

# Jie Peng

✉ jie.peng1004@gmail.com    🔗 <https://jiepeng104.github.io/>

## Education

### Harbin Institute of Technology

Sept 2018 – June 2022

*Bachelor of Engineering in Computer Science and Information Security*

- Score: 89.32/100
- **Coursework:** Set Theory and Graph Theory (93/100), Computer System (94/100), Introduction to machine learning (93/100), Cryptography Theory and Practice (96/100), Information Content Security (95/100)

### Harbin Institute of Technology

Sept 2022 – June 2025

*Master of Engineering in Computer Security*

- Score: 89.10/100
- **Advisors:** Prof. Hui He and Prof. Weizhe Zhang
- **Coursework:** Combinatorial Optimization and Convex Optimization (97/100), Data Mining: Algorithms and Applications (98/100), Network and Information Security (94/100)

## Publications

- **Jie Peng**, Hongwei Yang, Jing Zhao, Hengji Dong, Hui He, Weizhe Zhang and Haoyu He. “Circumventing Backdoor Space via Weight Symmetry”. ([ICML 2025](#) 🔗 , [arXiv](#) 🔗)
- **Jie Peng**, Hongwei Yang, Hui He, Jing Zhao, Haoyu He, Hengji Dong and Weizhe Zhang. “LS<sup>2</sup>: Boosting Hidden Separation for Backdoor Defense with Learning Speed-driven Label Smoothing”. ([T-IFS](#) 🔗 , [PDF](#) 🔗)
- Jing Zhao, Hongwei Yang, Hui He, **Jie Peng**, Weizhe Zhang, Jiangqun Ni, Arun Kumar Sangaiah, and Aniello Castiglione. “Backdoor Two-Stream Video Models on Federated Learning”. ACM Transactions on Multimedia Computing, Communications, and Applications ([TOMM](#) 🔗)

## Awards and Honors

**Runner-up** , The 7th Qiangwang International Elite Challenge on Cyber Mimic Defense (AI Track), 2024 (Team: **HiddenFace**) 🔗

- Developed adversarial attacks on face recognition systems without requiring attacker-specific model retraining, enhancing attack transferability and robustness under mimic defense scenarios. ([Code](#) 🔗)

## Industry Experience

### Shanghai Pudong Development Bank (SPD BANK, Shanghai)

May 2024 – August 2024

- Participated in developing a Graph-based Anomaly Detection algorithm within a federated learning setting to identify financial fraud patterns while maintaining data privacy
- Implemented the solution using FATE framework (Federated AI Technology Enabler), enabling secure and efficient collaboration between multiple financial institutions.
- Tools Used: Python, PyTorch, FATE

## Additional Information

**Skilled at:** C, Java, Python, SQL, L<sup>A</sup>T<sub>E</sub>X

**Languages:** Mandarin (native), English (Proficient, IELTS band score 7)