CSCI 1510

- Program Obfuscation (continued)
- Final Review

ANNOUNCEMENT: Course Feedback & Critical Review
Program Obfuscation

Goal: Make the program "unintelligible" without affecting its functionality.
Symmetric-Key to Public-Key

Obfuscate

Encrypt

Decrypt

M \rightarrow sk \rightarrow C

C \rightarrow sk \rightarrow M
**Formal Definition: Virtual Black Box (VBB)**

\[ \text{Obfuscator } O: \quad C \xrightarrow{O} O(C) \]

- **Functionality:** \( O(C) \) computes the same function as \( C \).
- **Polynomial Slowdown:** \( |O(C)| \leq \text{poly}(n) \cdot |C| \)
- **Security (Virtual Black Box):**
  \[ \forall \text{PPT} \, A, \exists \text{PPT} \, S, \text{s.t. } \forall C, \quad A(O(C)) \xrightarrow{\text{c.e.}} S^{C(\cdot)}(1^{|C|}) \]

\[ O(C) \simeq \begin{cases} \text{Simulator} \end{cases} \]

**Thm:** VBB obfuscator for all poly-sized circuits is impossible to achieve.

\[ C(x) := \begin{cases} b & \text{if } x = a \\ m & \text{if } x(a) = b \\ 0 & \text{otherwise} \end{cases} \]

Run \( O(C) \left( O(C) \right) \to m \)
Informal Definition: Indistinguishability Obfuscation (iO)

Obfuscator $O: C \xrightarrow{O} O(C)$

- **Functionality:** $O(C)$ computes the same function as $C$.
- **Polynomial Slowdown:** $|O(C)| \leq \text{poly}(n) \cdot |C|$
- **Security (indistinguishability obfuscation):**
  If $C_0$ & $C_1$ compute the same function and $|C_0| = |C_1|$, then $O(C_0) \approx O(C_1)$

- **Best Possible Obfuscation**

![Diagram of iO obfuscation]
PKE from iO

Let $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ be a length-doubling PRG.

- $\text{Gen}(1^n)$:
  - $sk \in \{0,1\}^n$
  - $pk := G(sk)$

- $\text{Enc}_{pk}(m)$:
  - $C_{pk,m}(x) := \begin{cases} m & \text{if } G(x) = pk \\ \bot & \text{otherwise} \end{cases}$

  Output $c \leftarrow iO(C_{pk,m})$

- $\text{Dec}_{sk}(c)$: $c(sk) \rightarrow m$

**Theorem**: If $G$ is a PRG and $iO(\cdot)$ is an indistinguishability obfuscator, then this PKE scheme is CPA-secure.
\( \text{Ho:} \quad \text{sk} \in \mathcal{G}_0, \{0,1\}^n \)
\( \text{Pk:} = G(\text{sk}) \)

\( \text{PRG}_1 \)
\( C_{pk,m}(x) = \begin{cases} m & \text{if } G(x) = \text{pk} \\ \bot & \text{otherwise} \end{cases} \)

Output \( c \leftarrow \text{iO}(C_{pk,m}) \)

\( \text{H}_1: \quad \text{pk} \in \mathcal{G}_0, \{0,1\}^{2^n} \)

Output \( c \leftarrow \text{iO}(C_{pk,m}) \)

\( \text{H}_2: \quad \text{pk} \in \mathcal{G}_0, \{0,1\}^{2^n} \)

Output \( c \leftarrow \text{iO}(C'_{pk,m}) \)

\( \text{iO}(C'_{pk,m_0}) \approx \text{iO}(C'_{pk,m_1}) \)
Is it possible?

- 2001: Notion introduced
- 2013: First “candidate” construction from multilinear maps
- 2013-2020: Attack, fixes, new constructions from new assumptions
- 2020: New construction from well-founded assumptions
Final Review

- Cryptographic Hardness Assumptions
  - Factoring / RSA Assumptions
  - DLOG / CDH / DDH Assumptions
  - LWE Assumption (Post-Quantum)

- Key Exchange
  - Definition
  - Construction: Diffie-Hellman

- Public-Key Encryption
  - Definition: CPA / CCA
  - Constructions: El Gamal / RSA / Regev
Final Review

- Theoretical Assumptions
  - One-Way Function / Permutation: Definition & Candidates
  - Hard-Core Predicate: Definition & Construction
  - PRG/PRF from OWP
  - Trapdoor Permutation: Definition & Candidate (RSA)
  - PKE from TDP

- Fully Homomorphic Encryption
  - Definition & Applications
  - Somewhat Homomorphic Encryption over Integers & from LWE (GSW)
  - Bootstrapping SWHE to FHE
Final Review

- Digital Signature
  - Definition
  - Hash-and-Sign Paradigm
  - Construction 1: RSA-FDH
  - Proof in the Random Oracle Model
  - Construction 2: Schnorr
  - Identification Scheme: Definition & Construction from DLOG (Schnorr)
  - Fiat-Shamir Transform
Final Review

- Zero-Knowledge Proof
  - Definition: Completeness / Soundness / Zero-Knowledge
  - Example: ZKP for Diffie-Hellman Tuples
  - Proof Technique: Rewinding
  - ZKP for All NP (Graph 3-Coloring)
  - Commitment Scheme
  - Non-Interactive ZK
Final Review

- Secure Multi-Party Computation
  - Definition: Semi-Honest/Malicious
  - Applications

- Example: Private Set Intersection from DDH

- MPC for Any Function (GMW)

- Oblivious Transfer: Definition & Construction from CDH

- Program Obfuscation
  - Definitions: VBB/iO

- Example: PKE from iO
Thank You 😊