RSA-OAEP IND-CCA2 증명

김동현(wlswudpdlf31@kookmin.ac.kr)

March 18, 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 trapdoor permutation

트랩도어 치환 체계(Trapdoor permutation scheme) $\Psi = (\mathcal{K}, \mathcal{F}, \mathcal{I})$를 다음과 같이 정의한다.

- $\mathcal{K}(1^\lambda)$: 확률론적 키 생성 알고리즘으로, 1^λ를 입력 받아 $(\mathsf{pk}, \mathsf{sk})$를 생성한다.
- $\mathcal{F}_{\mathsf{pk}}(x)$: 결정론적 알고리즘으로, pk와 $x \in \{0,1\}^\lambda$를 입력 받아 $y \in \{0,1\}^\lambda$를 출력한다.
- $\mathcal{I}_{\mathsf{sk}}(y)$: 결정론적 알고리즘으로, sk와 $y \in \{0,1\}^\lambda$를 입력 받아 $x \in \{0,1\}^\lambda$를 출력한다. $\mathcal{K}(1^\lambda)$로 생성한 모든 $(\mathsf{pk}, \mathsf{sk})$와 모든 $x \in \{0,1\}^\lambda$에 대해, $\mathcal{I}_{\mathsf{sk}}(\mathcal{F}_{\mathsf{pk}}(x)) = x$를 만족한다.

동작시간(Running time) τ를 가지는 공격자 $\mathcal{A}$와 트랩도어 치환 체계 Ψ에 대한 일방향성(One-wayness) 실험 $\mathsf{Exp}^{\mathsf{OW}}_{\Psi,\lambda}(\mathcal{A};\tau)$을 다음과 같이 정의한다.

$$
\begin{array}{ccc}
\underline{\text{Challenger } \mathcal{C}} & \xleftrightarrow{\mathsf{Exp}^{\mathsf{OW}}_{\Psi,\lambda}} & \underline{\text{Adversary } \mathcal{A}} \\
(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathcal{K}(1^\lambda) & & \\
x^* \xleftarrow{\$} \{0,1\}^\lambda & & \\
y^* \leftarrow \mathcal{F}_{\mathsf{pk}}(x^*) & \xrightarrow{1^\lambda, \mathsf{pk}, y^*} & \\
\text{Return } [x' \stackrel{?}{=} x^*] & \xleftarrow{x'} & \mathcal{A} \text{ chooses } x' \in \mathcal{X}
\end{array}
$$

$\mathcal{A}$의 능력치 $\mathsf{Adv}^{\mathsf{OW}}_{\mathcal{A},\Psi}(\lambda, \tau)$를 다음과 같이 정의한다.

$$\mathsf{Adv}^{\mathsf{OW}}_{\Psi,\lambda}(\mathcal{A};\tau) := \Pr[\mathsf{Exp}^{\mathsf{OW}}_{\Psi,\lambda}(\mathcal{A};\tau) = 1].$$

2.2 Partial-domain OW trapdoor permutation

트랩도어 치환 $\Psi = (\mathcal{K}, \mathcal{F}, \mathcal{I})$에서, $\mathcal{F}_{\mathsf{pk}}(x) : \{0,1\}^\lambda \to \{0,1\}^\lambda$를 다음과 같이 표현한다.

$$\mathcal{F}_{\mathsf{pk}} : \{0,1\}^{n+\lambda_1} \times \{0,1\}^{\lambda_0} \to \{0,1\}^{n+\lambda_1} \times \{0,1\}^{\lambda_0}.$$

이때 $\lambda = n + \lambda_0 + \lambda_1$이다.

메모 1. 예를 들어, $x = s \parallel t$라고 할 때, $y \leftarrow \mathcal{F}_{\mathsf{pk}}(x)$ 대신 $y \leftarrow \mathcal{F}_{\mathsf{pk}}(s \parallel t)$로 표현할 수 있다.

동작시간 τ를 가지는 공격자 $\mathcal{A}$와 트랩도어 함수 체계 Ψ에 대한 부분 일방향성(Partial-domain one-wayness) 실험 $\mathsf{Exp}^{\mathsf{OW\text{-}PD}}_{\Psi,\lambda}(\mathcal{A};\tau)$을 다음과 같이 정의한다.

$$
\begin{array}{ccc}
\underline{\text{Challenger } \mathcal{C}} & \xleftrightarrow{\mathsf{Exp}^{\mathsf{OW\text{-}PD}}_{\Psi,\lambda}} & \underline{\text{Adversary } \mathcal{A}} \\
(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathcal{K}(1^\lambda) & & \\
(s^*, t^*) \xleftarrow{\$} \{0,1\}^{n+\lambda_1} \times \{0,1\}^{\lambda_0} & & \\
y^* \leftarrow \mathcal{F}_{\mathsf{pk}}(s^*, t^*) & \xrightarrow{1^\lambda, \mathsf{pk}, y^*} & \\
\text{Return } [s' \stackrel{?}{=} s^*] & \xleftarrow{s'} & \mathcal{A} \text{ chooses } s' \in \{0,1\}^{n+\lambda_1}
\end{array}
$$

공격자 $\mathcal{A}$의 능력치 $\mathsf{Adv}^{\mathsf{OW\text{-}PD}}_{\Psi,\lambda}(\mathcal{A};\tau)$를 다음과 같이 정의한다.

$$\mathsf{Adv}^{\mathsf{OW\text{-}PD}}_{\Psi,\lambda}(\mathcal{A};\tau) := \Pr[\mathsf{Exp}^{\mathsf{OW\text{-}PD}}_{\Psi,\lambda}(\mathcal{A};\tau) = 1].$$

2.3 Set partial-domain OW trapdoor permutation

동작시간 τ를 가지고 l개의 원소를 출력하는 공격자 $\mathcal{A}$와 트랩도어 함수 체계 Ψ에 대한 집합 부분 일방향성(Set partial-domain one-wayness) 실험 $\mathsf{Exp}^{\mathsf{OW\text{-}PD\text{-}S}}_{\Psi,\lambda}(\mathcal{A};\tau,l)$을 다음과 같이 정의한다.

Challenger $\mathcal{C}$	$\xLeftrightarrow{\mathsf{Exp}^{\mathsf{OW\text{-}PD\text{-}S}}_{\Psi,\lambda}}$	Adversary $\mathcal{A}$
$(\mathsf{pk},\mathsf{sk}) \xleftarrow{\$} \mathcal{K}(1^\lambda)$		
$(s^*,t^*) \xleftarrow{\$} \{0,1\}^{n+\lambda_1} \times \{0,1\}^{\lambda_0}$ $y^* \leftarrow \mathcal{F}_{\mathsf{pk}}(s^*,t^*)$	$\xrightarrow{1^\lambda,\mathsf{pk},y^*}$	
Return $[s'_i \stackrel{?}{=} s^*]$	$\xleftarrow{s'_0,s'_1,\cdots,s'_{l-1}}$	$\mathcal{A}$ chooses $s'_0,s'_1,\cdots,s'_{l-1} \in \{0,1\}^{n+\lambda_1}$

공격자 $\mathcal{A}$의 능력치 $\mathsf{Adv}^{\mathsf{OW\text{-}PD\text{-}S}}_{\Psi,\lambda}(\mathcal{A};\tau,l)$를 다음과 같이 정의한다.

$$\mathsf{Adv}^{\mathsf{OW\text{-}PD\text{-}S}}_{\Psi,\lambda}(\mathcal{A};\tau,l) := \Pr[\mathsf{Exp}^{\mathsf{OW\text{-}PD\text{-}S}}_{\Psi,\lambda}(\mathcal{A};\tau,l) = 1].$$

2.4 IND security against CCA2

공개키 암호 체계(Public-key encryption scheme) $\Pi = (\mathcal{K},\mathcal{E},\mathcal{D})$를 다음과 같이 정의한다.

- $\mathcal{K}(1^\lambda)$: 확률론적 키 생성 알고리즘으로, 1^λ를 입력 받아 $(\mathsf{pk},\mathsf{sk})$를 생성한다.
- $\mathcal{E}_{\mathsf{pk}}(m)$: 암호화 알고리즘으로, pk와 $m \in \mathcal{M}$를 입력 받아 $c \in \mathcal{C}$를 출력한다. 확률론적 알고리즘으로, $r \xleftarrow{\$} \Omega$를 추가로 입력 받아 $\mathcal{E}_{\mathsf{pk}}(m;r)$으로 표현할 수도 있다.
- $\mathcal{D}_{\mathsf{sk}}(c)$: 결정론적 복호화 알고리즘으로, sk와 $c \in \mathcal{C}$를 입력 받아 $m \in \mathcal{M}$를 출력한다.

동작시간 τ를 가지고 복호화 오라클에 q회 질의하는 공격자 $\mathcal{A}$와 공개키 암호 체계 Π에 대해, 선택 암호문 공격(Adaptive chosen ciphertext attack, 이하 CCA2)에 대한 구별불가능성(Indistinguishability) 실험 $\mathsf{Exp}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\lambda}(\mathcal{A};\tau,q)$을 다음과 같이 정의한다.

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 $b' \in \{0,1\}$

공격자 $\mathcal{A}$의 능력치 $\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\lambda}(\mathcal{A};\tau,q)$를 다음과 같이 정의한다.

$$\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\lambda}(\mathcal{A};\tau,q) = 2\cdot\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\lambda}(\mathcal{A};\tau,q)=1]-1.$$

2.5 IND security against CCA2 in ROM

동작시간 τ를 가지고 복호화 오라클에 $q_{\mathcal{D}}$회, 랜덤 오라클에 q_H회 질의하는 공격자 $\mathcal{A}$와 공개키 암호 체계 Π에 대해, 랜덤 오라클 모델(Random oracle model)에서의 CCA2에 대한 구별불가능성 실험 $\mathsf{Exp}^{\mathsf{IND\text{-}CCA2\text{-}ROM}}_{\Pi,\lambda}(\mathcal{A};\tau,q_{\mathcal{D}},q_H)$을 다음과 같이 정의한다.

Challenger $\mathcal{C}$	$\xLeftrightarrow{\mathsf{Exp}^{\mathsf{IND\text{-}CCA2\text{-}ROM}}_{\Pi,\lambda}}$	Adversary $\mathcal{A}$
$\mathcal{O}_H \xleftarrow{\$} \Phi$		
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathcal{K}(1^\lambda)$	$\xrightarrow{1^\lambda,\mathsf{pk}}$	
	$\mathcal{O}^H, \mathcal{O}^{\mathcal{D}_{\mathsf{sk}}}$ 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 $b' \in \{0,1\}$

공격자 $\mathcal{A}$의 능력치 $\mathsf{Adv}^{\mathsf{IND\text{-}CCA2\text{-}ROM}}_{\Pi,\lambda}(\mathcal{A};\tau,q_{\mathcal{D}},q_H)$를 다음과 같이 정의한다.

$$\mathsf{Adv}^{\mathsf{IND\text{-}CCA2\text{-}ROM}}_{\Pi,\lambda}(\mathcal{A};\tau,q_{\mathcal{D}},q_H) = 2\cdot\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA2\text{-}ROM}}_{\Pi,\lambda}(\mathcal{A};\tau,q_{\mathcal{D}},q_H)=1]-1.$$

3 RSA-OAEP

다음과 같은 두 해시 함수 H, G를 준비한다.

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

트랩도어 치환 체계 $\Psi = (\mathcal{K}, \mathcal{F}, \mathcal{I})$를 포함하는 OAEP 변환 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$는 다음과 같이 동작한다.

- $\mathcal{K}(1^\lambda)$: $(\mathsf{pk}, \mathsf{sk})$를 생성한다. pk는 이후 트랩도어 치환 $\mathcal{F}$에서 사용하며, sk는 $\mathcal{I}$에서 사용한다.
- $\mathcal{E}_{\mathsf{pk}}(m; r)$: $m \in \{0,1\}^n$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 $c = \mathcal{F}_{\mathsf{pk}}(s, t)$를 출력한다.
- $\mathcal{D}_{\mathsf{sk}}(c)$: $(s, t) = \mathcal{I}_{\mathsf{sk}}(c)$을 계산한 후, r, M을 다음과 같이 계산한다.

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

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

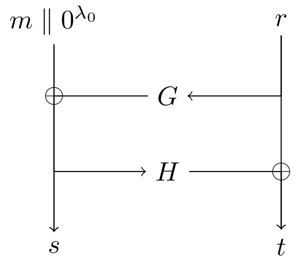

Figure 1: $\mathcal{E}_{\mathsf{pk}}(m; r)$에서 s, t를 계산하는 과정

4 증명

보조정리 1. *공격자 $\mathcal{A}$를 OAEP 변환 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$에 대해 동작시간 τ를 가지고, 복호화 오라클 $\mathcal{O}^{\mathcal{D}}$와 랜덤 오라클 $\mathcal{O}^H, \mathcal{O}^G$에 각각 $q_{\mathcal{D}}, q_H, q_G$회 질의하는 IND-CCA2 공격자라 하자. 어떤 OW-PD-S 공격자 $\mathcal{B}$에 대해, 다음을 만족한다.*

$$\mathsf{Adv}^{\text{OW-PD-S}}_{\Psi,\lambda}(\mathcal{B}; \tau', q_H) \geq \frac{\mathsf{Adv}^{\text{IND-CCA2}}_{\Pi,\lambda}(\mathcal{A}; \tau, q_{\mathcal{D}}, q_H, q_G)}{2} - \frac{2q_{\mathcal{D}}q_G + q_{\mathcal{D}} + q_G}{2^{\lambda_0}} - \frac{2q_{\mathcal{D}}}{2^{\lambda_1}}.$$

이 때, $\tau' \leq \tau \cdot q_H \cdot q_G \cdot (T_{\mathcal{F}} + O(1))$이고, $T_{\mathcal{F}}$는 트랩도어 치환 $\mathcal{F}$의 시간 복잡도를 의미한다.