

## Background

- 2007-2014 In *Communications and Signal Processing*  
2015-current In *Security and Privacy in Machine Learning*

## Education

- 8/2010-5/2020 **Ph.D. in Electrical Engineering**, *University of Southern California*, Los Angeles, CA, USA.  
PhD Thesis: *Security and Privacy in Information Processing*.  
Advisor: *Prof. Leana Golubchik*.
- 9/2007-6/2009 **M.S. in Communications Engineering**, *National Taiwan University*, Taipei, Taiwan.  
MS Thesis: *Performance Analysis of Spatial Diversity for MIMO-OFDM Systems with Power Allocation on Sub-carriers*.
- 9/2000-6/2004 **B.S. in Atomic Science**, *National Tsing Hua University*, Hsinchu, Taiwan.

## Areas of Interest

- **Data Privacy:** *Differential Privacy; Data Anonymization; Privacy-Utility Trade-offs*
- **Security and Privacy in Machine Learning:** *Poisoning Backdoor Attacks; Inference Attacks*
- **Machine Learning:** *Federated Learning; Meta-Learning; Attention Mechanisms; Autoencoder*
- **Communications and Signal Processing:** *Speech/Pattern Recognition; Cognitive Networks*

## Work Experience

- 5/2019-current **Research Assistant/Associate**, *University of Southern California*, Los Angeles, CA, USA.  
Project: **Deconstructing Distributed Deep Learning**, funded by *National Science Foundation*, USA.  
Investigated poisoning backdoor attacks and the associated defense methods in federated meta-learning.
- 8/2011-6/2013 **Research Assistant**, *University of Southern California*, Los Angeles, CA, USA.  
Project: **Positive Train Control**, funded by *Federal Transit Administration*, USA.  
Measured and/or simulated quality of Metrolink train control signals in Los Angeles metropolitan area.
- 7/2009-6/2010 **Research Associate (Full-Time)**, *Telecommunications Research Center, NTU*, Taipei, Taiwan.  
Project: **Cross-layer Design of OFDMA Cooperative and Cognitive Communications**, funded by *National Science Council*, Taiwan.  
Designed reliable communication schemes for multi-path multi-hop cognitive radio networks.

## Publications

- [1] **C-L. Chen**, L. Golubchik, and M. Paolieri, "Backdoor Attacks on Federated Meta Learning", to appear in *NeurIPS Workshop on Scalability, Privacy, and Security in Federated Learning (NeurIPS-SpicyFL)*, 2020. [arXiv:2006.07026](https://arxiv.org/abs/2006.07026)
- [2] **C-L. Chen**, L. Golubchik, and R. Pal, "Achieving Transparency Report Privacy in Linear Time," submitted October 2020.
- [3] **C-L. Chen**, L. Golubchik, and R. Pal, "Tractable Privacy Preservation in Transparency Reports," submitted November 2020.
- [4] **C-L. Chen**, R. Pal, and L. Golubchik, "Oblivious Mechanisms in Differential Privacy: Experiments, Conjectures, and Open Questions," *IEEE Security and Privacy Workshops*, San Jose, 2016.
- [5] I-W. Lai, **C-L. Chen**, C-H. Lee, K-C. Chen and E. Biglieri, "End-to-End Virtual MIMO Transmission in Ad Hoc Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, 2013.

## Awards, Professional Activities, and Services

- Awards ◦ **Best Paper Award Nominee**  
*NeurIPS Workshop on Scalability, Privacy, and Security in Federated Learning, 2020*

Paper Review	<ul style="list-style-type: none"> <li>◦ IEEE INFOCOM 2014</li> <li>◦ IEEE Trans. on Wireless Communications</li> <li>◦ ACM Trans. on Management Information System</li> </ul>	<ul style="list-style-type: none"> <li>◦ ACM SIGMETRICS 2016-2019</li> </ul>
Services	<ul style="list-style-type: none"> <li>◦ Camp Counselor, NTHU Interdisciplinary Science Summer Camp (2001, 2002)</li> <li>◦ Military Service, ROC (Taiwan) Army, Corporal (2005-2006)</li> <li>◦ Volunteer, USC Viterbi Summer Program: IIT Kharagpur Summer Research Internships (2012)</li> <li>◦ Research Volunteer, Department of Computer Science, University of Southern California (2020)</li> </ul>	
Teaching Assistant	<ul style="list-style-type: none"> <li>◦ Applied Cryptography</li> <li>◦ Introduction to Computer Networks</li> <li>◦ Operating Systems</li> </ul>	<ul style="list-style-type: none"> <li>◦ Introduction to Internetworking</li> <li>◦ Internet and Cloud Computing</li> <li>◦ Seminar in Computer Science Research</li> </ul>

## Related Graduate Coursework

Graded	<ul style="list-style-type: none"> <li>◦ Privacy in the World of Big Data</li> <li>◦ Mathematical Pattern Recognition</li> <li>◦ Analysis of Algorithms</li> <li>◦ Parallel and Distributed Computation</li> <li>◦ Error Correcting Codes</li> </ul>	<ul style="list-style-type: none"> <li>◦ Machine Learning</li> <li>◦ Uncertainty Modeling and Stochastic Optimization</li> <li>◦ Stochastic Network Optimization</li> <li>◦ Digital Signal Processing</li> <li>◦ Advanced Wireless Communications</li> </ul>
Audited	<ul style="list-style-type: none"> <li>◦ Machine Learning from Signals</li> </ul>	<ul style="list-style-type: none"> <li>◦ Convex and Combinatorial Optimization</li> </ul>

## Selected Research Experience

- 2019-2020
  - Investigated backdoor attacks and the associated defense methods in federated meta-learning.
    - Showed the effects of a one-shot backdoor attack can persist tens to hundreds of rounds in federated meta-learning; the fast-adaptation ability of meta-learning does not effectively remove backdoors during federated meta-training as well as during fine-tuning.
    - Proposed an *effective local* defense mechanism using matching network fine-tuning with customized attention mechanism to eliminate backdoors *without a centralized approach inspecting user updates*; backdoor accuracy can drop to *as low as 0% in only a few iterations*.
- 2016-2018
  - Investigated privacy breach brought on by releasing algorithmic transparency reports (ATRs) providing transparency schemes and measured fairness for opaque machine-learning models.
    - Explicitly demonstrated inference attacks on data subjects' private information via various transparency schemes and/or measured fairness in ATRs, with reasonable side-information.
    - Proposed a *linear-time optimal privacy preserving* scheme which provides optimal trade-offs for an ATR between the amount of disclosed information (utility) and data subjects' privacy.
- 2015-2016
  - Studied the unexplored spaces for designing utility-optimal differentially-private mechanisms.
    - Conducted an exploratory study to understand questions and challenges related to the design and analysis of optimal oblivious noise-generating mechanisms in differential privacy (DP).
    - Proposed a heuristic DP mechanism enhancing utility on the presence of side-information.
- 2009-2010
  - Designed reliable communication schemes for multi-path multi-hop cognitive radio networks.
    - Proposed a *low-complexity (as low as <1% of MAP)* joint sphere decoder to *efficiently* decode virtual MIMO space-time codes with unknown rank (due to opportunistic communications).
    - Provided error-resilient end-to-end transmission *without requiring end-to-end information*.

## Skills and Interests

Programming Languages	<b>Python:</b> experience with building federated meta-learning in which poisoning attack is performed. <b>MATLAB:</b> experience with simulating an end-to-end wireless MIMO-OFDM environment. <b>C/C++:</b> experience with helping students debug programming assignments in TA jobs.
Tools	Tensorflow, Keras, L <sup>A</sup> T <sub>E</sub> X
Interests	<i>Chinese chess:</i> ranked number 6 in the contest of Chinese chess in Taipei City (1994). <i>Piano:</i> Yamaha musical grading examination for piano performance Grade 7 passed.