Information-theoretic Methods in Security

Part I: Communication Aspect

Nicola Laurenti

- Ms and PhD in Electrical Engineering from University of Padova, Italy.
- Since 2001, he has been an Assistant Professor at Department of Information Engineering, University of Padova.
- In 2008-09 he was a Visiting Scholar at Coordinated Science Laboratory, University of Illinois at Urbana-Champaign.

Topics

- *Basic notions:* Shannon's cipher system. Perfect secrecy. The wiretap channel model. Achievable secrecy rates. Secrecy capacity for binary and Gaussian channels.
- *Security from uncertainty:*
  Secret key agreement from common randomness on noisy channels.
- *The jamming game:*
  Optimal strategies for transmitters, receivers and jammers in Gaussian and fading channels.
- *Alea iacta est:*
  Secure and true random number generation and randomness extractors.
- *Information theoretic democracy:*
  Privacy, reliability and variability in electronic voting systems.

Course Info

- Dec. 29th 13:20-16:20, Engineering Building 4 Room 203
- Dec. 30th 09:00-12:00, Engineering Building 4 Room 103
- Dec. 31st 13:20-16:20, Engineering Building 4 Room 203

Information-theoretic Methods in Security

Part II: Network Aspects

Nicola Laurenti

- Ms and PhD in Electrical Engineering from University of Padova, Italy.
- Since 2001, he has been an Assistant Professor at Department of Information Engineering, University of Padova.
- In 2008-09 he was a Visiting Scholar at Coordinated Science Laboratory, University of Illinois at Urbana-Champaign.

Topics

- *Basic notions:* Shannon's cipher system. Perfect secrecy. The wiretap channel model. Achievable secrecy rates. Secrecy capacity for binary and Gaussian channels.
- *Secrets in a crowd:* Information theoretic secrecy in a random network with random eavesdroppers. Secrecy graphs and large networks secrecy rates.
- *Leaky buckets and pipes:* Information leaking and covert channels. Timing channels.
- *The Big Brother:* An information theoretic formulation of database security: the privacy vs utility trade-off.

Course Info

- Jan. 5th 13:20-16:20, Engineering Building 4 Room 203
- Jan. 6th 09:00-12:00, Engineering Building 4 Room 103
- Jan. 7th 13:20-16:20, Engineering Building 4 Room 203