ANH-TU HOANG

Research Scientist Security Engineering and Privacy-Preserving Computing

CONTACT

hatu87@gmail.com

tuhoag

tuhoag

Anh-Tu Hoang

Tu Hoang

+39 389 142 8587

Jean Henry Dunant, 7, 21100, Varese, Italy

SKILLS

Anonymization 7+ yrs

Multi-Party Computation 1+ yrs

Zero-Knowledge Proof 1+ yrs

Homomorphic Encryption 1+ yrs

Hyperledger Fabric 1+ yrs

Machine Learning 1+ yrs

Deep Learning 1+ yrs

PROGRAMMING

Python 5+ yrs

Go 1+ yrs

TOOLS

Docker 5+ yrs

Git 7+ yrs

Linux 5+ yrs

CERTIFICATES

Cambridge English B2 First

B2
A certificate issued by Cambridge Assessment English.

ABOUT ME

I am a fast learner and an adventurer who is always eager to discover new directions of research and technology and apply them to solve problems in smart and effective ways.

WORK EXPERIENCE

Reviewer **Dec 20 - Now**
University of Insubria, Varese (Italy)

Review articles on various privacy-preserving technologies (differential privacy, k-anonymity, privacy-preserving machine learning/deep learning) from high-quality venues: VLDB, ACM Transactions on Privacy and Security, IEEE Internet Computing, International Journal of Cooperative Information Systems, ACM Transactions on Data Science, Data Science and Engineering.

Research Fellow **Dec 20 - Nov 22**
University of Insubria, Varese (Italy)

Researched on projects:

Personalized Anonymization of KGs: extended k-Attribute Degree (k-ad), the k-anonymity I presented in my Ph.D. thesis, to anonymize KGs according to many anonymity levels specified by data owners.

Sensitive Values Protection in Sequential Anonymization of KGs: extended l-diversity and k-ad to protect users' sensitive values even though attackers exploit all published anonymized KGs.

Decentralized Anonymization of KGs:

- created a non-interactive zero-knowledge-proof scheme relying on Pedersen commitment, a homomorphic commitment scheme, and ECIES, a hybrid encryption scheme.
- developed a Hyperledger Fabric-based blockchain platform that uses smart contracts to ensure anonymized KGs satisfying personalized k-ad, where anonymity levels are specified by data owners.

Decentralized Proximity Advertising System:

- introduced a non-interactive zero-knowledge-proof scheme using Pedersen commitment, ECIES, and Elgamal, a homomorphic encryption scheme.
- proposed a Hyperledger Fabric-based blockchain platform where advertisers, publishers, and customers can create advertising campaigns and evaluate the campaigns' effectiveness transparently.
- implemented smart contracts to generate the proofs through a multi-party computation protocol where each party is a verifier belonging to an advertiser or a publisher.

Supervised two master theses on developing blockchain-based systems using Hyperledger Fabric.

Machine Learning by Stanford University

100%
A certificate issued by Coursera to prove the understanding of machine learning and its applications such as supervised/unsupervised learning, SVM, and recommendation systems

REFERENCES

Prof.Elena Ferrari

elena.ferrari@uninsubria.it
University of Insubria

Prof.Barbara Carminati

barbara.carminati@uninsubria.it
University of Insubria

Presented in events of the CONCORDIA project, a Cyber-security project funded by the European Union's Horizon 2020 Research and Innovation program.

Ph.D. Student — **Oct 17 - Dec 20**
University of Insubria, Varese (Italy)

Researched on projects:

Directed Graph Anonymization: designed a new k-anonymity-based anonymization algorithm for directed graphs that is more efficient than the state-of-the-art algorithms for directed graphs.

KG Anonymization:

- introduced the k-Attribute Degree (k-ad), the first k-anonymity principle for KGs.
- extended node2vec (PyTorch) to generate users' vectors such that the information loss of anonymizing two users' data is similar to the distance between their vectors.
- developed a cluster-based anonymization algorithm that allows data providers to use all state-of-the-art clustering algorithms (e.g., k-means, HDBSCAN) to generate k-ad anonymized KGs. The algorithm is compatible with Scikit-Learn.

Sequential Anonymization of KGs:

- proposed the Time-Varying k^w-Attribute Degree (k^w-tad), an extension of k-ad, to protect users' identities when attackers exploit w continuous anonymized KGs.
- designed an efficient anonymization algorithm generating anonymized KGs such that w continuous KGs satisfy k^w-tad.

Marker centroid detection in X-ray radiographs: implemented an adapter library that is used for training a ResNet-based model to detect the centroids of metal markers in X-ray projections using MXNet and Python.

Research Intern — **Mar 13 - Sept 13**
National Institute of Informatics, Tokyo (Japan)

Researched on projects:

Watermarking on Anonymized Relational Datasets:

- proposed a watermarking technique that extracts generalization rules from k-anonymous dataset and associates the rules to data recipients.
- associated the rules extracted from illegal anonymous dataset to detect the traitor who illegally distributes the anonymized dataset.

Text Anonymization:

- detected temporal phrases containing users' location and time in tweets.
- anonymized the detected phrases.

Teaching Assistant & Lecturer — **Sept 09 - Oct 17**
University of Science-Vietnam National University, Ho Chi Minh City (Vietnam)

Researched anonymization techniques: designed an efficient anonymization algorithm for k-anonymity.

Gave lectures on: fundamental of databases, Oracle security technologies (DAC, RBAC, Virtual Private Database, and Oracle Label Security), NoSQL (Redis, MongoDB, Cassandra, sharding/replication), and web programming (Docker, Ruby on Rails, Node.js).

EDUCATION

Ph. D. - Computer Science **2017 - 2020**
University of Insubria - Varese (Italy)

Thesis work on anonymization techniques for knowledge graphs.

Master - Information Systems **2009 - 2012**
University Science, Vietnam National University - Ho Chi Minh City (Vietnam)

Thesis work on anonymization techniques for relational dataset.

Bachelor - Information Technology **2005 - 2009**
University Science, Vietnam National University - Ho Chi Minh City (Vietnam)

Thesis work on a platform that generates games on Windows Mobile.

PUBLICATIONS

1. **Anh-Tu Hoang**, Barbara Carminati, Elena Ferrari. Time-Aware Anonymization of Knowledge Graphs. The ACM Transactions on Privacy and Security (Under Review).
2. **Anh-Tu Hoang**, Barbara Carminati, Elena Ferrari. Personalized Anonymization of Knowledge Graphs. The IEEE Transactions on Dependable and Secure Computing (Under Preparation).
3. **Anh-Tu Hoang**, Barbara Carminati, Elena Ferrari. Proximity-Based Marketing Using Blockchain. The IEEE International Conference on Data Engineering (Under Preparation).
4. **Anh-Tu Hoang**, Barbara Carminati, Elena Ferrari. 2021. Privacy-Preserving Sequential Publishing of Knowledge Graphs. IEEE International Conference on Data Engineering. 2021–2026.
5. **Anh-Tu Hoang**, Barbara Carminati, Elena Ferrari. 2020. Cluster-based anonymization of knowledge graphs. Applied Cryptography and Network Security. Springer International Publishing. 104–123.
6. V. Nguyen, J. De Beenhouwer, S. Bazrafkan, **A-T Hoang**, S. Van Wassenbergh, and J. Sijbers. 2020. BeadNet: A Network for Automated Spherical Marker Detection in Radiographs for Geometry Calibration. CTMeeting-2020, Regensburg, Germany.
7. **Anh-Tu Hoang**, Barbara Carminati, Elena Ferrari. 2019. Cluster-Based Anonymization of Directed Graphs. IEEE International Conference on Collaboration and Internet Computing. IEEE. 91–100.
8. **Anh-Tu Hoang**, Hoang-Quoc Nguyen-Son, Minh-Triet Tran, and Isao Echizen. 2013. Detecting Traitors in Re-publishing Updated Datasets. Digital-Forensics and Watermarking. 205–220.
9. Hoang-Quoc Nguyen-Son, **Anh-Tu Hoang**, Minh-Triet Tran, and Isao Echizen. 2013. Anonymizing Temporal Phrases in Natural Language Text to be Posted on Social Networking Services. Digital-Forensics and Watermarking. 437–451.
10. **Anh-Tu Hoang**, Minh-Triet Tran, Anh-Duc Duong, and Isao Echizen. 2012. An Indexed Bottom-up Approach for Publishing Anonymized Data. International Conference on Computational Intelligence and Security. 641-645.