Hemanta K. Maji

Cryptography and Security

Cryptography & Security

Cryptography & Security

- Science of providing Controlled Access to Information

Cryptography & Security

- Science of providing Controlled Access to Information

- "Who learns what," and

Cryptography & Security

- Science of providing Controlled Access to Information
  - "Who learns what," and
  - "Who influences what"

Cryptography & Security

- Science of providing Controlled Access to Information
  - "Who learns what," and
  - "Who influences what"
- Goal: Discover Laws of Nature through the Lens of Security & Privacy using Mathematical Tools

Laws of Nature: Examples

Laws of Nature: Examples

- Channel Capacity: Law of Information Throughput

Laws of Nature: Examples

- Channel Capacity: Law of Information Throughput

- Circuit Complexity: Cost of Computation

My Perspective & Goal

My Perspective & Goal

- Cryptography is founded upon Atomic Components

My Perspective & Goal

- Cryptography is founded upon Atomic Components
- Law of "Privacy Throughput"
  - Transmuting various forms of Atomic Components of Privacy at Optimal Rate

My Perspective & Goal

- Cryptography is founded upon Atomic Components
- Law of "Privacy Throughput"
  - Transmuting various forms of Atomic Components of Privacy at Optimal Rate
- Cost of "Privacy-preserving Computation"
  - Securely Computing using Minimal Atomic Components

Applications: Secure Computation

Applications: Secure Computation

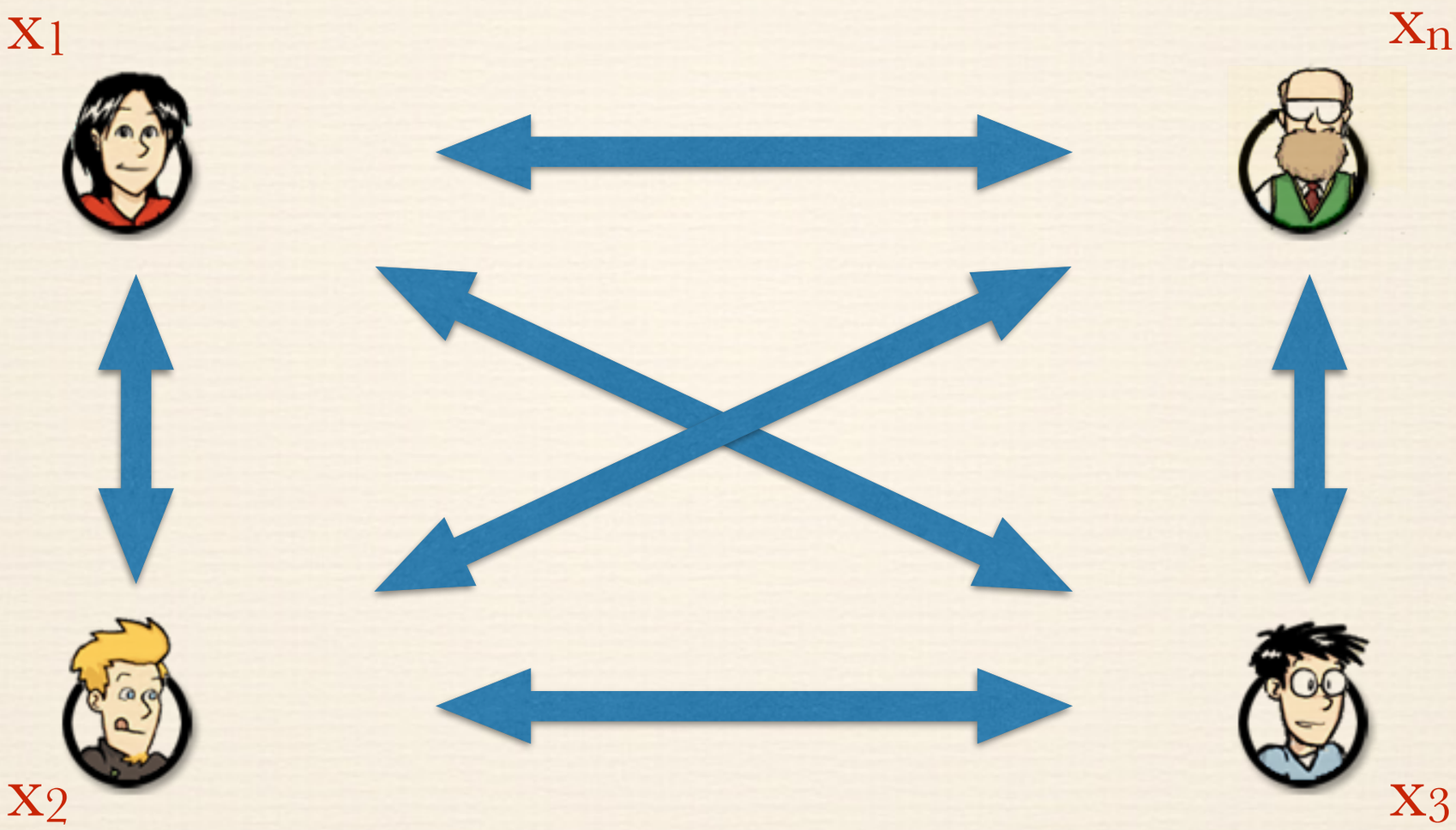
x_1

x_n

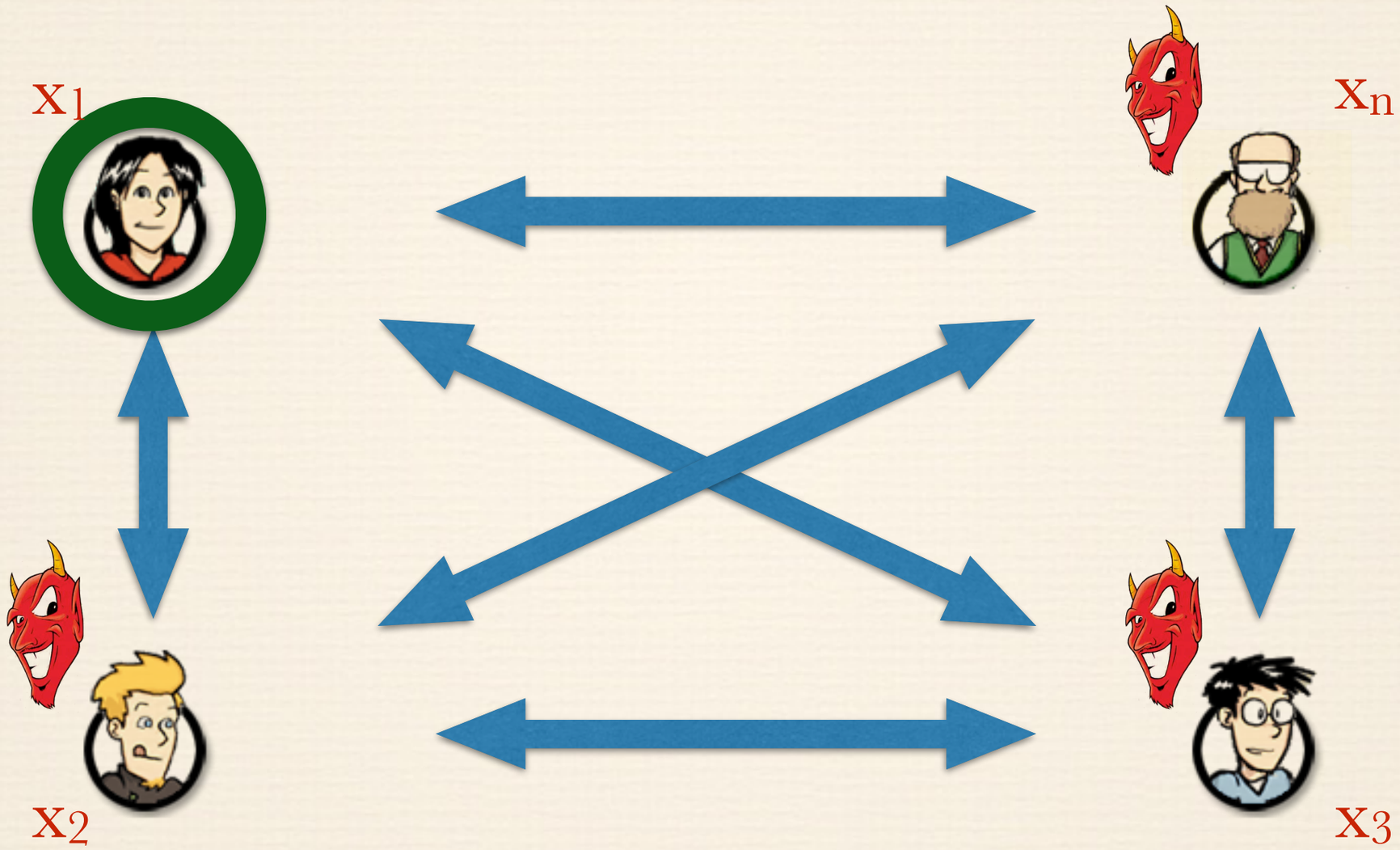
x_2

x_3

Applications: Secure Computation



Applications: Secure Computation



Applications: Secure Computation

Applications: Secure Computation

- With: Maximum Resource Efficiency

Applications: Secure Computation

- With: Maximum Resource Efficiency
- Using: Noisy Channels, Secure Hardware, Hardware Tokens, Conservative Computational Assumptions

Applications: Secure Computation

- With: Maximum Resource Efficiency
- Using: Noisy Channels, Secure Hardware, Hardware Tokens, Conservative Computational Assumptions
- Despite: Sophisticated Adversarial Attacks, like Leakage and Tampering

Summary

- Understand: Law of "Privacy Cost"
- Closely Correlated with the Practice of Cryptography
  - For example: Secure Computation

Thanks