

## RESEARCH INTERESTS

---

- **Machine Learning, Security (Privacy, Cryptography), Computer Vision**

## EDUCATION

---

- **Shanghai Jiao Tong University (SJTU)** Shanghai, China  
*B.Eng. in Information Security, School of Cyber Security* Sept 2015 – June 2019
  - **GPA:** 3.96/4.3 (91.6/100) **Rank:** 2/97
  - **Courses:** Data Structure and Algorithms (IS225, 99, 1<sup>st</sup>/212); Linear Algebra (MA077, 98, 19<sup>th</sup>/2172); C++ Programming (CS048, 96, 21<sup>st</sup>/571); Software Engineering (SE407, 99, 1<sup>st</sup>/118); Mathematical Methods in Physics (MA097, 94, 14<sup>th</sup>/885); Fundamental Circuit Theory (EI203, 94, 4<sup>th</sup>/438); Digital Electronics Technology (EI205, 93, 13<sup>th</sup>/390); Signal and Systems (EI210, 96, 5<sup>th</sup>/395); Data Mining (IS303, 95, 1<sup>st</sup>/40); Operating System (IS206, 95, 1<sup>st</sup>/100) – *Format: (ID, Grade, Rank)*
- **University of California, Berkeley (UC Berkeley)** California, USA\*  
*Research Intern, Berkeley Artificial Intelligence Research (BAIR) Lab* Mar 2018 – July 2018
  - **Advisor:** Profs. Bo Li and Dawn Song
  - **Research Focus:** Secure Machine Learning
- **University of Illinois Urbana-Champaign (UIUC)** Illinois, USA\*  
*Research Intern, Computer Science Department* Aug 2018 – Oct 2018
  - **Advisor:** Profs. Yang Liu and Bo Li
  - **Research Focus:** Robust Reinforcement Learning

## PUBLICATIONS

---

- **LiDAR-Video Driving Dataset: Learning Driving Policies Effectively** [pdf]  
Yiping Chen\*, **Jingkang Wang\***, Jonathan Li, Cewu Lu, Zhipeng Luo, Han Xue and Cheng Wang.  
*In Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018*

## MANUSCRIPTS

---

- **Reinforcement Learning with Perturbed Rewards** [pdf]  
**Jingkang Wang**, Yang Liu and Bo Li. (*arXiv:1810.01032*)
- **One Bit Matters: Understanding Adversarial Examples as the Abuse of Redundancy** [pdf]  
**Jingkang Wang**, Ruoxi Jia, Gerald Friedland, Bo Li and Costas Spanos. (*arXiv:1810.09650*)
- **The Helmholtz Method: Using Perceptual Compression to Reduce Machine Learning Complexity** [pdf]  
Gerald Friedland, **Jingkang Wang**, Ruoxi Jia, Bo Li and Nathan Mundhenk. (*arXiv:1807.10569*)
- **Multiple Character Embeddings for Chinese Word Segmentation** [pdf]  
**Jingkang Wang**, Jianing Zhou and Gongshen Liu. (*arXiv:1808.04963*)

## RESEARCH EXPERIENCE

---

- **Reinforcement Learning with Perturbed Rewards** July 2018 - Oct. 2018  
◦ **Advisor:** Profs. Yang Liu and Bo Li UIUC, USA\*  
◦ Introduce an unbiased estimator of reward in reinforcement learning which guarantees risk minimization without any assumptions on the true distribution.  
◦ Propose an efficient iterative algorithm for estimating the confusion matrices of corrupted rewards in the training.  
◦ Study the convergence and finite sample complexity theoretically under the proposed reward proxy.
- **Understanding Adversarial Examples as the Abuse of Redundancy** Mar 2018 - July 2018  
◦ **Advisor:** Profs. Bo Li and Dawn Song UC Berkeley, USA\*  
◦ Propose a model for adversarial examples consistent with related work, physics and information theory.  
◦ Reinterpret the Helmholtz free energy formula to explain the relationship between content and noise for sensor-based data.  
◦ Prove that input redundancy is a necessary condition for being able to generate adversarial examples.  
◦ Validate that adversarial examples are indeed overflowing perceptrons trained on a certain level of redundancy.
- **Multiple Embeddings for Chinese Word Segmentation** Feb 2018 - May 2018  
◦ **Advisor:** Prof. Gongshen Liu SJTU, China

- Leverage both semantic and phonetic features of Chinese characters in NLP tasks by introducing *Pinyin Romanization* and *Wubi Input* Embeddings.
- Achieve the state-of-the-art performance in AS and CityU corpora with F1 scores of 96.9 and 97.3.

• **Benchmark for Driving Policy Learning** ☹ ☹

*Apr 2017 - Feb 2018*

*SJTU, China*

- **Advisor:** Prof. Cewu Lu
- Propose a dataset which is the first policy learning benchmark composed of driving videos, LiDAR data, and corresponding driving behaviors.
- Conduct the complete analysis on how important depth information is, how to leverage depth information and what we can achieve by utilizing current techniques.

TEACHING EXPERIENCE

- **Teaching Assistant:** Operating System (IS206); Principle of Computer Virus (IS217)

*Spring 2019*

SELECTED PROJECTS

• **Blockchain-Based Genetic Privacy-Preserving System** ☹

*May 2018 - July 2018*

- **Advisor:** Prof. Lei Fan    **Award:** National First Prize in CISCN 2018 (**Top 1%**)
- Design a protocol of private set intersection (PSI) on the blockchain, namely BPSI, which establishes a crowdsourcing ecology and calculates PSI against collusion.
- Propose security, effectiveness and arbitration mechanism in BPSI, which guarantee the efficiency of the proposed protocol theoretically.

• **Dynamic Searchable Encryption System Based on Graph Database** ☹

*May 2017 - July 2017*

- **Advisor:** Prof. Lei Fan    **Award:** National Second Prize in CISCN 2017
- Adopt the *parallel-DSSE* algorithm in graph database and propose several policies to enhance the robustness.
- Implement the improved algorithm utilizing Neo4j Graph Database and validate its effectiveness, efficiency and scalability based on large-scale ciphers.

• **Data Mining on Large-scale Plain Passwords: A-Level in SJTU (Top 5%)**

*Jan 2017 - Oct 2017*

- **Advisor:** Prof. Gongshen Liu    **Remark:** two papers published on CCF conference/journal (Chinese).
- Analyze general rules of creating passwords based on 1.7 hundred million leaked real passwords.
- Adapt generative adversarial networks (GAN) into large-scale password generation, which outperforms other the state-of-the-art models such as OMEN, PCFGs and pure-LSTM/GRU.

HONORS & AWARDS

- **National Scholarships (Top 0.2% Nationwide – Highest Honor for Chinese Undergraduates)**    2016, 2017, 2018
- **Level-A SJTU Outstanding Scholarships (Top 1% in SJTU)**    2016, 2017, 2018
- **SenseTime Scholarship (Top 30 students selected in China per year)**    2018
- **Yitu Technology Scholarship (Top 1% in SJTU)**    2017
- **First Prize in National College Student Information Security Contest (Top 1% Nationwide)**    2018
- **Meritorious Winner Prize of Mathematical Contest in Modeling**    2018
- **Second Prize in National College Student Information Security Contest**    2017
- **Second Prize in The Chinese Mathematics Competitions (Shanghai)**    2017
- **SJTU Merit Students**    2016, 2017, 2018
- **SJTU Excellent League Cadres**    2016, 2017
- **First Prize in Chinese Mathematical Olympiad (10th in Shanxi Province)**    2014

OPEN-SOURCE INVOLVEMENT

- ☹ **OpenAI-baselines** : A set of high-quality implementations of RL algorithms (*Stars: 6.1k*)
- ☹ **DBNet** : A large-scale driving behavior dataset (videos + point clouds) (*Stars: 96*)
- ☹ **awesome-scs** : Programming reference for Information Security Major (*Stars: 25*)

INTERESTS & SKILLS

- **Hobbies:** Calligraphy, Violin, Badminton, Reading, Movie, Animation
- **Programming:** Python (Tensorflow, Pytorch), Matlab, C++, Java, Verilog
- **Others:** L<sup>A</sup>T<sub>E</sub>X, Spark, OpenCV, PCL

*Last Update: Jan 4, 2019*

\* equal contribution or remote collaboration