Zhuo Cai

zhuo.cai@icloud.com zcaiam@connect.ust.hk
https://zhuocai.github.io
http://www.linkedin.com/in/steinwaycaizhuo/

Education

2021 – Ongoing **Hong Kong University of Science and Technology, Hong Kong**
Master of Philosophy in Computer Science and Engineering
Supervisor: Amir Goharshady
Research Interest: Theoretical Computer Science, Blockchain, Cryptography, Game Theory
GPA: 3.93/4.3

2017 – 2021 **Tsinghua University, Beijing**
Bachelor of Automation
GPA(first 3 years): 3.81/4, GPA Ranking: 17/168

2019 Fall **National University of Singapore, Singapore**
Undergraduate Exchange
GPA: 4.0/4

Research Projects

Sept 2021 – Ongoing **Incentivize Randomness Generation in Proof-of-State Blockchains**
Independent Researcher, supervised by Assistant Professor Amir Goharshady
Department of Computer Science and Engineering, the Hong Kong University of Science and Technology
Decentralized randomness is an essential element of PoS protocols as it is used in the generation of block leaders. Existing protocols typically assume that some honest participants always try to submit good random numbers to facilitate the leader selection. However, there is no incentive for the honest participants to really submit good random numbers. On the other hand, there is no punishment for adversaries who do not draw from the uniformly random distribution. This project carefully designs a mechanism to reward participants who submit from uniformly random distribution and punish those who do otherwise. The mechanism can replace its counterpart in Ouroboros families and other PoS protocols in a straightforward way.

Apr 2022 – Ongoing **Bounding the Gas Cost of Public Function Calls in Ethereum Smart Contracts**
Research Assistant, supervised by Assistant Professor Amir Goharshady
Department of Computer Science and Engineering, the Hong Kong University of Science and Technology
Ethereum supports Turing-complete programmable smart contracts and designs a complicated gas cost model at EVM instruction level. If a transaction calls a public function without enough gas, the transaction will be reverted. However, it is challenging to estimate the upper bound of gas cost. This project models the problem as reachability analysis and applies Farkas' lemma, Putinar's Positivstellensatz and Hilbert's Strong Nullstellensatz to solve linear or polynomial cases. We implements the estimation of gas bounds at Solidity scripts level.

Research Projects (continued)

Aug 2019 – Dec 2019 **Unsupervised Group Anomaly Detection**
Independent Research, supervised by Assistant Professor Bryan Hooi
School of Computing, National University of Singapore
- Developed a novel indirect embedding method in which embeddings are parameters jointly learned to optimize an autoregressive model. The embedding technique can incorporate complex temporal information. With embeddings, autoregressive model can better accommodate multimodal data.
- Showed that Noise Contrastive Estimation is effective on individual samples, but not on segments due to difficulty of injecting reasonable noises to time series; Showed that existing generative models including GANs and Flows are not strong enough when applied to group anomaly detection.

June 2020 – Oct 2020 **Self-Supervised Learning in Medical Visual Question Answering**
Research Assistant, Supervised by Assistant Professor Pengtao Xie
Department of Electrical and Computer Engineering, University of California, San Diego
- Implemented visual question answering algorithms on our Pathology VQA dataset.
- Designed new cross-modality self-supervised learning tasks and implemented them in VQA models; Evaluated how different self-supervised pre-training improve downstream VQA performance in extensive experiments.

Aug 2018 – Jan 2019 **Collaborative SLAM of Multiple Unmanned Aerial Vehicles**
Research Assistant, supervised by Associate Researcher Yipeng Li
Department of Automation, Tsinghua University
- Designed and implemented a practical collaborative SLAM system based on visual SLAM, Lidar SLAM.
- Implemented fast visual SLAM based on video interpolation. Video interpolation generates intermediate frames, which facilitate matching of consecutive frames in visual SLAM.

Research Publications

Conference Proceedings

1 He, X., Cai, Z., Wei, W., Zhang, Y., Mou, L., Xing, E., & Xie, P. (2021). Towards visual question answering on pathology images. In *Proceedings of the 59th annual meeting of the association for computational linguistics and the 11th international joint conference on natural language processing (volume 2: Short papers)* (pp. 708–718). doi:10.18653/v1/2021.acl-short.90

Teaching

2022 Spring & Fall, TA **Hong Kong University of Science and Technology**
COMP 2012: Object-Oriented Programming and Data Structures

Skills

Languages Native in Mandarin Chinese, proficient in English (TOEFL:106, GRE:158+170).
Coding C/C++, Python, MATLAB, JAVA, PyTorch, HTML, LaTeX, …