Investigation of cryptographic primitives of atomic swaps performed on heterogeneous blockchains

Beáta Nagy

Supervisors: Dr. János Tapolcai, Dr. Bence Ladóczki

January 8, 2024

Elliptic curve cryptography

- Elliptic curve over a finite field $\mathbb{F}_p$:

$$y^2 \equiv x^3 + ax + b \,(mod\ p),$$

  p: prime, q: order of the curve, a, b: given elements of $\mathbb{F}_p$,
- $f : [1, q-1] \to E(\mathbb{F}_p)$, $f(v) = v \times G$, G: generator (homomorphy)
- Elliptic Curve Discrete Logarithm Problem (ECDLP): NP-hard
  - v: secret value
  - $f(v)$: public value

Digital Signature Schemes

Schnorr Signature:

$$s \equiv r + h \cdot x \pmod{q},$$

verification:

$$S = R \oplus h \times X,$$

ECDSA signature:

$$s \equiv (h + \mathcal{R} \cdot x) \cdot r^{-1} \pmod{q},$$

verification:

$$s \times R = (h \times G) \oplus (\mathcal{R} \times X),$$

q: order of the curve
s: signature, $f(s) = S$
r: random element, $f(r) = R$
h: hashed message: $h = H(m|R|X)$
x: secret key, $f(x) = X$
$\mathcal{R}$ = R - leftmost bit (mod q)

Application

Atomic swaps: exchange of cryptocurrencies in a decentralized way, in one single step

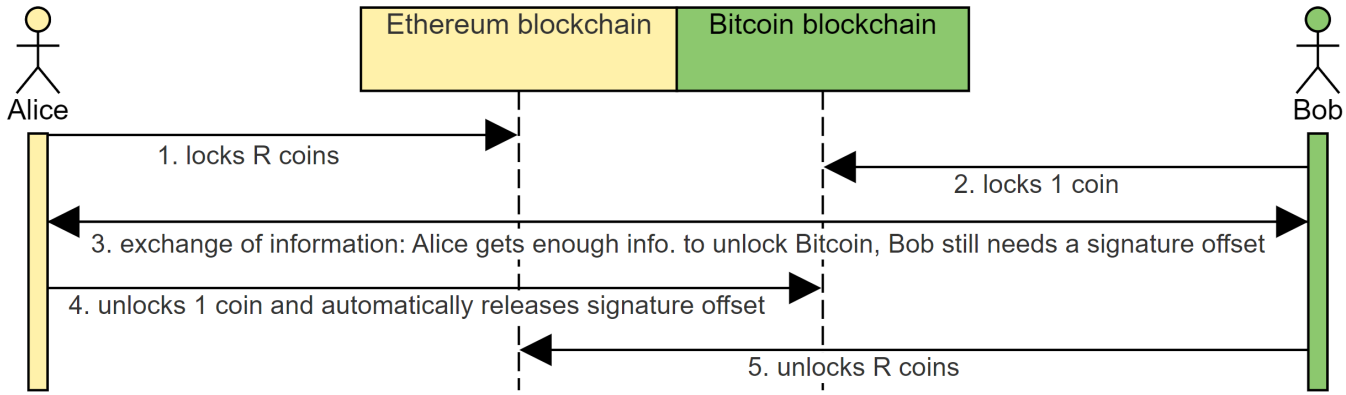

Figure: Sequence diagram of the atomic swap process

Goal: general protocol specification, independent of the blockchains

Steps of Atomic Swaps

1. X_{AB}: common public key formulation
2. m1 = transfer 1 coin from X_{AB} to X_A in Chain2
   m2 = transfer R coins from X_{AB} to X_B in Chain1
3. A generates offset t
4. A creates signature1, signature2 + offset signatures
5. B receives offset signatures, verifies
6. as A submits signature1, B can calculate offset

My implementation

- Tool: SageMath, Jupyter Notebook, WSL
- secp256k1 curve
- ECDSA and Schnorr signature primitives:
  1. Create, verify signature
  2. Offset signature, verify offset, obtain offset
- Schnorr-based atomic swap on homogeneous and heterogeneous (with different finite fields) blockchains
- Currently working on the ECDSA version
  - challenge: multi-signature: A's and B's private keys cannot be separated
    Schnorr: $s - t \equiv r_A + h \cdot x_A + r_B + h \cdot x_B \pmod{q}$
    ECDSA: $s \equiv (h + \mathcal{R} \cdot x_B + \mathcal{R} \cdot x_A)^{-1}(r_a + r_B) \pmod{q}$

Future Directions

- Boneh-Lynn-Shacham (BLS) signature scheme
- Atomic swap for ECDSA, BLS
- Comparison of methods

References


C. P. Schnorr (1990)
Efficient Identification and Signatures for Smart Cards
Advances in Cryptology — CRYPTO' 89 Proceedings 239–252.


Neal Koblitz, Alfred Menezes, and Scott Vanston (2000)
The State of Elliptic Curve Cryptography
Des. Codes Cryptography 19, 173–193.


Neal Koblitz, Alfred Menezes, and Scott Vanston (2000)
Short Signatures from the Weil Pairing
Advances in Cryptology — ASIACRYPT 2001. 514–532.


Neal Koblitz (1998)
An elliptic curve implementation of the finite field digital signature algorithm
Advances in Cryptology — CRYPTO' 98 327–337.

Thank you for your attention!