师文基-202200460138

密码 2 班

Project 1: 做 SM4 的软件实现和优化
a): 从基本实现出发 优化 SM4 的软件执行效率，至少应该覆盖 T-table、AESNI 以及最新的指令集（GFNI、VPROLD 等）
b): 基于 SM4 的实现，做 SM4-GCM 工作模式的软件优化实现

Project 2: 基于数字水印的图片泄露检测
编程实现图片水印嵌入和提取（可依托开源项目二次开发），并进行鲁棒性测试，包括不限于翻转、平移、截取、调对比度等

Project 3: 用 circom 实现 poseidon2 哈希算法的电路
1) poseidon2 哈希算法参数参考参考文档 1 的 Table1，用(n,t,d)=(256,3,5)或(256,2,5)
2）电路的公开输入用 poseidon2 哈希值，隐私输入为哈希原象，哈希算法的输入只考虑一个 block 即可。
3) 用 Groth16 算法生成证明
参考文档:
1. poseidon2 哈希算法 https://eprint.iacr.org/2023/323.pdf
2. circom 说明文档 https://docs.circom.io/
3. circom 电路样例 https://github.com/iden3/circomlib

Project 4: SM3 的软件实现与优化
a)：与 Project 1 类似，从 SM3 的基本软件实现出发，参考付勇老师的 PPT，不断对 SM3 的软件执行效率进行改进
b)：基于 sm3 的实现，验证 length-extension attack
c)：基于 sm3 的实现，根据 RFC6962 构建 Merkle 树（10w 叶子节点），并构建叶子的存在性证明和不存在性证明

Project 5: SM2 的软件实现优化
a). 考虑到 SM2 用 C 语言来做比较复杂，大家看可以考虑用 python 来做 sm2 的 基础实现以及各种算法的改进尝试
b). 20250713-wen-sm2-public.pdf 中提到的关于签名算法的误用 分别基于做 poc 验证，给出推导文档以及验证代码
c). 伪造中本聪的数字签名

Project 6: Google Password Checkup 验证
来自刘巍然老师的报告 google password checkup，参考论文

https://eprint.iacr.org/2019/723.pdf 的 section 3.1 ，也即 Figure 2 中展示的协议，尝试实现该协议，（编程语言不限）。