Zheng Li

No.1500 Shunhua Road, Jinan, Shandong – China

✉ zhenglisec@gmail.com ☎ (+86) 15866729082

RESEARCH INTEREST

Machine Learning for Cyber Security,
Attacks and Defenses of Machine Learning,
Privacy Preserving Machine Learning

EDUCATION

Shandong University **Jinan, China**
Master in Computer Science *September, 2017–June, 2020*
School of Computer Science and Technology

Shandong University, GPA 3.42/4 **Jinan, China**
Bachelor in Computer Science *September, 2013–June, 2017*
School of Computer Science and Technology

PUBLICATIONS

- **Zheng Li**, Ge Han, Shanqing Guo*, Chengyu Hu
  My Contributions: Idea, Coding (100%), Writing (80%).
  "DeepKeyStego: Protecting Communication by Key-dependent Steganography with Deep Networks" in Proceedings of the 21st IEEE International Conference on High Performance Computing and Communications (HPCC 2019) (**Acceptance rate: 230/1133=20.3%**) (Souce code: DeepKeyStego).
- **Zheng Li**, Chengyu Hu, Yang Zhang, Shanqing Guo*
  My Contributions: Idea, Coding (100%), Writing (99.9%).
  "How to Prove Your Model Belongs to You: A Blind-Watermark based Framework to Protect Intellectual Property of DNN" in Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019) (**Acceptance rate: 60/266=22.6%**) (Source code: BlindWatermarkDNN).
- Ge Han, **Zheng Li**, Yunqing Wei, Chengyu Hu, Shanqing Guo*
  My Contributions: Coding (100%), Writing (10%).
  "FuzzGAN: A Generation-Based Fuzzing Framework For Testing Deep Neural Networks" Under Review, ICSE 2020.

SELECTED PROJECTS

Web-Page Implement the Visual YACC *Nov 2016-Apr 2017*
Supervised by Xiaocheng Gao

- This is a web-page application for syntax analysis, the core part of the compilation process. Its task is to identify the string of words on the basis of lexical analysis, and to determine whether the grammar structure is consistent with the rules of grammar.
- It mainly works for students.

Symmetric and Asymmetric Cryptography based on deep learning *Apr 2017 – Sep 2017*

Supervised by Shanqing Guo

- A system consists of neural networks named Alice and Bob, and we aim to limit what a third neural network named Eve learns from eavesdropping on the communication between Alice and Bob. We do not prescribe specific cryptographic algorithms to these neural networks; instead, we train end-to-end, adversarially.
- The system demonstrates that the neural networks can learn how to perform forms of encryption and decryption.

Steganography based on deep learning *Dec 2017 – Mar 2018*
Supervised by Shanqing Guo

- The project is aiming to hide both the presence and the content of secret information against eavesdropping over public communication channels.
- It shows rather effectiveness and integrity in a practical situation.

Coding to reproduce the paper titled "DeepXplore" with Pytorch *July 2018 – Oct 2018*
Supervised by Shanqing Guo

- DeepXplore: Automated Whitebox Testing of Deep Learning Systems, published in SOSP'17
- DeepXplore efficiently finds thousands of incorrect corner case behaviors in state- of-the-art DL models with thousands of neurons trained on five popular datasets

Coding to reproduce the paper FGSM of adversarial learning *June 2018 – Aug 2018*
Supervised by Shanqing Guo

- The fast gradient sign method works by using the gradients of the neural network to create an adversarial example. For an input image, the method uses the gradients of the loss with respect to the input image to create a new image that maximizes the loss. This new image is called the adversarial image.

AWARDS AND ACHIEVEMENTS

- The Third Scholarship * 2
- The First Scholarship (Top 2/55, 2019)
- Excellent Graduation Design Project (2017)

PROFESSIONAL RECOGNITION

- CCF-CSP14 (Certified Software Professional) (Top 13.04% of 1749 participants)
- CET-4, CET-6

TECHNICAL STRENGTHS

- Programming Languages: Python (skilled), C++, Java.
- ML framework: Pytorch (skilled), tensorflow, keras, sklearn.

REFERENCES

- **Shanqing Guo**
  Professor, School of Cyber Science and Technology
  Shandong University, Qingdao, China.
  guoshanqing@sdu.edu.cn
  Cell:(+86) 18615270118