# Purdue CS555 Cryptography Lecture 1: Introduction

August 26, 2025

## Introduction

The course focuses on Cryptography's **Primitives**, **Toolkits**, **Applications**, and **Methodology**.

### Misconceptions

Cryptography is often narrowly perceived, but its true scope is broad:

- Crypto $\neq$ Cryptocurrencies.
- Crypto $\neq$ Encryption/Secure Communication.

It includes applications like proof of work (integrity), anonymous communication (onion network), and identifiable LLM generated data (watermark).

### 0.1 Crypto Research - High Level Picture

Cryptographic research sits at the intersection of two key areas:

1. **Theoretical Computer Science & Math**: Deals with assumptions and security proof via reduction
2. **System & Hardware**: Focuses on performance so on accelerating cryptography related computation.

## 1 Information Leakage and Privacy Foundations

### 1.1 Information Leakage

- **Definition**: Leakage is any information **statistically correlated** to the secret $X$.
- Any process involving a secret $X$ can lead to leakage, modeled by a **leakage function** $F(X)$.
- **Examples**:
  - Sensitive training data ($X$) $\rightarrow$ Model response ($F(X)$).
  - Password ($X$) $\rightarrow$ Power consumption or timing (side-channel $F(X)$).

### 1.2 Privacy Risk Quantification

The main concern is an informed adversary (with full knowledge of $F$) observing $F(X)$. The goal is to prevent the adversary from reconstructing features of $X$.

- **Quantification**: Measures the risk via the **posterior probability** that the adversary can achieve a satisfactory reconstruction of $X$.
- The risk depends on the secret's **entropy** (objective randomness) and the adversary's **belief** (subjective prior).
- **Worst-Case Analysis**: Privacy guarantees often remove assumptions on the secret distribution by performing worst-case analysis, meaning guarantees hold for an arbitrary distribution of $X$.

# 2 Perfect Secrecy and Indistinguishability

## 2.1 Definition of Perfect Secrecy

A leakage function $F(\cdot)$ satisfies perfect secrecy if, for a computationally-unbounded and rational adversary with an arbitrary prior belief on secret input $X$, their posterior belief after observing the leakage $F(X)$ is **identical to their prior belief**. This initializes privacy risk measurement from the **worst-case posterior advantage** angle (the difference between prior and posterior).

## 2.2 Equivalence to Indistinguishability

Perfect secrecy is equivalent to **input-independent indistinguishability**:

$$\forall Y, Y', c: \quad \Pr[F(Y) = c] = \Pr[F(Y') = c]$$

If the leakage $c$ is equally likely for any two input candidates $Y$ and $Y'$, the output is indistinguishable, and therefore reveals nothing about the specific input. This implies no additional advantage for any adversarial inference.

# 3 Two Types of Leakage

The course differentiates two main contexts for leakage:

## 3.1 Intermediate Secrecy (*Cryptography*)

- **Tradeoff**: A "free lunch" in terms of accuracy/utility is possible under additional assumptions, aiming for **perfect indistinguishability**.
- **Goal**: Achieving security with weaker assumptions and better computational efficiency.

## 3.2 Output Secrecy (*Information Theory and Statistics*)

- **Tradeoff**: There is **no free lunch** in terms of accuracy/utility. There is an inherent tradeoff between utility and privacy.
- **Goal**: Finding the **optimal utility-privacy tradeoff** (e.g., minimal randomization for required guarantees). This model generally accepts a **non-zero posterior advantage**.