CS276: Cryptography October 15, 2015

CCA2 Security in ROM and Digital Signatures

Instructor: Alessandro Chiesa *Scribe: Lynn Chua*

1 CCA2 Security in the Random Oracle Model

We construct a CCA2-secure encryption scheme $(G, \overline{E}, \overline{D})$ using a TOWP (S, Eval, Inv), a CCA2-secure encryption scheme (E,D) and a random oracle RO as follows.

- $\overline{G}^{RO}(1^k) := S(1^k)$
- $\overline{E}^{RO}(1^k, pk, m) :=$
  1. sample x for TOWP
  2. $y \leftarrow \text{Eval}(pk, x)$
  3. $c \leftarrow E(RO(x), m)$
  4. output $\overline{c} = (y, c)$
- $\overline{D}^{RO}(1^k, sk, \overline{c}) :=$
  1. $x \leftarrow \text{Inv}(sk, y)$
  2. $m \leftarrow D(RO(x), c)$
  3. output m

We prove the security of the above scheme by considering two cases. In the first case, the adversary queries the random oracle RO at x. We can then reduce the security of the scheme to the security of the TOWP. In the second case, the adversary does not query RO at x, and hence learns nothing about $RO(x)$. We can reduce this to the security of the encryption scheme (E, D).

Theorem 1 *The public key encryption scheme $(\overline{G}, \overline{E}, \overline{D})$ defined above is CCA2-secure in the random oracle model.*

Proof: Suppose there exists a PPT adversary A, and m_0, m_1 such that

$$\left| Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m_0)) = 1\right] - Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m_1)) = 1\right] \right| \tag{1}$$

is not negligble in k. We first consider the case where the adversary does not query RO at x. Using A, we construct B that attacks (E, D) as follows.

$B^{E(sk^*,\cdot),D(sk^*,\cdot)}(c) :=$

1. $(pk, sk) \leftarrow S(1^k)$
2. sample x
3. $y \leftarrow \text{Eval}(pk, x)$
4. $\overline{c} \leftarrow (y, c)$
5. Simulate $A^{RO,\overline{E},\overline{D}}(\overline{c})$ where
   - $RO(z)$: answer randomly but consistently but if $z = x$ then abort
   - $\overline{E}(m_i) :=$
     1. sample x_i
     2. $y_i \leftarrow \text{Eval}(pk, x_i)$
     3. if $x_i \neq x$, $c_i \leftarrow E(RO(x_i), m_i)$
     4. if $x_i = x$, $G \leftarrow E(sk^*, m_i)$
     5. $\overline{c_i} \leftarrow (y_i, c_i)$
   - $\overline{D}(\overline{c}) :=$
     1. $x_i \leftarrow \text{Inv}(sk, y_i)$
     2. if $x_i \neq x$, $m_i \leftarrow D(RO(x_i), c_i)$
     3. if $x_i = x$, $m_i \leftarrow D(sk^*, c_i)$

Let Q be the event that A queries RO at x. Then we have

$$Pr\left[B^{E,D}(E(m)) = 1\right] = Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m)) = 1 \ \& \ \overline{Q}\right] \tag{2}$$

We split the probabilities into the two cases as follows.

$$\begin{aligned}
& \left|Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m_0)) = 1\right] - Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m_1)) = 1\right]\right| && (3)\\
\leq\ & \left|Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m_0)) = 1 \ \& \ \overline{Q}\right] - Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m_1)) = 1 \ \& \ \overline{Q}\right]\right| && (4)\\
& + \left|Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m_0)) = 1 \ \& \ Q\right] - Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m_1)) = 1 \ \& \ Q\right]\right| && (5)\\
\leq\ & \max_{m\in\{m_0,m_1\}} Pr\left[A^{RO,\overline{E},\overline{D}}(pk, \overline{E}(m)) = 1 \ \& \ Q\right] && (6)\\
& + \left|Pr\left[B^{E,D}(E(m_0)) = 1\right] - Pr\left[B^{E,D}(E(m_1)) = 1\right]\right| && (7)
\end{aligned}$$

By the assumption on (1), (6) or (7) must be non-negligible. If (7) is non-negligible, then B breaks the security of (E, D). If not, then (6) is non-negligible. In this case, we show that we can construct an adversary C that breaks the TOWP.

$C(pk, y) :=$

1. sample sk^*
2. $c \leftarrow E(sk^*, m_0)$
3. $\overline{c} \leftarrow (y, c)$
4. Initialize list $\mathcal{L} = \{(\perp, y, sk^*)\}$
5. Simulate $A^{RO,\overline{E},\overline{D}}(\overline{c})$ where
   - $RO(z) :=$
     1. compute $y_z = \text{Eval}(pk, z)$
     2. if $y_z = y$, halt and output z.
     3. look in $\mathcal{L}$ and see if it contains $(\perp, y_z, sk)$ or (z, y_z, sk). If so, return sk, and in the first case, replace $\perp$ with z.
     4. sample sk, add (z, y_z, sk) to $\mathcal{L}$ and answer sk.
   - $\overline{E}(m_i) :=$
     1. sample x_i
     2. $y_i \leftarrow \text{Eval}(pk, x_i)$
     3. $c_i \leftarrow E(RO(x_i), m_i)$
     4. output (y_i, c_i)
   - $\overline{D}(\overline{c}_i) :=$
     1. if $(\cdot, y_i, sk_i) \in \mathcal{L}$ then return $D(sk_i, c_i)$
     2. sample sk_i, add $(\perp, y_i, sk_i)$ to $\mathcal{L}$. Output $D(sk_i, c_i)$.

C succeds in inverting the TOWP whenever Q occurs, which occurs with probability lower bounded by (6). Thus if (6) is non-negligible, then C succeeds with non-negligible probability, contradicting the security of the TOWP.

□

2 Signature Schemes

A signature scheme is the asymmetric analogue of a MAC. The setting is as follows. Alice has a public key pk and secret key sk, and she wants to send a message m with a signature σ to Bob in the presence of an active adversary Eve, such that the following properties are satisfied.

- *Completeness*: Alice can sign any message so that anyone else can verify the signature.
- *Security*: No one other than Alice can produce signatures on new messages.
- *Syntax*: (G, S, V)
  - $G(1^k) \to (pk, sk)$
  - $S(1^k, sk, m) \to \sigma$
  - $V(1^k, pk, m, \sigma) \to b$ where $b \in \{0, 1\}$

Definition 2 *A* signature scheme *is a triple* (G, S, V) *such that the following hold.*

1. Completeness: $\forall k \in \mathbb{N}$, $\forall (pk, sk) \in G(1^k)$, $\forall m \in \{0,1\}^{n(k)}$,
$$Pr[V(pk, m, S(sk, m)) = 1] = 1\,.$$
2. Security: *via existential unforgeability under chosen message attack. For all ppt* A, $Pr[A^{S(sk,\cdot)}(pk) forges]$ *is negligible in* k, *where "forges" means to output* (m, σ) *such that*
   (a) $V(pk, m, \sigma) = 1$.
   (b) m *not a query to* S.

Remark 3 *Signatures are transferrable. For example, Bob could take Alice's message and signature, and forward them to another party who can verify that Alice sent the message. This was not the case for MACs. Signatures are also non-repudiable.*