9
Private key crypto recap

We now review all that we have learned about *private key* cryptography before we embark on the wonderful journey to *public key* cryptography.

This material is mostly covered in Chapters 1 to 9 of the Katz Lindell book, and now would be a good time for you to read the corresponding proofs in the book. It is often helpful to see the same proof presented in a slightly different way. Below is a review of some of the various reductions we saw in class that are covered in the KL book, with pointers to the corresponding sections.

- Pseudorandom generators (PRG) length extension (from $n+1$ output PRG to $poly(n)$ output PRG): Section 7.4.2
- PRG's to pseudorandom functions (PRF's): Section 7.5
- PRF's to Chosen Plaintext Attack (CPA) secure encryption: Section 3.5.2
- PRF's to secure Message Authentication Codes (MAC's): Section 4.3
- MAC's + CPA secure encryption to chosen ciphertext attack (CCA) secure encryption: Section 4.5.4
- Pseudorandom permutation (PRP's) to CPA secure encryption / block cipher modes: Section 3.5.2, Section 3.6.2
- Hash function applications: fingerprinting, Merkle trees, passwords: Section 5.6
- Coin tossing over the phone: we saw a construction in class that used a *commitment scheme* built out of a pseudorandom generator. Section 5.6.5 shows an alternative construction using random oracles.
- PRP's from PRF's: we only sketched the construction which can be found inSection 7.6

One major point we did *not* talk about in this course was *one way functions*. The definition of a one way function is quite simple:

A function $f : \{0,1\}^* \to \{0,1\}^*$ is a *one way function* if it is efficiently computable and for every n and a $poly(n)$ time adversary A, the probability over $x \leftarrow_R \{0,1\}^n$ that $A(f(x))$ outputs x' such that $f(x') = f(x)$ is negligible.

The "OWF conjecture" is the conjecture that one way functions exist. It turns out to be a necessary and sufficient condition for much of cryptography. That is, the following theorem is known (by combining works of many people):

Theorem: The following are equivalent: * One way functions exist * Pseudorandom generators (with non trivial stretch) exist * Pseudorandom functions exist * CPA secure private key encryptions exist * CCA secure private key encryptions exist * Message Authentication Codes exist * Commitment schemes exist

(and others as well)

The key result in the proof of this theorem is the result of Hastad, Impagliazzo, Levin and Luby that if one way functions exist then pseudorandom generators exist. If you are interested in finding out more, Sections 7.2-7.4 in the KL book cover a special case of this theorem for the case that the one way function is a *permutation* on $\{0,1\}^n$ for every n. This proof has been considerably simplified and quantitatively improved in works of Haitner, Holenstein, Reingold, Vadhan, Wee and Zheng. See this talk of Salil Vadhan for more on this. See also these lecture notes from a Princeton seminar I gave on this topic (though the proof has been simplified since then by the above works).

9.0.1 Attacks on private key cryptosystems

Another topic we did not discuss in depth is attacks on private key cryptosystems. These attacks often work by "opening the black box" and looking at the internal operation of block ciphers or hash functions. One then often assigns variables to various internal registers, and then we look to finding collections of inputs that would satisfy some non-trivial relation between those variables. This is a rather vague description, but you can read KL Section 6.2.6 on *linear* and *differential* cryptanalysis for more information. See also this course of Adi Shamir. There is also the fascinating area of *side channel* attacks on both public and private key crypto.

III

PUBLIC KEY CRYPTOGRAPHY