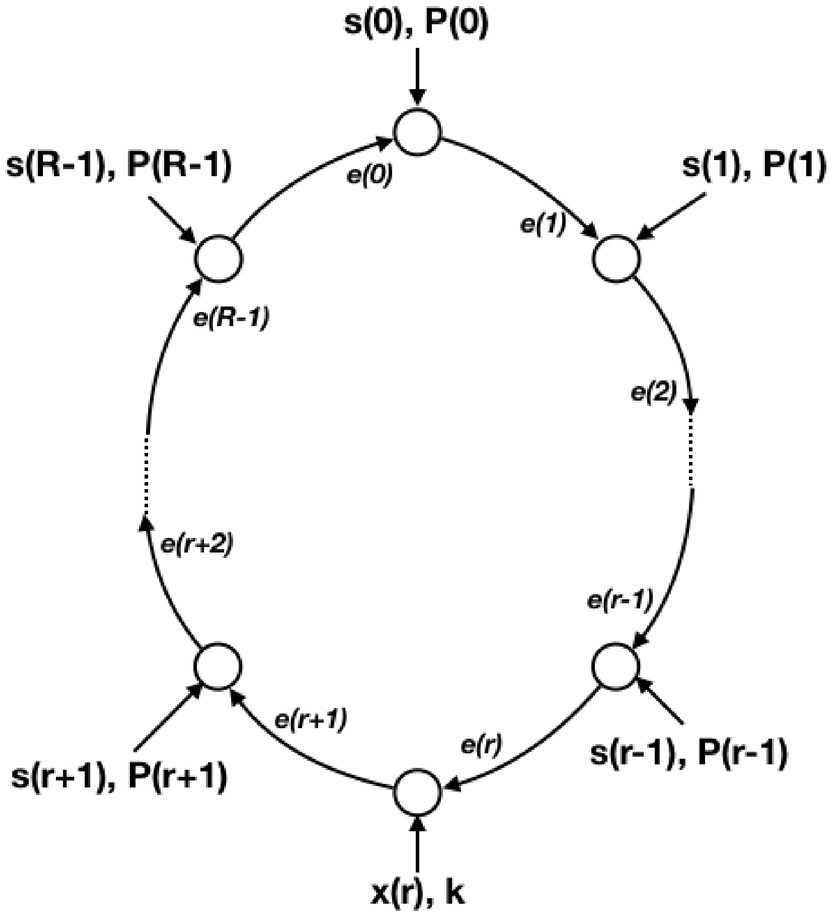
# Elliptic Curves

- $(x,y) \in \mathbb{Z}_p$ s.t. $y^2 = x^3 + ax + b\ [p]$
- $\mathcal{O}$ imaginary infinity point
- Point addition with identity $\mathcal{O}$
- Point doubling
- Under certain conditions, elliptic curve points form a cyclic group where the discrete log is hard
- Given a generator P and a point T, finding $d$ s.t. $T = dP$ is hard



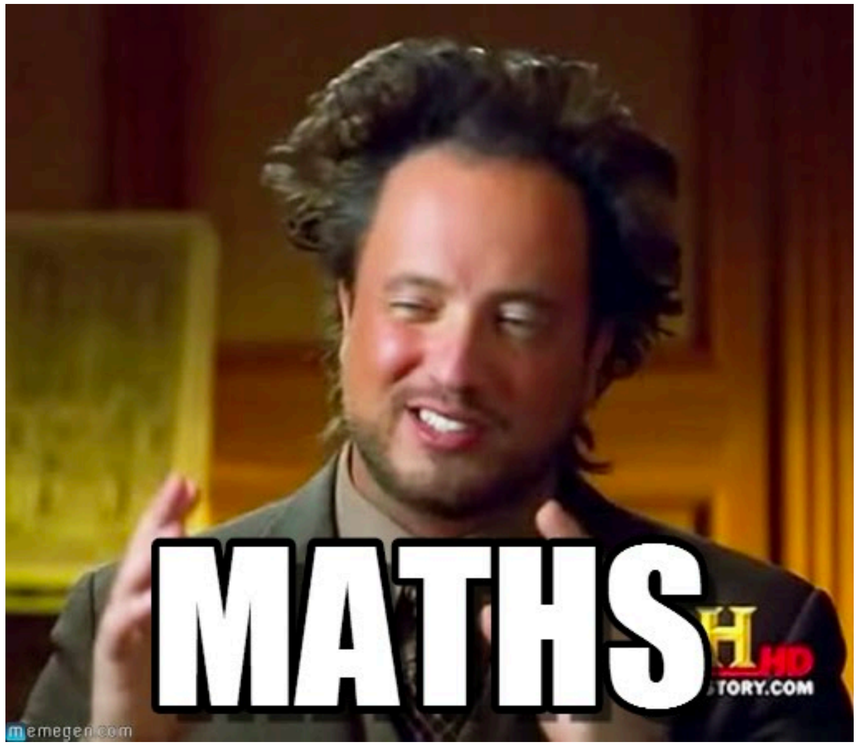
# Schnorr Ring Signature

- $\boldsymbol{R}$ = {P(0),P(1),...,P(R-1)}
- P($i$) = $x(i)\cdot$G
- $N$ order of the curve
- $r$ index of the signer in the ring
- $k \leftarrow [\![1; N\text{-}1]\!]$
- $e(r+1\ [R]) = H(m \parallel k\cdot G)$
- $i = r+1\ [R]$; $i \neq r$; $i{+}{+}\ [R]$
  - $s(i) \leftarrow [\![1; N\text{-}1]\!]$
  - $e(i+1\ [R]) = H(m \parallel s(i)\cdot G + e(i)\cdot P(i))$
- $s(r) = k - e(r)\star x(r)$
- Signature: (P(0),...,P(R-1),$e$(0), $s$(0),...,$s$(R-1))



# Schnorr Ring Signature

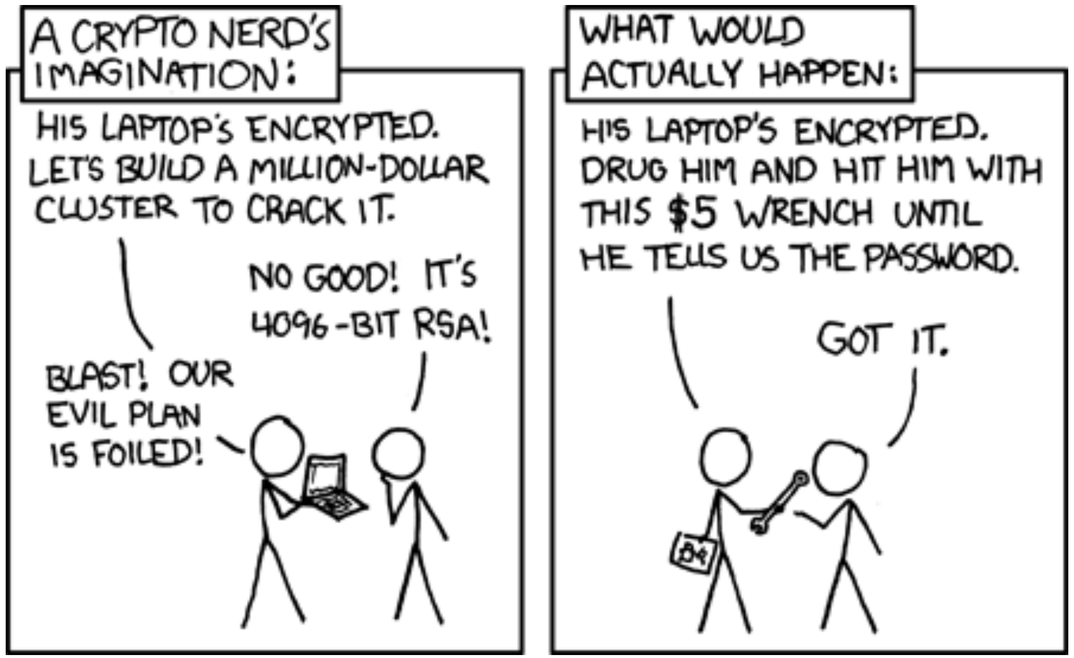
- Verify
- $e = e(0)$
- $i = 0; i < R; i{+}{+}$
  - $e = H(m \,||\, s(i) \circ G + e \circ P(i))$
- $e \stackrel{?}{=} e(0)$



# “Never roll your own crypto.”

*– https://github.com/t-bast/ring-signatures*

# Questions ???


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.