マルチシグアドレスの検証方法

Bitcoinサービスを提供し、ユーザには閾値署名のマルチシグアドレスに送金してもらう必要がある。
そのアドレスがサービスに使われるのか、詐欺で別のアドレスに送金させようとしているのかをユーザが検証できるようにしたい(そのサービス自体が詐欺かどうかは判断できない)。

 ChatGPT

アドレスでの判定

P2WSH はスクリプト専用なので区別は付くし、 `OP_MULTISIGCHECK` の形式であればスクリプトを公開してもらえばどの公開鍵が含まれているかもわかり、同じアドレスになるかの検証もできる。
GG18 閾値署名は ECDSA なので集約すると P2WPKH になり、これだけでは検証できない。

P2TR では単独鍵もスクリプトもアドレスでは区別が付かない。
`OP_CHECKADD` を使ったマルチシグであればスクリプトさえ公開してもらえばどの公開鍵が含まれているかもわかり、同じアドレスになるかの検証もできる。
FROST はシュノア署名を集約して単独鍵になり、これだけでは検証できない。

オフチェーン情報の公開による判定

Bitcoinスクリプトを使ったマルチシグの場合はスクリプトを公開してもらうことにより検証可能。
閾値署名を使った場合は単独鍵になるため、その工程を公開してもらわないと検証できない。

集約鍵 P の検証に必要な情報

- 参加者個別の公開鍵群 $P_1, P_2, ..., P_n$
  - アルゴリズムによっては鍵の順番が影響する
- 集約方式
- 集約結果 P
- P から導かれるBitcoinアドレス

集約に乱数要素は基本的には無いらしい。
少なくともオリジナルの MuSig2、GG18、FROST には鍵生成や署名以外では使わない。