姓名：王晖

学号：202100141110

完成项目：

\*Project1: implement the naïve birthday attack of reduced SM3

\*Project2: implement the Rho method of reduced SM3

\*Project3: implement length extension attack for SM3, SHA256, etc.

\*Project4: do your best to optimize SM3 implementation (software)

\*Project5: Impl Merkle Tree following RFC6962

\*Project8: AES impl with ARM instruction

\*Project9: AES / SM4 software implementation

\*Project10: report on the application of this deduce technique in Ethereum with ECDSA

\*Project11: impl sm2 with RFC6979

\*Project12: verify the above pitfalls with proof-of-concept code

\*Project13: Implement the above ECMH scheme

\*Project14: Implement a PGP scheme with SM2

\*Project15: implement sm2 2P sign with real network communication

\*Project16: implement sm2 2P decrypt with real network communication

\*Project17：比较Firefox和谷歌的记住密码插件的实现区别

\*Project18: send a tx on Bitcoin testnet, and parse the tx data down to every bit, better write script yourself

\*Project22: research report on MPT

未完成项目：

\*Project6: impl this protocol with actual network communication

\*Project7: Try to Implement this scheme

\*Project19: forge a signature to pretend that you are Satoshi

\*Project21: Schnorr Bacth