Lecture 9

FEBRUARY 16

Instructor: Fang Song

Disclaimer. Draft note. No guarantee on completeness nor soundness. Read with caution, and shoot me an email at fsong@pdx.edu for corrections/comments (they are always welcome!)

Logistics. Statistics. Supplement reading: BS more examples. Check resource page frequently. HW 3 2b) [KL: 4.14]
Last time. Theoretical constructions of Private-key primitives.
Today. Review. Quiz 3

1 Private-key crypto recap

FS NOTE: draw dependence diagram [KL: Fig. 8.1]

Main concepts.

- Encryption
  - Perfect secrecy (perfect indistinguishability in the presence of an eavesdropper)
  - Computational secrecy (computational indistinguishability in the presence of an eavesdropper)
  - CPA-security (computational indistinguishability under a chosen-plaintext attack)
- Message authentication
  - EUCMA
- PRG and stream ciphers
- PRF/PRP and block ciphers
- Hash functions, collision resistance
- One-way functions.

Main theorems.

- Perfect secrecy: OTP, neccesity of long key.
- Computational secrecy: PRG stream cipher.
- CPA encrytion: PRF (Baby version of Randomized counter mode), Block cipher modes: RCTR, CBC.
- MAC: PRF; PRF domain extension: CBC, Cascade, ECBC, NMAC; Hash-and-MAC, HMAC.

Proof by reduction. Hybrid argument.

2 Examples

2.1 PRF in RO model

Suppose $\mathcal{O} : \{0,1\}^{2n} \to \{0,1\}^n$ is given as an RO. Define $F_k(x) := \mathcal{O}(k\|x)$. $\mathcal{F}$ as usual is the set of functions from n-bit to n-bit.

Theorem 1. *F_k is a PRF in the RO model.*

Proof.

$$\left| \Pr_{k \leftarrow \{0,1\}^n} [D^{\mathcal{O},F_k}(1^n) - \Pr_{f \leftarrow \mathcal{F}} [D^{\mathcal{O},f}(1^n) = 1]] \right| = \varepsilon(n)\,.$$

Suppose D makes $q_{\mathcal{O}}$ and q_F queries to RO and $F = F_k/f$ respectively. Using the first property (uniform randomness), what D sees in two cases are identical, until D queries the RO on an input of the form $k\|\cdot$. However, since k is uniformly random, within $q_{\mathcal{O}}$ queries, this happens w.p. at most $q_{\mathcal{O}}/2^n$. Thus we claim that $\varepsilon(n) \le q_{\mathcal{O}}/2^n$, and F_k is pseudorandom even for unbounded distinguisher. Note we discussed in class that this is impossible in the real world. This may be taken as a demonstration of the power of the RO model as well as an objection to it. □

2.2 Selected Problems

- HW 1. expectation, linearity.
- Quiz 1. 2 d) combinatorics.
- PRG: HW2 4 iii), LATER Quiz2 2 c) reduction in part 1; PRF: 5 b)
- Quiz 2. 2.b) reduction.