Hideaki Takahashi

ht2673@columbia.edu | Koukyosyumei | Hideaki Takahashi

Summary

- First-year Ph.D. student at Columbia University, working on Zero Knowledge Proof.
- Passionate about the convergence of **AI**, **systems**, and **security**.
- Proven research excellence with multiple first-authored papers in top-tier conferences (**AAMAS**, **CVPR**).
- Skilled open-source developer of widely adopted tools (**400+ GitHub stars**), including a security risk simulator for machine learning and a symbolic execution engine.
- Extensive research & development experience at leading institutions (Tsinghua University, NAIST, The University of Tokyo) and industry internships (including Apple Inc.).
- Committed to the community as a reviewer (IEEE TNSE, IEEE T-MI) and active contributor to popular open-source projects (PySyft, Nebula).

Education

Columbia University in the City of New York — *New York, United States*

PH.D (COMPUTER SCIENCE) — *Sep. 2024 -*

- Supervised by Prof. Junfeng Yang

The University of Tokyo — *Tokyo, Japan*

BACHELOR OF ARTS AND SCIENCES (INFORMATICS) — *Apr. 2019 - Mar. 2024*

- Supervised by Prof. Alex Fukunaga., GPA: 3.85/4.0

Papers

[1] Hideaki Takahashi* and Alex Fukunaga. On the transit obfuscation problem. In *International Conference on Autonomous Agents and Multi-Agent Systems*, 2024. **Peer-reviewed @ AAMAS'24** (CORE Rank: A*, Acceptance Rate: 20.7%).

[2] Tianyuan Zou, Zixuan Gu, Yu He, Hideaki Takahashi, Yang Liu, Guangnan Ye, and Ya-Qin Zhang. VFLAIR: A research library and benchmark for vertical federated learning. In *The Twelfth International Conference on Learning Representations*, 2024. **Peer-reviewed @ ICLR'24** (CORE Rank: A*, Acceptance Rate: 31.1%).

[3] Hideaki Takahashi*, JingJing Liu, and Yang Liu. Breaching fedMD: Image recovery via paired-logits inversion attack. In *Conference on Computer Vision and Pattern Recognition*, 2023. **Peer-reviewed @ CVPR'23** (CORE Rank: A*, Acceptance Rate: 25.8%).

[4] Sally Junsong Wang, Jianan Yao, Kexin Pei, Hideaki Takahashi, and Junfeng Yang. Detecting buggy contracts via smart testing. *arXiv preprint arXiv:2409.04597*, 2024.

[5] Hideaki Takahashi*. Aijack: Security and privacy risk simulator for machine learning. *arXiv preprint arXiv:2312.17667*, 2023.

[6] Hideaki Takahashi*, JingJing Liu, and Yang Liu. Eliminating label leakage in tree-based vertical federated learning. *arXiv preprint arXiv:2307.10318*, 2023.

[7] Hideaki Takahashi*, Kohei Ichikawa, and Keichi Takahashi. Difficulty of detecting overstated dataset size in federated learning. Technical Report 10, 2021. `http://id.nii.ac.jp/1001/00214220/`.

Software

AIJack (`https://github.com/Koukyosyumei/AIJack`)

OWNER

- Security risk simulator for machine learning (more than 350 stars on GitHub and used in 8 papers.)

MyZKP (`https://github.com/Koukyosyumei/MyZKP`)

Owner

- Building Zero Knowledge Proof from Scratch in Rust

rhoevm (`https://github.com/Koukyosyumei/rhoevm`)

Owner

- Symbolic EVM execution engine written in Rust to find vulnerabilities within Ethereum smart contracts

Gymbo (`https://github.com/Koukyosyumei/Gymbo`)

Owner

- Gradient-based symbolic execution to debug neural networks and probabilistic algorithms.

Research Experience

Fukunaga Lab, The University of Tokyo *Tokyo, Japan*

Undergraduate Student *Apr. 2023 - Mar. 2023*

- Conducted research on the transit obfuscation problem, a new task of privacy-preserving AI planning, under the supervision of Prof. Alex Fukunaga.

Institute for AI Industry Research, Tsinghua University *Beijing, China*

Federated Learning & Privacy Computing Interns *Jan. 2022 - Feb. 2023*

- Conducted research on federated learning and privacy computing under the supervision of Prof. Yang Liu and Prof. Jingjing Liu.

Nara Institute of Science and Technology *Nara, Japan*

Visiting Student *Aug. 2021 - Sep. 2021*

- Conducted research on the free-rider problem of federated learning under the supervision of Prof. Kohei Ichikawa and Prof. Keichi Takahashi.

Industry Experience

Apple Inc. *Yokohama, Japan*

Technical Internship: AIML/Software Engineer *Feb. 2024 - Jul. 2024*

- Worked on AIML/software engineering.

UTokyo Economic Consulting Inc. *Tokyo, Japan*

Research Assistant *Oct. 2020 - Mar. 2024*

- Worked on social implementations of econometrics and machine learning.

RECRUIT *Tokyo, Japan*

Data Science Intern *Aug. 2020 - Sep. 2020*

- Worked on a location-based restaurant recommendation iOS app.

M3, Inc. *Tokyo, Japan*

Data Analysis Intern *Feb. 2020 - Jun. 2020*

- Worked on a data analysis project in the field of medical surveys.

FRONTEO,Inc. *Tokyo, Japan*

Research Intern *Sep. 2019 - Mar. 2020*

- Worked on the detection of anomaly documents with NLP and network analysis.

Awards & Fundings

Fundings

2024 - 2026 **Funai Overseas Scholarship**, Granted 2 years of tuition and stipend.

Competitions

2023 **45th / 616 teams (Silver Medal)**, Kaggle: Google - Fast or Slow? Predict AI Model Runtime
2021 **67th / 875 teams (Bronze Medal)**, Kaggle: Hungry Geese
2021 **52nd / 788 teams (Bronze Medal)**, Kaggle: Santa 2020 - The Candy Cane Contest
2020 **51st / 1138 teams (Silver Medal)**, Kaggle: Google Research Football with Manchester City F.C.
2020 **88th / 1390 teams (Bronze Medal)**, Kaggle: Cornell Birdcall Identification

Service

Reviewer IEEE Transactions on Network Science and Engineering (Impact Factor: 6.7),
IEEE Transactions on Medical Imaging (Impact Factor: 10.0).
OSS Contributor PySyft (platform for secure and private Deep Learning), Nebula (distributed graph database)

Skills

Programming C, C++, Python, Rust, Assembly, LLVM, Haskell, Solidity, Circom, R
Languages English, Japanese
DevOps AWS, Docker, GCP