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

\[
\begin{align*}
&\text{Encrypt} \\
&\quad \downarrow m \\
&\quad \downarrow sk \\
&\quad \downarrow C \\
&\Downarrow C \\
&\text{Decrypt} \\
&\quad \downarrow c \\
&\quad \downarrow sk \\
&\quad \downarrow m \\
&\Downarrow m
\end{align*}
\]
Formal Definition: Virtual Black Box (VBB)

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 (Virtual Black Box):**
  
  \[ \forall PPT A, \exists PPT S, \text{s.t.} \forall C, \ A(O(C)) \approx_S \lambda C : S^C(1^{\text{poly}}). \]

\[ O(C) \approx \text{Simulator} \]

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

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

$O: C \rightarrow O(C)$

- **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**
PKE from iO

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

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

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

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

- **Decsk ($c$): ?

**Thm.** If $G$ is a PRG and $iO(\cdot)$ is an indistinguishability obfuscator, then this PKE scheme is CPA-secure.
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 😊