Applied Cryptography

Lecture Note

Spring 2023

Cao, Ganyuan

Contents

1 Security Proof

1.1 Game-based Security Proof Framework

To prove the statment: *"If a scheme F_1 is $\mathcal{S}_1$ secure, then a scheme F_2 is $\mathcal{S}_2$ secure"*, we follow the steps:

1. Suppose by contraposition that there is an adversary $\mathcal{A}$ against $\mathcal{S}_2$ security of F_2 s.t. $\mathbf{Adv}^{\mathcal{S}_2}_{\mathsf{F}_2}(\mathcal{A})$ is not negligible.
2. Construct the adversary $\mathcal{B}$ against $\mathcal{S}_1$ security of F_1 with $\mathcal{A}$ as subroutine.
3. Deduce that $\mathbf{Adv}^{\mathcal{S}_1}_{\mathsf{F}_1}(\mathcal{B})$ is not negligible.

Remarks:

1. Assume that $\mathcal{B}$ is given an oracle $\mathrm{O}_{\mathcal{B}}$, we use $\mathrm{O}_{\mathcal{B}}$ to simulate the pre-defined oracle for $\mathrm{O}_{\mathcal{A}}$. In the adversary $\mathcal{B}$, the adversary $\mathcal{A}$ instead calls the simulation oracle $\mathrm{OS{\scriptsize IM}}_{\mathcal{A}}$.
2. The adversary $\mathcal{B}$ together with the oracle $\mathrm{OS{\scriptsize IM}}_{\mathcal{A}}$ simulates the $\mathcal{S}_2$ security game of F_2.
3. The framework also works for problem reduction. If we want to prove a problem $\mathcal{P}_1$ reduces to a problem $\mathcal{P}_2$, it is equivalent to prove *"if there is an adversary that break the problem $\mathcal{P}_2$ with non-negligible advantage, then there is an adversary $\mathcal{B}$ that break $\mathcal{P}_1$ with non-negligible advantage."*
4. In the case that the primitive $\mathcal{S}_1$ is too "far" from $\mathcal{S}_2$, and *distinguishibility* game in involved, it is better to use "game-chaining" method by decomposing the distinguishibility game into sub-games and chain the sub-games to prove the advantage. Note that the framework proposed by Ballare can be used to write the games for better readability.

1.2 Advantage Rewriting Lemma

Let b be a uniformly random bit, b' be the output of some algorithm. Then

$$\begin{aligned} 2\left|\Pr[b' = b] - \frac{1}{2}\right| &= \left|\Pr[b' = 1|b = 1] - \Pr[b' = 1|b = 0]\right| \\ &= \left|\Pr[b' = 0|b = 0] - \Pr[b' = 0|b = 1]\right| \end{aligned}$$

Proof.

$$\begin{aligned} \Pr[b' = b] - \frac{1}{2} &= \Pr[b' = b \mid b = 1] \cdot \Pr[b = 1] + \Pr[b' = b \mid b = 0] \cdot \Pr[b = 0] - \frac{1}{2} \\ &= \Pr[b' = b \mid b = 1] \cdot \frac{1}{2} + \Pr[b' = b \mid b = 0] \cdot \frac{1}{2} - \frac{1}{2} \\ &= \frac{1}{2}(\Pr[b' = 1 \mid b = 1] + \Pr[b' = 0 \mid b = 0] - 1) \\ &= \frac{1}{2}(\Pr[b' = 1 \mid b = 1] - (1 - \Pr[b' = 0 \mid b = 0])) \\ &= \frac{1}{2}(\Pr[b' = 1 \mid b = 1] - \Pr[b' = 1 \mid b = 0]) \end{aligned}$$

$\square$

1.3 The Difference Lemma

Let Z, W_1, W_2 be (any) events defined over some probability space. Suppose that $\Pr[W_1 \wedge \neg Z] = \Pr[W_2 \wedge \neg Z]$. Then we have $|\Pr[W_2] - \Pr[W_1] \leq \Pr[Z]|$. (In typical uses, we have that $(W_1 \wedge \neg Z)$ occurs if and only if $(W_2 \wedge Z)$ occurs)

Proof.

$$\begin{aligned}
|\Pr[W_2] - \Pr[W_1]| &= |\Pr[(W_1 \wedge Z) \vee (W_1 \wedge \neg Z)] - \Pr[(W_2 \wedge Z) \vee (W_2 \wedge \neg Z)]| \\
&= |\Pr[W_1 \wedge Z] + \Pr[W_1 \wedge \neg Z] - \Pr[W_2 \wedge Z] - \Pr[W_2 \wedge \neg Z]| \\
&= |\Pr[W_1 \wedge Z] - \Pr[W_2 \wedge Z]| \\
&\leq \Pr[Z]
\end{aligned}$$

□

2 Symmetric Encryption

2.1 Pseudorandom Permutation/Function

2.1.1 PRP Security

Let games be defined as in Figure 1 (or Figure 2), a block cipher E is defined to be (q, t, ε)-secure as a *pseudorandom permutation* (PRP), if for any adversary $\mathcal{A}$ running in time at most t and making at most q queries to the oracle $\textsc{Enc}$, the advantage $\mathbf{Adv}_E^{\mathrm{PRP}}(\mathcal{A}) \leq \varepsilon$ where

$$\begin{aligned}\mathbf{Adv}_E^{\mathrm{PRP}}(\mathcal{A}) &= 2 \cdot \left| \Pr[\mathrm{G}^{\mathrm{PRP}}(\mathcal{A}) \Rightarrow \mathsf{true}] - \frac{1}{2} \right| \\ &= \left| \Pr[\mathrm{G}^{\mathbf{PRP\text{-}0}}(\mathcal{A})] - \Pr[\mathrm{G}^{\mathbf{PRP\text{-}1}}(\mathcal{A})] \right|\end{aligned}$$

Game $\mathrm{G}_{\mathbf{PRP}}$

procedure $\textsc{Init}$

$b \leftarrow\!\!\$\ \{0,1\}$
$K \leftarrow\!\!\$\ \{0,1\}^k$
$\pi \leftarrow\!\!\$\ \mathcal{P}_n$

procedure $\textsc{Finalize}$

$b' \leftarrow\!\!\$\ \mathcal{A}^{\textsc{Enc}}(\cdot)$
return $b' = b$

Oracle $\textsc{Enc}(M)$

if $b = 0$ **then**
  $y \leftarrow E_K(M)$
else
  $y \leftarrow \pi(M)$
return y

Figure 1: PRP game for a block cipher E in the first style. Here $\mathcal{P}_n$ represents the set of permutations on length n.

$\mathrm{G}^{\mathbf{PRP\text{-}0}}$

procedure $\textsc{Init}$

$K \leftarrow\!\!\$\ \{0,1\}^\kappa$

procedure $\textsc{Enc}(M)$

$C \leftarrow E_K(M)$
return C

$\mathrm{G}^{\mathbf{PRP\text{-}1}}$

procedure $\textsc{Init}$

$\pi \leftarrow\!\!\$\ \mathcal{P}_n$

procedure $\textsc{Enc}(M)$

$C \leftarrow \pi(M)$
return C

Figure 2: PRP game for a block cipher E in the second style.

2.1.2 PRF Security

Let games be defined as in Figure 3 (or Figure 4), a block cipher E is defined to be (q, t, ε)-secure as a *pseudorandom function* (PRF), if for any adversary $\mathcal{A}$ running in time at most t and making at most q queries to $\textsc{Enc}$, the advantage $\mathbf{Adv}_E^{\mathrm{PRF}}(\mathcal{A}) \leq \varepsilon$ where

$$
\begin{aligned}
\mathbf{Adv}_E^{\mathrm{PRF}}(\mathcal{A}) &= 2 \cdot \left| \Pr[\mathrm{G}^{\mathrm{PRF}}(\mathcal{A}) \Rightarrow \mathsf{true}] - \frac{1}{2} \right| \\
&= \left| \Pr[\mathrm{G}^{\mathrm{PRF\text{-}0}}(\mathcal{A})] - \Pr[\mathrm{G}^{\mathrm{PRF\text{-}1}}(\mathcal{A})] \right|
\end{aligned}
$$

Game $\mathrm{G}^{\mathrm{PRF}}$

procedure INIT
- $b \leftarrow\!\!\$\ \{0,1\}$
- $K \leftarrow\!\!\$\ \{0,1\}^k$
- $\rho \leftarrow\!\!\$\ \mathcal{F}_n$

procedure FINALIZE
- $b' \leftarrow\!\!\$\ \mathcal{A}^{\textsc{Enc}}(\cdot)$
- **return** $b' = b$

Oracle $\textsc{Enc}(M)$
- **if** $b = 0$ **then**
  - $y \leftarrow E_K(M)$
- **else**
  - $y \leftarrow \rho(M)$
- **return** y

Figure 3: PRF game for a block cipher E in the first style.

$\mathrm{G}^{\mathrm{PRF\text{-}0}}$

procedure INIT
- $K \leftarrow\!\!\$\ \{0,1\}^\kappa$

procedure $\textsc{Enc}(M)$
- $C \leftarrow E_K(M)$
- **return** C

$\mathrm{G}^{\mathrm{PRF\text{-}1}}$

procedure INIT
- $\rho \leftarrow\!\!\$\ \mathcal{F}_n$

procedure $\textsc{Enc}(M)$
- $C \leftarrow \rho(M)$
- **return** C

Figure 4: PRF games for a block cipher E in the second style.

2.2 Ciphertext Indistinguishability

2.2.1 LoR-CPA Security

A symmetric encryption scheme SE is said to have (q,t,ε)-*indistinguishability under chosen plaintext attack with left-or-right oracle* (LoR-CPA), if for any adversaries $\mathcal{A}$ running in time at most t and making at most q encryption queries, the advantage $\mathbf{Adv}_{\mathsf{SE}}^{\mathrm{LoR\text{-}CPA}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}_{\mathsf{SE}}^{\mathrm{LoR\text{-}CPA}}(\mathcal{A}) = 2 \cdot | \Pr[\mathrm{G}^{\mathrm{LoR\text{-}CPA}}(\mathcal{A}) \Rightarrow \mathsf{true}] - \frac{1}{2}|$$

$\mathrm{G}^{\text{LoR-CPA}}$

procedure INIT

$b \leftarrow\!\$ \{0,1\}$

$K \leftarrow\!\$ \mathcal{K}$

procedure FINALIZE

$b' \leftarrow\!\$ \mathcal{A}^{\textsc{Enc}}(\cdot)$

return $b' = b$

Oracle $\textsc{Enc}(N, M_0, M_1)$

if $|M_0| \neq |M_1|$ **then**

  return $\perp$

$C \leftarrow\!\$ \mathcal{E}_K^N(M_b)$

return C

Figure 5: LoR-CPA Game for a SE scheme Π.

2.2.2 RoR-CPA Security

A symmetric encryption scheme SE is said to have (q, t, ε)-*indistinguishibility under chosen plaintext attack with real-or-random oracle* (RoR-CPA), if for any adversaries $\mathcal{A}$ running in time at most t and making at most q encryption queries, the advantage $\mathbf{Adv}_{\mathsf{SE}}^{\text{RoR-CPA}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}_{\mathsf{SE}}^{\text{RoR-CPA}}(\mathcal{A}) = \left|\Pr[\mathrm{G}^{\text{RoR-CPA-0}}(\mathcal{A})] - \Pr[\mathrm{G}^{\text{RoR-CPA-1}}(\mathcal{A})]\right|$$

$\mathrm{G}^{\text{RoR-CPA-0}}$

procedure INIT

$K \leftarrow\!\$ \mathcal{K}$

$\mathcal{Q} \leftarrow \emptyset$

procedure $\textsc{Enc}(N, M)$

if $(N, M) \in \mathcal{Q}$ **then**

  return $\perp$

$C \leftarrow \mathcal{E}_K^N(M)$

$\mathcal{Q} \leftarrow \mathcal{Q} \cup \{(N, M)\}$

return C

$\mathrm{G}^{\text{RoR-CPA-1}}$

procedure INIT

$\mathcal{Q} \leftarrow \emptyset$

procedure $\textsc{Enc}(N, M)$

if $(N, M) \in \mathcal{Q}$ **then**

  return $\perp$

$C \leftarrow\!\$ \{0,1\}^{|M|}$

$\mathcal{Q} \leftarrow \mathcal{Q} \cup \{(N, M)\}$

return C

Figure 6: RoR-CPA game for a SE scheme Π

Remarks:

1. IND-CPA security imples decryption security.
2. IND-CPA security implies key recovery (TKR) security.
3. IND-CPA security ensures that every bit of the plaintext is hidden.
4. One-time Pad is IND-CPA is 1-query IND-CPA secure.

5. Here oracle LoR refers to "left or right".

6. A special form of IND-CPA security, which formalize the indistinguishability of a symmetric encryption scheme from random bits, named IND\$-CPA, is defined as in Figure 5.

2.2.3 LoR-CCA Security

A symmetric encryption scheme SE is defined to be $(q_e, q_d, t, \varepsilon)$-*indistinguishibility under chosen ciphertext attack* secure (IND-CCA), if for any adversaries $\mathcal{A}$ running in time at most t and making at most q_e encryption queries to oracle LoR and at most q_d decryption queries to oracle ODec, the advantage $\mathbf{Adv}_{\mathsf{SE}}^{\text{IND-CPA}}(\mathcal{A}) \leq \varepsilon$.

$$\mathbf{Adv}_{\mathsf{SE}}^{\text{LoR-CCA}}(\mathcal{A}) = 2 \cdot |\mathrm{G}^{\text{LoR-CCA}}(\mathcal{A}) \Rightarrow \mathsf{true}] - \frac{1}{2}|$$

$\mathrm{G}^{\text{LoR-CCA}}$

procedure Init
- $b \leftarrow\!\!\$ \{0,1\}$
- $K \leftarrow\!\!\$ \mathcal{K}$
- $\mathcal{Q}_d \leftarrow \emptyset$

Oracle Dec(N, C)
- **if** $(N, C) \in \mathcal{Q}$ **then**
  - **return** $\perp$
- $M \leftarrow \mathcal{D}_K^N(C)$
- $\mathcal{Q}_d \leftarrow \mathcal{Q}_d \cup \{(N, C)\}$
- **return** M

Oracle Enc(N, M_0, M_1)
- **if** $|M_0| \neq |M_1|$ **then**
  - **return** $\perp$
- $C \leftarrow\!\!\$ \mathcal{E}_K^N(M_b)$
- **return** C

procedure Finalize
- $b' \leftarrow\!\!\$ \mathcal{A}^{\text{Enc,Dec}}(\cdot)$
- **return** $b' = b$

Figure 7: LoR-CPA Game for a SE scheme Π.

2.2.4 RoR-CCA Security

A symmetric encryption scheme SE is said to have (q, t, ε)-*indistinguishibility under chosen plaintext attack with real-or-random oracle* (RoR-CPA), if for any adversaries $\mathcal{A}$ running in time at most t and making at most q encryption queries, the advantage $\mathbf{Adv}_{\mathsf{SE}}^{\text{RoR-CPA}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}_{\mathsf{SE}}^{\text{RoR-CPA}}(\mathcal{A}) = \left|\Pr[\mathrm{G}^{\text{RoR-CPA-0}}(\mathcal{A})] - \Pr[\mathrm{G}^{\text{RoR-CPA-1}}(\mathcal{A})]\right|$$

2.3 Message Integrity

2.3.1 INT-CTXT Security

A symmetric encryption scheme SE is said to have $(q_e, q_d, t, \varepsilon)$-*ciphertext integrity* (INT-CTXT) secure, if for any adversary $\mathcal{A}$ running in time t and making at most q_e encryption

$\mathrm{G}^{\text{RoR-CCA-0}}$

procedure INIT

$K \leftarrow\!\!\$\ \mathcal{K}$

$\mathcal{Q}_e, \mathcal{Q}_d \leftarrow \emptyset$

procedure ENC(N, M)

if $(N, M) \in \mathcal{Q}_e$ **then**

  return $\perp$

$C \leftarrow \mathcal{E}_K^N(M)$

$\mathcal{Q}_e \leftarrow \mathcal{Q}_e \cup \{(N, M)\}$

$\mathcal{Q}_d \leftarrow \mathcal{Q}_d \cup \{(N, C)\}$

return C

procedure DEC(N, C)

if $(N, C) \in \mathcal{Q}_d$ **then**

  return $\perp$

$M \leftarrow \mathcal{D}_K^N(C)$

return C

$\mathrm{G}^{\text{RoR-CCA-1}}$

procedure INIT

$\mathcal{Q}_e, \mathcal{Q}_d \leftarrow \emptyset$

procedure ENC(N, M)

if $(N, M) \in \mathcal{Q}_e$ **then**

  return $\perp$

$C \leftarrow\!\!\$\ \{0,1\}^{|M|}$

return C

procedure DEC(N, C)

$C \leftarrow \mathcal{D}_K^N(N, C)$

return C

Figure 8: RoR-CPA game for a SE scheme Π

oracle queries and exact one try query to oracle OTRY, the advantage $\mathbf{Adv}_{\mathsf{SE}}^{\mathrm{INT-CTXT}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}_{\mathsf{SE}}^{\mathrm{INT-CTXT}}(\mathcal{A}) = \Pr[\mathrm{G}^{\text{INT-CTXT}}(\mathcal{A}) \Rightarrow 1]$$

$\mathrm{G}^{\text{INT-CTXT}}$

procedure INIT

$K \leftarrow\!\!\$\ \mathcal{K}$

$\mathcal{Q} \leftarrow \emptyset$

$\mathsf{win} \leftarrow \mathsf{false}$

procedure ENC(M)

$C \leftarrow \mathcal{E}_K(M)$

$\mathcal{Q} \leftarrow \mathcal{Q} \cup \{C\}$

return C

procedure DEC(C)

$M \leftarrow \mathcal{D}_K(C)$

if $C \notin \mathcal{Q} \wedge M \neq \perp$ **then**

  $\mathsf{win} \leftarrow \mathsf{true}$

return $(M \neq \perp)$

procedure FINALIZE

return win

Figure 9: INT-CTXT game for a LPSE scheme Π

2.3.2 INT-PTXT Security

A symmetric encryption scheme Π is said to be (q_e, t, ε)-*plaintext integrity* (INT-PTXT) secure if for all adversary $\mathcal{A}$ running in time t and making at most q_e encryption oracle queries with $\mathbf{Adv}_{\Pi}^{\mathrm{INT-PTXT}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}_{\Pi}^{\text{INT-PTXT}}(\mathcal{A}) = \Pr[\mathrm{G}^{\text{INT-PTXT}}(\mathcal{A}) \Rightarrow 1]$$

$\mathrm{G}^{\text{INT-PTXT}}$

procedure Init

$K \leftarrow\!\!\$\ \mathcal{K}$

$\mathcal{Q} \leftarrow \emptyset$

$\mathsf{win} \leftarrow \mathsf{false}$

procedure Enc(M)

$C \leftarrow \mathcal{E}_K(M)$

$\mathcal{Q} \leftarrow \mathcal{Q} \cup \{M\}$

return C

procedure Dec(C)

$M \leftarrow \mathcal{D}_K(C)$

if $C \notin \mathcal{Q} \wedge M \neq \bot$ **then**

  $\mathsf{win} \leftarrow \mathsf{true}$

return $(M \neq \bot)$

procedure Finalize

return win

Figure 10: INT-PTXT game for a LPSE scheme Π

Theorem 1. *If a symmetric encryption scheme* Π *is* INT-CTXT *secure, then it is also* INT-PTXT *secure.*

Proof. We prove by contraposition that if is not INT-CTXT, then it is not INT-PTXT. Let $\mathcal{A}$ be a INT-CTXT adversary against , we construct an adversary $\mathcal{B}$ against INT-PTXT of such that $\mathcal{B}$ runs $\mathcal{A}$ and replys $\mathcal{A}$'s queries to $\mathcal{B}$'s OEnc and OTry.

We have that $\mathcal{B}$ simulates the INT-CTXT game of $\mathcal{A}$ since $\mathcal{B}$ makes the exact the same number of queries as $\mathcal{A}$ and $\mathcal{B}$ returns the same c^* as $\mathcal{A}$.

We have that $\mathcal{B}$ wins if $\mathcal{A}$ wins. Let c^* be the ciphertext query $\mathcal{A}$ makes to OTry. Since $\mathcal{A}$ wins, we have that $c^* \notin \mathcal{Q}_c$, which implies $m^* \notin \mathcal{Q}_m$ where $m^* = \textsc{Dec}(K, c^*)$. Thus $\mathcal{B}$ wins if $\mathcal{A}$ wins.

$\square$

3 Hash Function

3.1 Collision Resistance

Let $H : \mathcal{D} \to \mathcal{R}$ be a hash function. An algorithm $\mathcal{A}$ is said to be (t, ε) *collision resistance* (CR) adversary against H if $\mathcal{A}$ runs in time t with advantage

$$\mathbf{Adv}_H^{\mathrm{CR}}(\mathcal{A}) = \Pr[\mathrm{G}^{\mathrm{CR}} \Rightarrow 1] = \varepsilon$$

$\mathrm{G}^{\mathbf{CR}}$

procedure

```
(m, m') ←$ A(·)
if m ≠ m' ∧ H(m) = H(m') then
    return 1
else
    return 0
```

Figure 11: Collision Resistance (CR) Game

Remarks:

1. Collision must exist because $|\mathcal{D}| \gg |\mathcal{R}|$.
2. Fix a hash function H, there must be an efficient algorithm $\mathcal{A}$ that outputs collisions.
3. Thus we cannot have a security definition for collision resistance that quantifies over all efficient algorithms $\mathcal{A}$.

3.1.1 Second Pre-image Resistance

Let $H : \mathcal{D} \to \mathcal{R}$ be a hash function. An algorithm $\mathcal{A}$ is said to be (t, ε) *second preimage* (2PRE) adversary against H if $\mathcal{A}$ runs in time t with advantage

$$\mathbf{Adv}_H^{\mathrm{2PRE}}(\mathcal{A}) = \Pr[\mathrm{G}^{\mathrm{2PRE}} \Rightarrow 1] = \varepsilon$$

3.1.2 Pre-image Resistance

Let $H : \mathcal{D} \to \mathcal{R}$ be a hash function. An algorithm $\mathcal{A}$ is said to be (t, ε) *preimage resistance* (PRE) adversary against H if $\mathcal{A}$ runs in time t with advantage

$$\mathbf{Adv}_H^{\mathrm{PRE}}(\mathcal{A}) = \Pr[\mathrm{G}^{\mathrm{PRE}}(\mathcal{A}) \Rightarrow 1] = \varepsilon$$

$\mathrm{G}^{\mathbf{2PRE}}$

procedure

$m \leftarrow\!\!\$\ \mathcal{D}$
$h \leftarrow H(m)$
$m' \leftarrow\!\!\$\ \mathcal{A}(m, h)$
if $m \neq m' \wedge H(m') = h$ **then**
  return 1
else
  return 0

$\mathrm{G}^{\mathbf{PRE}}$

procedure

$h \leftarrow\!\!\$\ \mathcal{R}$
$m \leftarrow\!\!\$\ \mathcal{A}(h)$
if $H(m) = h$ **then**
  return 1
else
  return 0

Figure 12: **Left**: Second Preimage Resistance (2PRE) Game. **Right**: Preimage Resistance (PRE) Game

3.1.3 One-wayness

Let $H : \mathcal{D} \to \mathcal{R}$ be a hash function. An algorithm $\mathcal{A}$ is said to be (t, ε) *one-wayness* (OWF) adversary against H if $\mathcal{A}$ runs in time t with advantage

$$\mathbf{Adv}_H^{\mathrm{OWF}}(\mathcal{A}) = \Pr[\mathrm{G}^{\mathrm{OWF}}(\mathcal{A}) \Rightarrow 1] = \varepsilon$$

$\mathrm{G}^{\mathbf{OWF}}$

procedure

$m \leftarrow\!\!\$\ \mathcal{D}$
$h \leftarrow H(m)$
$m' \leftarrow\!\!\$\ \mathcal{A}(h)$
if $H(m') = h$ **then**
  return 1
else
  return 0

Figure 13: One-wayness (OWF) Game

3.1.4 Universal Hashing

A keyed hash funcion H is an ε-bounded *universal hash function* (ε-UHF) if for any adversary $\mathcal{A}$, the advantage $\mathbf{Adv}_H^{\mathrm{UHF}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}_H^{\mathrm{UHF}}(\mathcal{A}) = \Pr[\mathrm{G}^{\mathrm{UHF}}(\mathcal{A}) \Rightarrow 1]$$

$\mathrm{G}^{\mathbf{UHF}}$

procedure

$K \leftarrow\!\!\$\ \mathcal{K}$
$(m_0, m_1) \leftarrow\!\!\$\ \mathcal{A}(\cdot)$
if $H(K, m_0) = H(K, m_1)$
  $\wedge\, m_0 \neq m_1$ **then**
  return 1
else
  return 0

Figure 14: UHF Game

3.1.5 Difference Unpredictable Hashing

A keyed hash function H with digest space $\mathcal{T}$ equipped with a group operation "+", is an ε-bounded *difference unpredictable hashing function* if for any adversary $\mathcal{A}$, the advantage $\mathbf{Adv}_H^{\mathrm{DUHF}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}_H^{\mathrm{DUHF}}(\mathcal{A}) = \Pr[\mathrm{G}^{\mathrm{DUHF}}(\mathcal{A}) \Rightarrow 1]$$

$\mathrm{G}^{\mathbf{DUHF}}$

procedure

$K \leftarrow\!\!\$\ \mathcal{K}$
$(m_0, m_1, \delta) \leftarrow\!\!\$\ \mathcal{A}(\cdot)$
if $H(K, m_0) - H(K, m_1) = \delta$
  $\wedge\, m_0 \neq m_1$ **then**
  return 1
else
  return 0

Figure 15: DUHF Game

4 Message Authentication Code

4.1 EUF-CMA Security

A MAC scheme is $(q_t, q_v, t, \varepsilon)$-*existential unforgeability under chosen message attack* (EUF-CMA) secure, if for any adversaries making q_t queries to tagging oracle OTAG, q_v queries to verification OVFY, and running in time at most t, the advantage $\mathbf{Adv}^{\text{EUF-CMA}}_{\text{MAC}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}^{\text{EUF-CMA}}_{\text{MAC}}(\mathcal{A}) = \Pr[\mathrm{G}^{\text{EUF-CMA}}(\mathcal{A}) \Rightarrow 1]$$

4.2 SUF-CMA Security

A MAC scheme is $(q_t, q_v, t, \varepsilon)$-*strong existential unforgeability under chosen message attack* (SUF-CMA) secure, if for any adversaries making q_t queries to tagging oracle OTAG, q_v queries to verification oracle OVFY, and running in time at most t, the advantage $\mathbf{Adv}^{\text{SUF-CMA}}_{\text{MAC}}(\mathcal{A}) \leq \varepsilon$ where

$$\mathbf{Adv}^{\text{SUF-CMA}}_{\text{MAC}}(\mathcal{A}) = \Pr[\mathrm{G}^{\text{SUF-CMA}}(\mathcal{A}) \Rightarrow 1]$$

$\mathrm{G}^{\text{EUF-CMA}}$ $\boxed{\mathrm{G}^{\text{EUF-CMA}}}$

procedure INIT

$K \leftarrow\!\!\$\ \mathcal{K}$

$\mathcal{Q} \leftarrow \emptyset$

procedure FINALIZE

$(m^*, \tau^*) \leftarrow\!\!\$\ \mathcal{A}^{\text{TAG},\text{VFY}}(\cdot)$

if $(m^*, \boxed{\tau^*}) \in \mathcal{Q}$ **then**

  return 0

else

  $b \leftarrow \mathcal{V}_K(m, \tau)$

  return b

Oracle TAG(m)

$\tau \leftarrow \mathcal{T}_K(m)$

$\mathcal{Q} \leftarrow \mathcal{Q} \cup \{(m, \boxed{\tau})\}$

return τ

Oracle VFY(m, τ)

$b \leftarrow \mathcal{V}_K(m, \tau)$

return b

Figure 16: EUF-CMA and SUF-CMA Game for a MAC scheme. The dox-boxed code is exclusive for $\mathrm{G}^{\text{SUF-CMA}}$.