**TOPIC IN INFORMATION SECURITY**

Lectures will discuss the motivation and background for the following topics:

* **Overview**
* [ *Topic* 1] **Verifying Deep Learning Models**
  + [Reluplex: An Efficient SMT Solver for Verifying Deep Neural Networks](https://arxiv.org/pdf/1702.01135.pdf)
  + [An Abstract Domain for Certifying Neural Networks](https://files.sri.inf.ethz.ch/website/papers/DeepPoly.pdf)
  + [Quantitative Verification of Neural Networks and Its Security Applications](https://www.comp.nus.edu.sg/~prateeks/papers/NPAQ.pdf)
* [ Topic *2* ] **Differentially Private ML Training**
  + [Deep Learning with Differential Privacy](https://arxiv.org/pdf/1607.00133.pdf)
  + [On the Intrinsic Privacy of Stochastic Gradient Descent](https://arxiv.org/abs/1912.02919)
* [ Topic *3* ] **Provable Robustness of ML Models**
  + [Certified Robustness to Adversarial Examples with Differential Privacy](https://arxiv.org/pdf/1802.03471.pdf)
  + [Certified Adversarial Robustness via Randomized Smoothing](https://arxiv.org/pdf/1902.02918.pdf) (Video: [Provable Robustness Beyond Bound Propagation](https://www.youtube.com/watch?v=UHs2mGBH0Fg))
* [ Topic *4*]  **Scalable Consensus for Permissionless Blockchains**
  + [On the Security of Blockchain Consensus Protocols](http://www.comp.nus.edu.sg/~prateeks/papers/Invited-consensus.pdf)
  + [OHIE: Blockchain Scaling Made Simple](http://www.comp.nus.edu.sg/~prateeks/papers/Ohie.pdf)
  + [Algorand: Scaling Byzantine Agreements for Cryptocurrencies](https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf)
* [ Topic *5* ] **Next-generation Trusted Computing**
  + [MI6: Secure Enclaves in a Speculative Out-of-Order Processor](https://arxiv.org/abs/1812.09822)
  + [Keystone: An Open Framework for Architecting TEEs](https://arxiv.org/abs/1907.10119)
  + [Spectre Attacks: Exploiting Speculative Execution](https://cseweb.ucsd.edu/~dstefan/cse291-winter18/papers/spectre.pdf)
  + [Meltdown: Reading Kernel Memory from User Space](https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-lipp.pdf)

[Topic 6] Watermarks in Generative AI

* + A novel model watermarking for protecting generative adversarial network
  + AdvEWM- Generating image adversarial examples by embedding digital watermarks
  + Deep Model Intellectual Property Protection via Deep Watermarking