CS 346 Class Notes

Mark Lindberg

Apr 25, 2016

This Time:

Late HWs will only be penalized 2% per day up to Monday, May 2. You lose 10% for each day after that. Slip days are, of course, not counted towards this.

Check the notes that the professor has posted on Piazza about problem set 5.

The last problem is probably the most difficult problem.

KEM/DEM paradigm (Key/Data Encapsulation Mechanism). Hybrid encryption produces a PKE scheme. DEM used private-key encryption.

KEM: $(\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps})$.

- $\mathsf{Gen}(1^n)$ produces (pk, sk).
- $\mathsf{Encaps}_{pk}(1^n)$ produces (c, k), a Ciphertext and a Key in $\{0,1\}^{\ell(n)}$ (We'll assume $\ell(n) = n$).
- $\mathsf{Decaps}_{sk}(c) = k$.

Construction 11.10. Hybrid Encryption.
KEM $\Pi = (\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps})$
Private Key Encryption Scheme: $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$.
Produces a PKE: $\Pi'' = (\mathsf{Gen}'', \mathsf{Enc}'', \mathsf{Dec}'')$.

- Gen'': Same as Gen. (Yields (pk, sk).)
- Gen'': On input $pk, m \in \mathcal{M}$
  1. $(c, k) \leftarrow \mathsf{Encaps}(1^n)$.
  2. $c' \leftarrow \mathsf{Enc}'_k(m)$.
  3. Output c, c'
- Dec'': On input sk and (c, c'):
  1. $k := \mathsf{Decaps}_{sk}(c)$.
  2. $m := \mathsf{Dec}'_k(c')$.

Section 11.3.1: CPA-security.
We want to define the notion of a CPA-secure KEM. Later, we'll also see CCA-secure.
Experiment $\mathsf{KEM}^{\mathsf{CPA}}_{\mathcal{A},\Pi}(n)$.

1. $\mathsf{Gen}(1^n)$ is run to obtain (pk, sk), $\mathsf{Encaps}_{pk}(1^n)$ is run to obtain (c, k). [We'll assume $k \in \{0,1\}^n$.]
2. Uniform bit b is chosen. If $b = 0$, set $k' = k$. Else, let $k \in \{0,1\}^n$ be chosen uniformly at random.
3. Give (pk, c, k') to $\mathcal{A}$. $\mathcal{A}$ outputs b'.
4. $\mathcal{A}$ succeeds iff $b = b'$.

Definition 11.11: KEM Π is CPA-secure if $\forall$ PPT $\mathcal{A}$,

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

Theorem 11.12: (There is a lengthy proof of this theorem in the textbook.) Construction 11.10 is CPA-secure if Π is CPA-secure and Π' is ENV-secure.
Section 11.3.2: CCA-security.
$\mathsf{KEM}^{\mathsf{CCA}}_{\mathcal{A},\Pi}(n)$. The first 2 steps are the same as $\mathsf{KEM}^{\mathsf{CPA}}_{\mathcal{A},\Pi}$. Then:

3. $\mathcal{A}$ is given (pk, c, k') and access to Decaps_{sk} oracle, which it can call on anything but c.
4. $\mathcal{A}$ outputs b', and success is as above.

Definition 11.13: CCA-secure KEM.
Theorem 11.14: Construction 11.10 is CCA-secure if Π, Π' are both CCA-secure.
It remains to be shown how to create a CPA- or CCA-secure KEM.
11.4: CHD/DDH-based Encryption.
11.4.1: El Gamal Encryption. It's a variant of the Diffie-Hellman key exchange protocol. (1976).
In 1977, we got RSA!
in 1985, we got the El Gamal extension of Diffie-Hellman for public key encryption.
Lemma 11.15: Let $\mathbb{G}$ be a finit group, $m \in \mathbb{G}$, and k a uniformly random elemnt of $\mathbb{G}$. Then $m \cdot k$ is a uniformly random element of $\mathbb{G}$.
EL GAMAL!

- Group generation algorithm G is the same as in Diffie-Hellman. $G(1^n) = (\mathbb{G}, g, q)$, where $\mathbb{G}$ is a cyclic group of order q, $||q|| = n$, and g Is a generator of G.
- Gen: Run $G(1^n)$ to get (G, q, g). Choose a uniform $x \in \mathbb{Z}_q$. Let $h = g^x$. (h is a uniformly random element of $\mathbb{G}$.) The public key pk is (G, q, g, h). And the private key sk is (G, q, g, x).

- Enc: On input $pk = (G, q, g, h)$ and a message $m \in \mathbb{G}$, choose a uniform $y \in \mathbb{Z}_q$, and output ciphertext $(g^y, h^y \cdot m) = (c_1, c_2)$.
- Dec: On input (c_1, c_2), compute $g^{-xy} \cdot c_2$ to obtain m.

Theorem 11.18: If DDP is hard relative to G, then El Gamal Encryption is CPA-secure.
11.4.2 DDH-based key encapsulation:
Construction 11.19

- Gen: Run $G(1^n)$ to get $(\mathbb{G}, q, g)$. Choose a uniform $x \in \mathbb{Z}_q$. Set $h = g^x$. Specify $H : G \to \{0,1\}^{\ell(n)}$. Public key is $(\mathbb{G}, q, g, h, H)$. Private key is $(\mathbb{G}, g, q, x)$.
- Encaps: On input $pk = (\mathbb{G}, q, g, h, H)$, choose a uniform $y \in \mathbb{Z}_q$, set $c = g^y$ and $k = H(h^y)$.
- Decaps: On input $sk = (G, q, g, x)$ and $c(= g^y)$, set k to $H(c^x)$.

Theorem 11.20: If DDH hard relative to G, and H satisfies certain technical conditions listed in the textbook, then the construction 11.19 (above) is CPA-secure.

Theorem 11.22: If "GAP-CDH" hard relative to G, and H is modeled as a random oracle, then construction 11.19 (again, above) is CCA-secure.