完成的项目：

Project: implement the naïve birthday attack of reduced SM3

Project: implement the Rho method of reduced SM3

Project: implement length extension attack for SM3, SHA256, etc

未完成的项目：

Project: do your best to optimize SM3 implementation (software)

Project: verify the above pitfalls with proof-of-concept code

Project: Impl Merkle Tree following RFC6962

Project: Implement a PGP scheme with SM2

Project: Implement the above ECMH scheme

Project: implement sm2 2P sign with real network communication

Project: implement sm2 2P decrypt with real network communication

Project: Try to Implement this scheme SM2

Project: report on the application of this deduce technique in Ethereum with EC

Project: impl sm2 with RFC6979

Project: PoC impl of the scheme, or do implement analysis by Google

Project: forge a signature to pretend that you are Satoshi

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

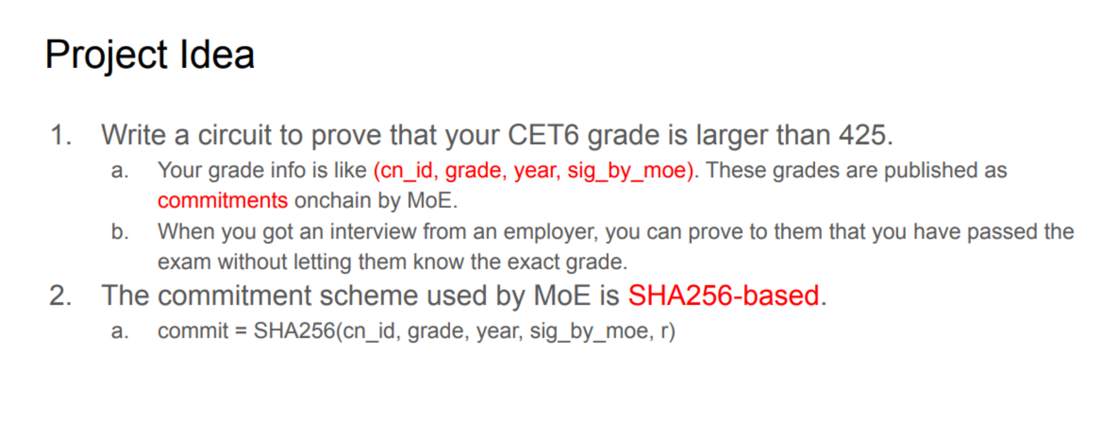
Password Hashing Competition

Project: research report on MP

Project: Find a key with hash value "*sdu_cst_20220610*" under a message composed of *your name* followed by *your student ID*. For example, "*San Zhan*

202000460001”.

Project: Find a 64-byte message under some k fulfilling that their hash value is symmetrical.



Project Idea

1. Write a circuit to prove that your CET6 grade is larger than 425.
    a. Your grade info is like (cn_id, grade, year, sig_by_moe). These grades are published as commitments onchain by MoE.
    b. When you got an interview from an employer, you can prove to them that you have passed the exam without letting them know the exact grade.
2. The commitment scheme used by MoE is SHA256-based.
    a. commit = SHA256(cn_id, grade, year, sig_by_moe, r)