

APPLIED CRYPTOGRAPHY

LECTURE NOTE

SPRING 2023

CAO, GANYUAN

Contents

1	Security Proof	2
1.1	Game-based Security Proof Framework	2
1.2	Advantage Rewriting Lemma	2
1.3	The Difference Lemma	3
2	Symmetric Encryption	4
2.1	Pseudorandom Permutation/Function	4
2.1.1	PRP Security	4
2.1.2	PRF Security	4
2.2	Ciphertext Indistinguishability	5
2.2.1	LoR-CPA Security	5
2.2.2	RoR-CPA Security	6
2.2.3	LoR-CCA Security	7
2.2.4	RoR-CCA Security	7
2.3	Message Integrity	7
2.3.1	INT-CTXT Security	7
2.3.2	INT-PTXT Security	9
3	Hash Function	10
3.1	Collision Resistance	10
3.1.1	Second Pre-image Resistance	10
3.1.2	Pre-image Resistance	10
3.1.3	One-wayness	11
3.1.4	Universal Hashing	11
3.1.5	Difference Unpredictable Hashing	12
4	Message Authentication Code	13
4.1	EUF-CMA Security	13
4.2	SUF-CMA Security	13

1 Security Proof

1.1 Game-based Security Proof Framework

To prove the statement: "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. $\mathbf{Adv}_{F_2}^{\mathcal{S}_2}(\mathcal{A})$ 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 $\mathbf{Adv}_{F_1}^{\mathcal{S}_1}(\mathcal{B})$ is not negligible.

Remarks:

1. Assume that \mathcal{B} is given an oracle $O_{\mathcal{B}}$, we use $O_{\mathcal{B}}$ to simulate the pre-defined oracle for $O_{\mathcal{A}}$. In the adversary \mathcal{B} , the adversary \mathcal{A} instead calls the simulation oracle $OSIM_{\mathcal{A}}$.
2. The adversary \mathcal{B} together with the oracle $OSIM_{\mathcal{A}}$ 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 *distinguishability* game is involved, it is better to use "game-chaining" method by decomposing the distinguishability 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

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

Proof.

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

□

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 ENC, the advantage $\mathbf{Adv}_E^{\text{PRP}}(\mathcal{A}) \leq \varepsilon$ where

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

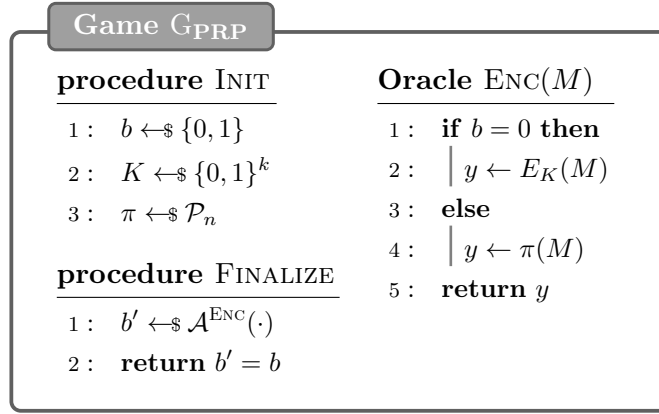


Figure 1: PRP game for a block cipher E in the first style. Here \mathcal{P}_n represents the set of permutations on length n .

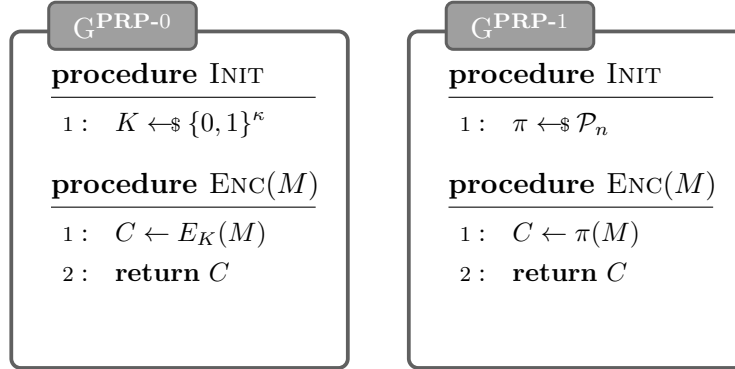


Figure 2: PRP game for a block cipher E in the second style.

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 ENC, the advantage $\mathbf{Adv}_E^{\text{PRF}}(\mathcal{A}) \leq \varepsilon$ where

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

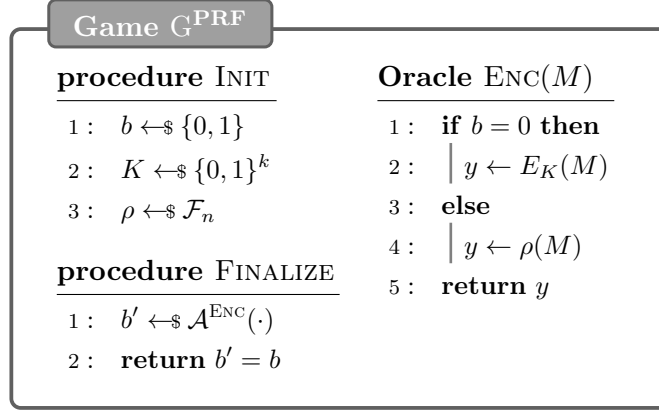


Figure 3: PRF game for a block cipher E in the first style.

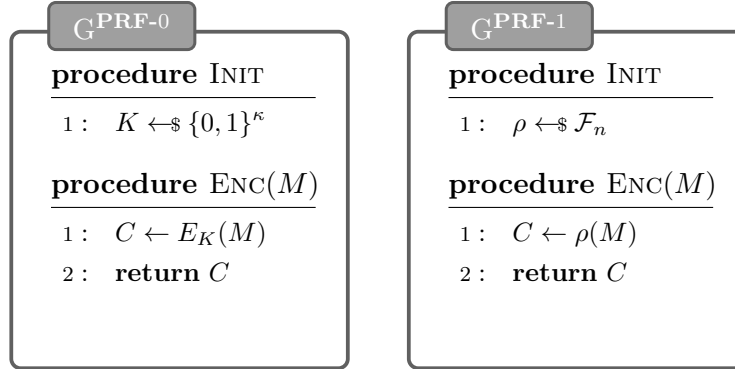


Figure 4: PRF games for a block cipher E in the second style.

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 $\mathbf{Adv}_{\text{SE}}^{\text{LoR-CPA}}(\mathcal{A}) \leq \varepsilon$ where

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

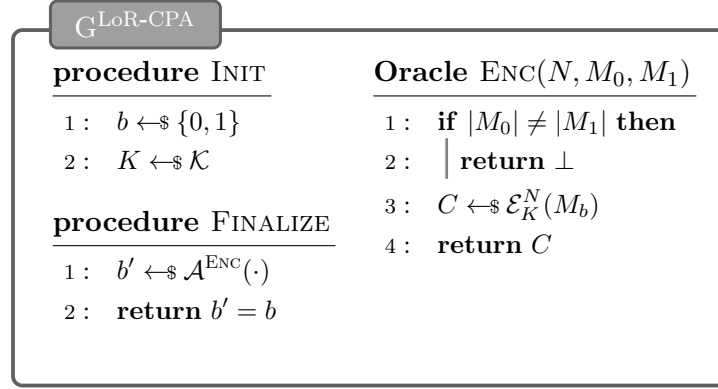


Figure 5: LoR-CPA Game for a SE scheme Π .

2.2.2 RoR-CPA Security

A symmetric encryption scheme SE is said to have (q, t, ε) -indistinguishability 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 $\text{Adv}_{\text{SE}}^{\text{RoR-CPA}}(\mathcal{A}) \leq \varepsilon$ where

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

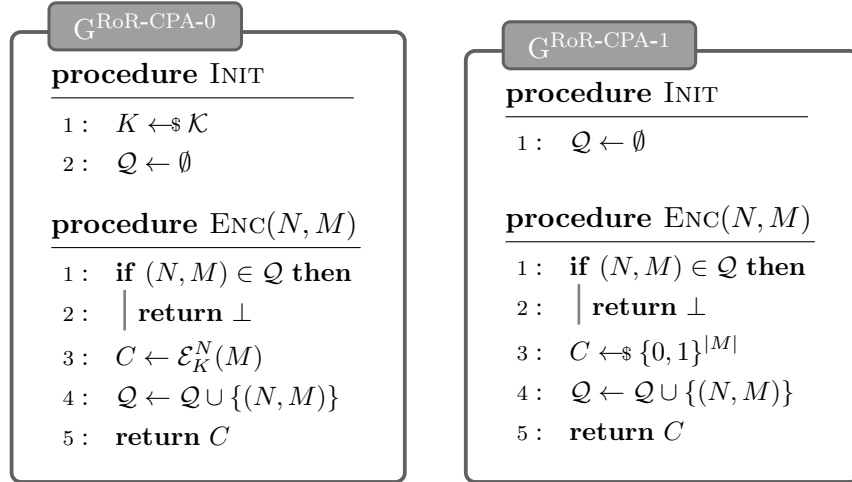


Figure 6: RoR-CPA game for a SE scheme Π

Remarks:

1. IND-CPA security implies 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 $(q_e, q_d, t, \varepsilon)$ -*indistinguishability 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 $\text{Adv}_{\text{SE}}^{\text{IND-CPA}}(\mathcal{A}) \leq \varepsilon$.

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

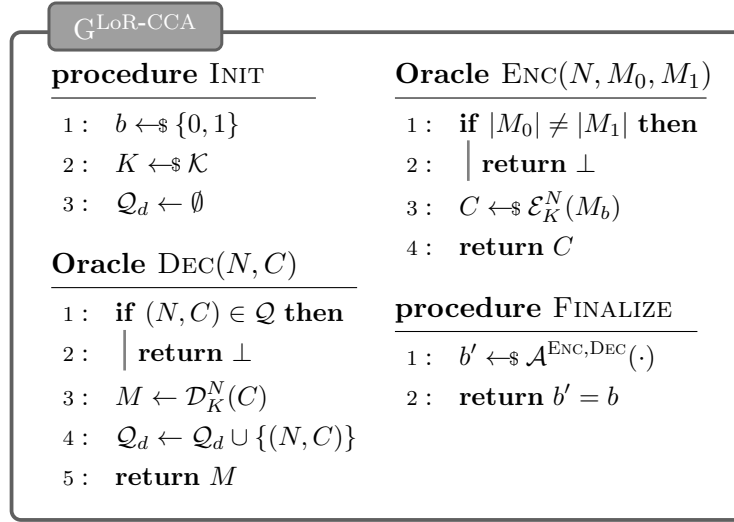


Figure 7: LoR-CPA Game for a SE scheme Π .

2.2.4 RoR-CCA Security

A symmetric encryption scheme SE is said to have (q, t, ε) -*indistinguishability 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 $\text{Adv}_{\text{SE}}^{\text{RoR-CPA}}(\mathcal{A}) \leq \varepsilon$ where

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

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

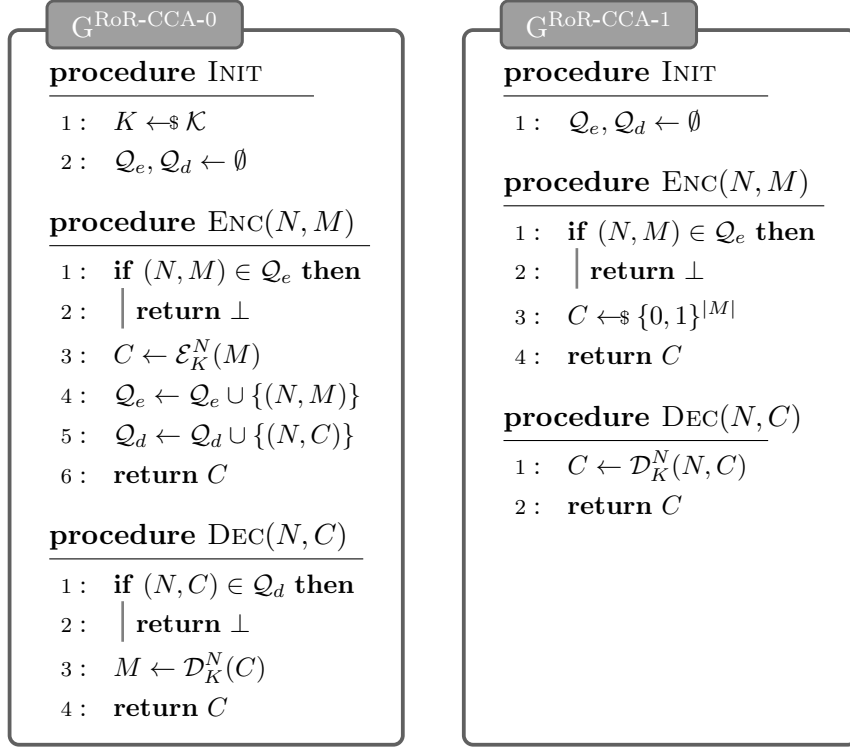


Figure 8: RoR-CPA game for a SE scheme Π

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

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

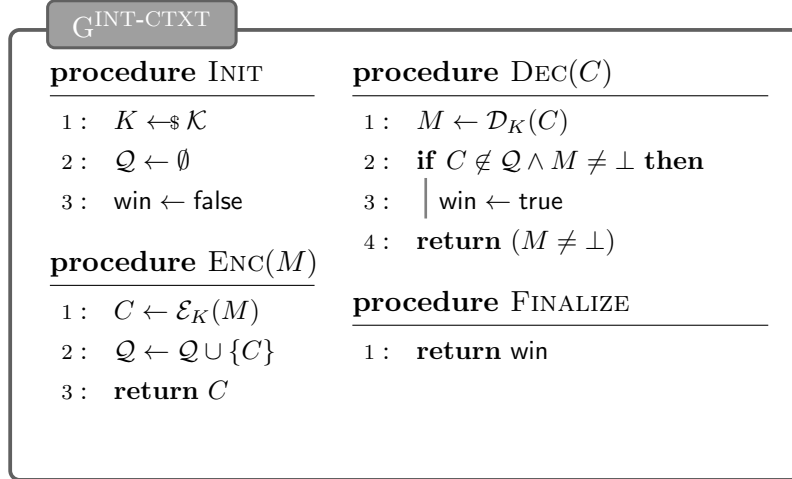


Figure 9: INT-CTXT game for a LPSE scheme Π

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 $\text{Adv}_{\Pi}^{\text{INT-PTXT}}(\mathcal{A}) \leq \varepsilon$ where

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

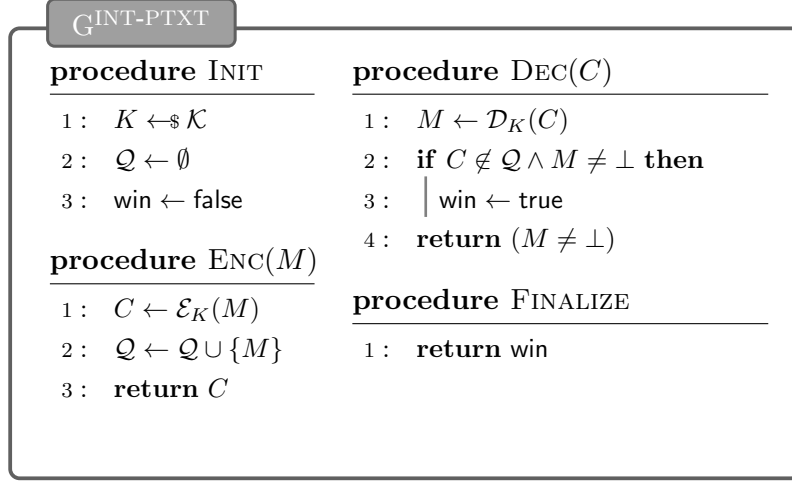


Figure 10: INT-PTXT game for a LPSE scheme Π

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 Π is not INT-CTXT, then it is not INT-PTXT. Let \mathcal{A} be a INT-CTXT adversary against Π , we construct an adversary \mathcal{B} against INT-PTXT of such that \mathcal{B} runs \mathcal{A} and replays \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 $m^* = \text{DEC}(K, c^*)$. Thus \mathcal{B} wins if \mathcal{A} wins.

□

3 Hash Function

3.1 Collision Resistance

Let $H : \mathcal{D} \rightarrow \mathcal{R}$ 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

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

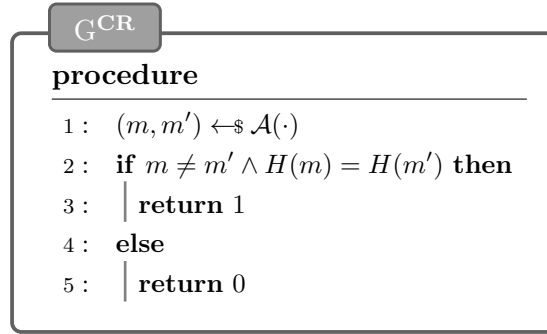


Figure 11: Collision Resistance (CR) Game

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 $H : \mathcal{D} \rightarrow \mathcal{R}$ 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

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

3.1.2 Pre-image Resistance

Let $H : \mathcal{D} \rightarrow \mathcal{R}$ 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

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

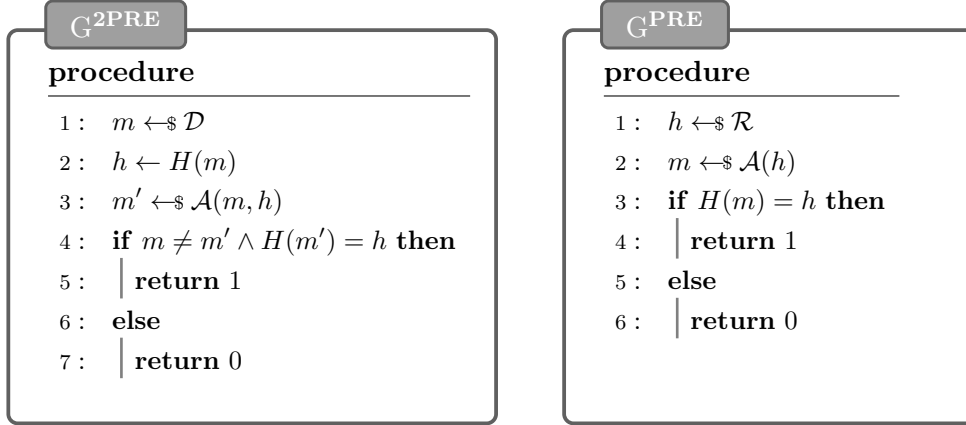


Figure 12: **Left:** Second Preimage Resistance (2PRE) Game. **Right:** Preimage Resistance (PRE) Game

3.1.3 One-wayness

Let $H : \mathcal{D} \rightarrow \mathcal{R}$ 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

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

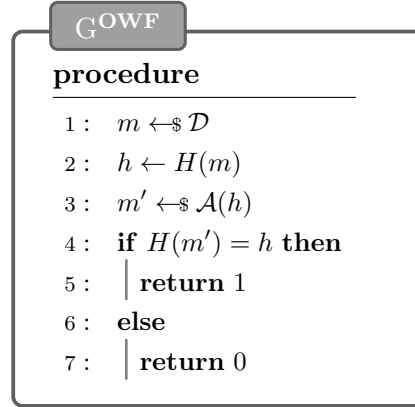


Figure 13: One-wayness (OWF) Game

3.1.4 Universal Hashing

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

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

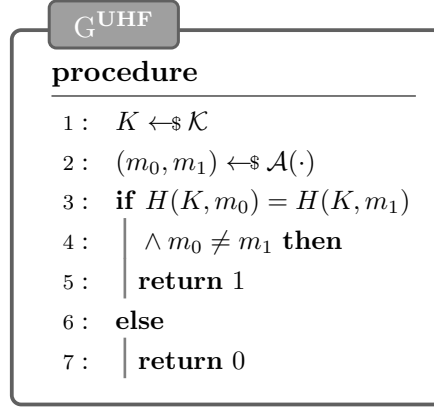


Figure 14: UHF Game

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 $\text{Adv}_H^{\text{DUHF}}(\mathcal{A}) \leq \varepsilon$ where

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

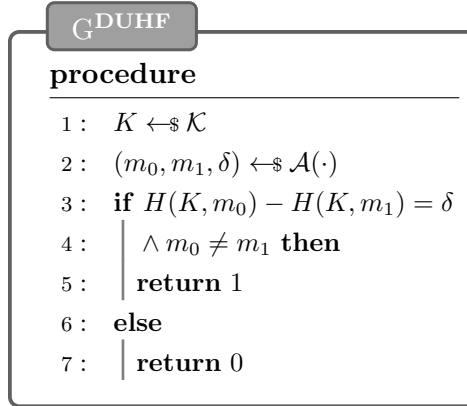


Figure 15: DUHF Game

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 oracle OVFY, and running in time at most t , the advantage $\mathbf{Adv}_{\text{MAC}}^{\text{EUF-CMA}}(\mathcal{A}) \leq \varepsilon$ where

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

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 $\mathbf{Adv}_{\text{MAC}}^{\text{SUF-CMA}}(\mathcal{A}) \leq \varepsilon$ where

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

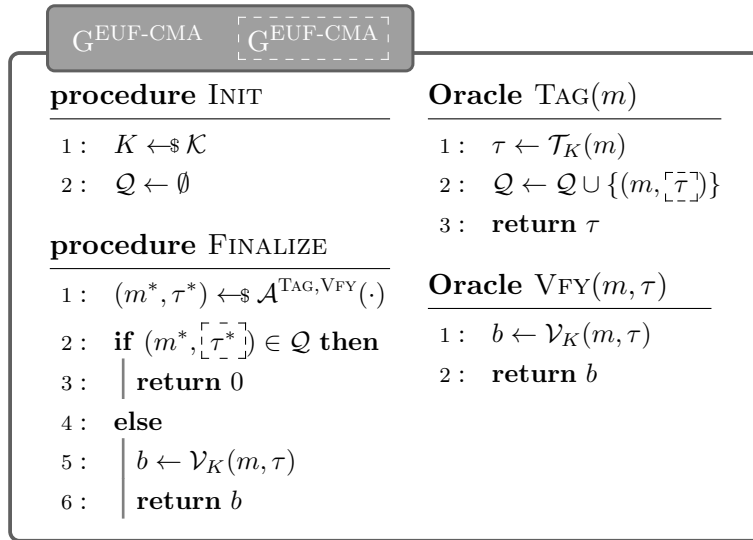


Figure 16: EUF-CMA and SUF-CMA Game for a MAC scheme. The dox-boxed code is exclusive for $\mathbf{G}^{\text{SUF-CMA}}$.