CS 346 Class Notes

Mark Lindberg

Apr 18, 2016

This Time:

Chapter 11: Public-key encryption. PKE.

Definition 11-1. A PKE scheme is a set of PPT algorithms $\mathsf{GenEncDec}$ where

1. $\mathsf{Gen}(1^n)$ produces (pk, sk). Assume pk, sk are at least n bits long, and can determine n from pk, sk.

2. $\mathsf{Enc}_{pk}(m)$. Randomized, yields ciphertext c. m is drawn from the message space, which can depend on pk.

3. $\mathsf{Dec}_{sk}(m)$. Computes m or $\perp$, which indicates failure. Deterministic.

Correctness: Except for the possibility with $\mathtt{negl}$ probability over (pk, sk) produced by Gen, $\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m$ for all m in message space.

PKE security notions. Start with indistinguishable in the presence of an eavesdropper. (EAV-security).

Experiment: $\mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$. $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

1. Run $\mathsf{Gen}(1^n)$ to get (pk, sk).

2. $\mathcal{A}$ is given pk (!) and outputs equal-length m_0, m_1. (From the message space associated with pk.

3. Choose a random bit b. $c \leftarrow \mathsf{Enc}_{pk}(m_b)$. Give c to $\mathcal{A}$.

4. $\mathcal{A}$ outputs b'. $\mathcal{A}$ succeeds if $b' = b$.

Definition 11.2: Π is EAV-secure if $\forall$ PPT adversaries $\mathcal{A}$,

$$\Pr[\mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathtt{negl}(n).$$

This experiment is analogous to the CPA experiment in the private key setting, since $\mathcal{A}$ can compute polynomially many encryptions, because it was given the public key pk. (It can make its own oracle.)

Proposition 11.3. If a PKE scheme satisfies definition 11.2, then it is CPA-secure.

Impossibility of perfectly secret PKE. Related to 11.1 (Also 11.2?)

Modify definition 11.2 to

1. Allow $\mathcal{A}$ to take an arbitrary amount of time...
2. Require $\Pr[\mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2}$.

Proof of impossibility: Let t denote the upper bound on random bits used by Enc_{pk} on input m_0.

$\mathcal{A}$ can ~~run~~ simulate $\mathsf{Enc}_{pk}(m_0)$ using all possible sequences of t random bits, and see if c is produced. Correctness is now guaranteed.

Insecurity of a deterministic PKE.

Theorem 11.4: No deterministic PKE scheme is secure:

It's easy to compute the c and check with no random bits...

11.2.2: Multiple Encryptions.

Definition 11.5: A PKE scheme Π has indistinguishable multiple encryptions if for all PPT $\mathcal{A}$,

$$\Pr[\mathsf{PubK}^{\mathsf{LR-CPA}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathtt{negl}(n).$$

Theorem 11.6: (There is a lengthy proof of this in the textbook) If a PKE scheme is CPA-secure, then it is secure with respect to definition 11.5.

Encryption of arbitrary-length messages.

Claim 11.7:

CPA-secure PKE Π for fixed length messages $\rightarrow$ CPA-secure Π' for arbitrary length messages.

CCA-security: $\mathsf{PubK}^{\mathsf{CCA}}_{\mathcal{A},\Pi}(n)$. Main difference here is that $\mathcal{A}$ gets access to a decryption oracle, except it can't call $\mathsf{Dec}_{sk}(c)$.

Definition 11.8: Π has indistinguishable encryption under a chosen-ciphertext attack if $\forall$ PPT $\mathcal{A}$,

$$\Pr[\mathsf{PubK}^{\mathsf{CCA}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathtt{negl}(n).$$

The analogue of theorem 11.6 holds!

Unfortunately, claim 11.2 does not.

Section 11.3: Hybrid encryption and the KEM/DEM paradigm.

Private vs public key encryption:

- PKE building blocks are *much* slower.
- Also, PKE has greater "expansion".
- No need for a shared key. ($O(n)$ vs $O(n^2)$).

KEM: Key-Encapsulation Mechanism. We'll use a PKE to implement this.

DEM: Data-Encapsulation Mechanism. We'll use private-key encryption here.

KEM=(Gen,Encaps, Decaps)

- $\mathsf{Gen}(1^n)$ produces (pk, sk).

- $\text{Encaps}_{pk}(1^n)$ produces (c, k), where length of $k = \ell(n)$.
- $\text{Decaps}_{sk}(c)$ produces k.

Figure 11.2 from the textbook. Whee. :P