RSA-OAEP IND-CCA2 증명

김동현(wlswudpdlf31@kookmin.ac.kr)

March 17, 2025

Contents

1 논문정보

- 제목: RSA-OAEP is Secure under the RSA Assumption
- 저자: Eiichiro Fujisaki1, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern
- 년도: 2001년
- 초록: 최근 Victor Shoup은 적응적 선택 암호문 공격에 대한 OAEP의 보안성에 관한 널리 받아들여진 결과에 틈이 있음을 지적하였다. 더욱이, 그는 기본 트랩도어 치환의 단방향성만으로는 OAEP의 보안성을 증명할 수 없을 것으로 예상된다는 점을 보였다. 본 논문은 OAEP의 보안성에 대한 또 다른 결과를 제시한다. 즉, 본 논문에서는 무작위 오라클 모델에서, 기본 치환의 부분 영역 단방향성(partial-domain one-wayness) 하에서, OAEP가 적응적 선택 암호문 공격에 대해 의미론적 보안성을 제공함을 증명한다. 따라서, 이는 형식적으로 더 강한 가정을 사용한다. 그럼에도 불구하고, RSA 함수의 부분 영역 단방향성이 (전체 영역) 단방향성과 동치이므로, RSA-OAEP의 보안성은 단순한 RSA 가정만으로도 증명될 수 있음을 알 수 있다. 다만, 그 축소(reduction)는 타이트하지 않다.

2 보안 개념

2.1 OW-CPA

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

2.2 OWF

$f : \{0,1\}^\lambda \to \{0,1\}^\lambda$ is a trapdoor one-way permutation.

Challenger $\mathcal{C}$	$\xleftrightarrow{\mathsf{Exp}^{\mathsf{OWF}}_{f,\lambda}}$	Adversary $\mathcal{A}$
	$\xrightarrow{f}$	
$m^* \xleftarrow{\$} \mathcal{M}$		
$c^* \leftarrow f(m^*)$	$\xrightarrow{c^*}$	
Return $[m' \stackrel{?}{=} m^*]$	$\xleftarrow{m'}$	$\mathcal{A}$ chooses $m' \in \mathcal{M}$

2.3 OWF-PD

$f : \{0,1\}^{\lambda-\lambda_0} \times \{0,1\}^{\lambda_0} \to \{0,1\}^{\lambda-\lambda_0} \times \{0,1\}^{\lambda_0}$ is a trapdoor one-way permutation.

Challenger $\mathcal{C}$	$\xleftrightarrow{\mathsf{Exp}^{\mathsf{OWF\text{-}PD}}_{f,\lambda}}$	Adversary $\mathcal{B}$
	$\xrightarrow{f}$	
$(s^*, t^*) \xleftarrow{\$} \{0,1\}^{\lambda-\lambda_0} \times \{0,1\}^{\lambda_0}$		
$c^* \leftarrow f(s^*, t^*)$	$\xrightarrow{c^*}$	
Return $[s' \stackrel{?}{=} s^*]$	$\xleftarrow{s'}$	$\mathcal{A}$ chooses $s' \in \{0,1\}^{\lambda-\lambda_0}$

2.4 OWF-PD-S

??

2.5 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 $m_0^* \neq m_1^*$
$b \xleftarrow{\$} \{0,1\}$ $c^* \leftarrow \mathcal{E}_{\mathsf{pk}}(m_b^*)$	$\xrightarrow{c^*}$	
	$\mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}$ Query Phase 2	
Return $[b' \stackrel{?}{=} b]$	$\xleftarrow{b'}$	$\mathcal{A}$ chooses $b' \in \{0,1\}$

2.6 IND-CCA2-ROM

Challenger $\mathcal{C}$	$\xleftrightarrow{\mathsf{Exp}^{\mathsf{IND\text{-}CCA2\text{-}ROM}}_{\Pi,\lambda}}$	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 $m_0^* \neq m_1^*$
$b \xleftarrow{\$} \{0,1\}$ $c^* \leftarrow \mathcal{E}_{\mathsf{pk}}(m_b^*)$	$\xrightarrow{c^*}$	
	$\mathcal{O}^H, \mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}$ Query Phase 2	
Return $[b' \stackrel{?}{=} b]$	$\xleftarrow{b'}$	$\mathcal{A}$ chooses $b' \in \{0,1\}$

3 RSA-OAEP

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

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

이때, $\lambda = n+\lambda_0+\lambda_1$이다. 그리고 다음과 같은 두 해시 함수 H, G를 준비한다.

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

OAEP 암호체계(Cryptosystem) $(\mathcal{K},\mathcal{E},\mathcal{D})$는 다음과 같이 동작한다.

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

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

  s,t를 계산하는 과정을 도식화하면 그림 1와 같다. 이후 암호문 $c=f(s,t)$를 출력한다. 같다.
- $\mathcal{D}_{\mathsf{sk}}(c)$: $(s,t)=g_{\mathsf{sk}}(c)$을 계산한 후, r,M을 다음과 같이 계산한다.

  $$r=t\oplus H(s)a\quad M=s\oplus G(r).$$

  만약 $[M]_{\lambda_1}=0^{\lambda_1}$이면 $[M]^n$을 출력하고, 아니라면 “Reject”를 출력한다.

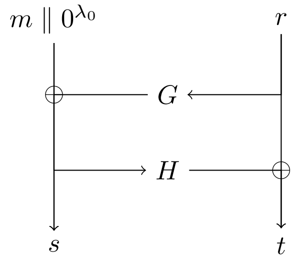

Figure 1: $\mathcal{E}_{\mathsf{pk}}(m,r)$에서 s,t를 계산하는 과정

4 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 $\mathcal{C}$	$\xleftrightarrow{\mathsf{Exp}^{\mathsf{OWF\text{-}PD}}_{f,\lambda}}$	Adversary $\mathcal{B}$	$\xleftrightarrow{\mathsf{Exp}^{\mathsf{IND\text{-}CCA2\text{-}ROM}}_{\Pi,\lambda}}$	Adversary $\mathcal{A}$
	$\xrightarrow{f}$			
$(s^*, t^*) \xleftarrow{\$} \{0,1\}^{\lambda-\lambda_0} \times \{0,1\}^{\lambda_0}$				
$c^* \leftarrow f(s^*, t^*)$	$\xrightarrow{c^*}$			
		$\mathcal{L}_H, \mathcal{L}_G \leftarrow \{\}, \{\}$	$\xrightarrow{1^\lambda, \mathsf{pk}}$	
		$\mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}, \mathcal{O}^H, \mathcal{O}^G$ Query Phase 1		
			$\xleftarrow{m_0^*, m_1^*}$	$\mathcal{A}$ chooses $m_0^*, m_1^* \in \mathcal{M}$ such that $\|m_0^*\| = \|m_1^*\|$ and $m_0^* \neq m_1^*$
			$\xrightarrow{c^*}$	
		$\mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}, \mathcal{O}^H, \mathcal{O}^G$ Query Phase 2		
Return $[s' \stackrel{?}{=} s^*]$	$\xleftarrow{s'}$	$\mathcal{B}$ chooses $s' \in \{0,1\}^{\lambda-\lambda_0}$	$\xleftarrow{b'}$	$\mathcal{A}$ chooses $b' \in \{0,1\}$

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.