Fragile Nonce Selection and

ZKPs as a Solution

2nd ZKProof Workshop, 2019

Andrew Poelstra

Director of Research, Blockstream

Schnorr Signatures

$$P = xG$$

$$k \leftarrow \$$$
$$R = kG$$
$$e = H(P, R, m)$$
$$s = k + ex$$

In practice "$" is by far the most difficult part of this protocol.
(see Breitner and Heninger, 2019)

Schnorr Signatures

- Standard solution: use RFC6979: $k = H(x \| m)$.
- Not verifiable.
- Use a ZKP? Better hope your host doesn't leak the ZKP.
- . . . and if you trust the host, just use sign-to-contract.

Schnorr Signatures

- Consider the "sign-to-contract" construction which overloads a signature as a signature on another, auxiliary message.
- Used for timestamping, wallet audit logging, and anti-covert-sidechannel resistance.

$$
\begin{aligned}
R^0 &= kG \\
R &= R^0 + H(R^0 \| c)G \\
e &= H(P, R, m) \\
s &= (k + H(R^0 \| c)) + ex
\end{aligned}
$$

Multisignatures

- Consider Schnorr multisignatures with combined keys of the form $P = \sum \mu_i P_i$ (MuSig).
- Participant i creates partial signatures with secret key $\mu_i x_i$.
- But the challenge $e = H(P, R, m)$ will have contributions from all participants. R could change without P or m changing.
- Replay attacks, parallel attacks, VM forking, etc.
- So RFC6969 is out. Back to physical randomness?

Multisignatures

- Suppose instead each party used RFC6979 (or a moral equivalent) but provide a ZKP that they produced their nonce deterministically.
- What's a "moral equivalent"? A PRF but verifiable. Like a VRF. But not.
- Upcoming research (Ruffing, Seurin, Wuille 2020)

Multisignatures

In general, ZKPs of deterministic PRNG operation can

- Turn randomized signatures into unique ones (sooorta. Ignore the ZKP's randomness).
- Prevent replay attacks.
- Eliminate the need for broadcast channels?

Threshold Signatures

- Consider now *threshold* Schnorr signatures (Stinson & Strobl 2001)
- Here each participant i shards his key x_i into shards x_i^j from which x_i can be reconstructed by Lagrange interpolation (Pedersen 1991, GJKR 1999)
- During signing, participant i similarly shards his nonce k_i.
- Final signature is assembled by interpolating partial signatures.

Threshold Signatures

- Requires potentially many rounds; accusations and defenses
- Could simplify accusation process using zk-PoKs rather than GJKR'99 protocol, using PVSS (Stadler '96) (maybe.)
- Or we could just avoid secret-sharing at signing time, still having potentially many rounds
- No matter what, we **need a broadcast channel.**

Threshold Signatures

- **Alternately**, suppose each participant produces her interpolation polynomial using deterministic randomness.
- Does PVSS where the public coefficients are accompanied by a ZKP that they were formed deterministically.
- Now a participating signer's entire transcript must be unique.
- No replays; no physical randomness; fixed number of rounds.
- And it appears our broadcast channel can be replaced with a set-reconciliation phase.

Thank you.

Andrew Poelstra
apoelstra@blockstream.com