CS276: Cryptography	October 13, 2015
Lecture 14	
Instructor: Alessandro Chiesa	*Scribe: Peter Manohar*

1 Hybrid Encryption

Let (G_1, E_1, D_1) be a one message indistinguishable asymmetric encryption scheme. Let (E_2, D_2) be a one message indistinguishable symmetric encryption scheme. Define (G, E, D) as follows:

- $G(1^k) = G_1(1^k)$
- $E(1^k, pk, m) =$

  Sample sk_2 for (E_2, D_2)

  output $(E_1(1^k, pk, sk_2), E_2(1^k, sk, m))$
- $D(1^k, sk, c) =$

  $sk_2 \leftarrow D_1(1^k, sk, c_1)$

  $m \leftarrow D_2(1^k, sk_2, c_2)$

Theorem 1 *(G, E, D) is a one message indistinguishable asymmetric encryption scheme*

Proof: Assume $\exists$ ppt A, $\{m_k^{(0)}, m_k^{(1)}\}$ such that $\delta(k) = \left|\Pr[A(pk, E(pk, m_k^{(0)})) = 1] - \Pr[A(pk, E(pk, m_k^{(1)})) = 1]\right|$ is nonnegligible.

$$
\begin{aligned}
\implies \delta(k) &= \left|\Pr[A(pk, E(pk, m_k^{(0)})) = 1] - \Pr[A(pk, E(pk, m_k^{(1)})) = 1]\right| \\
&= \left|\Pr[A(pk, (E_1(pk, sk_2), E_2(sk_2, m_k^{(0)})) = 1] - \Pr[A(pk, (E_1(pk, sk_2), E_2(sk_2, m_k^{(1)})) = 1]\right| \\
&\leq \left|\Pr[A(pk, (E_1(pk, sk_2), E_2(sk_2, m_k^{(0)})) = 1] - \Pr[A(pk, (E_1(pk, 0^k), E_2(sk_2, m_k^{(0)})) = 1]\right| \quad (1) \\
&+ \left|\Pr[A(pk, (E_1(pk, 0^k), E_2(sk_2, m_k^{(0)})) = 1] - \Pr[A(pk, (E_1(pk, 0^k), E_2(sk_2, m_k^{(1)})) = 1]\right| \quad (2) \\
&+ \left|\Pr[A(pk, (E_1(pk, 0^k), E_2(sk_2, m_k^{(1)})) = 1] - \Pr[A(pk, (E_1(pk, sk_2), E_2(sk_2, m_k^{(1)})) = 1]\right| \quad (3)
\end{aligned}
$$

If (1) is nonnegligible, then we can attack (G_1, E_1, D_1). Let $B(1^k, pk, c) = A(pk, c, E_2(sk_2^*, m_k^{(b)}))$, where $c = E_1(pk, 0^k)$ or $E_1(pk, sk_2^*)$. Then B breaks (G_1, E_1, D_1) with nonnegligible probability. By symmetry, if (3) is nonnegligible, then we can also break (G_1, E_1, D_1) with nonnegligible probability.

If (2) is nonnegligible, then we can attack E_2. Let $C(c) = A(pk^*, (E_1(pk^*, 0^k), c))$, for some fixed public key pk^*, where $c = E_2(sk_2, m^{(0)})$ or $E_2(sk_2, m^{(1)})$. Then C breaks (E_2, D_2) with nonnegligible probability. This completes the proof. $\square$

2 DDH Assumption

The Decisional Diffie Hellman (DDH) assumption is a computational hardness assumption about the discrete log problem in a cyclic group.

Definition 2 *A cyclic group sampler is a ppt algorithm S such that $\forall k \in \mathbb{N}$, $S(1^k)$ is a distribution over tuples $(\mathbb{G}, q, g)$, where $|\mathbb{G}| = q$, and $\mathbb{G} = <g>$.*

Definition 3 *DDH holds for S if*
$\{(1^k, \mathbb{G}, q, g, g^x, g^y, g^{xy}) \mid (\mathbb{G}, q, g) \leftarrow S(1^k),\ x, y \leftarrow \{0, 1, ..., q-1\}\}$ *and*
$\{(1^k, \mathbb{G}, q, g, g^x, g^y, g^r) \mid (\mathbb{G}, q, g) \leftarrow S(1^k),\ x, y, r \leftarrow \{0, 1, ..., q-1\}\}$ *are computationally indistinguishable*

2.1 El Gamal Encryption Scheme

Suppose S satisfies DDH.

- $G(1^k) =$
  - $(\mathbb{G}, q, g) \leftarrow S(1^k)$
  - $x \leftarrow \{0, 1, ..., q-1\}$
  - $h = g^x$
  - $pk = (\mathbb{G}, q, g, h)$
  - $sk = (\mathbb{G}, q, g, x)$
  - output (pk, sk)
- $E(1^k, pk, m) =$
  - $y \leftarrow \{0, 1, ..., q-1\}$
  - $c \leftarrow (g^y, h^y m)$
- $D(1^k, sk, c) = c_2 \cdot c_1^{-x}$

Theorem 4 *If DDH holds for S, then (G, E, D) is one message indistinguishable*

Proof: Suppose $\exists$ ppt A, m_0, m_1, such that $|\Pr[A(g^x, g^y, g^{xy}m_0) = 1] - \Pr[A(g^x, g^y, g^{xy}m_1) = 1]|$ is nonnegligible. Then

$$|\Pr[A(g^x, g^y, g^{xy}m_0) = 1] - \Pr[A(g^x, g^y, g^{xy}m_1) = 1]| \leq |\Pr[A(g^x, g^y, g^{xy}m_0) = 1] - \Pr[A(g^x, g^y, g^r m_0) = 1]|$$
$$+ |\Pr[A(g^x, g^y, g^r m_0) = 1] - \Pr[A(g^x, g^y, g^r m_1) = 1]| + |\Pr[A(g^x, g^y, g^r m_1) = 1] - \Pr[A(g^x, g^y, g^{xy}m_1) = 1]|$$

Note that $|\Pr[A(g^x, g^y, g^r m_0) = 1] - \Pr[A(g^x, g^y, g^r m_1) = 1]| = 0$, so either $|\Pr[A(g^x, g^y, g^{xy}m_0) = 1] - \Pr[A(g^x, g^y, g^r m_0) = 1]|$ or $|\Pr[A(g^x, g^y, g^r m_1) = 1] - \Pr[A(g^x, g^y, g^{xy}m_1) = 1]|$ is nonnegligible. Since one of these is nonnegligible, we can construct $B(1^k, \mathbb{G}, q, g, a, b, c) = A(1^k, \mathbb{G}, q, g, a, b, cm_\sigma)$, where $\sigma = 0$ or 1, depending on which term is large. The existence of B contradicts the DDH assumption for S, completing the proof. $\square$

2.2 Remarks on DDH

- If DDH holds for S, then discrete log assumption holds for S
- There are examples of S where we know DDH is false, but DL is believed to be true

2.3 Example: $\mathbb{Z}_p^*$

DDH does not hold for $\mathbb{Z}_p^*$ (see homework 1). However, we believe that DDH holds for $QR_p \subset \mathbb{Z}_p^*$, the subgroup of quadratic residues. $|QR_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}$. If $p = 2q + 1$ for some prime q, then p is called a *safe prime*, and $|QR_p| = q$.

3 CCA2 Security in the Asymmetric Case

El Gamal is not CCA2 secure. If (c_1, c_2) in an encryption of m, then $(c_1, 2c_2)$ is an encryption of $2m$.

In the symmetric setting, CPA + MAC = CCA2. In the asymmetric setting, CPA + DS $\neq$ CCA2.

Some approaches:

- Cramer-Shoup: variant of El-Gamal that is CCA2 secure only under DDH assumption
- Naor-Yung: CPA + NIZK = CCA2
- CCA2 symmetric scheme + TOWP + Random Oracle Model = CCA2

We will focus on the 3rd approach. The construction and proof are covered in the next lecture.