Shi Yan

131 Changfeng Street, Taiyuan City, Shanxi Province, China
☎ (+86) 13593140301 | ✉ shiyan.aloys@gmail.com | 🪪 Personal Website

Education

Wuhan University (WHU) Wuhan, China
Bachelor of Engineering in Information Security *Sept. 2020 – June 2024 (Expected)*

- **Overall GPA:** 3.83/4.00, **Weighted Average Score:** 90.11/100.
- **Selected Courses:** Operation System Design and Practice, Database Systems, Data Structures, Trusted Computing, Assembly Language, Digital Logic and EDA, Computer Organization Principles, Advanced Mathematics, Linear Algebra, Probability Theory and Mathematical Statistics, Discrete Mathematics, Mathematical Foundations of Information Security, Artificial Intelligence in Practice, Social Computing, Cryptography, etc.

Publications

[1] **Yan, S,** Tu, A, Ling, C, Ou, C. (2023). Collision Spanning Tree: Quick Key Recovery for Side-Channel Collision Attacks. Submitted to Design Automation Conference 2024 (DAC 2024).
[2] Yan, S. (2022). Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake. [Paper Presentation]. 2022 International Conference on Mobile Computing, Algorithms and Network Security (MCANS 2022) Hangzhou, China.

Research Experience

Transferable Adversarial Attack on VITs and CNNs

Supervisor: Prof. Shuhui Wang April 2023 – Present

- Explored the transferability of adversarial samples between different models, such as VITs and CNNs.
- Reproducing recent works in the field of adversarial machine learning, recognized the importance of security in AI models, and motivated to pursue further research in LLM security.

Collision Spanning Tree: Quick Key Recovery for Side-Channel Collision Attacks

Supervisor: Prof. Changhai Ou March 2022 – Nov. 2023

- Led the project and served as the first author of the paper submission.
- Developed a strategy to select collision positions based on dispersion of correlation coefficients obtained from CECA and developed a new spanning tree algorithm utilizing xor operation relationship between collisions to recover collisions chain with low complexity.
- Proposed an algorithm combining graph theory and side channel collision attack to reduce enumeration space, added a method of using single distinguisher in field of collision attack.
- Submitted paper to Design Automation Conference 2024 (DAC 2024), which is a top international conference.

The Method based on T-test Improves the Success Rate of Side-Channel Correlation Enhanced Collision Attack

Supervisor: Prof. Changhai Ou Oct. 2022 – Feb. 2023

- Independently conducted research on t-test method and collision attack methods and promoted scientific research projects.
- Constructed a virtual dataset using the Hamming weight model and Gaussian distribution noise; applied t-test on the normal distribution sample groups corresponding to the power consumption data, resulting in a slight improvement in the success rate of the attack.
- First entry into novel scientific research, enhanced literature reading and project reproduction skills, improved problemsolving and innovative thinking abilities.

Introduction to Modern Cryptography Online Research Seminar

Supervisor: Prof. Vipul Goyal Jan. 2022 – March 2022

- Learned the fundamental principles of modern cryptography, researched the blockchain, Bitcoin, Ethereum, two consensus mechanisms, smart contracts, and used Python to build a simple virtual currency trading environment.
- Completed a review article as the first author (listed in publication section) based on the researches and my own understanding of this field, which exercised my ability to reproduce algorithms, and write academic paper.

Selected Coursework Assignments

Bypass file system and encrypt files based on underlying disk data

Supervisor: Prof. Xianbin Wang — June 2023

- Directly read disk data by file cluster; applied AES encryption to each data cluster.
- Proposed an innovative key generation strategy based on key seeds to ensure that each data cluster has a unique key.

Easy Operating System Project

Supervisor: Prof. Fei Yan — Jan. 2023

- Designed a simple system with functions including file system, process scheduling, input/output, interrupt handling, etc.
- Responsible for interrupt handling, process scheduling, file system and shell functions, expanded the OS and designed an automated trigger program from a security perspective.

File Encryption Software Based on SM2 Elliptic Curve Cryptography and Trusted Third Party Cloud

Supervisor: Prof. Changhai Ou — Dec. 2022

- Based on the SM2 encryption algorithm and SM2 signature, designed and implemented a digital signature and encryption system client with a complete graphical interface, while deploying a trusted third party in the cloud.
- Proposed a solution based on trusted third parties to address the issue of Man-in-the-Middle Attack.

Analysis and recommendation of films in 2022

Supervisor: Prof. Xiaochuan Shi — Nov. 2022

- Evaluated and analysed films from multiple dimensions, such as film scoring, comment sentiment analysis, fan distribution, cloud of words, box office, etc.
- Drew a recommendation report, made predictions of the annual film box office based on a simple BP neural network.

Analysis of Cancer Datasets And Prediction Based on Classification and Clustering Algorithms

Supervisor: Prof. Chao Ma — Dec. 2021

- Used KNN, decision tree, decision tree algorithm and K-means respectively to predict cancer prognosis in patients.

Extra-Curricular Roles

2022 National Encryption Technology Competition

Team Leader — Sept. 2022 – Dec. 2022

- Developed a parallel implementation of the collision tree based on side channel Correlation Enhanced Collision Attack.
- Stored the same prefix of the collision chain in the parallel implementation and used pruning to improve key search performance and fault tolerance, achieving good results in the competition.

The 4th "Huashu Cup" National Undergraduate Mathematical Contest in Modelling

Team Member — Aug. 2023

- Responsible for the algorithm and programming part, as well as the writing of the paper.
- Achieved National Third Prize.

Awards & Honors

Second Prize Scholarship (Top 14%)	Sept. 2023
Outstanding Student Prize	Sept. 2023
National Cyber-security Center Outstanding Student Scholarship	June 2023
Merit Student Prize	Sept. 2022
Second Prize Scholarship (Top 7%)	Sept. 2022

Other Skills & Interests

Professional Skills: Proficient in using C, C++, MATLAB, Python, LaTeX, frameworks such as Flask, foundation in Machine Learning and Deep Learning, familiar with MySQL, Verilog

Languages: English (IELTS level 7), Chinese (native)

Hobbies: Guitar, skiing, football, comprehensive grasp of video editing