CS276: Cryptography October 8, 2015

Lecture 13

Instructor: Alessandro Chiesa *Scribe: Xingyou Song*

The following topics are covered:
- asymmetric cryptography
- encryption schemes
- trapdoor OWP

Asymmetric Key Cryptography

Intro

So far we've assumed Alice and Bob shared a secret key (SK).

What's wrong with this assumption?
-1. How does this meeting take place? We also need to keep the key fresh.
-2. For n people, we will need $\binom{n}{2}$ keys.

We come up with the following solution:
(Public Key Infrastructure): Each person has a public key, PK. Every person also has a secret key, SK, given only to himself.
We will need to define the requirements of public key encryption schemes.
- encryption
- authentication

Definition: Public Key Encryption
A public key encryption scheme is:
A triple of efficient algorithms: (G,E,D) that satisfy:

1. Completeness

$\forall k \in N, \forall (PK, SK) \in G(1^k)$,

$$\Pr[D(1^k, SK, E(1^k, PK, m)) = m] = 1$$

The difference here is that $SK \neq PK$, so it's "asymmetric."

2. Security via message indistinguishability $\forall \{m_k^{(0)}\}_k, \{m_k^{(1)}\}_k$ with $m_k^{(i)} \in \{0,1\}^{\ell(k)}, i \in \{0,1\}$

$$\{(PK, E(1^k, PK, m_k^{(0)}))\} \stackrel{C}{=} \{(PK, E(1^k, PK, m_k^{(1)}))\}$$

where $(PK, SK) \leftarrow G(1^k)$. In comparison to symmetric key crypto, we had

$$E(1^k, U_k, m_k^{(0)}) \stackrel{C}{=} E(1^k, U_k, m_k^{(1)})$$

where U_k is randomly chosen.

2'. Security, via message indistinguishability against CPA: $\forall \{m_k^{(0)}\}_k, \{m_k^{(1)}\}_k$, same size messages, $\forall$ PPTA,

$$|\Pr[A^{E(1^k,PK,\cdot)}(1^k, PK, E(1^k, PK, m_k^{(0)}) = 1] - \Pr[...]|$$

is negligible.

Remark/Special theorem: (G,E,D) is 1 MI $\longleftrightarrow$ MI is CPA.

Trapdoor OWP, a motivation:
If we know some information about the OWP, then we can invert.
Before: Given OWP f with hardcore predicate b, we proved that $f(U_k)||b(U_k) \stackrel{C}{=} U_{k+1}$.

We could've constructed a symmetric encryption scheme using this, which is a motivation from one-bit messages:

$$E(1^k, SK, m) = f(SK), b(SK) \oplus m$$
$$D(1^k, SK, c) = f(SK), b(SK) \oplus m$$

Definition: Trapdoor OWP: A TOWP is a (G, Eval, Inverter)
(1) Permutation: $\forall k \in N, \forall (PK, SK) \in G(1^k)$,
$\text{Eval}(1^k, PK, \cdot)$ is a permutation.
(2) Inversion:

$$\text{Inv}(1^k, SK, \text{Eval}(1^k, PK, m)) = m$$

(3) $\forall$ PPT A,
$x \leftarrow \{0,1\}^{\ell(k)}$, $(PK, SK) \leftarrow G(1^k)$, $y = \text{Eval}(1^k, PK, x)$, $x' = A(1^k, PK, y)$,

$$\Pr[\text{Eval}(1^k, PK, x') = y]$$

is negligible.

Define: B is hardcore for TOWP (G, Eval, Inv) if $\forall$ PPT A, we do the same experiment as above, but let $b \leftarrow A(1^k, PK, y)$,

$$\Pr[b = B(x)] \leq \frac{1}{2} + \text{neg}(k)$$

Now we construct a public-key encryption.

Theorem: (TOWP $\rightarrow$ PKI) (Goldreich-Levin makes OWP $\rightarrow$ hardcore bit)
Proof: Consider (G,E,D): $G(1^k) = G_{TOWP}(1^k)$, $E(1^k, PK, m) = \text{Eval}(1^k, PK, U_1), B(r) \oplus m$, $D(1^k, SK, c) = \text{Invert}(1^k, SK, c_0) \oplus c_1$
Proof that this is PKI:
Assume it's not secure. Then $\exists$ PPT $A, (m_k^{(0)})_k, (m_k^{(1)})_k$ s.t.

$$\delta(k) = |\Pr[A(PK, E(PK, m_k^{(0)}) = 1] - \Pr[...] \quad |$$

Construct A' that attacks B. Let $A'(1^k, PK, y)$ do the following:

$$1. \sigma \leftarrow (0,1)$$
$$2. b \leftarrow A(PK, y, \sigma)$$
$$3. b = 0 \rightarrow \bar{\sigma}, b = 1 \rightarrow \sigma$$

Then this predictor will be correct with probability $\frac{1}{2} + \frac{\delta(k)}{2}$, contradiction.

Example: RSA Trapdoor OWP (probably one of the only OWP that is TOWP):
$G(1^k)$ do the following:
1. Pick two random k-bit primes p, q
2. $N = pq$
3. Find de, s.t. $de \equiv 1 \mod \phi(n)$
4. $PK = (N, e), SK = (N, d)$
5. $\text{Eval}(1^k, PK, x) = x^e \mod (N)$

Now let $\text{Inv}(1^k, sk, y) = y^d \mod (N)$, it is clear by simple number theory that $\forall \gcd(N, e) = 1$, $x \to x^e \mod (N)$ is a permutation, as well as $y \to y^{e^{-1}} \mod (N)$ is invertible.

Hybrid Encryption:
Ingredients: (G_1, E_1, D_1), which is a PK encryption scheme, with (E_2, D_2) which is a SK encryption scheme.

Construction: (G, E, D)
$G(1^k) = G_1(1^k)$

$E(1^k, PK, m) :=$
1. Sample SK_2 for (E_2, D_2)
2. $c_0 \leftarrow E_1(1^k, PK, SK_2)$
3. $c_1 \leftarrow E_2(1^k, SK_3, m)$
4. Output (c_0, c_1)

$D(1^k, SK, c) :=$
1. $SK_2 \leftarrow D_1(1^k < SK, c_0)$
2. $m \leftarrow D_2(1^k, SK_2, c_1)$
3. Output m.