Course Business

- Midterm is on March 1 (Wednesday next week)
  - Allowed to bring one index card (double sided)

- Final Exam is Monday, May 1 (7 PM)
  - Location: Right here

Cryptography
CS 555

Topic 20: Assumptions for Private-Key Cryptography + Computational Indistinguishability

Recap

Last Class:

- One Way Functions, PRGs, PRFs

- **Today:**
  - Assumptions for Private Key Cryptography
  - Computational Indistinguishability

One-Way Functions (OWFs)

$$\mathrm{f}(x) = y$$

Definition: A function $\mathrm{f}: \{0,1\}^* \to \{0,1\}^*$ is one way if it is

1. **(Easy to compute)** There is a polynomial time algorithm (in |x|) for computing f(x).
2. **(Hard to Invert)** Select $\mathrm{x} \leftarrow \{0,1\}^n$ uniformly at random and give the attacker input 1^n, f(x). The probability that a PPT attacker outputs x' such that $\mathrm{f}(x') = f(x)$ is negligible.

From OWFs (Recap)

Theorem: Suppose that there is a PRG G with expansion factor $\ell(n) = n + 1$. Then for any polynomial p(.) there is a PRG with expansion factor p(n).

Theorem: Suppose that there is a PRG G with expansion factor $\ell(n) = 2n$. Then there is a secure PRF.

Theorem: Suppose that there is a secure PRF then there is a strong pseudorandom permutation.

From OWFs (Recap)

Corollary: If one-way functions exist then PRGs, PRFs and strong PRPs all exist.

Corollary: If one-way functions exist then there exist CCA-secure encryption schemes and secure MACs.

Are OWFs Necessary for Private Key Crypto

- Previous results show that OWFs are <u>sufficient</u>.

- Can we build Private Key Crypto from weaker assumptions?

- **Short Answer:** No, OWFs are also <u>*necessary*</u> for most private-key crypto primitives

PRGs → OWFs

Proposition 7.28: If PRGs exist then so do OWFs.

Proof: Let G be a secure PRG with expansion factor $\ell(n) = 2n$.

Question: why can we assume that we have an PRG with expansion 2n?

Answer: Last class we showed that a PRG with expansion factor $\ell(n) = n + 1$. Implies the existence of a PRG with expansion p(n) for any polynomial.

PRGs → OWFs

Proposition 7.28: If PRGs exist then so do OWFs.

Proof: Let G be a secure PRG with expansion factor $\ell(n) = 2n$.

Claim: G is also a OWF!

(Easy to Compute?) ✓

(Hard to Invert?)

Intuition: If we can invert G(x) then we can distinguish G(x) from a random string.

PRGs → OWFs

Proposition 7.28: If PRGs exist then so do OWFs.

Proof: Let G be a secure PRG with expansion factor $\ell(n) = 2n$.

Claim 1: Any PPT A, given G(s), cannot find s except with negligible probability.

Reduction: Assume (for contradiction) that A can invert G(s) with non-negligible probability p(n).

Distinguisher D(y): Simulate A(y)

Output 1 if and only if A(y) outputs x s.t. G(x)=y.

PRGs → OWFs

Proposition 7.28: If PRGs exist then so do OWFs.

Proof: Let G be a secure PRG with expansion factor $\ell(n) = 2n$.

Claim 1: Any PPT A, given G(s), cannot find s except with negligible probability.

Intuition for Reduction: If we can find x s.t. G(x)=y then y is not random.

Fact: Select a random 2n bit string y. Then (whp) there does not exist x such that G(x)=y.

Why not?

PRGs → OWFs

Proposition 7.28: If PRGs exist then so do OWFs.

Proof: Let G be a secure PRG with expansion factor $\ell(n) = 2n$.

Claim 1: Any PPT A, given G(s), cannot find s except with negligible probability.

Intuition: If we can invert G(x) then we can distinguish G(x) from a random string.

Fact: Select a random 2n bit string y. Then (whp) there does not exist x such that G(x)=y.

- Why not? Simple counting argument, 2^{2n} possible y's and 2^n x's.
- Probability there exists such an x is at most 2^{-n} (for a random y)

What other assumptions imply OWFs?

- PRGs → OWFs
- (Easy Extension) PRFs → PRGs → OWFs

- Does secure crypto scheme imply OWFs?
  - CCA-secure? (Strongest)
  - CPA-Secure? (Weaker)
  - EAV-secure? (Weakest)
    - As long as the plaintext is longer than the secret key
  - Perfect Secrecy? X (Guarantee is information theoretic)

EAV-Secure Crypto → OWFs

Proposition 7.29: If there exists a EAV-secure private-key encryption scheme that encrypts messages twice as long as its key, then a one-way function exists.

Recap: EAV-secure.

- Attacker picks two plaintexts m_0,m_1 and is given c=$Enc_K(m_b)$ for random bit b.
- Attacker attempts to guess b.
- No ability to request additional encryptions (chosen-plaintext attacks)
- In fact, no ability to observe any additional encryptions

EAV-Secure Crypto → OWFs

Proposition 7.29: If there exists a EAV-secure private-key encryption scheme that encrypts messages twice as long as its key, then a one-way function exists.

Reduction: $\boldsymbol{f(m,k,r) = Enc_k(m;r) \| m}$.

Input: 4n bits

(For simplicity assume that $\textbf{Enc}_k$ accepts n bits of randomness)

Claim: f is a OWF

EAV-Secure Crypto → OWFs

Proposition 7.29: If there exists a EAV-secure private-key encryption scheme that encrypts messages twice as long as its key, then a one-way function exists.

Reduction: $\boldsymbol{f(m,k,r) = Enc_k(m;r) \| m}$.

Claim: f is a OWF

Reduction: If attacker A can invert f, then attacker A' can break EAV-security as follows. Given $c=Enc_k(m_b;r)$ run $A(c\|m_0)$. If A outputs (m',k',r') such that $f(m', k', r') = c\|m_0$ then output 0; otherwise 1;

MACs→ OWFs

In particular, given a MAC that satisfies MAC security (Definition 4.2) against an attacker who sees an arbitrary (polynomial) number of message/tag pairs.

Conclusions: OWFs are necessary and sufficient for all (non-trivial) private key cryptography.

→OWFs are a minimal assumption for private-key crypto.

Public Key Crypto/Hashing?

- OWFs are known to be necessary
- Not known (or believed) to be sufficient.

Computational Indistinguishability

- Consider two distributions X_ℓ and Y_ℓ (e.g., over strings of length ℓ).
- Let D be a distinguisher that attempts to guess whether a string s came from distribution X_ℓ or Y_ℓ.

The advantage of a distinguisher D is

$$Adv_{D,\ell} = \left| Pr_{s \leftarrow X_\ell}[D(s) = 1] - Pr_{s \leftarrow Y_\ell}[D(s) = 1] \right|$$

Definition: We say that an ensemble of distributions $\{X_n\}_{n \in \mathbb{N}}$ and $\{Y_n\}_{n \in \mathbb{N}}$ are <u>computationally indistinguishable</u> if for all PPT distinguishers D, there is a negligible function negl(n), such that we have

$$Adv_{D,n} \leq negl(n)$$

Computational Indistinguishability

The advantage of a distinguisher D is

$$Adv_{D,\ell} = \left|Pr_{s \leftarrow X_\ell}[D(s) = 1] - Pr_{s \leftarrow Y_\ell}[D(s) = 1]\right|$$

- Looks similar to definition of PRGs
  - X_n is distribution $G(U_n)$ and
  - Y_n is uniform distribution $U_{\ell(n)}$ over strings of length $\ell(n)$.

Computational Indistinguishability

Definition: We say that an ensemble of distributions $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are <u>computationally indistinguishable</u> if for all PPT distinguishers D, there is a negligible function negl(n), such that we have

$$Adv_{D,n} \leq negl(n)$$

Theorem 7.32: Let t(n) be a polynomial and let $P_n = X_n^{t(n)}$ and $Q_n = Y_n^{t(n)}$ then the ensembles $\{P_n\}_{n\in\mathbb{N}}$ and $\{Q_n\}_{n\in\mathbb{N}}$ are <u>computationally indistinguishable</u>

Computational Indistinguishability

Definition: We say that an ensemble of distributions $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are computationally indistinguishable if for all PPT distinguishers D, there is a negligible function negl(n), such that we have

$$Adv_{D,n} \leq negl(n)$$

Fact: Let $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ be computationally indistinguishable and let $\{Z_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ be computationally indistinguishable

Then

$\{X_n\}_{n\in\mathbb{N}}$ and $\{Z_n\}_{n\in\mathbb{N}}$ are computationally indistinguishable

Next Class

- Review for Midterm
- Review Homework Solutions
- Review Key Definitions and Results
  - Perfect Secrets/EAV-Security/CPA-Security/CCA-Security + Constructions
  - Primitives: PRGs, PRFs, MACs, Collision Resistant Hash Functions

- Multiple Choice Questions
- Allowed to bring index card