RSA-OAEP IND-CCA2 증명

김동현(wlswudpdlf31@kookmin.ac.kr)

March 8, 2025

1 서론

RSA-OAEP IND-CCA2 증명.

2 기호

- λ 보안 매개변수
- pk 공개키
- sk 비밀키
- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda)$ 키 생성 알고리즘, 확률론적
- m 메시지
- c 암호문
- $c \leftarrow \mathcal{E}(m, \mathsf{pk})$ 암호화 함수, 확률론적
- $m \leftarrow \mathcal{D}(c, \mathsf{sk})$ 복호화 함수, 결정론적
- $\mathcal{A}$ 공격자
- r 랜덤 코인
- $\mathcal{M}$ 메시지 공간
- Ω 랜덤 코인 공간
- b 0 또는 1
- H, G 암호학적 해시 함수
- n 메시지 길이

3 보안 개념

3.1 OW-CPA

$$
\begin{array}{ccc}
\underline{\text{Challenger } \mathcal{C}} & \xLeftrightarrow{\mathsf{Exp}^{\mathsf{OW\text{-}CPA}}_{\Pi,\lambda}} & \underline{\text{Adversary } \mathcal{A}} \\
(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda) & \xrightarrow{1^\lambda, \mathsf{pk}} & \\
m^* \xleftarrow{\$} \mathcal{M} & & \\
c^* \leftarrow \mathcal{E}_{\mathsf{pk}}(m^*) & \xrightarrow{c^*} & \\
\text{Return } [m' \stackrel{?}{=} m^*] & \xleftarrow{m'} & \mathcal{A} \text{ chooses } m' \in \mathcal{M}
\end{array}
$$

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathcal{A},\Pi}(\lambda) &= \Pr[\mathsf{Exp}^{\mathsf{OW\text{-}CPA}}_{\Pi,\lambda}(\mathcal{A}) = 1] \\
&= \Pr_{m^*}[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda) : \mathcal{A}(\mathsf{pk}, \mathcal{E}_{\mathsf{pk}}(m^*)) = m^*].
\end{aligned} \tag{1}
$$

trapdoor one-way function:

$$
\begin{array}{ccc}
\underline{\text{Challenger } \mathcal{C}} & \xLeftrightarrow{\mathsf{Exp}^{\mathsf{OWF}}} & \underline{\text{Adversary } \mathcal{A}} \\
(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda) & \xrightarrow{1^\lambda, \mathsf{pk}} & \\
m^* \xleftarrow{\$} \mathcal{M} & & \\
c^* \leftarrow \mathcal{E}_{\mathsf{pk}}(m^*) & \xrightarrow{c^*} & \\
\text{Return } [m' \stackrel{?}{=} m^*] & \xleftarrow{m'} & \mathcal{A} \text{ chooses } m' \in \mathcal{M}
\end{array}
$$

Π is (t, ε)-OW-CPA secure:
Adversary $\mathcal{A}$ whose running time is bounded by t, $\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathcal{A},\Pi}(\lambda) \le \varepsilon$.

$$
\begin{array}{ccc}
\underline{\text{Challenger } \mathcal{C}} & \xLeftrightarrow{\mathsf{Exp}^{\mathsf{OW\text{-}CPA}}_{\Pi,\lambda}} & \underline{\text{Adversary } \mathcal{B}} \\
(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda) & \xrightarrow{1^\lambda, \mathsf{pk}} & \\
(s^*, t^*) \xleftarrow{\$} \{0,1\}^{\lambda-\lambda_0} \times \{0,1\}^{\lambda_0} & & \\
c^* \leftarrow \mathcal{E}_{\mathsf{pk}}(s^*, t^*) & \xrightarrow{c^*} & \\
\text{Return } [s' \stackrel{?}{=} s^*] & \xleftarrow{s'} & \mathcal{A} \text{ chooses } s' \in \{0,1\}^{\lambda-\lambda_0}
\end{array}
$$

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{OW\text{-}CPA\text{-}PD}}_{\mathcal{A},\Pi}(\lambda) &= \Pr[\mathsf{Exp}^{\mathsf{OW\text{-}CPA\text{-}PD}}_{\Pi,\lambda}(\mathcal{A}) = 1] \\
&= \Pr_{s^*,t^*}[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda) : \mathcal{A}(\mathsf{pk}, \mathcal{E}_{\mathsf{pk}}(s^*, t^*)) = s^*].
\end{aligned} \tag{2}
$$

3.2 IND-CCA2

Challenger $\mathcal{C}$	$\xleftrightarrow{\mathsf{Exp}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\lambda}}$	Adversary $\mathcal{A}$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda)$	$\xrightarrow{1^\lambda, \mathsf{pk}}$	
	$\mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}$ Query Phase 1	
	$\xleftarrow{m_0^*, m_1^*}$	$\mathcal{A}$ chooses $m_0^*, m_1^* \in \mathcal{M}$ such that $\lvert m_0^* \rvert = \lvert m_1^* \rvert$ and $m_0^* \neq m_1^*$
$b^* \xleftarrow{\$} \{0,1\}, r^* \xleftarrow{\$} \Omega$ $c^* \leftarrow \mathcal{E}_{\mathsf{pk}}(m^*_{b^*}; r^*)$	$\xrightarrow{c^*}$	
	$\mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}$ Query Phase 2	
Return $[b' \stackrel{?}{=} b^*]$	$\xleftarrow{b'}$	$\mathcal{A}$ chooses $b' \in \{0,1\}$

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\mathcal{A},\Pi}(\lambda) &= 2 \cdot \Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\lambda}(\mathcal{A}) = 1] - 1 \\
&= \Pr_{b^*, r^*}[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda); (m_0^*, m_1^*) \leftarrow \mathcal{A} : \mathcal{A}(\mathsf{pk}, \mathcal{E}_{\mathsf{pk}}(m^*_{b^*}; r^*)) = b^*].
\end{aligned}
\tag{3}
$$

Π is (t, ε)-IND-CCA2 secure:
Adversary $\mathcal{A}$ whose running time is bounded by t, $\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathcal{A},\Pi}(\lambda) \leq \varepsilon$.

3.3 Random Oracle Model

Challenger $\mathcal{C}$		Adversary $\mathcal{A}$
$\mathcal{L}_H \leftarrow \{\}$		
	$\xleftarrow{x}$	$\mathcal{A}$ chooses $x \in \{0,1\}^*$
If $(x, y') \in \mathcal{L}$ then $y \leftarrow y'$ else $y \xleftarrow{\$} \{0,1\}^n$ $\mathcal{L}_H \leftarrow \mathcal{L}_H \cap (x, y)$	$\xrightarrow{y}$	

Challenger $\mathcal{C}$	$\xleftrightarrow{\mathsf{Exp}_{\Pi,\lambda}^{\mathsf{IND\text{-}CCA2\text{-}ROM}}}$	Adversary $\mathcal{A}$
$\mathcal{L}_H \leftarrow \{\}$ $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda)$	$\xrightarrow{1^\lambda, \mathsf{pk}}$	
	$\mathcal{O}^H, \mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}$ Query Phase 1	
	$\xleftarrow{m_0^*, m_1^*}$	$\mathcal{A}$ chooses $m_0^*, m_1^* \in \mathcal{M}$ such that $\lvert m_0^* \rvert = \lvert m_1^* \rvert$ and $m_0^* \neq m_1^*$
$b^* \xleftarrow{\$} \{0,1\}, r^* \xleftarrow{\$} \Omega$ $c^* \leftarrow \mathcal{E}_{\mathsf{pk}}(m_{b^*}^*; r^*)$	$\xrightarrow{c^*}$	
	$\mathcal{O}^H, \mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}$ Query Phase 2	
Return $[b' \stackrel{?}{=} b^*]$	$\xleftarrow{b'}$	$\mathcal{A}$ chooses $b' \in \{0,1\}$

4 RSA-OAEP

치환(permutation) $f : \{0,1\}^\lambda \longrightarrow \{0,1\}^\lambda$를 다음과 같이 표현한다.

$$f : \{0,1\}^{n+\lambda_1} \times \{0,1\}^{\lambda_0} \longrightarrow \{0,1\}^{n+\lambda_1} \times \{0,1\}^{\lambda_0}.$$

이 때, $\lambda = n + \lambda_0 + \lambda_1$이다.

함수 f와 그 역함수 g로부터 얻은 OAEP 암호 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$를 나타내기 위해, 다음과 같은 두 해시 함수 H, G가 필요하다.

$$H : \{0,1\}^{\lambda_0} \to \{0,1\}^{\lambda-\lambda_0} \quad G : \{0,1\}^{\lambda-\lambda_0} \to \{0,1\}^{\lambda_0}.$$

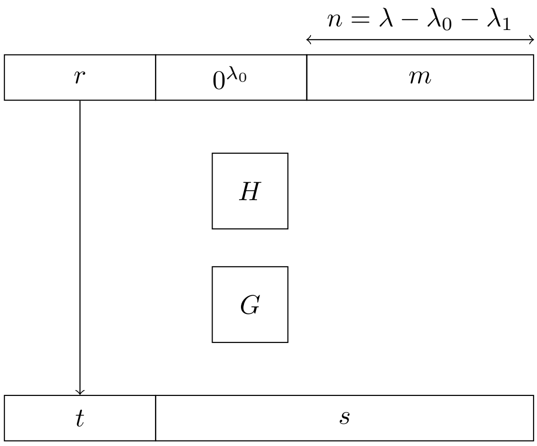
OAEP 암호 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$는 다음과 같다.

- $\mathcal{K}(1^\lambda)$: 함수 f의 인스턴스 pk, 함수 g의 인스턴스 sk를 생성한다.
- $\mathcal{E}_{\mathsf{pk}}(m, r)$: $m \in \{0,1\}^n$과 $r \xleftarrow{\$} \{0,1\}^{\lambda_0}$가 주어졌을 때, 다음을 계산한다.

  $$s = (m \parallel 0^{\lambda_1}) \oplus G(r) \quad t = r \oplus H(s).$$

  이후 암호문 $c = f(s,t)$를 출력한다.
- $\mathcal{D}_{\mathsf{sk}}(c)$: sk를 사용하여 다음을 순서대로 계산할 수 있다.
  - $(s,t) = g(c)$
  - $r = t \oplus H(s), M = s \oplus G(r)$

  만약 $[M]_{\lambda_1} = 0^{\lambda_1}$이면 $[M]_n$을 출력하고, 아니라면 "Reject"를 출력한다. 이 표현에서, $[M]_{k_1}$은 M의 하위 λ_1 비트를, $[M]_n$은 M의 상위 n 비트를 의미한다.



5 OAEP IND-CCA2 증명

정리 1. *$\mathcal{A}$를 OAEP 변환 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$에 대해 능력치(advantage) ε과 시간(running time) t를 가지고, 복호화 오라클, 해시 함수 H 및 G에 각각 $q_\mathcal{D}, q_H, q_G$ 회 질의하는 IND-CCA2 공격자라 하자. 다음을 만족한다.*

$$S \geq \frac{1}{q_H}\left(\frac{\varepsilon}{2} - \frac{2q_\mathcal{D}q_G + q_\mathcal{D} + q_G}{2^{\lambda_0}} - \frac{2q_\mathcal{D}}{2^{\lambda_1}}\right).$$

이 때, $t' \leq t \cdot q_H \cdot q_G \cdot (T_f + O(1))$이고, T_f는 함수 f의 시간 복잡도를 의미한다.

우리는 보조정리 2를 세 단계로 증명한다. 첫 번째 단계에서는 IND-CCA2 적대자 $\mathcal{A}$를 부분 도메인 일방성(partial-domain one-wayness) f를 깨뜨리는 알고리즘 $\mathcal{B}$로 환원하는 과정을 제시한다. 현재의 증명에서는 원본 논문 [3]에서와 같은 전체 도메인 일방성(full-domain one-wayness)이 아니라, 부분

도메인 일방성 하에서의 보안성에만 관심을 둔다. 두 번째 단계에서는 이 환원에서 사용된 복호화 오라클 시뮬레이션이 부분 도메인 일방성 하에서 압도적인 확률로 올바르게 동작함을 보인다. 이 부분은 원본 증명 [3]과 다르며, 최근 발견된 오류 [15]를 수정한다. 마지막으로, 우리는 복호화 오라클 시뮬레이션에 대한 위에서 언급한 분석을 포함하여 전체적인 환원의 성공 확률을 분석한다.

이 첫 번째 부분에서는 환원이 어떻게 작동하는지를 다시 살펴본다. $\mathcal{A}$를 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$의 IND-CCA2 공격자로 가정하자. 시간 제한 t 내에서, $\mathcal{A}$는 복호화 오라클에 대해 $q_{\mathcal{D}}$개의 질의를 하고, 무작위 오라클 H, G에 대해 각각 q_H, q_G개의 질의를 수행하며, 특정 확률 ε보다 높은 능력치로 올바른 평문을 구별해낸다. 이제 환원 $\mathcal{B}$을 설명한다.

Challenger $\mathcal{C}$	$\xLeftrightarrow{\mathsf{Exp}^{\text{OW-CPA}}_{\Pi,\lambda}}$	Adversary $\mathcal{B}$	$\xLeftrightarrow{\mathsf{Exp}^{\text{IND-CCA2}}_{\Pi,\lambda}}$	Adversary $\mathcal{A}$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda)$	$\xrightarrow{1^\lambda, \mathsf{pk}}$			
$m^* = (s^*, t^*) \xleftarrow{\$} \{0,1\}^{\lambda-\lambda_0} \times \{0,1\}^{\lambda_0}$				
$c^* \leftarrow \mathcal{E}_{\mathsf{pk}}(m^*)$	$\xrightarrow{c^*}$			
		$\mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}, \mathcal{O}^H, \mathcal{O}^G$ Query Phase 1		
			$\xleftarrow{m_0^*, m_1^*}$	$\mathcal{A}$ chooses $m_0^*, m_1^* \in \mathcal{M}$ such that $\lvert m_0^* \rvert = \lvert m_1^* \rvert$ and $m_0^* \neq m_1^*$
		$b \xleftarrow{\$} \{0,1\}$	$\xrightarrow{c^*}$	
		$\mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}, \mathcal{O}^H, \mathcal{O}^G$ Query Phase 2		
Return $[s' \stackrel{?}{=} s^*]$	$\xleftarrow{s'}$	$\mathcal{B}$ chooses $s' \in \{0,1\}^{\lambda-\lambda_0}$	$\xleftarrow{b'}$	$\mathcal{A}$ chooses $b' \in \{0,1\}$

이 실험에서 세 개의 오라클을 $\mathcal{B}$가 처리하기 때문에, 다음을 고려해야한다.

- 공격자 $\mathcal{A}$의 질의에 대해서, 오라클은 유효한 응답을 해야 한다. $\mathcal{A}$가 오라클이 잘못된 응답을 하고 있다는 것을 감지해서는 안된다.
- 오라클이 기대하는 확률분포와 일관되어야 한다. 일관되지 않으면 $\mathcal{A}$가 이상을 감지할 수 있다.
- 오라클 응답은 일관되어야 한다.
- 복호화 오라클은 $\mathcal{B}$가 비밀키를 모름에도 수행할 수 있어야 한다.

How $\mathcal{B}$ simulate $\mathcal{O}^G$?

- If $\gamma \in \mathcal{L}_G$, then response G_γ and $\mathcal{L}_G \leftarrow \mathcal{L}_G \cap (\gamma, G_\gamma)$.
- Otherwise, do following:
  - For some $\delta \in \mathcal{L}_H$, if $c^* = f(\delta, \gamma \oplus H_\delta)$, then $G_\gamma \leftarrow \delta \oplus (m_b \parallel 0^{\lambda_1})$.
  - For all $\delta \in \mathcal{L}_H$, if $c^* \neq f(\delta, \gamma \oplus H_\delta)$, then $G_\gamma \xleftarrow{\$} \{0,1\}^\lambda$.
  - response G_γ and $\mathcal{L}_G \leftarrow \mathcal{L}_G \cap (\gamma, G_\gamma)$.

How $\mathcal{B}$ simulate $\mathcal{O}^{H}$?

- If $\delta \in \mathcal{L}_H$, then response H_δ.
- Otherwise, response $H_\delta \xleftarrow{\$} \{0,1\}^\lambda$ and $\mathcal{L}_H \leftarrow \mathcal{L}_H \cap (\delta, H_\delta)$.

How $\mathcal{B}$ simulate $\mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}$?

- If $c = f(\delta, H_\delta \oplus \gamma)$ and $[G_\gamma \oplus \delta]_{\lambda_1} = 0^{\lambda_1}$, then response $[G_\gamma \oplus \delta]^n$.
- Otherwise, response reject.