1、implement the naïve birthday attack of reduced SM3

2、implement the Rho method of reduced SM3

\*3、implement length extension attack for SM3, SHA256, etc

\*4、do your best to optimize SM3 implementation (software)

\*5、Impl Merkle Tree following RFC6962

\*6、Try to Implement this scheme

\*7、report on the application of this deduce technique in Ethereum with ECDSA

\*8、verify the above pitfalls with proof-of-concept code

\*9、Implement the above ECMH scheme

\*10、implement sm2 2P sign with real network communication

\*11、implement sm2 2P decrypt with real network communication

\*12、PoC impl of the scheme, or do implement analysis by Google

13、research report on MPT

\*14、forge a signature to pretend that you are Satoshi

\*15、send a tx on Bitcoin testnet, and parse the tx data down to every bit, better write script yourself