

## EDUCATION

---

- **Shanghai Jiao Tong University (SJTU)** Shanghai, China  
*B.E. in Information Security, School of Cyber Security* Sept. 2015 – June. 2019 (Expected)
  - **GPA:** 3.96/4.3 (91.6/100) **Rank:** 2/98
  - **TOEFL:** R27, L27, S20, W28, Total 102 **GRE:** V145, Q170, AW4.0

## HONORS & AWARDS

---

- **National Scholarships (top 2%)** 2016, 2017
- **Level-A SJTU Outstanding Scholarships (1st in each major)** 2016, 2017
- **First Prize in National College Students Information Security Competition (1st in Shanghai)** 2018
- **Meritorious Winner Prize of Mathematical Contest in Modeling** 2018
- **Second Prize in National College Students Information Security Competition** 2017
- **Second Prize in The Chinese Mathematics Competitions** 2017
- **SJTU Merit Students** 2016, 2017, 2018
- **SJTU Excellent League Cadres** 2016, 2017
- **First Prize in National Mathematical Olympiad in Senior (10th in Shanxi)** 2014

## PUBLICATIONS

---

- **LiDAR-Video Driving Dataset: Learning Driving Policies Effectively.**  
**Jingkang Wang\***, Chenyi Ping\*, Jonathan Li, Cewu Lu, Zhipeng Luo, Han Xue and Cheng Wang.  
*In Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018*
- **Data Mining and Password Generation Based on Large-Scale Real Plain Passwords.**  
**Jingkang Wang**, Yutao Luo, Hao Zhou, Bo Wang and Gongshen Liu.  
*In Proceedings of CCF Conference on Computer Networks and Information Security (CCNIS), 2018*
- **Overview of Plaintext Password Generation Models.**  
Hao Zhou, **Jingkang Wang**, Bo Wang, Yutao Luo and Gongshen Liu.  
*In CCF Transaction on Computer Engineering and Applications, 2018*

## SUBMISSIONS & PRE-PRINT ARTICLES

---

- **Reinforcement Learning with Noisy Rewards**  
**Jingkang Wang**, Yang Liu and Bo Li.  
*In Submission to 7th International Conference on Learning Representations (ICLR), 2019*
- **One Bit Matters: Understanding Adversarial Examples as the Abuse of Data Redundancies.**  
Bo Li, Gerald Friedland, **Jingkang Wang**, Ruoxi Jia, Costas J. Spanos and Dawn Song.  
*In Submission to 7th International Conference on Learning Representations (ICLR), 2019*
- **The Helmholtz Method: Using Perceptual Compression to Reduce Machine Learning Complexity.**  
Gerald Friedland, **Jingkang Wang**, Ruoxi Jia, Bo Li and Dawn Song.  
*In Submission to 31st AAAI Conference on Artificial Intelligence (AAAI), 2019 (arXiv:1807.10569)*
- **Multiple Character Embeddings for Chinese Word Segmentation.**  
**Jingkang Wang**, Jianing Zhou and Gongshen Liu.  
*In Submission to 31st AAAI Conference on Artificial Intelligence (AAAI), 2019 (arXiv:1808.04963)*

## RESEARCH PROJECTS

---

- **Reinforcement Learning with Noisy Rewards** July 2018 - Sept. 2018
  - 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.
- **Blockchain-Based Genetic Privacy-Preserving System** May 2018 - July. 2018
  - 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 proposed protocol theoretically.
- Understanding Adversarial Examples as the Abuse of Data Redundancies** *March 2018 - May. 2018*
  - Propose a model for adversarial examples consistent with related work, physics and information theory.
  - Prove that input redundancy is indeed a necessary condition for being able to generating adversarial examples.
  - Validate that adversarial examples are indeed overflowing perceptrons trained on a certain level of redundancy.
- Multiple Embeddings for Chinese Word Segmentation** *Feb. 2017 - May. 2018*
  - Leverage both semantic and phonetic meanings 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 96.9 and 97.3.
- Reinterpreting Helmholtz Free Energy in Machine Learning** *March 2018 - June. 2018*
  - Propose to reinterpret the Helmholtz free energy formula to explain the relationship between content and noise for sensor-based data.
  - Demonstrate this relationship can be observed as predicted in machine learning experiments on diverse datasets.
  - Verify our noise quantification method can be used to speed up the training of deep learning classifiers significantly while maintaining, or sometimes even improving, overall classification accuracy.
- Dynamic Searchable Encryption System Based on Graph Database** *May 2017 - July. 2017*
  - Improve the parallel dynamic searchable algorithm and propose several auxiliary policies to enhance the security.
  - Implement, visualize and validate the efficient and scalable algorithm based on Neo4j graph database.
- Benchmark for Driving Policy Learning** *Apr. 2017 - Feb. 2018*
  - Propose a dataset which is the first policy learning benchmark composed of driving videos, LiDAR data and corresponding driving behaviors.
  - Conduct complete analysis on how important depth information is, how to leverage depth information and what we can achieve by utilizing current techniques.

## RESEARCH EXPERIENCES

---

- Machine Vision and Intelligence Group (MVG)** Shanghai, China  
*Undergraduate Researcher* *Apr. 2017 - Present*
  - **Advisor:** Professor Cewu Lu
  - **Research Focus:** Computer Vision, Deep Learning, Autonomous Driving
- University of California, Berkeley** Shanghai, China  
*Research Intern (Remotely)* *March 2018 - Oct. 2018*
  - **Advisor:** Professor Bo Li and Dawn Song
  - **Research Focus:** Secure AI, Reinforcement Learning
- Shanghai Key Laboratory of Integrated Technology** Shanghai, China  
*Research Assistant (National Security Competition Targeted)* *May 2017/18 - July 2017/18*
  - **Advisor:** Professor Lei Fan
  - **Research Focus:** Blockchain, Privacy Preserving, Searchable Encryption
- National Engineering Lab for Information Context Analysis Technology** Shanghai, China  
*Research Assistant (Undergraduate Research Program in College)* *Jan. 2017 - Sept. 2017*
  - **Advisor:** Professor Gongshen Liu
  - **Research Focus:** Data mining, Password Generation, Natural Language Processing