4720 Forbes Ave CIC 2225A,
Carnegie Mellon University,
Pittsburgh, PA 15213.

(412) 327-3973 ☎
gko@andrew.cmu.edu ✉
https://www.ece.cmu.edu/~gko 🌐

Gihyuk Ko

research interests

Security and Privacy, Formal Methods, Probabilistic Programming, Machine Learning

education

Carnegie Mellon University, Pittsburgh, PA, USA

Ph.D. Candidate in Electrical and Computer Engineering *August 2012 - present*
Advisors: Anupam Datta, Matt Fredrikson

M.S. in Electrical and Computer Engineering *August 2015*

Seoul National University, Seoul, South Korea

B.S. in Electrical and Computer Engineering *August 2012*
Thesis: Wireless Sensor Networks Performance Evaluation using H-mote
Advisor: Saewoong Bahk
Honored as *summa cum laude*, Final GPA: 3.99/4.30

publications

A. Datta, M. Fredrikson, G. Ko, P. Mardziel, S. Sen. *Use Privacy in Data-Driven Systems: Theory and Experiments with Machine Learnt Programs*, In Proceedings of the ACM Conference in Computer and Communications Security (CCS), *October 2017*

A. Datta, M. Fredrikson, G. Ko, P. Mardziel, S. Sen. *Proxy Non-Discrimination in Data-Driven Systems*, Preprint, *July 2017*

A. Datta, M. Fredrikson, G. Ko, P. Mardziel, S. Sen. *Use Privacy in Data-Driven Systems: Theory and Experiments with Machine Learnt Programs*, Preprint, *May 2017*

posters & talks

Posters

Use Privacy in Data-Driven Systems: Theory and Experiments with Machine Learnt Programs
In Proceedings of the IEEE Symposium on Security and Privacy (S&P), *May 2017*
CyLab Partners Conference, *September 2017*
Samsung Academic Camp, *July 2017*
Privacy Day, *January 2017*

Talks

Accountability in Machine Learning Systems via Program Analysis
Seminar talk at KAIST, Korea University, SKKU, *Jun 2017*

Towards Accountable Machine Learning System
Seminar talk at KDisTech, Carnegie Mellon University, *December 2016*

Use Privacy in Machine Learning Systems via Proxy Use
Seminar talk at SODA Group, Carnegie Mellon University, *November 2016*

Deception Game on Decoy Systems
Qualifying exam talk, Carnegie Mellon University, *April 2015*

research experience

Use Restriction as Probabilistic Program Property
Carnegie Mellon University, *Nov 2016 - present*

Use privacy and proxy non-discrimination detects and restricts a certain 'use' of sensitive information in complex machine learnt programs. Such restriction can be viewed as an enforcement of some probabilistic program property. In this research we formalize a notion of use restriction as probabilistic program property, and develop an efficient algorithm for enforcing such properties.

Proxy Non-Discrimination in Machine Learnt Programs
Carnegie Mellon University, *Nov 2016 - present*

Machine learnt programs can be problematic when used in making social decisions, because unfair biases in training data can be learned without any restriction. We formalize the notion of 'proxy discrimination' for machine learnt programs, and develop an efficient algorithm to detect and repair them.

Use Privacy in Machine Learnt Programs
Carnegie Mellon University, *May 2016 - May 2017*

Traditional notion of privacy such as differential privacy limits 'leakage' of amount of information. However, a more critical condition for the violation of privacy is to check whether the leaked information is actually used in certain context. In this research we present a formal notion of 'use privacy' via 'proxy use', which keeps track whether any information on individual was used in a decision making procedure.

Reproducible Research: Balacing Utility and Privacy of the Learning System
Carnegie Mellon Universiy, *December 2015 - May 2016*

Recent studies on privacy-preserving data handling has enabled the researchers to process and publish database without having to worry about participants' privacy breach. However, it is still questionable whether the published work is reproducible as the original dataset might have been compromised with certain noises. My current research aims to formalize relation between utility and privacy, especially on the learning systems to seek a systematic methodology to publish a dataset in a reproducible way.

Privacy and Transparency Report on Healthcare Domain
Carnegie Mellon University, *December 2015 - Feb 2016*

Providing a well-formed transparency report to the user of any learning-recommendation system is often critical as the user might want to know the reason for the result. On the other side, providing transparency report might be a good auxiliary information to the attackers who seek to breach person's privacy. In this research we look for the formal relationship between privacy and transparency report, in order to provide a well-formed transparency report while minimizing privacy threat.

Deception Games on Decoy Systems

Carnegie Mellon University, *August 2014 - July 2015*

Decoy systems are a useful tool to mitigate attackers' intrusions as they lure attackers into accessing decoys, while there are little literature on the strategic usage of such systems. In this research, we proposed a game of deception, which involves a network attacker and a defender who uses decoy systems. The equilibrium result for certain attackers show that against an attacker with strategy, a defender choosing optimal strategy can always outperform an attacker.

Automatic Detection of Unfairness on Games

Carnegie Mellon University, *January 2014 - May 2014*

Internet users often encounter a game situation, where they are not sure if the game is fair or not. In this work, I used computational game theory to develop an algorithm which enables a user to figure out whether the game is fair or not, given the game definition.

Wireless Sensor Networks Performance Evaluation Using H-mote

Seoul National University, *September 2011 - May 2012*

In this research we evaluated performance of IEEE 802.15.14/ZigBee protocol by implementing and testing VoIP packets on actual physical sensor device named H-mote. Each sensor node was programmed using nesC, which consisted a low-power OS named tinyOS. Experiment results provided that VoIP was not fit for the sensor network, as both R-factor and MOS(Mean Opinion Score) significantly decayed to negative value when the network had more than two hops.

This research was done under professor Saewoong Bahk's guidance, as my undergraduate thesis work.

Cooperative Driving of Unmanned Vehicles under Multi-flow Traffics

Seoul National University, *March 2010 - February 2011*

This work aims to model cooperative driving of unmanned vehicles under multi-flow traffic situation, motivated from schooling of fish. We proposed a new ellipse-shaped 'safety boundary' around each vehicle, applying virtual repulsive and attractive force field according to each other's distance. Simulation using Java and Torcs resulted in enhancement of both safety and throughput of the traffic.

This research was done as a part of Undergraduate Research Program(URP) funded by Korea Foundation for Advanced Science and Creativity(KOFAC), advised from professor Seung-woo Seo in Seoul National University.

n-dimensional Volume and Pythagorean Theorem on n-polytope

Daejeon Science High School, *March 2007 - July 2007*

This work generalizes the concept of volume in 3-dimensional space to n-dimensional space, suggesting and proving n-dimensional Pythagorean Theorem on n-polytope. I proved given n vectors of n-polytope, n-dimensional volume of a polytope can be calculated as a scaled determinant of a square matrix which has n vectors as its rows. Using induction, I was able to prove generalized n-dimensional Pythagorean Theorem, which involves an arbitrary $(n-1)$-dimensional volume of a $(n-1)$-polytope on n-dimensional space.

Building a Probabilistic Knowledge Diagnosis System
Daejeon Science High School, *March 2006 - February 2007*

A carefully designed knowledge diagnosis system benefits educating students in that they can be used on examining how well they are educated. We built a dependence knowledge map for high school Mathematics curriculum, modeled it as a Bayesian probabilistic network to build a diagnosis system, and tested the system based on actual survey.

professional services

External Reviewer - IEEE S&P'13,'14, ACM CCS'16,'17, NDSS'17, FATML'16

grants, honors, & awards

Samsung Scholarship, Samsung Scholarship *August 2012 - present*

Dean's Fellowship, Carnegie Mellon University *August 2012 - July 2013*

Undergraduate Research Program(URP) Funding, Korea Foundation for Advanced Science and Creativity(KOFAC) *March 2010 - February 2011*

Undergraduate Student Scholarship, Korea Foundation for Advanced Studies(KFAS) *March 2008 - February 2012*

National Science and Technology Scholarship, Korea Student Aid Foundation(KOSAF) *March 2008 - February 2012*

Outstanding Academic Achievement Fellowship, Seoul National University *July 2008*

Outstanding Student Fellowship, Gwangju Institute of Science and Technology(GIST) *May 2007*

Sungdu Scholarship, Daejeon Science High School *May 2006*

technical skills & miscs

Programming Language: Python, Java, C, C++, Scala, F#, OCaml
Web Development: HTML, JavaScript, CSS, PHP
Mobile Development: Android/iOS dev
Productivity Applications: LaTeX, Git, Subversion
Language: Korean(born), English(second), Japanese, French

teaching assistant

Carnegie Mellon University

Fall 2013	Introduction to Comupter Security	Virgil Gligor
Spring 2014	Applied Cryptography	Virgil Gligor
Spring 2017	Applied Cryptography	Anupam Datta

relevant courseworks

Carnegie Mellon University

Fall 2012	Introduction to Computer Security	Virgil Gligor
Fall 2012	Network Security	Adrian Perrig
Spring 2013	Secure Software Systems	Lujo Bauer, Anupam Datta
Spring 2013	Applied Cryptography	Virgil Gligor
Spring 2013	Machine Learning	Alex Smola, Barnabas Poczos
Fall 2013	Foundations of Privacy	Anupam Datta
Spring 2014	Information Theory	Rohit Negi
Spring 2014	Graduate Artificial Intelligence	Zico Kolter, Zachary Rubenstein
Spring 2016	Formal Foundations of Software Security	Matt Fredrikson, Limin Jia

references

Anupam Datta

Associate Professor
CSD and ECE
Carnegie Mellon University

Phone: +1-412-268-4254
Email: danupam@cmu.edu

Matt Fredrikson

Assistant Professor
CSD and ISR
Carnegie Mellon University

Phone: +1-412-268-3992
Email: mfredrik@cs.cmu.edu

Saewoong Bahk

Professor
Department of Electrical and Computer Engineering
Seoul National University

Phone: +82-2-880-8414
Email: sbahk@snu.ac.kr

Seung-woo Seo

Professor
Department of Electrical and Computer Engineering
Seoul National University

Phone: +82-2-880-8418
Email: sseo@snu.ac.kr