Alin Tomescu, CSE408
Tuesday, February 15th, Lecture #5

Pseudo random functions

Pseudorandom functions (PRFs) are not to be confused with pseudorandom generators (PRGs). The guarantee of a PRG is that a single output appears random if the input was chosen at random. On the other hand, the guarantee of a PRF is that all its outputs appear random, regardless of how the corresponding inputs were chosen, as long as the function was drawn at random from the PRF family.

A family of functions F_k is a (t, q, ε)-secure PRF if $\forall$ adversaries A running in time $\leq t$ and making at most q oracle queries, then the advantage of A is $\leq \varepsilon$

$$Adv\ A = |\Pr[A^{F_k} = 0 | k \leftarrow u] - \Pr[A^R = 0 | R \leftarrow funcs]| \leq \varepsilon$$

$$F_k \overset{t,q}{\underset{\varepsilon}{\sim}} R$$

Things to know:

- If you look at a PRNG you want the output to look random. If you look at a family of functions you want the collection to look random. You don't want the attacker to tell whether you're using a RC4 box or a random-generating box. As an attacker you want to know what box you're attacking.
- Random and pseudo-random are both supposed to be deterministic. If you feed x two times in a row, the second output should be the same output as the first one. Otherwise the attacker could easily distinguish between a PRNG and a RNG by just feeding it the same input.
- The difference between pseudo-random and random is essentially that the random function will choose its output with equal probability from the co-domain of the function. In reality, the pseudo-random function will never be able to choose uniformly. Therefore, the goal of security is to have the PRF imitate the RF as good as it can so that an attacker cannot distinguish between the two.
- Most block-ciphers are pseudo-random functions or pseudo-random permutations.

Let $F_k: \{0,1\}^l \rightarrow \{0,1\}^L$ be a function family. How many such functions are possible?

- How many possible inputs do you have? 2^l
- How many possible outputs do you have? 2^L
- You have 2^L choices for each one of the 2^l possible inputs: So $2^L \times 2^L \times \ldots \times 2^L = (2^L)^{2^l} = 2^{L2^l}$

DPI for PRFs

Theorem

If f runs in time t' and F is a (t, q, ε)-PRF then $f(F_k)$ is a $(t - O(q), q, \varepsilon)$-indistinguishable from $f(R)$.

$$F_k \overset{t,q}{\underset{\varepsilon}{\sim}} R \Rightarrow f(F_k) \overset{t-O(q),q}{\underset{\varepsilon}{\sim}} f(R)$$

Actually, $O(q) = t'q$

Alin Tomescu, CSE408
Tuesday, February 15th, Lecture #5

Transitivity

Theorem

If $F_k \underset{\varepsilon}{\sim} G_k \underset{\varepsilon'}{\sim} H_k$ then $F_k \underset{\varepsilon+\varepsilon'}{\sim} H_k$.

Examples

AES

Conjecture: AES is $\left(t, q, \frac{t}{2^{128}} + \frac{q^2}{2^{129}}\right)$-PRF

RSA

Last time we used: Pick $N = pq$ and e relatively prime to $(p-1)(q-1)$ and $f(x) = lsb_{11}\left(x^{\frac{1}{e}} mod\ N\right)$ to generate a PRNG.

Building a PRG from a PRF

Theorem: If F_k is a (t, q, ε)-PRF then $G(k) = (F_k(0), F_k(1), \ldots F_k(q))$ is a (t, ε)-secure PRG.