The MuSig Schnorr Signature Scheme

November 16, 2018

1 Introduction

This report investigates MuSig, which is provably secure in the *plain public-key model.* However, the case of interactive signature aggregation where each signer signs their own message must still be proven by a complete security analysis.

Multisignatures are a form of technology used to add additional security for cryptocurrency transactions.[1]

2 Schnorr Signatures for Bitcoin

Schnorr signatures produce a smaller on-chain size, support faster validation and have better privacy. They natively allow for combining multiple signatures into one through aggregation. They permit more complex spending policies, including k-of-n and more to be represented as as single signature for a single key.

Signature aggregation also has its challenges. This included the rogue-key attack, where a participant steals funds using a specifically constructed key. This is easily solved for simple multi-signatures, however, through an enrollment procedure, where the keys sign themselves, supporting it across multiple inputs of a transaction requires plain public-key security, meaning there is no setup.

An additional attack, termed the Russel attacks, after Russel O'Connor, who was discovered for multi-party schemes where a party could claim ownership of someone else's key and so spend their other outputs.

Peter Wuille discussed the issues and their solutions, which refines the Bellare-Neven (BN) scheme. He also discussed the performance improvements that were implemented for the scaler multiplication fo the BN scheme and how they enable batch validation on the blockchain. A pair of BIPs are in process to make these advances a reality for Bitcoin.[2]

3 Key Aggregation for Schnorr Signatures

MuSig is a simple multi-signature scheme that is novel in combining:

1. Support for key aggregation

2. Security in the plain public-key model

There are two versions of MuSig, that are provably secure, which differ based on the number of communication rounds:

- Three-round MuSig only relies on the Discrete Logarithm (DL) assumption, which ECDSA (Elliptic Curve Digital Signature Algorithm) also relies on
- Two-round MuSig instead relies on the slightly stronger One-More Discrete Logarithm (OMDL) assumption

A multi-signature scheme is a combination of a signing and verification algorithm, where multiple signers (each with their own private/public key) jointly sign a single message, resulting in a single signature. This can then be verified by anyone knowing the message and the public keys of the signers.

Note: in the context of Bitcoin, the term 'multisig' refers to a k-of-n policy, where k can be different from n. While in the cryptographic literature, the term multi signature really only refers to n-of-n policies, however, k-of-n can be constructed on top of n-of-n.

The term *key aggregation* refers to multi-signatures that look like a single-key signature, but with respect to an aggregated public key that is a function of only the participants' public keys. Thus, verifiers do not require the knowledge of the original participants' public keys- they can just be given the aggregated key. In some use cases, this leads to better privacy and performance. MuSig is effectively a key aggregation scheme for Schnorr signatures.

There are other multi-signature schemes that already exist that provide key aggregation for Schnorr signatures, however they come with some limitations, such as needing to verify that participants actually have the private key corresponding to the pubic keys that they claim to have. *Security in the plain public-key model* means that no limitations exist. All that is needed from the participants is their public keys. [3]

3.1 Applications of mulit-signatures in Bitcoin

The most obvious use case for mulit-signatures with regards to Bitcoin is as a more efficient replacement of n-of-n multisig scripts and other policies that permit a number of possible combinations of keys (including k-of-n, using key trees, MAST, or traditional threshold schemes). For these, a native multisignature scheme means that what is left is one signature per transaction input.

A key aggregation scheme also lets us reduce the number of public keys per input to one, as a user can send coins to the aggregate of all involved key, rather than including them all in the script. This leads to smaller on-chain footprint, faster validation, and better privacy. As a result, MuSig is a good choice here.

Instead of creating restrictions with one signature per input, one signature can be used for the entire transaction. Key aggregation cannot be used across multiple inputs, as the public keys are committed to by the outputs, and those can be spent independently. MuSig can be used here (with key aggregation done by the verifier).

On a technical standing, in order to combine all the transaction inputs' signatures, a multi-signature scheme is not necessary, instead an aggregate signature scheme can be used. The distinction is simply that in an aggregate signature, each signer has their own message, instead of one message shared by all.

Aggregate signatures can be categorized as being:

- Interactive: Interactive aggregate signatures (IAS) require the signers to cooperate, while non-interactive schemes all the aggregation to be done by anyone

- Non-interactive: These allow the aggregation to be done by anyone

No non-interactive aggregation schemes are known that only rely on the DL assumption, but interactive ones are trivial to construct.

4 Bellare and Neven

Bellare-Neven (BN) is a more widely known plain public-key multi-signature scheme, that does not support key aggregation. It is possible to use BN multi-signatures where the individual keys are MuSig aggregates.

References

[1] **G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille, "Simple Schnorr Multi-Signatures with Applications to Bitcoin," pp. 1–34, 2018.**

[2] **Blockstream, "Schnorr Signatures for Bitcoin - BPASE '18," 2018. [Online]. Available: https://blockstream.com/2018/02/15/schnorr-signatures-bpase/**

[3] **P. Wuille, "Key Aggregation for Schnorr Signatures," 2018.**