# Yisheng Zhong

+1 (703)8327843 | yzhong7@gmu.edu | Beijng
linkedin.com/in/yisheng-zhong | easonzhong99.github.io

## SUMMARY

I am a PhD student in Cybersecurity at George Mason University, with a Master's degree from the University of Chinese Academy of Sciences. My research focuses on the security and privacy of large language models (LLMs), particularly LLM unlearning techniques. Additionally, I have previously conducted research at the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, where I focused on Byzantine-robust Privacy-preserving Federated Learning. I am a member of the SPARK Lab, led by Prof. Zhuangdi Zhu, where we explore cutting-edge solutions to enhance privacy and security in AI-driven technologies.

## EDUCATION

**University of Chinese Academy of Sciences | Master of Cyber Security** Double 1st-Class Sep 2021 - Jun 2024

- GPA: 3.56/4.0
- Relevant Courses: Machine Learning, Deep Learning, Security Protocols, Applied Cryptography
- Focus on Privacy-preserving computing and Defense against adversarial attacks and their application in machine learning

**Harbin University of Science and Technology | Bachelor of Computer Science** Sep 2017 - Jun 2021

- GPA: 3.8/4.0 (Top 1%)
- Relevant Courses: Advanced Mathematics, Data Structure, Discrete Mathematics, Signalistics and Systematics, Probability and Statistics, Linear Algebra, Pattern Recognition, Complex Function and Integral Transform, Principles of Computer Composition
- Obtained direct admission offer to pursue a Master's degree at the Chinese Academy of Sciences

## RESEARCH EXPERIENCE

**PROFL: A Privacy Preserving Federated Learning Method with Stringent Defense Against Poisoning Attacks** Sep 2022 - Jun 2023

- Proposed PROFL, a privacy-preserving Byzantine-robust federated learning framework that utilizes a composite approach based on similarity and statistical methods to defend against various hidden poisoning attacks. In the defense process, secure computation is performed for privacy protection using the two-trapdoor Homomorphic Encryption algorithm.
- Compared to similar privacy-preserving defense schemes, our work has higher security and improve prediction accuracy in extreme cases by 13%-56%.
- Authored a paper as the first author on this work, which has been accepted by CSCWD 2024.

**Semi-supervised Corrupted Face Classification via Graph Learning** Jan 2021 - May 2021

- Proposed a method to enhance the robustness and classification accuracy of semi-supervised face classification algorithms by recovering complete facial data from low-rank subspaces, effectively addressing pixel missing or occlusion issues.
- This significantly improved algorithmic robustness, resulting in an approximate 10% increase in classification accuracy.
- Based on this work, authored a paper as the first author, which has been accepted by the *"MobileMedia"* Conference organized by the European Alliance for Innovation (EAI).

**Methods for Linear Star Map Processing under Large Dynamic Conditions** Jan 2020 - Dec 2020

- Participated in a collaborative project between the university and a research institute under the China National Space Administration, focusing on Fast object recognition in images.
- Responsible for designing and optimizing image processing algorithms, coding for the demonstration system, and serving as a representative in the project's closing presentation.
- Proposed algorithms that fulfilled the operational requirements in specific environments, exhibiting 2-4 orders of magnitude faster runtime compared to similar algorithms. The project has successfully passed acceptance.

## COMPETITION EXPERIENCE

**2020 Mathematical Contest In Modeling** Apr 2020

- Participated in the 2020 Mathematical Contest In Modeling, where the team simulated the problem using a 3D cellular automata described by differential equations and then solved it using a genetic algorithm.
- As the team leader, organized regular pre-competition meetings for knowledge exchange and simulated competitions. During the competition, allocated tasks, coordinated members' work, and made decisions. Took responsibility for mathematical model formulation, algorithm design, optimization, and implementation.
- Finally, the team won the *"Meritorious Winner"* award (International First Prize).

**Enhancing Face Recognition Security through Lip Reading Integration** Jan 2020 - Dec 2020

- Headed the university student innovation project, which aimed to combine lip reading and facial recognition for improved security in the latter. Utilizing lip reading recognition technology to accomplish both liveness detection and identity authentication tasks.
- Responsibilities included project proposal initiation, team organization, system development, and paper writing.
- Successfully completed the project and authored the paper with the same title as the first author in the *"Journal of Intelligent Computing and Applications"* of HIT.

## HONORS & AWARDS

| | |
|---|---|
| Meritorious Winner at the Mathematical Contest In Modeling (First Prize) | 2020 |
| Annual Scholarships of University of Chinese Academy of Sciences | 2021-2023 |
| First-Class Scholarships of Harbin University of Science and Technology | 2017-2021 |
| Merit Student of Harbin University of Science and Technology | 2017-2021 |
| Second Prize of the Ladder Competition of China University Computer Competition | 2020 |
| Second Prize in Provincial "Lanqiao" Cup Competition | 2019 |
| Second Prize in WeChat Mini Program Design Competition | 2020 |
| Third Prize in "Internet+" Innovation Competition | 2021 |